# ACS 5.2 configureren voor poortgebaseerde verificatie met een LAP

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten **Conventies** Achtergrondinformatie Configureren Netwerkdiagram Aannames Configuratiestappen LAMP configureren Switch configureren **RADIUS-server configureren** Netwerkbronnen configureren Gebruikers configureren Beleidselementen definiëren Toegangsbeleid toepassen Verifiëren Problemen oplossen Gerelateerde informatie

# Inleiding

Dit document beschrijft hoe u een lichtgewicht access point (LAP) kunt configureren als een 802.1x-applicatie om te verifiëren tegen een RADIUS-server zoals een Access Control Server (ACS) 5.2.

# **Voorwaarden**

## Vereisten

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

- Basiskennis hebben van de draadloze LAN-controller (WLC) en LAN's.
- Functionele kennis van de AAA-server hebben.
- Zorg voor een grondige kennis van draadloze netwerken en problemen met de draadloze

beveiliging.

#### Gebruikte componenten

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

- Cisco 5508 WLC met firmwarerelease 7.0.220.0
- Cisco 3502 Series router
- Cisco Secure ACS-softwarerelease 5.2
- Cisco 3560 Series Switch

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 <u>Cisco Technical Tips Conventions</u> (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

# **Achtergrondinformatie**

LAP's hebben in de fabriek X.509-certificaten geïnstalleerd - ondertekend door een privésleutel die op het apparaat worden gebrand op het moment van productie. De LAP's gebruiken dit certificaat om bij het samenvoegen te authenticeren met de WLC. Deze methode beschrijft een andere manier om LAP's te verifiëren. Met WLC-software kunt u de 802.1x-verificatie configureren tussen een Cisco Aironet access point (AP) en een Cisco switch. In dit geval werkt het toegangspunt als de 802.1x-aanvrager en wordt het door de switch geverifieerd op basis van een RADIUS-server (ACS) die EAP-FAST gebruikt met anonieme PAC-levering. Zodra de switch is geconfigureerd voor 802.1x-verificatie, kan alleen 802.1x-verkeer door de poort worden doorgegeven totdat het apparaat dat is aangesloten op de poort, met succes wordt geverifieerd. Een AP kan worden geverifieerd of voordat het zich aansluit bij een WLC of nadat het zich heeft aangesloten bij een WLC, in welk geval u 802.1x configureert op de switch nadat de LAP zich aansluit bij de WLC.

## **Configureren**

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

## **Netwerkdiagram**

Het netwerk in dit document is als volgt opgebouwd:



Dit zijn de configuratiedetails van de componenten die in dit diagram worden gebruikt:

- Het IP-adres van de ACS-server (RADIUS) is 192.168.150.24.
- Het beheer en AP-manager interfaceadres van de WLC is 192.168.75.44.
- De DHCP-servers richten zich op 192.168.150.25.
- LAP wordt geplaatst in VLAN 253.
- VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.10
- VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

## **Aannames**

- Switches zijn geconfigureerd voor alle Layer 3 VLAN's.
- De DHCP-server is een DHCP-scope toegewezen.
- Layer 3-connectiviteit bestaat tussen alle apparaten in het netwerk.
- De LAP is al aangesloten bij de WLC.
- Elk VLAN heeft een /24 masker.
- ACS 5.2 heeft een zelfondertekend certificaat geïnstalleerd.

# **Configuratiestappen**

Deze configuratie is verdeeld in drie categorieën:

- 1. LAMP configureren.
- 2. Configureer de switch.
- 3. Configureer de RADIUS-server.

#### LAMP configureren

Aannames:

LAP is al geregistreerd in de WLC met optie 43, DNS of statisch geconfigureerde WLCbeheerinterface IP.

