LAP를 사용한 포트 기반 인증을 위한 ACS 5.2 구 성

목차

<u>소개</u> 사전 요구 사항 요구 사항 사용되는 구성 요소 표기규칙 배경 정보 구성 네트워크 다이어그램 가정 컨피그레이션 단계 LAP 구성 스위치 구성 RADIUS 서버 구성 네트워크 리소스 구성 사용자 구성 정책 요소 정의 액세스 정책 적용 다음을 확인합니다. 문제 해결 관련 정보

소개

이 문서에서는 ACS(Access Control Server) 5.2와 같은 RADIUS 서버에 대해 인증하기 위해 LAP를 802.1x 신청자로 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

- 이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.
 - WLC(Wireless LAN Controller) 및 LAP에 대한 기본 지식을 갖추고 있습니다.
 - AAA 서버에 대한 기능적 지식이 있어야 합니다.
 - 무선 네트워크 및 무선 보안 문제에 대해 철저하게 알고 있어야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 7.0.220.0을 실행하는 Cisco 5508 WLC
- Cisco 3502 Series LAP
- 버전 5.2를 실행하는 Cisco Secure ACS
- Cisco 3560 Series 스위치

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 표기 규칙</u>을 참조하십시오.

배경 정보

LAP는 제조 시 디바이스에 구워지는 X.509 인증서(개인 키로 서명됨)를 공장에서 출하하여 설치했 습니다. LAP는 가입 프로세스에서 WLC를 인증하기 위해 이 인증서를 사용합니다. 이 방법은 LAP를 인증하는 또 다른 방법을 설명합니다. WLC 소프트웨어를 사용하면 Cisco Aironet AP(액세 스 포인트)와 Cisco 스위치 간에 802.1x 인증을 구성할 수 있습니다. 이 경우 AP는 802.1x 신청자 역할을 하며 익명 PAC 프로비저닝과 함께 EAP-FAST를 사용하는 RADIUS 서버(ACS)에 대해 스위 치에 의해 인증됩니다. 802.1x 인증을 위해 구성된 경우, 스위치에 포트에 연결된 디바이스가 성공 적으로 인증될 때까지 802.1x 트래픽 이외의 트래픽은 포트를 통과할 수 없습니다. AP가 WLC에 연 결되기 전 또는 WLC에 연결된 후 AP를 인증할 수 있습니다. 이 경우 LAP가 WLC에 연결된 후 스위 치에 802.1x를 구성합니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



다음은 이 다이어그램에서 사용되는 구성 요소의 컨피그레이션 세부 정보입니다.

- ACS(RADIUS) 서버의 IP 주소는 192.168.150.24입니다.
- WLC의 관리 및 AP 관리자 인터페이스 주소는 192.168.75.44입니다.
- DHCP 서버 주소는 192.168.150.25입니다.
- LAP는 VLAN 253에 배치됩니다.
- VLAN 253: 192.168.153.x/24. 게이트웨이: 192.168.153.10
- VLAN 75: 192.168.75.x/24. 게이트웨이: 192.168.75.1

가정

• 스위치는 모든 레이어 3 VLAN에 대해 구성됩니다.

- DHCP 서버에는 DHCP 범위가 할당됩니다.
- 레이어 3 연결은 네트워크의 모든 디바이스 간에 존재합니다.
- LAP가 이미 WLC에 연결되어 있습니다.
- 각 VLAN에는 /24 마스크가 있습니다.
- ACS 5.2에는 자체 서명 인증서가 설치되어 있습니다.

컨피그레이션 단계

이 컨피그레이션은 3가지 카테고리로 구분됩니다.

- 1. <u>LAP를 구성합니다.</u>
- 2. <u>스위치를 구성합니다.</u>
- 3. <u>RADIUS 서버를 구성합니다</u>.

LAP 구성

가정:

LAP는 옵션 43, DNS 또는 정적으로 구성된 WLC 관리 인터페이스 IP를 사용하여 WLC에 이미 등 록되었습니다.

다음 단계를 완료하십시오.

