

Per gebruiker ACL-controllers met draadloze LAN-controllers en Cisco Secure ACS-configuratievoorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configureren](#)

[De draadloze LAN-controller configureren](#)

[Een VLAN voor draadloze gebruikers maken](#)

[Configuratie van de WLC om voor Verificatie met Cisco Secure ACS te zorgen](#)

[Een nieuw WLAN voor draadloze gebruikers maken](#)

[Bepaal de ACL's voor gebruikers](#)

[De Cisco Secure ACS-server configureren](#)

[Configureer de draadloze LAN-controller als een AAA-client voor Cisco Secure ACS](#)

[Gebruikers en gebruikersprofiel instellen op Cisco Secure ACS](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Tips bij het oplossen van problemen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document legt door een voorbeeld uit hoe u toegangscontrolelijsten (ACL's) op de WLC's kunt maken en past deze toe op gebruikers die afhankelijk zijn van RADIUS-toestemming.

[Voorwaarden](#)

[Vereisten](#)

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

- Basiskennis van de manier waarop u een Cisco Secure ACS-server kunt configureren om draadloze clients te authenticeren

- Kennis van de configuratie van Cisco Aironet lichtgewicht access points (LAP's) en Cisco draadloze LAN-controllers (WLC's)
- Kennis van Cisco Unified Wireless Security-oplossingen

Gebruikte componenten

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

- Cisco 4400 Series draadloze LAN-controller op versie 5.0.148.0
- Cisco Aironet 1231 Series lichtgewicht access points (LAP's)
- Cisco Aironet 802.11a/b/g Cisco draadloze LAN-clientadapter die versie 3.6 draait
- Cisco Aironet desktophulpprogramma versie 3.6
- Cisco Secure ACS Server versie 4.1
- Cisco 2800 Series geïntegreerde services router die IOS-versie 12.4(11)T uitvoeren
- Cisco Catalyst 2900XL Series Switch met versie 12.0(5)WC3b

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 de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Achtergrondinformatie

De per gebruiker Access Control List (ACL) maakt deel uit van Cisco Identity-netwerken. Cisco draadloze LAN-oplossing ondersteunt identiteitsnetwerken, die, terwijl het netwerk kan adverteren met één SSID, ook specifieke gebruikers in staat stelt om verschillend beleid te erven op basis van hun gebruikersprofielen.

De functie per gebruiker ACL biedt de mogelijkheid om een ACL toe te passen die op de draadloze LAN-controller is ingesteld op een gebruiker op basis van de RADIUS-opdracht. Dit wordt bereikt met de Airespace-ACL-naam leverancierspecifieke eigenschap (VSA).

Deze eigenschap geeft de ACL-naam aan die op de client moet worden toegepast. Wanneer het ACL-kenmerk in de RADIUS Access Accept aanwezig is, past het systeem de ACL-naam op het clientstation toe nadat dit voor echt is verklaard. Dit heeft betrekking op ACL's die aan de interface zijn toegewezen. Het negeert de toegewezen interface-ACL en past de nieuwe toe.

Hieronder vindt u een samenvatting van het formaat van de ACL-naam. De velden worden van links naar rechts verzonden

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+++++
|   Type   | Length | Vendor-Id
+++++
Vendor-Id (cont.) | Vendor type | Vendor length |
+++++
```

```

|           ACL Name...
+-----+-----+-----+-----+-----+
• Type - 26 for Vendor-Specific
• Length - >7
• Vendor-Id - 14179
• Vendor type - 6
• Vendor length - >0
• Value - A string that includes the name of the ACL to use for the client.
      The string is case sensitive.