Voer de volgende stappen uit:

 Ga naar Wireless > Access points > Alle AP's om LAP-registratie op de WLC te verifiëren.

 cisco	BONITOR	VILANS	CONTROLLER	WIRELESS	SECORITY	MANAGEMENT	COMMANDS	HELP	(LEDBACK	54	ye Configuration	Bas   L	igout jafrad
Wireless	All APs											Entrie	n 1 - 1 of 1
* Access Points All APU	Current Filt	er.		Rone		[Change	Fiter) (Clear F	iller]					
<ul> <li>Kados</li> <li>802.11a/n</li> <li>802.11b/g/h</li> <li>Global Configuration</li> </ul>	Number of	APs		1									
> Advanced	AP Name		AP	Model		AP MAC	AP	Up Time		Admin Status	Operational Status	Part	AP Mode
Mesh HREAP Groups	3302e		AD	CAP3502E-A	K9	00:eft48:fa:53	19 1 6	, 42 h 32 e	n 42 s	Enabled	REG	13	Local
▶ 802.11a/n													
▶ 902.11b/g/n													
Media Stream													
Country													
Timers													
1 640													

2. U kunt de 802.1x-referenties (dat wil zeggen, gebruikersnaam/wachtwoord) voor alle LAP's op twee manieren configureren: WereldwijdVoor een reeds aangesloten bij LAP, kunt u de geloofsbrieven globaal plaatsen zodat elke LAP die zich bij WLC aansluit die geloofsbrieven zal

erven.

uludu cisco	HONETOR WLAND CON	TROLLER WIRELESS	SECURETY MENAGEMENT	COMMANDS HELP FEEDBACK	Saye Configuration   Bing   Legout Belie	
Wireless	Global Configuration				Apply	
<ul> <li>Access Points         Al APs         Kodios         tot.312n/n         tot.312n/n         Kodios         Advanced         Hesk         IBKAP Groups         902.116/n         802.116/n         Kodian Stream     </li> </ul>	CDP CDP State			High Availability AP Heartbest Timesut(1-33) [30		
	Ethernet Interface# 1 2 3 Radio Slot# 0	CDP State		Lood Mode AP Fast Neartheat Timer State Databa  HREAP Mode AP Fast Neartheat Timer State Disable  AP Primery Discovery Timesa(30 to 3500) Back-up Primery Controller 3P Address Back-up Secondary Controller rame Back-up Secondary Controller name Deck-up Secondary Controller name		
Country Timers	3	p .		TCP MSS		
⊧ QeS	Login Credentials			Globel TCP Adjust MSS		
	Usemanie			AP Retransmit Config Parameters		
	Fessiond Enable Password			AP Retransmit Count AP Retransmit Interval	5	
	802.1x Supplicant Cre 902.1x Authentication Usernama Password Canfirm Password	lentials				
	AP Failover Priority Global AP Pailover Priorit	Dicable •				
	AP Image Pre-downlos Download Primary Interchange Image	Develoa	d Backup			

IndividueelConfigureer 802.1 x profielen per AP. In ons voorbeeld, zullen wij geloofsbrieven per AP vormen.Ga naar Draadloos > Alle toegangspunten en selecteer het betreffende toegangspunt.Voeg de gebruikersnaam en het wachtwoord toe in de velden 802.1x Supplicant



**Opmerking:** inlogreferenties worden gebruikt om Telnet, SSH of console in te schakelen op het toegangspunt.

3. Configureer de sectie Hoge beschikbaarheid en klik op **Toepassen**.

 cisco	MONITOR MLANS CONTROLLER MIRE	LESS SECURITY MANAGEMENT ODMMAN	Saya Canfiguration Brig Logout Ba NDS HELP (EEEDBACK
Wireless	All APs > Details for 3502e		< Bock Appl
<ul> <li>Access Points All APs</li> <li>Rodos</li> <li>832.11a/n</li> <li>832.11a/n</li> <li>832.11a/n</li> <li>Globel Confugration</li> <li>Advanced</li> <li>Mesh</li> <li>HREAP Groups</li> <li>802.11a/n</li> <li>802.11a/n</li> <li>802.11a/n</li> <li>802.11b/g/s</li> <li>Media Streams</li> <li>Country</li> <li>Country</li> </ul>	Geseral Credeations Interfaces Norme Primary Castroller Secondary Castroller Tertiary Costroller AP Pailover Priority Low	High Availability Investory Advan	KM