1. WLC에서 LAP 등록을 확인하려면 Wireless(무선) > Access Points(액세스 포인트) > All APs(모든 AP)로 이동합니다.

uluulu cisco	MONITOR MLANS	CONTROLLER WIRELESS SECURIT	Y MANADEMENT C	OMMANOS HELP	Sa	ge Configuration	Bing Lagout Befred
Wireless	All APs						Entries 1 - 1 of 1
* Access Points All APE	Current Filter	Rone	[Change Fit	ar] [Clear.Filter]			
 Hadica 802.11a/n 802.11b/g/h Cichal Configuration 	Number of APs	1					
+ Advanced	AP Name	AP Nodel	AP MAC	AP Up Time	Admin Status	Operational Status	Port AP Mode
HREAP Groups	3502e	AIR-CAP3502E-A-H5	cc:cf)48:fe:53:19	1 d, 42 h 32 d	n 42 s Enabled	REG	13 Local
▶ 802.11a/n							
▶ 802.11b/g/n							
Hedia Stream							
Country							
Timers							
F Qu5							

- 2. 모든 LAP의 802.1x 자격 증명(사용자 이름/비밀번호)을 두 가지 방법으로 구성할 수 있습니다
 - 전 세계

이미 조인된 LAP의 경우 WLC에 조인하는 모든 LAP가 이러한 자격 증명을 상속하도록

자격 증명을 전역으로 설정할 수 있습니다.

ululu cisco	HONETOR WLAND CON	ROLLER WIRELESS	SECONELLA NORMAEMEN	ат сомманов	HELP EEEDONCK	Saye Configuration Bing Legout Belle
Wireless	Global Configuration					Apply
Access Points Al APs Kodos C2.15e/n Ac2.55e/n C2.25e/n C2.25e/n	CDP			High Av	alability	
	CCP Soon Ethernet Interface# 0 1 2 3 Radio Slot# 0 1 2	CDP State		Local P H-REAL AP Pri Back- Back- Back-	tobe AP Feat Heartbeat Timer State Node AP Feat Heartbeat Timer State Node AP Feat Heartbeat Timer Dis- nery Discovery Timesui(30 to 300 ap Primary Controller 2P Address ap Primary Controller rame ap Secendary Controller name	Dise bla Dise bla Dise bla Dise bla Dise bla Dise bla
Timers	3	2		TCP MS	9 700 5-6-4 HEE	
r des	Userneme Peterand Enable Password			AP Retri	ansmit Config Parameters transmit Count transmit Interval	8 0
	802.1x Supplicant Cree 902.1x Authentication Usernama Password Canfirm Password	fentiols				
	AP Failover Priority Global AP Pailover Priorit AP Image Pre-downlos	v Disable •				
	Download Primary Interchange Image	Downlo	sad Backup			

• 개별적으로

AP당 802.1 x 프로필을 구성합니다. 이 예에서는 AP당 자격 증명을 구성합니다.

- a. Wireless(무선) > All APs(모든 AP)로 이동하여 관련 AP를 선택합니다.
- b. 802.1x Supplicant Credentials(신청자 자격 증명) 필드에 사용자 이름 및 비밀번호 를 추가합니다.

 cisco	MONITOR MLANS C	ONTROLLER WER		MANAGEMENT	COMMINDS	нцр	BERNACK	Sage Configuration Bing	Logout Exfre
Wireless	All APs > Details for	3502e						< Beck	Apply
 Access Points All APs Radios 802.113/h 802.113/h 802.113/h 802.113/g/s Global Configuration Advanced Mesb HREAP Groups 802.11a/n 802.11a/n 802.11b/g/e 	General Credent Logis Crodentials Override Global ere Usernere Presvord Enable Presvord	dertiels jose	riigh Aveilebii	ity Inventory	Advanced				
 Media Stream Country Timers QoS 	Over-ride Global orec Username Pessword Confirm Password	dentials 9802a +++++ ++++++	¥						

참고: 로그인 자격 증명은 텔넷, SSH 또는 콘솔에서 AP에 로그인하는 데 사용됩니다.