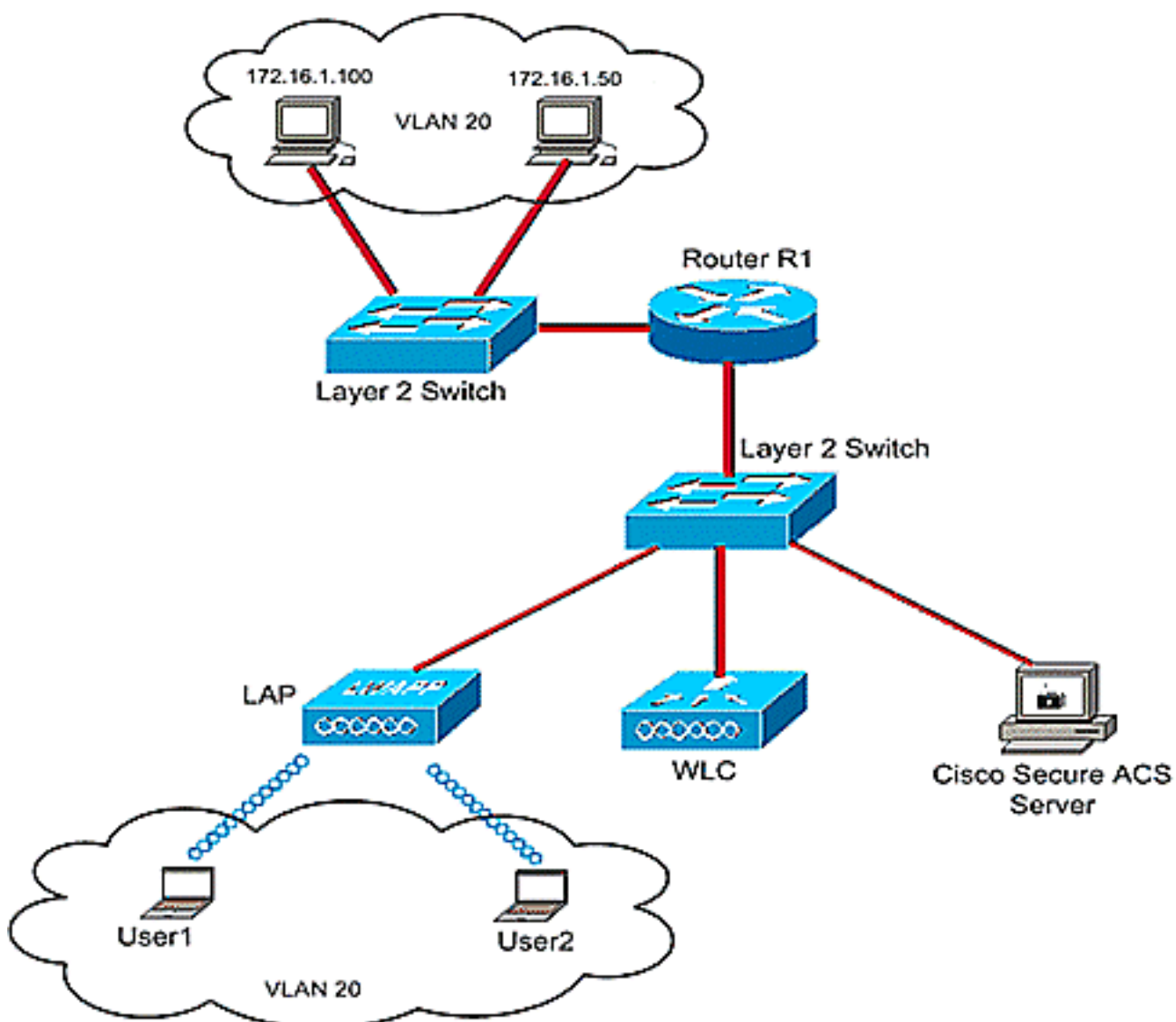
```

Raadpleeg voor meer informatie over de Cisco Unified Wireless Network Identity Network Services Engine het gedeelte [Configuration Identity Network](#) van het document [Security Solutions](#).

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:

In deze opstelling, worden de Draadloze LAN Controller WLC en LAP gebruikt om draadloze services te leveren aan de gebruikers in Afdeling A en Afdeling B. Alle draadloze gebruikers gebruiken een gemeenschappelijk WLAN (SSID) Office om toegang tot het netwerk te krijgen en zijn in VLAN Office-VLAN aanwezig.



De Cisco Secure ACS-server wordt gebruikt om draadloze gebruikers te authenticeren. EMAE-authenticatie wordt gebruikt om gebruikers te authenticeren. De WLC-, LAP- en Cisco Secure

ACS-server worden aangesloten met een Layer 2-Switch zoals wordt weergegeven.

De router R1 sluit de servers aan de bekabelde kant door de Layer 2 Switch zoals getoond. De router R1 treedt ook op als een server van DHCP, die IP adressen aan draadloze cliënten van netto 172.16.0.0/16 verstrekt.

U dient de apparaten zo te configureren dat dit voorkomt:

Gebruiker1 van Afdeling A heeft alleen toegang tot server 172.16.1.100

Gebruiker2 van Afdeling B heeft alleen toegang tot server 172.16.1.50

Om dit te bereiken, moet u 2 ACLs op de WLC creëren: Eén voor User1, en de andere voor User2. Zodra de ACL's zijn gecreëerd, moet u de Cisco Secure ACS-server configureren om de ACL-naameigenschap aan de WLC terug te geven bij succesvolle verificatie van de draadloze gebruiker. WLC past dan ACL op de gebruiker toe, en zo is op het netwerk beperkt afhankelijk van het gebruikersprofiel.

Opmerking: In dit document wordt gebruik gemaakt van LEAP-verificatie voor het authenticeren van gebruikers. Cisco LEAP is kwetsbaar voor woordenboekaanvallen. In real-time netwerken moeten veiliger authenticatiemethoden zoals EAP FAST worden gebruikt. Aangezien de focus van het document is om uit te leggen hoe je per gebruiker ACL-functie moet configureren, wordt LEAP gebruikt voor eenvoud.

De volgende sectie verschaft de stap-voor-stap instructies om de apparaten voor deze installatie te configureren.

[Configureren](#)

Voordat u de functie per gebruiker ACL's configureren, moet u de WLC configureren voor basisbediening en de LAP's registreren in het WLC. Dit document gaat ervan uit dat de WLC is ingesteld voor een eenvoudige bediening en dat de LAP's zijn geregistreerd op de WLC. Als u een nieuwe gebruiker bent, die probeert de WLC in te stellen voor basisbediening met LAP's, raadpleegt u [Lichtgewicht AP \(LAP\) Registratie aan een draadloze LAN-controller \(WLC\)](#).

Nadat de LAP's zijn geregistreerd, volgt u deze stappen om de apparaten voor deze instelling te configureren:

1. [Configureer de draadloze LAN-controller.](#)
2. [Configureer de Cisco Secure ACS-server.](#)
3. [Controleer de configuratie.](#)

N.B.: Dit document behandelt de configuratie die aan de draadloze kant vereist is. Het document gaat ervan uit dat de knoppen op het scherm zijn ingeschakeld.

[De draadloze LAN-controller configureren](#)

Op de draadloze LAN-controller moet u dit doen:

- [Maak een VLAN voor de draadloze gebruikers.](#)
- [Configuratie van de WLC om draadloze gebruikers met Cisco Secure ACS voor authenticatie te](#)

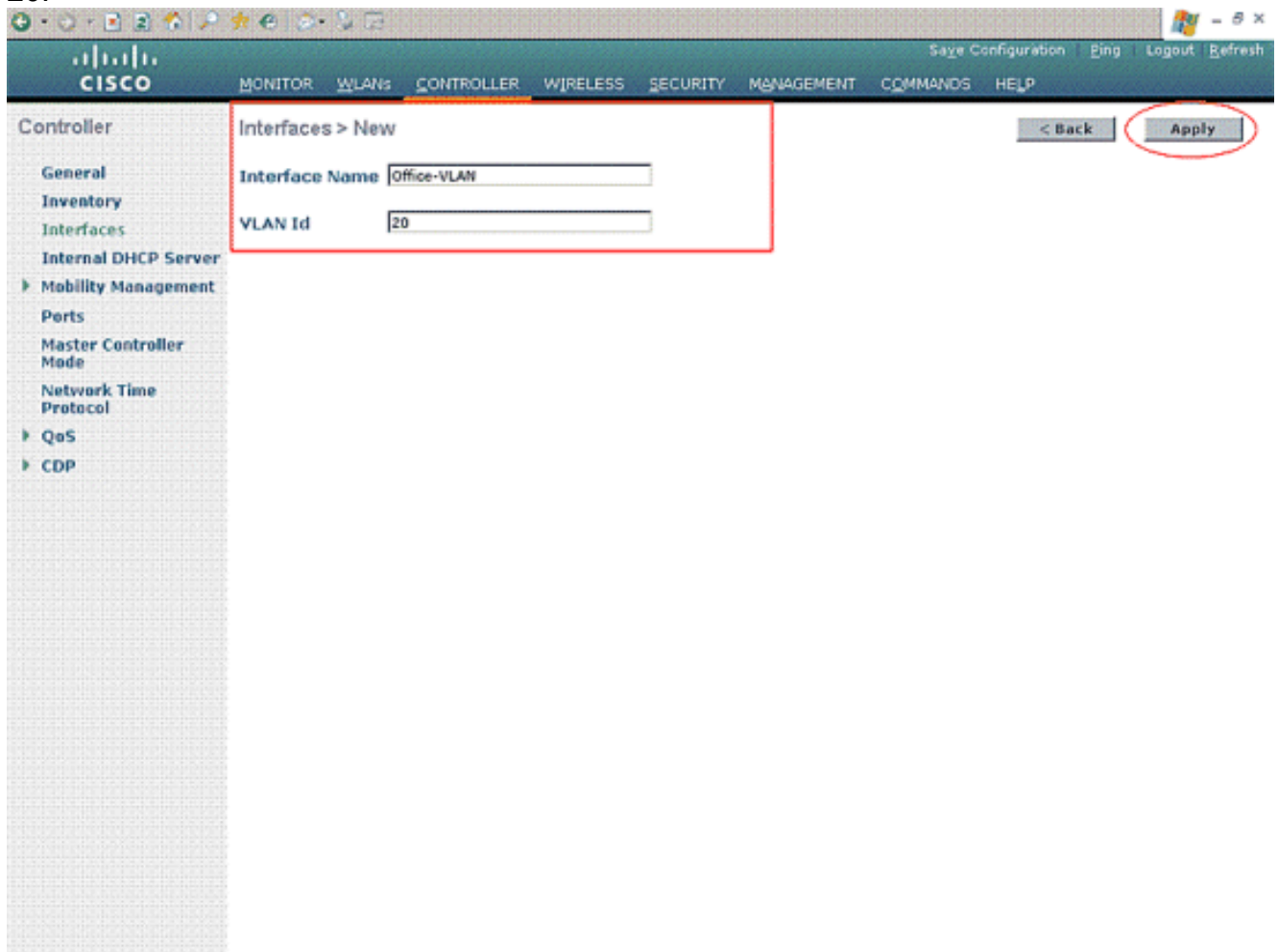
[verklaren.](#)

- [Maak een nieuw WLAN voor de draadloze gebruikers.](#)
- [Bepaal de ACL's voor de draadloze gebruikers.](#)

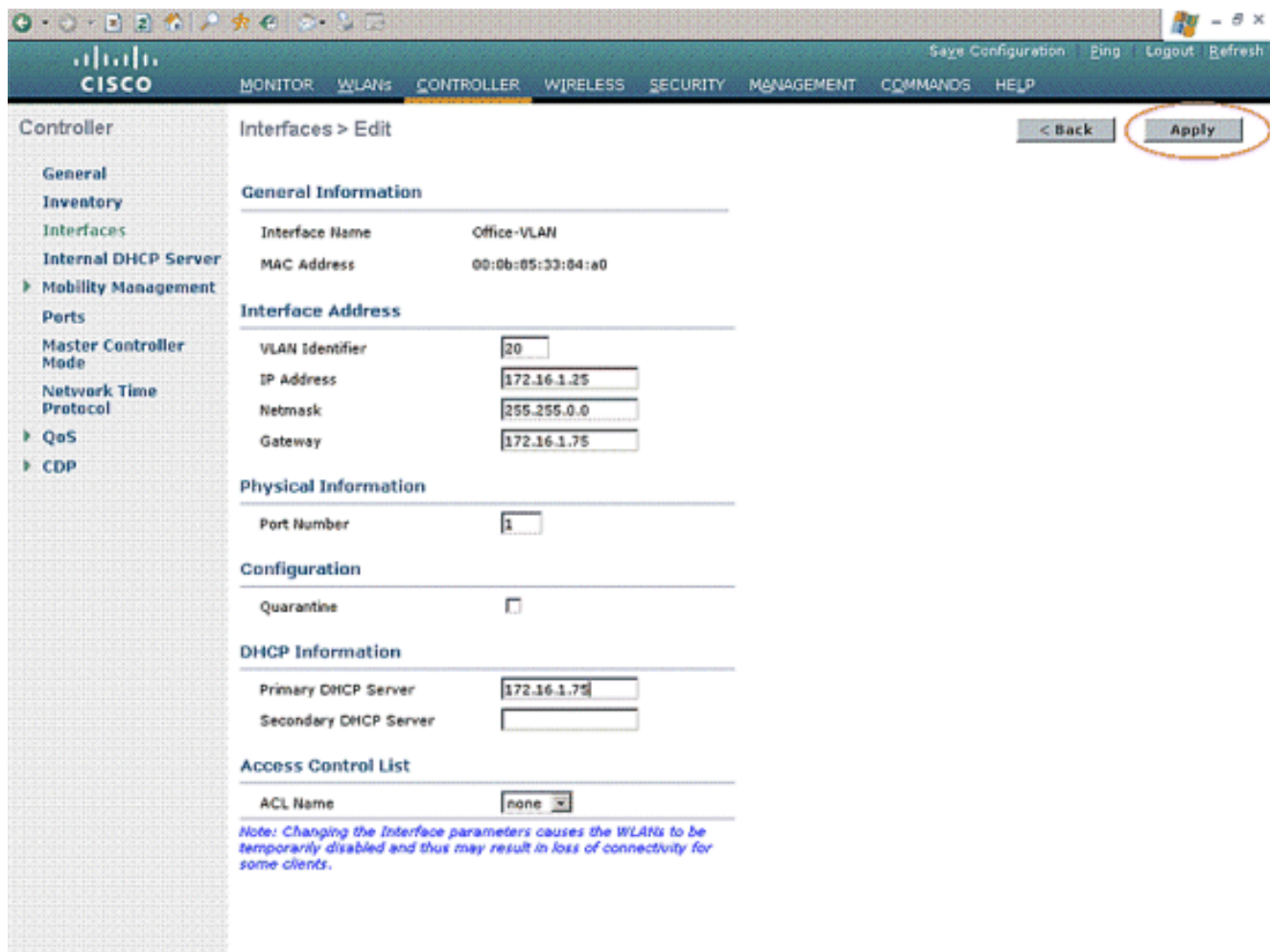
Een VLAN voor draadloze gebruikers maken

Om een VLAN voor de draadloze gebruikers te maken, voltooiën deze stappen.

1. Ga naar de WLC GUI en kies **Controller > Interfaces**. Het venster Interfaces verschijnt. Dit venster toont de interfaces die op de controller zijn ingesteld.
2. Klik op **Nieuw** om een nieuwe dynamische interface te maken.
3. In het **venster Interfaces > New**, voert u de interfacenaam en de VLAN-ID in. Klik vervolgens op Toepassen. In dit voorbeeld, wordt de dynamische interface genoemd Office-VLAN, en VLAN ID wordt toegewezen 20.



4. In het venster **Interfaces > Bewerken**, voer het IP-adres, het subnetmasker en de standaardgateway voor de dynamische interface in. Pas het aan een fysieke poort op WLC toe, en voer het IP adres van de DHCP-server in. Klik vervolgens op **Toepassen**.



Dit voorbeeld, deze parameters worden gebruikt voor de interface van Office-VLAN:

Office-VLAN

IP address: 172.16.1.25

Netmask: 255.255.0.0

Default gateway: 172.16.1.75 (sub-interface on Router R1)

Port on WLC: 1

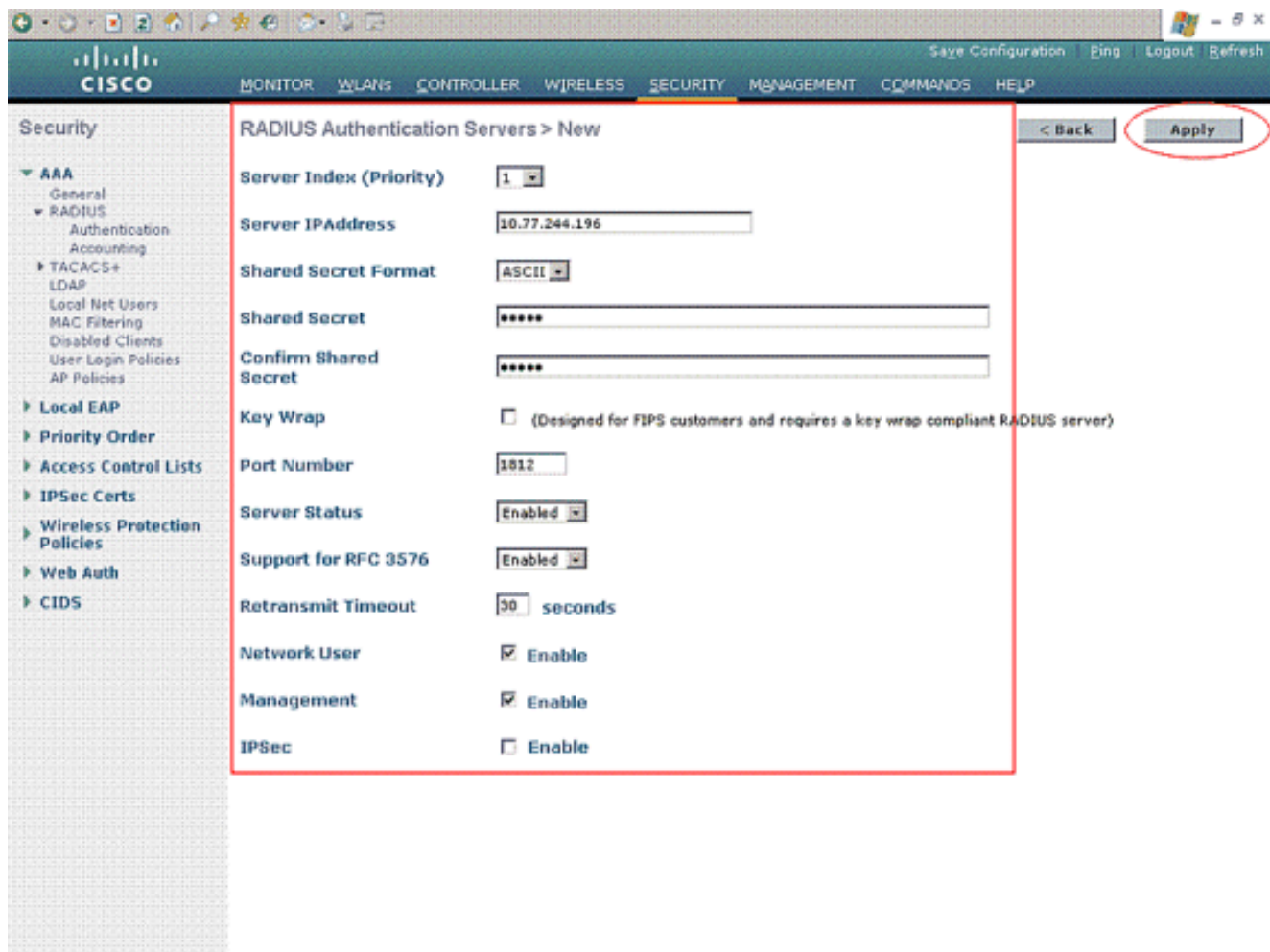
DHCP server: 172.16.1.75

[Configuratie van de WLC om voor Verificatie met Cisco Secure ACS te zorgen](#)