**Opmerking:** na het opslaan blijven deze referenties behouden over de WLC en de APherstart. De referenties veranderen alleen wanneer de LAP zich aansluit bij een nieuwe WLC. De LAP gaat uit van de gebruikersnaam en het wachtwoord die op de nieuwe WLC zijn ingesteld.Als de AP zich nog niet bij een WLC heeft aangesloten, moet u in de LAP console om de referenties in te stellen. Geef deze CLI-opdracht uit in de inschakelmodus:LAP#Iwapp ap dot1x-gebruikersnaam <gebruikersnaam>wachtwoord <wachtwoord> ofLAP#capwap ap dot1x gebruikersnaam <gebruikersnaam> wachtwoord <wachtwoord> Opmerking: deze opdracht is alleen beschikbaar voor AP's die het herstelbeeld uitvoeren.De standaardgebruikersnaam en het wachtwoord voor de LAP zijn respectievelijk cisco en cisco.

#### Switch configureren

De switch fungeert als een verificator voor de LAP en verifieert de LAP op een RADIUS-server. Als de switch niet over de juiste software beschikt, upgrade dan de switch. In de switch CLI, geef deze opdrachten uit om de 802.1x-verificatie op een switch poort in te schakelen:

```
switch#configure terminal
switch(config)#dot1x system-auth-control
switch(config)#aaa new-model
!--- Enables 802.1x on the Switch. switch(config)#aaa authentication dot1x default group radius
switch(config)#radius server host 192.168.150.24 key cisco
!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x
information to the RADIUS server for authentication. switch(config)#ip radius source-interface
vlan 253
!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.
switch(config)interface gigabitEthernet 0/11 switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253 switch(config-if)mls gos trust dscp switch(config-
if)spanning-tree portfast !--- gig0/11 is the port number on which the AP is connected.
switch(config-if)dot1x pae authenticator !--- Configures dot1x authentication. switch(config-
if)dot1x port-control auto !--- With this command, the switch initiates the 802.1x
authentication.
```

**Opmerking:** als u andere AP's op dezelfde switch hebt en u wilt niet dat ze 802.1x gebruiken, kunt u de poort niet geconfigureerd laten voor 802.1x of deze opdracht geven:

#### **RADIUS-server configureren**

LAP is geverifieerd met EAP-FAST. Zorg ervoor dat de RADIUS-server die u gebruikt deze EAPmethode ondersteunt als u geen Cisco ACS 5.2 gebruikt.

De RADIUS-serverconfiguratie is verdeeld in vier stappen:

- 1. Configureer de netwerkbronnen.
- 2. Gebruikers configureren.
- 3. Beleidselementen definiëren.
- 4. Toegangsbeleid toepassen.

ACS 5.x is een beleidsgebaseerde ACS. Met andere woorden, ACS 5.x gebruikt een op regel gebaseerd beleidsmodel in plaats van het op groep gebaseerde model dat in de 4.x-versies wordt gebruikt.

Het op regels gebaseerde ACS 5.x-beleidsmodel biedt krachtigere en flexibelere toegangscontrole in vergelijking met de oudere groepsgebaseerde aanpak.

In het oudere op groepen gebaseerde model definieert een groep beleid omdat het drie soorten informatie bevat en aan elkaar koppelt:

- Identiteitsinformatie Deze informatie kan worden gebaseerd op lidmaatschap in AD- of LDAP-groepen of een statische toewijzing voor interne ACS-gebruikers.
- Andere beperkingen of voorwaarden Tijdbeperkingen, apparaatbeperkingen, enzovoort.
- Toestemmingen VLAN's of Cisco IOS<sup>®</sup>-prioriteitsniveaus.

Het ACS 5.x-beleidsmodel is gebaseerd op de vormregels:

Als de voorwaarde dan resultaat

Bijvoorbeeld, gebruiken wij de informatie die voor het op groep-gebaseerde model wordt beschreven:

Indien identiteitsvoorwaarde, beperkingsvoorwaarde dan vergunningsprofiel.

Dit geeft ons de flexibiliteit om de voorwaarden waaronder de gebruiker toegang tot het netwerk krijgt te beperken en ook het toegestane autorisatieniveau te beperken wanneer aan bepaalde voorwaarden wordt voldaan.

#### Netwerkbronnen configureren

In dit gedeelte configureren we de AAA-client voor de switch op de RADIUS-server.