3. High Availability 섹션을 구성하고 Apply를 클릭합니다.

 cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MUNAGEMENT COMMANDS HELP EEEDBACK	Daya Configuration Bing	Logout <u>B</u> eiro
Wireless	All APs > Details for 3502e	< Sock	Apply
 Access Points All APs Rados 332.114/m 332.114/m/s Global Configuration Advanced Hesh HIREAP Groups S02.111a/m S02.11a/m 	General Credentials Interfaces High Availability Inventory Advanced Normo Hexagoneord 3P Address Primary Cantroliar 5508-3 192.368.75.44 Secondary Cantroliar Image (Secondary Cantroliar) Tertiary Cantroliar Image (Secondary Cantroliar) AP Failover Priority Low		
Hedia Stream Country Timers QoS			

참고: 저장되면 이러한 자격 증명은 WLC에서 유지되고 AP가 재부팅됩니다. 자격 증명은 LAP가 새 WLC에 조인할 때만 변경됩니다. LAP는 새 WLC에 구성된 사용자 이름 및 비밀번 호를 사용합니다.

AP가 아직 WLC에 조인하지 않은 경우 자격 증명을 설정하려면 LAP에 콘솔로 로그인해야 합니다. 활성화 모드에서 다음 CLI 명령을 실행합니다.

LAP#Iwapp ap dot1x 사용자 이름 <username> 암호 <password>

또는

LAP#capwap ap dot1x 사용자 이름 <username> 암호 <password>

참고: 이 명령은 복구 이미지를 실행하는 AP에만 사용할 수 있습니다.

LAP의 기본 사용자 이름 및 비밀번호는 각각 cisco 및 Cisco입니다.

스위치 구성

스위치는 LAP의 인증자 역할을 하며 RADIUS 서버에 대해 LAP를 인증합니다. 스위치에 호환 소프 트웨어가 없는 경우 스위치를 업그레이드합니다. 스위치 포트에서 802.1x 인증을 활성화하려면 스 위치 CLI에서 다음 명령을 실행합니다.

<#root>

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

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 qos 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.

참고: 동일한 스위치에 다른 AP가 있고 802.1x를 사용하지 않으려는 경우 802.1x에 대해 포트를 구 성하지 않은 상태로 두거나 다음 명령을 실행할 수 있습니다.

<#root>

switch(config-if)authentication port-control force-authorized

RADIUS 서버 구성

LAP는 EAP-FAST로 인증됩니다. Cisco ACS 5.2를 사용하지 않는 경우 사용하는 RADIUS 서버가 이 EAP 방법을 지원하는지 확인합니다.

RADIUS 서버 컨피그레이션은 4단계로 나뉩니다.

- 1. <u>네트워크 리소스를 구성합니다.</u>
- 2. <u>사용자를 구성합니다.</u>
- 3. <u>정책 요소를 정의합니다.</u>
- 4. <u>액세스 정책을 적용합니다.</u>

ACS 5.x는 정책 기반 ACS입니다. 즉, ACS 5.x는 4.x 버전에서 사용된 그룹 기반 모델 대신 규칙 기 반 정책 모델을 사용합니다.

ACS 5.x 규칙 기반 정책 모델은 이전의 그룹 기반 접근 방식에 비해 더 강력하고 유연한 액세스 제 어를 제공합니다.

이전 그룹 기반 모델에서 그룹은 세 가지 유형의 정보를 포함하고 연결하므로 정책을 정의합니다.

- ID 정보 이 정보는 AD 또는 LDAP 그룹의 멤버십 또는 내부 ACS 사용자에 대한 정적 할당을 기반으로 할 수 있습니다.
- 기타 제한 또는 조건 시간 제한, 장치 제한 등
- 권한 VLAN 또는 Cisco IOS[®] 권한 레벨

ACS 5.x 정책 모델은 다음 형식의 규칙을 기반으로 합니다.

조건이 충족되면

예를 들어, 그룹 기반 모델에 대해 설명된 정보를 사용합니다.

ID-condition, restriction-condition, authorization-profile이 있는 경우

그 결과 사용자가 네트워크에 액세스할 수 있는 조건 및 특정 조건이 충족될 때 허용되는 권한 수준 을 제한할 수 있는 유연성을 제공합니다.