De WLC moet worden geconfigureerd om de gebruikersreferenties naar een externe RADIUS-server te kunnen doorsturen (in dit geval Cisco Secure ACS). De RADIUS-server bevestigt vervolgens de gebruikersreferenties en geeft de ACL-naameigenschap naar de WLC terug bij succesvolle verificatie van de draadloze gebruiker.

Volg deze stappen om de WLC voor de RADIUS-server te configureren:

1. Kies **Security** en **RADIUS-verificatie** van de controller GUI om de pagina **RADIUS-verificatieservers** weer te geven. Klik vervolgens op **New** om een RADIUS-server te definiëren.
2. Definiëert de parameters van de RADIUS-server in de **RADIUS-verificatieservers > Nieuwe** pagina. Deze parameters omvatten het IP-adres van de RADIUS-server, gedeeld geheim, poortnummer en serverstatus.

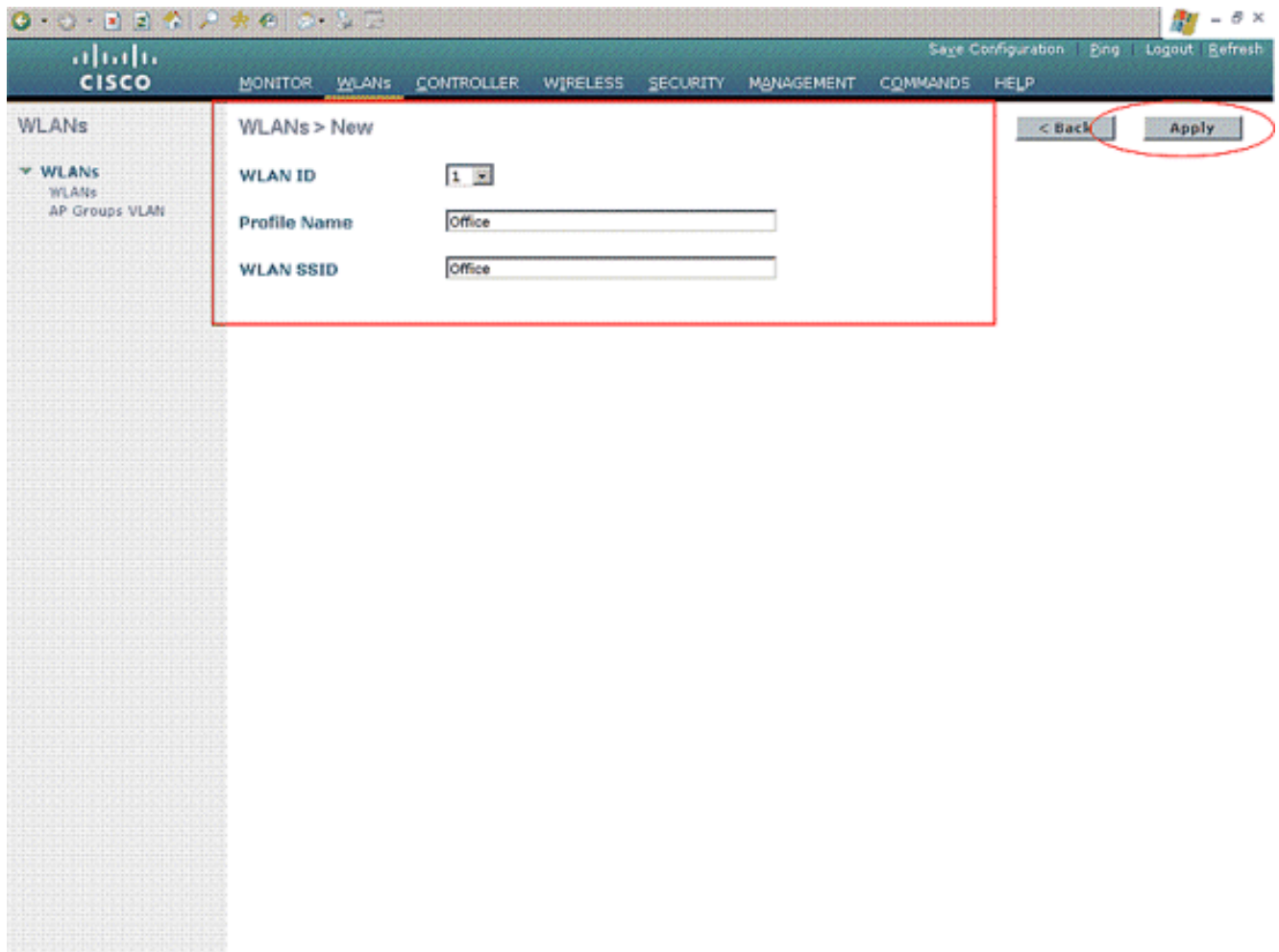


3. De vinkjes **Netwerkgebruiker** en **Beheer** bepalen of de op RADIUS gebaseerde verificatie van toepassing is op beheer- en netwerkgebruikers. Dit voorbeeld gebruikt de Cisco Secure ACS als de RADIUS-server met IP-adres 10.7.24.196. Klik op **Toepassen**.

[Een nieuw WLAN voor draadloze gebruikers maken](#)

Vervolgens moet u een WLAN-verbinding maken waaraan de draadloze gebruikers zich kunnen aansluiten. Voltooi de volgende stappen om een nieuw WLAN-netwerk te maken:

1. Klik vanuit de GUI van de draadloze LAN-controller op **WLAN's**. Deze pagina toont de WLAN's die op de controller bestaan.
2. Kies **Nieuw** om een nieuw WLAN te maken. Voer de WLAN-id, de naam van het profiel en de WLAN-sid in voor de WLAN en klik op **Toepassen**. Maak voor deze installatie een WLAN-kantoor.



3. Zodra u een nieuw WLAN hebt gemaakt, wordt de **WLAN >** pagina **bewerken** voor de nieuwe WLAN weergegeven. In deze pagina kunt u verschillende parameters definiëren die specifiek zijn voor dit WLAN dat algemeen beleid, beveiliging, QoS en geavanceerde parameters omvat.

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'WLANs' section is active, and the 'WLANs > Edit' page is displayed. The 'General' tab is selected, showing the following configuration:

Profile Name	Office
WLAN SSID	Office
WLAN Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	office-vlan
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Below the configuration fields, there are 'Foot Notes' in blue text:

- 1 CKIP is not supported by 10xx model APs
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

The 'Apply' button in the top right corner is circled in red.

Controleer **WLAN-status** onder Algemeen beleid om de WLAN-functie in te schakelen. Kies de juiste interface in het keuzemenu. In dit voorbeeld, gebruik de interface **Office-VLAN**. De andere parameters op deze pagina kunnen worden gewijzigd op basis van de vereisten van het WLAN-netwerk.

4. Kies het **tabblad Beveiliging**. Kies **802.1x** in het keuzemenu Layer 2 security (aangezien dit een LEAP-verificatie is). Kies de juiste grootte van de EFN-toets onder 802.1x-parameters.

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'WLANs > Edit' page is active, with tabs for 'General', 'Security', 'QoS', and 'Advanced'. Under the 'Security' tab, there are sub-tabs for 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'Layer 2 Security' dropdown is set to '802.1X', and the 'MAC Filtering' checkbox is unchecked. Below this, the '802.1X Parameters' section has a table for '802.11 Data Encryption' with columns for 'Type' and 'Key Size'. The 'Type' is set to 'WEP' and the 'Key Size' is '104 bits'. Two red ovals highlight the '802.1X' dropdown and the 'WEP' and '104 bits' settings. At the bottom, there are 'Foot Notes' with five numbered items.

Foot Notes

- 1 CKIP is not supported by 10xx model APs
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

5. Selecteer onder het tabblad Security het subtabblad **AAA-server**. Kies de AAA server die wordt gebruikt om draadloze clients te authenticeren. In dit voorbeeld, gebruik ACS server 10.77.244.196 om draadloze cliënten te authenticeren.

WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

Radius Servers		LDAP Servers	
Authentication Servers	Accounting Servers	Server 1	Server 2
Server 1	IP:10.77.244.196, Port:1812	None	None
Server 2	None	None	None
Server 3	None	None	None

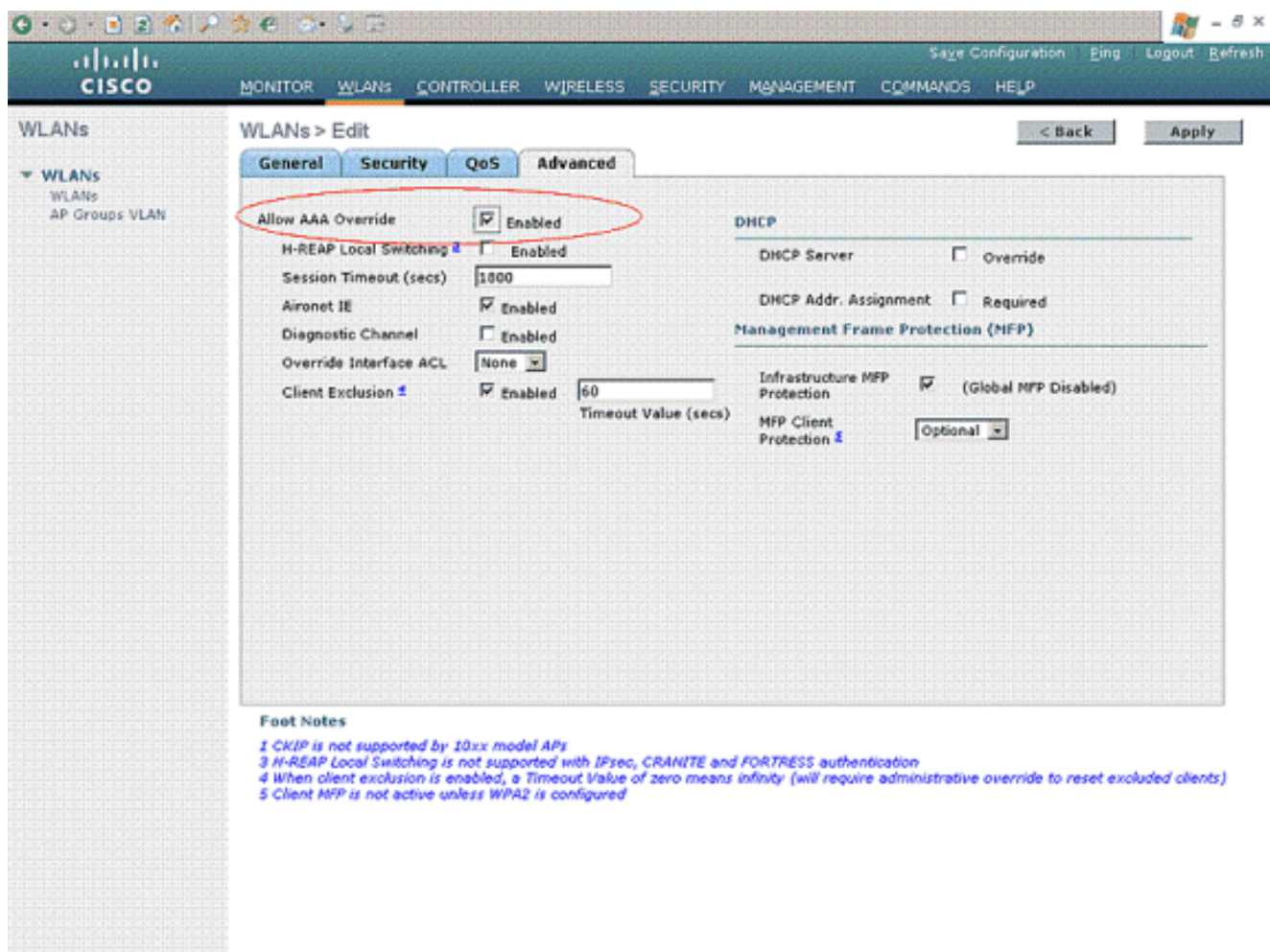
Local EAP Authentication

Local EAP Authentication enabled

Foot Notes

1 CKIP is not supported by 10xx model APs
3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
5 Client MFP is not active unless WPA2 is configured

6. Kies het tabblad **Geavanceerd**. Schakel de optie **AAA negeren** in om het gebruikersbeleid te configureren met voorrang door de AAA via een draadloos LAN.