Deze procedure legt uit hoe u de switch als AAA-client aan de RADIUS-server kunt toevoegen, zodat de switch de gebruikersreferenties van de LAP aan de RADIUS-server kan doorgeven.

Voer de volgende stappen uit:

- 1. Klik vanuit de ACS GUI op Netwerkbronnen.
- 2. Klik op Netwerkapparaatgroepen.
- 3. Ga naar Locatie > Aanmaken (onderaan

My Workspace	Network Resources > Network Device Groups > Location
🔹 🦛 Network Resources	Network Device Groups
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter: Vatch it Go
Network Devices and AAA Clients Default Network Device External RADIUS Servers Musers and Identity Stores Policy Elements	Name  Description  All Locations
Access Policies     Monitoring and Reports	
System Administration	

).
4. Voeg de vereiste velden toe en klik op Indienen.

cisco Cisco Secure ACS					
+ 🛞 My Workspace	Network Resources > Network Device Groups > Location > Create				
In Network Resources     Network Device Groups     Location     Device Type     Notwork Devices and AAA Clients     Default Network Device     External RADIUS Servers	Device Group - General         o Name:       LAB         Description:       LAB Devices         o Parent       All Locations         0 = Required fields	Select			
<ul> <li>B Users and Identity Stores</li> </ul>					
Policy Elements					
Access Policies					
<ul> <li>Monitoring and Reports</li> </ul>					
System Administration					

5. Het venster vernieuwt:

cisco Cisco Secure ACS						
► 🖑 My Workspace	Network Resources > Network Device Groups > Location					
🐱 🛵 Network Resources	Network Device Groups					
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter: 💌 Match if: 💌 Go 🗢					
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name      Description     All Locations					
B Users and Identity Stores	LAB LAB Device:s					
Sp. Policy Elements						
Access Policies						
Monitoring and Reports						
System Administration						

6. Klik op **Apparaattype >** Aanmaken.

cisco Cisco Secure A	ICS	
+ 🕀 My Workspace	Network Resources > Network Device Broups > Device Type > Edit "Device Type:Al Device Types:Switch	ies"
Interview Resources		
Network Device Groups     Location     Device Type	Device Group - General     Switches     Description: Switch where LAP is connected	
Network Devices and AAA Clients Default Network Device External RADIUS Servers	Parent All Device Types Select     Select	
Big Users and Identity Stores		
Policy Elements		
Access Policies		
Monitoring and Reports	Carlos Martin and a start and	
🕞 🍓 System Administration		

7. Klik op Verzenden. Als het venster is voltooid, wordt het

cisco Cisco Secure ACS					
► 💮 My Workspace	Network Resources > Network Device Groups > Device Type				
• 📢 Network Resources	Network Device Groups				
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter. 💌 Match it. 💌 Go 🗢				
Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name      Description     * <u>All Device Types</u> All Device Types				
Users and Identity Stores	Switches Switch where LAP is connected				
► Sp Policy Elements					
Access Policies					
Monitoring and Reports					
System Administration					

vernieuwd:

- 8. Ga naar Network Resources > Network Devices en AAA Clients.
- 9. Klik op **Maken** en vul de details in zoals hier wordt
  - weergegeven:

cisco Cisco Secure A	CS	accedimic SAUL-ACS52 (Primary)		
+ 🛃 Ny Workspace	Network Resources - Network Devices and AAA Clients - Create			
Lin Network Resources     Network Device Groups     Location     Device Trop     Network Devices and AUAChents     Default Network Device     External RADIUS Servers	Name: 2500-Switch-LAP     Description: Switch where LAP is connected     Network Device Groups     Location	Select		
	IP Address P Single IP Address C IP Range(s) • IP: 102.168.153.10	Authentication Options • TAGACB+ F • RADUS P • RADUS P • Shared Secret [citics		
	0 - Regard Salta	CaApert  1730 Enable KeyWhop Key Encryption Key Message Authenticator Cede Key Key Input Format C ASCII (P HEXADECIMAL		