네트워크 리소스 구성

이 섹션에서는 RADIUS 서버의 스위치에 대해 AAA 클라이언트를 구성합니다.

이 절차에서는 스위치가 RADIUS 서버에 LAP의 사용자 자격 증명을 전달할 수 있도록 RADIUS 서 버에서 스위치를 AAA 클라이언트로 추가하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

- 1. ACS GUI에서 Network Resources(네트워크 리소스)를 클릭합니다.
- 2. Network Device Groups(네트워크 디바이스 그룹)를 클릭합니다.
- 3. 위치 > 생성(하단)으로 이동합니다.

cisco Secure ACS							
+ 🤔 My Workspace	Network Resources > Network Device Groups > Location						
🔹 😜 Network Resources	Network Device Groups						
Network Device Groups Location	Filter: 💌 Match it 💌 Go 🛩						
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Image: Name ▲ Description Image: All Locations All Locations						
🕞 🏙 Users and identity Stores							
So Policy Elements							
+ 🔂 Access Policies							
• 📄 Monitoring and Reports							
🕞 🍇 System Administration							

4. 필수 필드를 추가하고 Submit(제출)을 클릭합니다.

cisco Cisco Secure A	CS
My Workspace	Network Resources > Network Device Groups > Location > Create
In Network Resources Network Device Groups Incestion 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 Select Select
 Jusers and Identity Stores 	
Operation Policy Elements	
► 🔂 Access Policies	
Monitoring and Reports	
System Administration	

5. 창이 업데이트됩니다.

cisco Cisco Secure A	CS
🕨 💮 My Workspace	Network Resources > Network Device Groups > Location
🐱 🛵 Network Resources	Network Device Groups
 Network Device Groups Location 	Filter: 💽 Match if: 💽 Go 🗢
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name Description * <u>All Locations</u>
Users and Identity Stores	LAB LAB Device:s
Policy Elements	
+ 🔂 Access Policies	
 Monitoring and Reports 	
System Administration	

6. Device Type(디바이스 유형) > Create(생성)를 클릭합니다.

cisco Cisco Secure /	ICS	
+ 🛃 My Workspace	Network Resources > Network Device Groups > Device Type > Edit "Device Type:Al Device Types Switc	ches"
🔹 🌆 Network Resources	Darley Ground Ground	
 Network Device Groups Location 	o Name: Switches	
Device Type	Description: Switch where LAP is connected	
Network Devices and AAA Clients Default Network Device External RADIUS Servers	Parent All Device Types Select Select	
Users and Identity Stores		
Policy Elements		
Access Policies		
Monitoring and Reports	and the White the second second second	
🕞 🍕 System Administration		

7. Submit(제출)을 클릭합니다. 완료되면 창이 새로 고쳐집니다.

Cisco Secure ACS						
🕨 🌍 My Workspace	Network Resources > Network Device Groups > Device Type					
🖡 🦛 Network Resources	Network Device Groups					
 Network Device Groups Location 	Filter. 💌 Match it. 💌 Go 🗢					
Device Type						
Network Devices and AAA Clients Default Network Device	Name A Description					
External RADIUS Servers	* All Device Types All Device Types					
🕨 🏭 Users and Identity Stores	Switches Switch where LAP is connected					
Sp Policy Elements						
Access Policies						
Monitoring and Reports						
🕨 🍓 System Administration						

- 8. Network Resources(네트워크 리소스) > Network Devices and AAA Clients(네트워크 디바이 스 및 AAA 클라이언트)로 이동합니다.
- 9. Create(생성)를 클릭하고 여기에 표시된 대로 세부사항을 입력합니다.