Als AAA-opheffing is ingeschakeld en een client tegenstrijdige AAA en Cisco draadloze LAN-controller detectieparameters heeft, wordt client-verificatie uitgevoerd door de AAA-server. Als deel van deze verificatie verplaatst het besturingssysteem klanten van de standaard Cisco draadloze LAN-oplossing voor draadloos LAN VLAN naar een VLAN dat wordt teruggestuurd door de AAA-server en vooraf is gedefinieerd in de Cisco draadloze LAN-controller-interfaceconfiguratie, die alleen wordt ingesteld voor MAC-filtering, 802.1X en/of WAP-bewerking. In alle gevallen maakt het besturingssysteem ook gebruik van QoS, DSCP, 802.1p prioriteitsmerkwwaarden en ACL die door de AAA-server zijn meegeleverd, zolang deze waarden vooraf zijn gedefinieerd in de interfacemodule voor Cisco draadloze LAN-controllers.

7. Kies de andere parameters die zijn gebaseerd op de eisen van het netwerk. Klik op **Apply** (Toepassen).

Bepaal de ACL's voor gebruikers

U moet twee ACL's maken voor deze instelling:

- ACL1: Zo geeft u alleen toegang tot User1 op de server 172.16.1.100
- ACL2: Zo geeft u alleen toegang tot User2 aan de server 172.16.1.50

Voltooi deze stappen om de ACL's op de WLC te configureren:

1. Kies in de WLC GUI, **Security > Access Control Lists**. De pagina Toegangscontrolelijsten wordt weergegeven. Deze pagina toont de ACL's die op WLC zijn geconfigureerd. Het stelt u ook in om een van de ACL's te bewerken of te verwijderen. Om een nieuwe ACL te maken, klikt u op **Nieuw**.

- Met deze pagina kunt u nieuwe ACL's maken. Voer de naam van ACL in en klik op **Toepassen**. Zodra ACL wordt gecreëerd, klik op **Bewerken** om regels voor ACL te creëren.
- Gebruiker1 hoeft alleen toegang te hebben tot server 172.16.1.100 en moet toegang tot alle andere apparaten worden geweigerd. Daarvoor moet je deze regels definiëren. Raadpleeg de [ACL's op configuratievoorbeeld voor draadloze LAN-controllers](#) voor meer informatie over de manier waarop u ACL's op draadloze LAN-controllers kunt configureren.

The screenshot shows the Cisco configuration interface for 'Access Control Lists > Edit' for 'User1'. The table below is a representation of the ACL rules shown in the interface:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	172.16.0.0 / 255.255.0.0	172.16.1.100 / 255.255.255.255	Any	Any	Any	Any	Inbound
2	Permit	172.16.1.100 / 255.255.255.255	172.16.0.0 / 255.255.0.0	Any	Any	Any	Any	Outbound

- Op dezelfde manier moet u een ACL voor User2 maken, die User2 toegang tot server 172.16.1.50 slechts toestaat. Dit is ACL vereist voor Gebruiker2.

Security

Access Control Lists > Edit

General

Access List Name: User2

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	172.16.0.0 / 255.255.0.0	172.16.1.50 / 255.255.255.255	Any	Any	Any	Any	Inbound
2	Permit	172.16.1.50 / 255.255.255.255	172.16.0.0 / 255.255.0.0	Any	Any	Any	Any	Outbound

U hebt nu de draadloze LAN-controller voor deze installatie ingesteld. De volgende stap is de Cisco Secure Access Control Server te configureren om de draadloze clients te authenticeren en de ACL Name eigenschap aan de WLC terug te geven bij succesvolle verificatie.

[De Cisco Secure ACS-server configureren](#)

U moet deze stappen voltooien voor Cisco Secure ACS om draadloze clients te kunnen authenticeren:

- [Configureer de draadloze LAN-controller als een AAA-client in Cisco Secure ACS.](#)
- [Configureer de gebruikers en gebruikersprofielen in de Cisco Secure ACS.](#)

[Configureer de draadloze LAN-controller als een AAA-client voor Cisco Secure ACS](#)

Om de draadloze LAN-controller als een AAA-client in Cisco Secure ACS te configureren voert u deze stappen uit:

1. Klik op **Network Configuration > Add AAA client**. De pagina **Add AAA client** verschijnt. In deze pagina definieert u de WLC-systeemnaam, IP-adres van beheerinterface, gedeeld geheim en authenticer het gebruik van **Radius-interface**. Hierna volgt een voorbeeld:

Network Configuration

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Shared Secret:

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ASCII Hexadecimal

Authenticate Using:

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

[Back to Help](#)

Help

- AAA Client Hostname
- AAA Client IP Address
- Shared Secret
- Network Device Group
- RADIUS Key Wrap
- Authenticate Using
- Single Connect TACACS+ AAA Client
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press Enter.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1

Opmerking: het gedeelde geheim dat op Cisco Secure ACS is ingesteld, moet overeenkomen met het gedeelde geheim dat op de WLC is ingesteld onder **RADIUS-verificatieservers > New**.

2. Klik op **Inzenden+Toepassen**.

[Gebruikers en gebruikersprofiel instellen op Cisco Secure ACS](#)

Om gebruikers op Cisco Secure ACS te configureren voert u deze stappen uit:

1. Klik op **Gebruikersinstelling** in de ACS GUI, voer de gebruikersnaam in en klik op **Toevoegen/Bewerken**. In dit voorbeeld is de gebruiker **Gebruiker1**.

User Setup

Select

User:

List users beginning with letter/number:

A B C D E F G H I J K L M
 N O P Q R S T U V W X Y Z
 0 1 2 3 4 5 6 7 8 9

Help

- [User Setup and External User Databases](#)
- [Finding a Specific User in the ACS Internal Database](#)
- [Adding a User to the ACS Internal Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the ACS Internal Database](#)
- [Changing a Username in the ACS Internal User Database](#)
- [Remove Dynamic Users](#)

User Setup enables you to configure individual user information, add users, and delete users in the database. **User Setup and External User Databases**

Before ACS can authenticate users with an external user database:

- You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
- You must have configured the applicable parameters in the External User Databases section.

Note: User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.

External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.

Note: User Setup does not add or delete usernames in an external user database. [Back to Top](#)

Finding a Specific User in the ACS Internal Database

To find a user already in the ACS internal database, type the first few letters of the username in the User field, add an asterisk (*) as a wildcard, and click Find. From the list of usernames displayed, click the username whose information you want to view or change.

[Back to Top](#)

Adding a User to the ACS Internal Database

To add a new user or edit a configuration for an existing user, type a username

2. Wanneer de pagina **Gebruikersinstellingen** wordt weergegeven, definieert u alle parameters die specifiek zijn voor de gebruiker. In dit voorbeeld worden de gebruikersnaam, het wachtwoord, de aanvullende gebruikersinformatie en de RADIUS-kenmerken ingesteld omdat u deze parameters alleen nodig hebt voor MAP-verificatie.

User Setup

Edit

User: UserA (New User)

Account Disabled

Supplementary User Info

Real Name: User 1

Description:

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

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IEEE RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[\[Back to Top\]](#)

Deleting a Username

The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click **Delete**. When asked to confirm your action, click **OK**.

[\[Back to Top\]](#)

Supplementary User Info

Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click **Interface**

RoI naar beneden tot u de RADIUS-kenmerken van Cisco Airespace specifiek voor de gebruiker ziet. Controleer de **Aire-ACL-naam** om ACS in staat te stellen om de ACL-naam naar de WLC terug te sturen samen met de succesvolle authenticatiereactie. Creëer voor User1 een ACL User1 op de WLC. Voer de ACL-naam in als Gebruiker1.

User Setup

Date exceeds: Sep 9 2007

Failed attempts exceed: 5
Failed attempts since last successful login: 0
 Reset current failed attempts count on submit

Cisco Airespace RADIUS Attributes

[14179002] Aire-QoS-Level: Bronze

[14179003] Aire-DSCP: 0

[14179004] Aire-802.1P-Tag: 0

[14179005] Aire-Interface-Name:

[14179006] Aire-Act-Name: User1

[Back to Help](#)

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IEEE RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top](#)

Deleting a Username

The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click **Delete**. When asked to confirm your action, click **OK**.

[Back to Top](#)

Supplementary User Info

Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click **Interface**

3. Herhaal de zelfde procedure om Gebruiker2 te maken zoals hier getoond wordt.

Cisco Systems User Setup

Select

User:

List users beginning with letter/number:

A B C D E F G H I J K L M
 N O P Q R S T U V W X Y Z
 0 1 2 3 4 5 6 7 8 9

Help

- [User Setup and External User Databases](#)
- [Finding a Specific User in the ACS Internal Database](#)
- [Adding a User to the ACS Internal Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the ACS Internal Database](#)
- [Changing a Username in the ACS Internal User Database](#)
- [Remove Dynamic Users](#)

User Setup enables you to configure individual user information, add users, and delete users in the database. [User Setup and External User Databases](#)

Before ACS can authenticate users with an external user database:

- You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
- You must have configured the applicable parameters in the External User Databases section.

Note: User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.

External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.

Note: User Setup does not add or delete usernames in an external user database. [Back to Top](#)