10. Klik op **Verzenden**. Het venster vernieuwt:

cisco Cisco Secure A	CS				ecentren 1	IAUL AC
* 🔂 My Workspace	Network Resources > Network	Devices and AAA Clents				
Jan Network Resources	Network Devices					Showin
Location	Filter:	💌 Match it	<u>•</u> 60	<b>.</b>		
Network Devices and AAACREME	Rame +	8P / Mask	NDG:Location	NDG:Device Type	Description	
Detaut Network Device External RADIUS Servera	Step-Switch-LAP	192.168.153.10/32	All Locations:LAB	All Device Types:Switches	Switch wittere LAP is connected	
+ 🔐 Users and identity Stores						
Policy Elements						
» 💭 Access Policies						
* 📑 Nonitoring and Reports						
+ 🧟 System Administration						

## Gebruikers configureren

In deze sectie, zult u zien hoe u een gebruiker op eerder gevormde ACS te creëren. U wijst de gebruiker toe aan een groep die "LAP-gebruikers" wordt genoemd.

Voer de volgende stappen uit:

1. Ga naar Gebruikers en Identiteitswinkels > Identiteitsgroepen >

#### Aanmaken.

Cisco Cisco Secure A	Users and Identity Stores > Identity Groups > Edit: "IdentityGroup:All Groups:Wireless Users"
Network Resources      Series and Identity Stores      Identity Croups      Internal Identity Stores      External Identity Stores      LDAP	General         Image: Name: LAP users         Description: LAPs authenticating over wired Network.         Image: Parent All Groups         Select         Image: Parent All Groups         Image: Parent Parent All Groups         Image: Parent P
Active Directory RSA SecuriD Token Servers RADIUS Identify Servers Certificate Authorities Certificate Authentication Profile Identity Store Sequences	

#### 2. Klik op

Verzenden.

Cisco Secure ACS						
My Workspace	Users and Identity Stores > Identity Groups					
Network Resources	Identity Groups					
Users and Identity Stores  Identity Groups	Filter: 💌 Match if: 💌 Go 🔫					
<ul> <li>Internal Identity Stores</li> <li>External Identity Stores</li> </ul>	Name Description					
LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers	All Groups Identity Group Root     LAP users LAPs authenticating over wired Network.					
Certificate Authorities Certificate Authoritication Profile Identity Store Sequences						

- 3. Maak 3502e en wijs het toe aan groep "LAP-gebruikers".
- 4. Ga naar Gebruikers en Identiteitswinkels > Identiteitsgroepen > Gebruikers > Aanmaken.



5. U ziet de bijgewerkte informatie:

cisco Cisco Secure A	ICS
	Users and identity Stores > Internal identity Stores > Users
	Internal Users
Users and identity Stores	Filter: Match it: Go 🐨
Internal Identity Stores	Status User Name A Identity Group Description
Usars	B 3502e     All Groups:LAP users LAP 3502e in vian 253
External Identity Stores     Certificate Authorities     Certificate Authorities     Identity Store Sequences	

## Beleidselementen definiëren

Controleer of Permit Access is ingesteld.

cisco Cisco Secure A	ICS
+ 💮 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
Network Resources	Authorization Profiles
Users and identity Stores	Filter 🛛 🔻 Match if 🖉 💽 🐨
<ul> <li>Policy Elements</li> </ul>	
Session Conditions     Authorization and Permissions	Permit Access
<ul> <li>Network Access Authorization Profiles</li> </ul>	
Device Administration     Named Permission Objects	
+ 🔂 Access Policies	
<ul> <li>Monitoring and Reports</li> </ul>	
🕨 🦓 System Administration	

## Toegangsbeleid toepassen

In dit gedeelte selecteert u EAP-FAST als de verificatiemethode die wordt gebruikt voor LAP's om te verifiëren. U maakt vervolgens regels op basis van de vorige stappen.