cisco Cisco Secure A	CS	accadimic SALIL-ACSS2 (Primary)
+ 🚭 Ny Workspace	Network Resources - Xetwort Devices and AAA Clerits - Create	
Network Resources Network Device Groups	Name: 2500-Deltdr-LAP	
Location	Description: Switch where LAP is connected	
Network Devices and AAA Clients	Network Device Groups	Entra 1
Default Network Device External RACILIS Servers	Device Type All Device Types Switches	Select
+ 🗿 Users and Identity Stores	Level 100	
+ Sp Policy Elements	IP Address	Authentication Options
* 🔂 Access Policies	Single IP Address (C IP Range(s)	▼RADUS P
 Nonitoring and Reports 	• IP: 102.168.153.10	9 Shared Secret, cloca
 System Administration 		CoApert 1790
1000		Enable KeyWrop
		Key Encryption Key
de la companya de la		Massage Authenticator Cede Key
	• -Regiraditelds	Kay ingua Portfazi 🐂 ABUI 🥍 HEAADECBAA,

10. Submit(제출)을 클릭합니다. 창이 업데이트됩니다.

cisco Cisco Secure A	CS	econdrum SALIL-ACT
+ 💮 Mr Workspace	Network Resources > Network Devices and AAA Clients	
 Jø Network Resources 	Network Devices	Showin
Network Device Groups Location	Filter: Vilatch it. V Go V	
Network Devices and AM-Clients	Rame - IP/Mask NDGLocation NDGDevice Type	Description
Detault Network Device External RADIUS Servers	□ 3550-Swhth-LAP 192.166.153.10/32 All Lecalions:LAB All Device Types:Bwitches	Switch where LAP is connected
 Stores 		
Policy Elements		
» 💭 Access Policies		
* 📑 Nonitoring and Reports		
+ 🧟 System Administration		

사용자 구성

이 섹션에서는 이전에 구성된 ACS에서 사용자를 생성하는 방법을 살펴봅니다. "LAP 사용자"라는 그룹에 사용자를 할당합니다.

다음 단계를 완료하십시오.

1. Users and Identity Stores(사용자 및 ID 저장소) > Identity Groups(ID 그룹) > Create(생성)로 이동합니다.

cisco Cisco Secure A	CS	
 My Workspace Network Resources Wers and Identity Stores Internal Identity Stores 	Users and identity Stores > identity Groups > Edit: "identityGroup:All Groups:Wireless Use General Warne: LAP users Description: LAPs authenticating over wired Network.	13"
External identity Stores LDAP Active Directory RSA SecuriD Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authentication Profile Identity Store Sequences	a = Required fields	Selea

2. Submit(제출)을 클릭합니다.

cisco Cisco Secure A	CS
State My Workspace My Workspace My Network Resources States	Users and Identity Stores > Identity Groups
Identity Groups Internal Identity Stores External Identity Stores LDAP Active Directory	Filter: ✓ Match if: ✓ Go ✓ Name ▲ Description ✓ All Groups Identity Group Root
RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authentication Profile Identity Store Sequences	LAP users LAPs authenticating over wired Network.

- 3. 3502e를 생성하고 그룹 "LAP 사용자"에 할당합니다.
- 4. Users and Identity Stores(사용자 및 ID 저장소) > Identity Groups(ID 그룹) > Users(사용자) > Create(생성)로 이동합니다.

cisco Cisco Secure A	cs
🕨 🚭 My Workspace	Users and identity Stores > Internal identity Stores > Users > Create
Detwork Resources	Canacal
 B Users and Identity Stores 	Nama: 3502e Status: Enabled - 9
Identity Groups Identity Stores	Description: LAP 3502e in vian 253
Users	Identity Group: All Groups:LAP users Select
External Identity Stores Certificate Authonities Certificate Authentication Profile Identity Store Sequences	Password Information Password must Contain 4 - 32 characters
 Policy Elements 	Password:
Access Policies	Confirm Passwort
 Monitoring and Reports 	Change password on next login
System Administration	User information There are no additional identity attributes defined for user records • Required fields

5. 업데이트된 정보가 표시됩니다.

💮 My Workspace	Users and	Identity Store	es > Internal identity Sto	res >	Users	
Network Resources	Interna	al Users				
B Users and Identity Stores Identity Groups	Filter:	Filter: Match it: Go 💌				
Internal Identity Stores	F	Status	User Name		Identity Group	Description
Users			35024		All Groups:LAP users	LAP 3502e in vian 253

정책 요소 정의

Permit Access(액세스 허용)가 설정되어 있는지 확인합니다.