Finding a Specific User in the ACS Internal Database

To find a user already in the ACS internal database, type the first few letters of the username in the User field, add an asterisk (*) as a wildcard, and click Find. From the list of usernames displayed, click the username whose information you want to view or change.

[Back to Top](#)

Adding a User to the ACS Internal Database

To add a new user or edit a configuration for an existing user, type a username

Cisco Systems User Setup

Edit

User: UserA (New User)

Account Disabled

Supplementary User Info

Real Name:

Description:

User Setup

Password Authentication:

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:

Help

- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IEEE RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top](#)

Deleting a Username

The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to confirm your action, click OK.

[Back to Top](#)

Supplementary User Info

Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click Interface

User Setup

Date exceeds: Sep 9 2007

Failed attempts exceed: 5
Failed attempts since last successful login: 0
 Reset current failed attempts count on submit

Cisco Airespace RADIUS Attributes

[14179002] Aire-QoS-Level: Bronze

[14179003] Aire-DSCP: 0

[14179004] Aire-802.1P-Tag: 0

[14179005] Aire-Interface-Name:

[14179006] Aire-Ac-Name: User2

[Back to Help](#)

Help

- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IEEE RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top](#)

Deleting a Username

The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click **Delete**. When asked to confirm your action, click **OK**.

[Back to Top](#)

Supplementary User Info

Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click **Interface**

4. Klik op **System Configuration** en **Global Authentication Setup** om te verzekeren dat de verificatieserver is ingesteld voor het uitvoeren van de gewenste MAP-verificatiemethode. Kies in de MAP-configuratie de juiste MAP-methode. In dit voorbeeld wordt gebruik gemaakt van MAP-authenticatie. Klik op **Inzenden** als u klaar bent.

The screenshot shows the Cisco Systems System Configuration window. On the left is a navigation pane with options like 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, and Device Documentation. The main area is divided into sections for PEAP, EAP-FAST, EAP-TLS, and LEAP. The LEAP section is circled in red and contains the option 'Allow LEAP (For Aironet only)' which is checked. The PEAP section has options for 'Allow EAP-MSCHAPv2', 'Allow EAP-GTC', and 'Allow Posture Validation'. Below these are options for 'Allow EAP-TLS' and 'Certificate SAN comparison', 'Certificate CN comparison', and 'Certificate Binary comparison'. The EAP-TLS session timeout is set to 120 minutes. The EAP-FAST section has a link to 'EAP-FAST Configuration'. The right side of the screen shows a Help window with a list of links for various authentication protocols and detailed text about EAP Configuration, PEAP, and LEAP.

Verifiëren

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

Probeer een draadloze client te associëren met de lichtgewicht AP met 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 meer informatie over het configureren van de 802.11a/b/g draadloze clientadapter voor LEAP-verificatie.

Nadat het profiel voor de draadloze client is geactiveerd, wordt de gebruiker gevraagd de gebruikersnaam/het wachtwoord voor LEAP-verificatie te verstrekken. Dit is wat er gebeurt wanneer Gebruiker1 probeert om voor de LAP echt te maken.

Enter Wireless Network Password [X]

Please enter your LEAP username and password to log on to the wireless network.

User Name :

Password :

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : Office

Lichtgewicht AP en dan geeft WLC de gebruikersgeloofsbriefen aan de externe server van de RADIUS (Cisco Secure ACS) door om de geloofsbriefen te valideren. De RADIUS-server vergelijkt de gegevens met de gebruikersdatabase en geeft, bij succesvolle verificatie, de ACL-naam die voor de gebruiker is ingesteld, terug naar de WLC. In dit geval, wordt ACL Gebruiker1 teruggebracht naar WLC.

Cisco Aironet Desktop Utility - Current Profile: Office-TSWEB [?] [X]

Action Options Help

Current Status Profile Management Diagnostics

CISCO SYSTEMS


Profile Name: Office-TSWEB

Link Status: Authenticated Network Type: Infrastructure

Wireless Mode: 5 GHz 54 Mbps Current Channel: 64

Server Based Authentication: LEAP Data Encryption: WEP

IP Address: 172.16.0.14

Signal Strength:  Excellent

De draadloze LAN-controller past deze ACL op User1 toe. Deze ping-uitvoer toont aan dat User1

alleen toegang heeft tot server 172.16.1.100, maar niet tot een ander apparaat.