Voer de volgende stappen uit:

 Ga naar Toegangsbeleid > Toegangsservices > Standaard netwerktoegang > Bewerken: "Standaard netwerktoegang"

😽 My Workspace	Access Folicies > Access Services > Default Network Access > Edit "Default Network A
(b) Network Resources	
🔐 Users and Identity Stores	General Allowed Protocols
So Policy Elements	Name: Default Network Access
🕵 Access Policies	Description: Default Network Access Service
Access Services	Service Type : Network Access
Service Selection Rules     O Default Device Admin	Policy Structure
Default Network Access	Identity
▶ 🖉 deleterne	Group Mapping
G Desch New Reveals	Group Mapping
Restance Administration	

2. Zorg ervoor dat u **EAP-FAST** en **Anonymous In-Band PAC Provisioning** hebt ingeschakeld.



• 🛃 Access Policies	► E Allow LEAP
Access Services     If Service Selection Rules     O Default Device Admin     O Default Network Access     Idently     Authorization     Ø deleteme     Monitoring and Reports     Ø System Administration	<ul> <li>✓ ✓ Allow PEAP</li> <li>PEAP Inner Methods</li> <li>✓ Allow EAP-IJS-CHAPV2</li> <li>✓ Allow Password Change Retries: 1</li> <li>✓ Allow EAP-GTC</li> <li>✓ Allow Password Change Retries: 1</li> </ul>
	<ul> <li>Allow EAP-FAST</li> <li>EAP-FAST Inner Methods</li> <li>Allow EAP-MS-CHAPv2</li> <li>Allow Password Change Retries: 3</li> <li>Allow EAP-GTC</li> <li>Allow FAS-GTC</li> <li>Allow TL3-Renegotiation</li> <li>Use PACs C Don't Use PACs</li> <li>Tunnel PAC Time To Live: 90</li> <li>Proactive PAC update will occur after 10</li> <li>% of PAC Time To Live has expired</li> <li>Allow Authenticated In-Band PAC Provisioning</li> <li>Server Returns Access Accept After Authenticated Provisioning</li> <li>Allow Machine Authentication</li> <li>Machine PAC Time To Live: 1</li> <li>Weeks v</li> <li>Enable Stateless Session Resume</li> <li>Authorization PAC Time To Live: 1</li> <li>Hours v</li> </ul>
	Submit Cancel

- 3. Klik op Verzenden.
- 4. Controleer de groep Identity die u hebt geselecteerd. In dit voorbeeld, gebruik **Interne Gebruikers** (die op ACS) werd gemaakt en sla de veranderingen

op.

cisco Cisco Secure A	CS academin SAL
+ 🎯 My Workspace	Access Policies > Access Services > Default Network Access > Identity
<ul> <li>By Network Resources</li> </ul>	Single result selection Rule based result selection
+ 🐉 Users and Identity Stores	Identify Source: Internal Users Select
Policy Elements	· Attacked Centers
🖌 🕵 Access Policies	Tarmentrative failed Read
Access Services     J Service Selection Rules     O Detault Device Admin	if user not found Reject  If process failed Drop
Go Default Network Access	Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will
Authorization	De rejached
<ul> <li>I Monitoring and Reports</li> </ul>	
🕨 😼 System Administration	

5. Ga naar **Toegangsbeleid > Toegangsservices > Standaard netwerktoegang > Autorisatie** om het autorisatieprofiel te verifiëren.U kunt aanpassen onder welke voorwaarden u een gebruiker toegang tot het netwerk zal verlenen en welk autorisatieprofiel (attributen) u zal overgaan zodra het is geverifieerd. Deze granulariteit is alleen beschikbaar in ACS 5.x. In dit voorbeeld worden Locatie, **Apparaattype**, **Protocol**, **Identity Group** en **EAP-verificatiemethode** geselecteerd.



- 6. Klik op OK en sla wijzigingen op.
- 7. De volgende stap is het opstellen van een regel. Als er geen regels zijn gedefinieerd, krijgt LAP zonder voorwaarden toegang.
- 8. Klik op **Aanmaken > Regel-1**. Deze regel is voor gebruikers in de groep "LAPgebruikers".