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 That hit to the second se
🗸 🚳 Policy Elements	
Session Conditions Authorization and Permissions	Permit Access
 Network Access Authorization Profiles 	
Device Administration Named Permission Objects	
+ 🔂 Access Policies	
Monitoring and Reports	
🕨 🦓 System Administration	

액세스 정책 적용

이 섹션에서는 인증을 위해 LAP에 사용되는 인증 방법으로 EAP-FAST를 선택합니다. 그런 다음 이 전 단계를 기반으로 규칙을 생성합니다.

다음 단계를 완료하십시오.

1. Access Policies(액세스 정책) > Access Services(액세스 서비스) > Default Network Access(기본 네트워크 액세스) > Edit: "Default Network Access(기본 네트워크 액세스)"로 이 동합니다.

cisco Cisco Secure A	CS
🕞 🖌 My Workspace	Access Policies > Access Services > Default Network Access > Edit "Default Network Access"
Metwork Resources Metwork Resour	
Busers and Identity Stores	General Allowed Protocols
▶ S Policy Elements	Name: Default Network Access
🔹 🕵 Access Policies	Description: Default Network Access Service
Access Services Il Service Selection Rules O Default Device Admin	Service Type : Network Access
Default Network Access	Identity
▶ Ø deleteme	Group Mapping
Monitoring and Reports	Authorization
🕨 🍓 System Administration	

2. EAP-FAST 및 익명 대역 내 PAC 프로비저닝을 활성화했는지 확인합니다.

cisco Cisco Secure AC	CS
+ 🚭 My Workspace	Access Policies > Access Services > Default Network Access > Edit "Default Network Access"
 My Workspace Network Resources Users and Identity Stores Policy Elements Access Policies Access Services Service Selection Rules Obtault Network Access Identity Authorization Ø deleteme Monitoring and Reports System Administration 	Access Pelicies > Access Services > Default Network Access* General Allowed Protocols Image: Process Host Lookup Authentication Protocols Image: Process Host Lookup Image: Process Host Lookup

• 👗 Access Policies	► Allow LEAP
Access Services More Selection Rules Operault Device Admin Operault Device Admin Operault Network Access Identity Authorization ✓ deleteme Monitoring and Reports System Administration	Allow PEAP PEAP Inner Methods P Allow EAP-MS-CHAPV2 P Allow Password Change Retries: 1 Allow EAP-GTC P Allow Password Change Retries: 1
	 Allow EAP-FAST EAP-FAST Inner Methods Allow EAP-MS-CHAPv2 Allow Password Change Retries: 3 Allow EAP-GTC Allow TLS-Renegotiation Use PACs © Don't Use PACs Tunnel PAC Time To Live: 90 Poactive PAC update will occur after 10 % of PAC Time To Live has expired Allow Authenticated In-Band PAC Provisioning Berver Returns Access Accept After Authenticated Provisioning Allow Nachine Authentication Machine PAC Time To Live: 1 Hours
	Submit Cancel

- 3. Submit(제출)을 클릭합니다.
- 4. 선택한 ID 그룹을 확인합니다. 이 예에서는 ACS에서 생성된 Internal Users(내부 사용자)를 사 용하고 변경 사항을 저장합니다.

cisco Cisco Secure A	CS according SAL
+ 🚭 My Workspace	Access Policies > Access Services > Default Network Access > Mently
+ ity Network Resources	⁶ Single result selection ⁶ Bule based result selection
+ 🐉 Users and Identity Stores	Identity Source: Internal Users Select
Policy Elements	· Attended Options
🖌 🕵 Access Policies	if active tailed React
Access Services Service Selection Rules O Detault Device Admin	if user notifound Reject If process failed Drop
O Delaut Network Access	Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS NSCHAP 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	be rejected
 Monitoring and Reports 	
 Kig System Administration 	

5. Access Policies(액세스 정책) > Access Services(액세스 서비스) > Default Network Access(기본 네트워크 액세스) > Authorization(권한 부여)으로 이동하여 권한 부여 프로파일 을 확인합니다.