```
D:\Documents and Settings\Administrator>ping 172.16.1.100
```

```
Pinging 172.16.1.100 with 32 bytes of data:
```

```
Reply from 172.16.1.100: bytes=32 time=3ms TTL=255  
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255  
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255  
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
```

```
Ping statistics for 172.16.1.100:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

```
D:\Documents and Settings\Administrator>ping 172.16.1.50
```

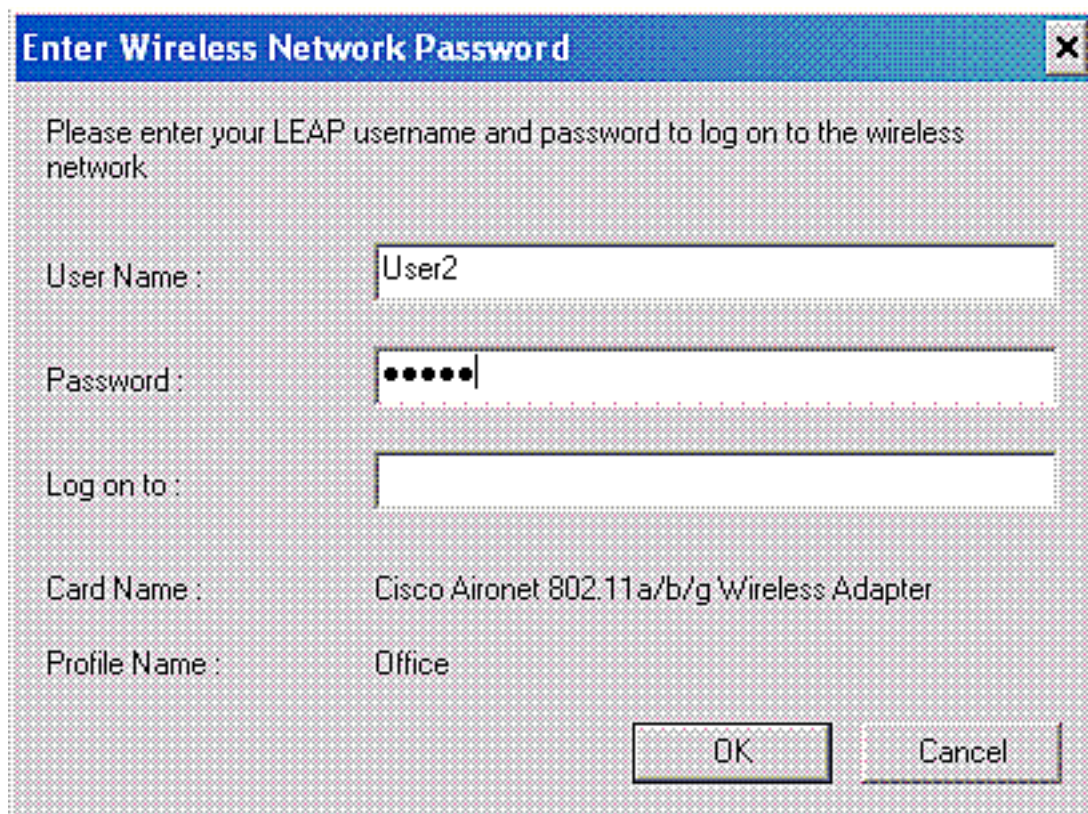
```
Pinging 172.16.1.50 with 32 bytes of data:
```

```
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.
```

```
Ping statistics for 172.16.1.50:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Op dezelfde manier keert ACL wanneer User2 probeert om toegang te krijgen tot de WLAN-server van de RADIUS, na succesvolle verificatie, User2 naar de WLC terug.



Enter Wireless Network Password

Please enter your LEAP username and password to log on to the wireless network.

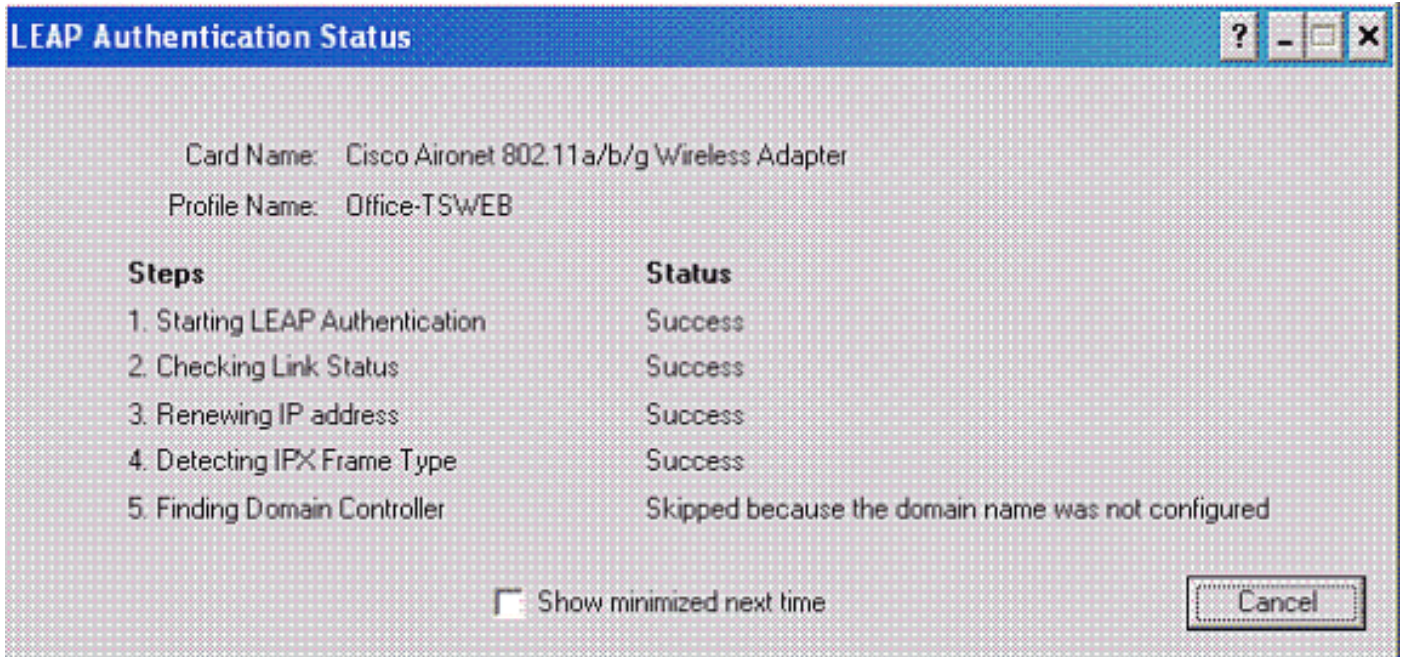
User Name :

Password :

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : Office



De draadloze LAN-controller past deze ACL op User2 toe. Deze ping-uitvoer toont aan dat User2 alleen toegang heeft tot server 172.16.1.50, maar niet tot een ander apparaat.

```
D:\Documents and Settings\Administrator>ping 172.16.1.50
```

```
Pinging 172.16.1.50 with 32 bytes of data:
```

```
Reply from 172.16.1.50: bytes=32 time=3ms TTL=255
Reply from 172.16.1.50: bytes=32 time=18ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
```

```
Ping statistics for 172.16.1.50:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 18ms, Average = 5ms
```

```
D:\Documents and Settings\Administrator>ping 172.16.1.100
```

```
Pinging 172.16.1.100 with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 172.16.1.100:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Op de draadloze LAN-controller kunt u deze debug-opdrachten ook gebruiken om AAA-verificatie bij te stellen

- **debug in alle** schakelt u het debug van alle AAA-berichten in
- **bug dot1x-pakket activeren** - hiermee kan het debug van alle punten 1x worden opgeslagen
- **debug client <MAC-adres>**—hiermee kan draadloze client worden gedetecteerd