cisco Cisco Secure AC			scaudmin
・ 役争 My Workspace	cess Policies > Autoris Services > Default Network Access > Autor	ization	
+ 🞲 Network Resources	andard Policy Exception Policy		
+ 🐉 Users and Identity Stores	Caco Secure ACS - Mozilla Firefex		×
• Q> Policy Elements			
- 🛱 Access Policies	132.196.130.24 https://132.166.130.24/acsadmin/Pol	cyinputAction.de	W
Access Services     El Sentce Selection Rules     M Default Device Admin     O Default Network Access     Mentity     Access     Access     Access     Access     Access     Access     Access	1 Status: Enabled The Customize button in the lower m policy conditions and results are aver	ight area of the policy rules screen cont aliable here for use in policy rules.	rois which
Monitoring and Reports	Cardillana		
🔸 💐 System Administration		* All I ocañena I AD	Select
	MCC Davies Time:	All Device Types Switches	Salert
	Protocol: match	Radus	Balect
	Videntity Group:	All Groups LAP users	Select
	Eap Authentication Method: -ANY-		
	Results Authoritzation Profiles:  Fermit Access Select Deselect	You may select multiple authorization profi dofined in multiple profiles will use the val profile defined.	les. Attributes ue from the first
	OK Cancel	• Died rule matches.	Help
	Create1 Duplicate1 Edt Detete A Move	10 V	

9. Klik op **Wijzigingen opslaan**. Als u wilt dat gebruikers die niet voldoen aan de voorwaarden die moeten worden geweigerd, bewerk de standaardregel om "Deny Access" te zeggen.

cisco Cisco Secure A	CS	ramary) Lag Dut About the
	Access Psices > Access Services > Terfail Veteent Access > Autostration Standord Policy <u>Exception Policy</u> Network Access Authoritation Policy	
Access Person     Access Services     Berrice Selecton Rules     Goldeuti Device Admin     Octauti Device Admin     Octauti Network Access	Filter         Etatus         Watch if         Exactle         Coorditions           Status         Name         NDGLocation         NDGDevice Type         Protection         Monoperative Status         Eac Authentication Method           @         Bute:1         In All LocationsLAB         In All Device Types Dividutes         match Radius         In All Dovides LAP usets         MOT	Results He Acthorization Profiles Permit Access 0
Inertik Part reveal > 27 desterne > 20 Ronterne and Reports Ronterne Administration		
	Ensing the rules defined or no enabled rule matches.	Permit Access
	Create	Custorrize Hit Count

10. De laatste stap is het definiëren van regels voor servicesselectie. Gebruik deze pagina om een eenvoudig of regel-gebaseerd beleid te vormen om te bepalen welke dienst om op inkomende verzoeken van toepassing te zijn. Voorbeeld:

3) Network Resources						
	C Sno	de result seler	dian 🕫 F	Rule based result selection		
🐕 Users and Identity Stores	Service	Selection Po	licy			
> PolicyElements	Filter	Status	Natch it	Equals . Enabled . Clear Fi	ter   Qo   -	
Access Policies		C Status	Name	Conditions Protocol	Resulta	Hit Count
Delaut Device Admin	1		Rule-1	match Radius	Default Network Access	0
O Detault Network Access Identity Authorization     deteteme	2	<b>F 0</b>	Rule-2	match Tacacs	Default Device Admin	0

## **Verifiëren**

Als 802.1x is ingeschakeld op de poortpoort, wordt al het verkeer behalve het 802.1x-verkeer geblokkeerd door de switch. De LAP, die al bij de WLC is geregistreerd, wordt losgekoppeld. Enkel na een succesvolle 802.1x-verificatie mag ander verkeer door. Succesvolle registratie van de LAP naar de WLC nadat de 802.1x is ingeschakeld op de switch geeft aan dat de LAP-verificatie succesvol is.

AP-console:

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
  192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
  192.168.75.44:5247
!--- AP disconnects upon adding dot1x information in the gig0/11. *Jan 29 09:10:30.104: %WIDS-5-
DISABLED: IDS Signature is removed and disabled. *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP
changed state to DISCOVERY *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to
DISCOVERY *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface DotllRadiol, changed
state to administratively down *Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset *Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed
state to up *Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset Translating
"CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25) *Jan 29 09:10:36.203: status of
voice_diag_test from WLC is false
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST]
*Jan 29 09:11:08.947: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0 assigned DHCP address
192.168.153.106, mask 255.255.255.0, hostname 3502e
!--- Authentication is successful and the AP gets an IP. Translating "CISCO-CAPWAP-
CONTROLLER.Wlab"...domain server (192.168.150.25) *Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND:
DTLS connection request sent peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.000:
%CAPWAP-5-CHANGED: CAPWAP changed state to *Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS
```

connection created successfully peer\_ip: 192.168.75.44 peer\_port: 5246 \*Jan 29 09:11:37.578: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44 \*Jan 29 09:11:37.578: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN

\*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan wmmAC status is FALSEged state to CFG \*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to