네트워크에 대한 사용자 액세스를 허용할 조건 및 인증 후 전달 할 인증 프로파일 (특성) 하에 서 사용자 정의 할 수 있습니다. 이 세분화는 ACS 5.x에서만 사용할 수 있습니다. 이 예에서는 Location, Device Type, Protocol, Identity Group 및 EAP Authentication Method를 선택합니다

cisco Cisco Secure Ad	CS SALE ACESS (Primary) Lag C	a Alad Re
* 🛃 My Werkspace	Adress Polices > Adress Terrices > Defaul Hervion Addess > Aufferication	
+ 👸 Network Resources	Standard Dollaw Evrontee Dollaw	
 M Users and Identity Stores 	Natansk krean fatherizite Daiss	
 Policy Elements 	Elter Ethins - Math & Equila - Enabled - Claw Etw. 6a -	
s 🕵 Ancess Policies		
Access Services	Results Name ND01.station Time And Date Authorization Profiles	
+ G Default Device Admin	No della fo display	
+ O Default Notwork Access		
Latracation	Mosile Firefox X	
 g deleterns 	202168350.24 https://202168150.34/accadmin/Polici/hpubliction.do	
D Montering and Hepuits		
s System Administration	Customize Conditions	
	Compound Condition	
	Device Pitter Device Pitter Padress NDC Device Tige 2	
	Device Port Filter Sector Greep 🔨	
	End Station Filter	
	Time And Date	
	UseCaso Was llachine Auberticated	
	OK Cancel	
	44	
	V	
	Default It no rules defined or no enabled rule matches. Permit Access 0	
	Cesterios Cesterios	HECount

- 6. OK(확인)를 클릭하고 Save Changes(변경 사항 저장)를 클릭합니다.
- 7. 다음 단계는 규칙을 생성하는 것입니다. 정의된 규칙이 없으면 조건 없이 LAP에 액세스할 수 있습니다.
- 8. Create(생성) > Rule-1을 클릭합니다. 이 규칙은 "LAP 사용자" 그룹의 사용자를 위한 것입니 다.

cisco Cisco Secure Al	CIS ***	edmin S
+ 🕀 My Workspace	Access Policies > Access Services > Definit Network Access > Authorization	
+ 🞲 Network Resources	Standard Belgel Exception Doller	
+ 🤮 Users and identity Stores	Manager Porcy Exception Porcy	
	Net Caco Secure ACS - Mozilla Finefica	×
🖌 🕵 Access Policies	Fite 192.168.150.24 https://192.168.150.24/ acsadmin/PolicyInputAction.do	<u>合</u>
Access Services Service Selection Rules O Default Device Admin O Default Network Access Identity Access device Admin Service	Image: The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.	
+ 📳 Monitoring and Reports	Conditions	
+ 🥞 System Administration	VICtionation	
	NDC Davide Type: In TAIl Device Types Switches Select	
	Protocol: metch - Radius Select	
	Identity Group: In All Groups LAP users Select	5
	Eap Authentication Method: ANY-	
	Results #utholization Profiles: Fermit Accords Fermit Accords Formation and the second	
	OK Cancel	Help
	The rules denned or no enabled rule matches.	
	Cenate Duplicate I* Edit Delete A Move to Y	
	Save Changes Discard Changes	

9. Save Changes(변경 사항 저장)를 클릭합니다. 조건과 일치하지 않는 사용자를 거부하도록 하 려면 기본 규칙을 편집하여 "Deny Access(액세스 거부)"라고 말합니다.

cisco Cisco Secure A	ICS SALE ACSS	(Primery) Log Dut About the
	Access Polices > Access Services > Defaul Retwort Access > Autorization Stancord Policy (<u>Exception Policy</u> Network Access Authorization Policy	
Access Services Service Services Service Services Service Services Order Davice Admin Service Service Service Administration	Film (class Conditions Status NOGLocation NDGDevice Type Protocal Martiny Group Eap Authentication Mathe Ø Bate_1 In All LocationsLAB In All Device Types Dwitches match Radius In All DroupsLAP users HVP	Results Hi Authorization Profiles D Permit Access D
	Delaxit If no rules defined or no enabled rule matches. Create	Permit Access

10. 마지막 단계는 서비스 선택 규칙을 정의하는 것입니다. 이 페이지에서는 수신 요청에 적용할 서비스를 결정하기 위해 단순 또는 규칙 기반 정책을 구성할 수 있습니다. 예를 들면 다음과 같습니다.