Hier is een voorbeeld van het **debug a** die **allen opdracht** geven

Opmerking: Sommige lijnen in de uitvoer zijn naar de tweede regel verplaatst als gevolg van ruimtebeperkingen.

```

Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:      Callback.....0x85ed228
Thu Aug 16 14:42:54 2007:      protocolType.....0x00140001
Thu Aug 16 14:42:54 2007:      proxyState.....00:40:96:AF:3E:93-03:01
Thu Aug 16 14:42:54 2007:      Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet
  (id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99  b4 19 27 28 eb 5f 35 9c
  ....-4....'(_5.
Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73  65 72 31 1f 13 30 30 2d
  .....user1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
  40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
  00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
  0:Office-TSWEB..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
  .....M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
  ...7c.....
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
  .....=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 27 02
  ...A.....Q.200'.
Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d  87 9d 0b f9 dd e5 39 0d
  ..%......9.
Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96  dc c3 55 ff 7c 51 4e 75
  ....#....U.|QNu
Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
  ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0  c6 2f 5e f5 65 e9 3e 2d
  ..;5^..../^e.>-
Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4  27 e6 d4 0e 1b 8e 5d 19
  ...6.1j.'.....].
Thu Aug 16 14:42:54 2007: 00000010: 60 1c c2 16 4f 06 03 01  00 04 18 0a 53 56 43 3d
  ...O.....SVC=
Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb  90 ec 48 9b fb d7 ce ca
  0.1;P.l...H.....
Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09          ;d...
Thu Aug 16 14:42:54 2007: ***Enter processIncomingMessages: response code=11
Thu Aug 16 14:42:54 2007: ***Enter processRadiusResponse: response code=11
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Access-Challenge received from RADIUS server
  10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:      structureSize.....104
Thu Aug 16 14:42:54 2007:      resultCode.....255
Thu Aug 16 14:42:54 2007:      protocolUsed.....0x00000001
Thu Aug 16 14:42:54 2007:      proxyState.....
  00:40:96:AF:3E:93-03:01

```

Thu Aug 16 14:42:54 2007: Packet contains 3 AVPs (not shown)
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xblabl04
Thu Aug 16 14:42:54 2007: Callback.....0x85ed228
Thu Aug 16 14:42:54 2007: protocolType.....0x00140001
Thu Aug 16 14:42:54 2007: proxyState.....
00:40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007: Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812,
proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20 ff 5b f2 16 64 df 02 61
....8....[.d..a
Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73 65 72 31 1f 13 30 30 2d
...K..User1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46 2d 33 45 2d 39 33 1e 20
40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35 2d 35 42 2d 46 42 2d 44
00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65 2d 54 53 57 45 42 05 06
0:Office..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1a
.....M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 00 00 01 06 06 00 00 00
...7c.....
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d 06 00 00 00 13 40 06 00
.....=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00 06 51 04 32 30 4f 17 01
...A.....Q.200..
Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f 14 05 65 1b 28 61 c9 75
.....e.(a.u
Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56 43 3d 30 2e 31 3b 50 12
ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1 a2 94 f8 39 80 ca 3c 96
..k.....9..<.
Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8 6c 07 8e fb 58 84 8d f6
.....=].l...X..
Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff ff ff 4f 27 02 01 00 25
3m.!.....O'...%
Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e 33 b5 4e 69 90 e7 84 25
.....1.3.Ni...%
Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87 ca dc c9 b3 75 73 65 72
B....3.....user
Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01 35 6c 65 61 70 3a 73 65
1.;.....5leap:se
Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65 79 3d 29 80 1d 2c 1c 85
ssion-key=)....
Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93 69 2a 55 d2 e5 46 89 8b
..)~@...i*U..F..
Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e 95 29 47 54 1a 1f 00 00
;eI>D.~.)GT....
Thu Aug 16 14:42:54 2007: 00000080: 00 09 01 19 61 75 74 68 2d 61 6c 67 6f 2d 74 79
....auth-algo-ty
Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c 65 61 70 1a 0d 00 00 37
pe=eap-leap....7
Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31 19 14 43 41 43 53 3a 30
c..User1..CACS:0
Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34 64 32 2f 31 50 12 9a 71
/9/a4df4d2/1P..q
Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5 c8 b1 71 94 97 d1
..}t.....q..
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=2
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=2
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Access-Accept received from RADIUS server


```

10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:      structureSize.....236
Thu Aug 16 14:42:54 2007:      resultCode.....0
Thu Aug 16 14:42:54 2007:      protocolUsed.....0x0
0000001
Thu Aug 16 14:42:54 2007:      proxyState.....00:
40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007: Packet contains 6 AVPs:
Thu Aug 16 14:42:54 2007: AVP[01] Framed-IP-Address.....0xffffffff (-1)
(4 bytes)
Thu Aug 16 14:42:54 2007: AVP[02] EAP-Message.....DATA (37 bytes)
Thu Aug 16 14:42:54 2007: AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes)
Thu Aug 16 14:42:54 2007: AVP[04] Airespace / ACL-Name.....User1 (5 bytes)
Thu Aug 16 14:42:54 2007: AVP[05] Class.....CACs:0/9/a4df4d2/1
(18 bytes)
Thu Aug 16 14:42:54 2007: AVP[06] Message-Authenticator.....DATA (16 bytes)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override
for station 00:40:96:af:3e:93
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values
for station 00:40:96:af:3e:93
source: 4, valid bits: 0x400
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTAVgC: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfName: '',
aclName:User1
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Inserting new RADIUS override into chain for station 00:40:96:af:3e:93

```

U kunt een combinatie van de opdracht **Show WLAN** gebruiken om te herkennen welke van uw WLAN's RADIUS-serververificatie gebruiken. Vervolgens kunt u de opdracht **voor de samenvatting van de client** bekijken om te zien welke MAC-adressen (clients) met succes geauthentiseerd zijn op RADIUS WLAN's. U kunt dit ook correleren met uw Cisco Secure ACS-doorgegeven pogingen of mislukte pogingen.

Cisco raadt u aan uw ACL-configuraties met een draadloze client te testen om er zeker van te zijn dat u deze correct hebt ingesteld. Als zij niet correct werken, controleer de ACL's op de ACL-webpagina en controleer of uw ACL-wijzigingen zijn toegepast op de interface van de controller.

U kunt deze showopdrachten ook gebruiken om uw configuratie te verifiëren:

- **Laat acl samenvatting zien**—Om de ACL's weer te geven die op de controller zijn ingesteld, gebruikt u de opdracht **samenvatting tonen**.

Hierna volgt een voorbeeld:

```
(Cisco Controller) >show acl summary
```

```

ACL Name                               Applied
-----
User1                                   Yes
User2                                   Yes

```

- **Toon ACL gedetailleerd <ACL_Name>** —Toont gedetailleerde informatie over de geconfigureerde ACL's.Hierna volgt een voorbeeld:**Opmerking:** Sommige lijnen in de uitvoer

zijn naar de tweede regel verplaatst als gevolg van ruimtebeperkingen.

Cisco Controller) >show acl detailed User1

		Source			Destination	
	Source Port	Dest Port				
I	Dir	IP Address/Netmask			IP Address/Netmask	
Prot	Range	Range	DSCP	Action		
1	In	172.16.0.0/255.255.0.0			172.16.1.100/255.255.255.255	
	Any	0-65535	0-65535	Any	Permit	
2	Out	172.16.1.100/255.255.255.255			172.16.0.0/255.255.0.0	
	Any	0-65535	0-65535	Any	Permit	

(Cisco Controller) >show acl detailed User2

		Source			Destination	
	Source Port	Dest Port				
I	Dir	IP Address/Netmask			IP Address/Netmask	
Prot	Range	Range	DSCP	Action		
1	In	172.16.0.0/255.255.0.0			172.16.1.50/255.255.255.255	
	Any	0-65535	0-65535	Any	Permit	
2	Out	172.16.1.50/255.255.255.255			172.16.0.0/255.255.0.0	
	Any	0-65535	0-65535	Any	Permit	

- **Geef clientgegevens weer <MAC-adres van de client>** - Hiermee geeft u gedetailleerde informatie weer over de draadloze client.

Tips bij het oplossen van problemen

Gebruik deze tips om problemen op te lossen:

- Controleer op de controller dat de RADIUS-server actief is en niet op stand-by of uitgeschakeld.
- Controleer op de controller of de RADIUS-server is geselecteerd in het vervolgkeuzemenu van de WLAN (SSID).
- Controleer of de RADIUS-server de verificatieaanvraag van de draadloze client ontvangt en bevestigt.
- Controleer de Geautomatiseerde verificaties en mislukte meldingen op de ACS-server om dit te bereiken. Deze verslagen zijn beschikbaar onder Rapporten en Activiteiten op de ACS-server.

Gerelateerde informatie

- [ACL's op draadloze LAN-controllers: Regels, beperkingen en voorbeelden](#)
- [Configuratievoorbeeld van ACL's op draadloze LAN-controllers](#)
- [Configuratievoorbeeld van MAC-filters met draadloze LAN-controllers \(WLC's\)](#)
- [Configuratie-gids voor Cisco draadloze LAN-controllers, release 5.2](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)