```
down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
  reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
   5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
  Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
  down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
  reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radiol, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface DotllRadio0, changed state to
  down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
  reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
  keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
  established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled
!--- AP joins the 5508-3 WLC.
ACS-logs:
```

 Bekijk de Hit tellingen: Als u logbestanden controleert binnen 15 minuten van verificatie, zorg er dan voor dat u de Hit Count ververst. Op dezelfde pagina, onderaan heb je een Hit Count tabblad.

cisco Cisco Secure A	CS								
+ 🛞 My Workspace	Access	Policies	> Access	Services >	Service Selection Rules				
+ 🎲 Network Resources	0.0	innia ra	oult octa	tion 🖲 E	nia hosarina fusarina alu				
+ 👪 Users and Identity Stores	Serv	Service Selection Policy							
+ S. Policy Elements	Filte	Stat	18 -	Match if	Equals - Enabled	Clear Filter	Go		
<ul> <li>Access Policies</li> </ul>		10.00			Conditions		Basulta		
<ul> <li>Access Services</li> </ul>			Status	Name	Protocol		Service	Hit Count	
El Service Serection Milles     H Default Device Admin	1			Rule-1	match Radius		Default Network Access	1	
+ 🤨 Default Network Access	2			Rule-2	match Tacaca		Default Device Admin	0	
Identity Authorization									
+ 📳 Monitoring and Reports									
🕨 🍇 System Administration									

cisco Cisco Secure A	CS SALE A	CSAD (Prinnary) Lag Out About M								
<ul> <li>Ity Workspace</li> </ul>	Access Polities + Anness Centres + Cellest Intervent Anness + Authenization									
+ 10 Network Resources	Standard Enline Excertion Delice									
🕫 🐉 Users and identity Stores	Network Access Authorization Policy									
Policy Elements	The Date of the Court of Tested of Courtses of the									
- 🛃 Access Policies										
Access Services     Conjos Relaction Relac	Name Conditions     NDG Location NDG Davide Tate Photodi Method     Esp Authentication Veltod	Authorization Profiles Hill Count								
<ul> <li>Default Device Admin</li> </ul>	Rule-1 In Al Locations LAB In All Device Types Switches match Radius In All Groups LAP users -ANY-	Permit Access 1								
G Default Network Access										
<ul> <li>Monitoring and Reports</li> </ul>										
» 😽 Dystem Administration										
	<	Parril Array								
	Saw Changes Discard Changes									

Klik op Bewaking en rapporten en er verschijnt een nieuw pop-upvenster. Klik op Verificaties
 -RADIUS -vandaag. U kunt ook op Details klikken om te verifiëren welke serviceselectieregel
 is

toegepast.

2. 💁 🖻								Launch Interact	ive these
Showing Page	a 1 of 1 )			I Geto	Pager Go				
AAA Protocol > RAD	US Authenticatio	n							
Authentication Status : Date :	Pass or Pail January 29, 2012 (La	a130 Ninules   LastHo	uri <u>Lasi 12 Hows</u> i To	day i <u>Yesferdar i Last 7 Dav</u>	s (Last30 Davs )				
Generated on January 2	29, 2012 9:15:01 PM 8	ST							
Relati	¶+Click for details	9 -Mouss over item i	or additional informa	úan .					
Logged At	RADUS NAS Status Failure	Details Usemame	MACIP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Gr
Jan 29,12 9 11:12 966	PM 🖌	% 3502e	CC-EF-48-FA-53-19	Default Network Access	EAP-FAST (EAP-MSCHAP\2)	3590-Switch-LAP	192.168,153.10	GigabitEthemet0/11	

# Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

## Gerelateerde informatie

- <u>Cisco Secure Access Control System</u>
- Technische ondersteuning en documentatie Cisco Systems

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.