A My Workspace	Access	Publics	> Access	Services >	Service Selection Rules		
3 Network Resources		incle re	sult selec	tion 🕫 i	Rule based result selection		
🚜 Users and Identity Stores	Sen	ice Sel	ection Po	licy			
Sy Policy Elements	Filte	e Stat		Natch it	Equals + Enabled + ClearF	iter Go -	
Access Policies	IL	E	Status	Name	Conditions Protocol	Results Service	Hit Count
O Default Device Admin	1			Rule-1	match Radius	Default Network Access	0
O Detault Network Access Identity Authorization Ø determe	2		9	Rule-2	match Tacacs	Default Device Admin	0
C Harberton and Barreto							

다음을 확인합니다.

스위치 포트에서 802.1x가 활성화되면 802.1x 트래픽을 제외한 모든 트래픽이 포트를 통해 차단됩니다. WLC에 이미 등록된 LAP의 연결이 끊어집니다. 802.1x 인증이 성공한 후에만 다른 트래픽이 통과할 수 있습니다. 스위치에서 802.1x가 활성화된 후 WLC에 LAP를 성공적으로 등록하면 LAP 인증이 성공했음을 나타냅니다.

AP 콘솔:

<#root>

*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 Dot11Radio1, 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

!--- 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 Dot11RadioO, 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 Dot11Radio1, changed state to up *Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, 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 로그:

1. 적중 횟수 보기:

인증 후 15분 내에 로그를 확인하는 경우 Hit Count를 새로 고쳐야 합니다. 같은 페이지의 하 단에 Hit Count(적중 횟수) 탭이 있습니다.

cisco Cisco Secure A	CS	-	-	-			aca			
+ 🛞 My Workspace	Access Policies > Access Services > Service Selection Rules Single result selection Service Selection Policy									
 Network Resources 										
Users and Identity Stores										
Policy Elements	Filter	Stat	us -	Match if:	Equals - Enabled - Clear P	ilter Go 🔻				
 Access Policies 		-			Conditions	Results				
Access Services			Status	Name	Protocol	Service	Hit Count			
H) Default Device Admin	1			Bule-1	match Radius	Default Network Access	1			
+ 🤨 Default Network Access	2		0	Rule-2	match Tacaca	Default Device Admin	0			
Identity Authorization > 2 deleterne										
+ 📳 Monitoring and Reports										
+ 🧏 System Administration										

cisco Cisco Secure At	CS academo SALE.40	SAT (Primary) Log Out About Pr							
» -∯ Ny Workspace	Access Prillies + Access Centrices + Cellarit Instruct Access + Authorization	(1)))))							
» (b) Network Resources	Standard Delicel Exception Delice								
× 🐉 Users and Identity Stores	Users and identity Stores Biotectic Access Authorization Endow								
G. Policy Elements	Filter Blatus • Natch ff Equais • Enabled • GenerFilter Go •								
Access Services T Bonics Selection Rates	Name NDG1.ocston NDGDexte Type Protocol Identity Group Eap Authentication Wethod	Authorization Profiles HE Count							
 Default Device Admin 	Rule-1 in All Locations:LAB in All Device Types Switches match Radius in All Groups LAP users -ANY-	Permit Access 1							
icenth Senerative - V dalatame									
 Monitoring and Reports 									
» 🖏 Dyalem Administration									
	4	л.							
	If no rules defined or no enabled rule matches.	Permit Access 0							
	Create - Dublicite - Edit Delate A Nove to Y	Customize Hit Gount							
	Saw Changes Discard Changes								

2. Monitoring and Reports(모니터링 및 보고서)를 클릭하면 새 팝업 창이 나타납니다. Authentications -RADIUS -Today를 클릭합니다. 어떤 서비스 선택 규칙이 적용되었는지 확인 하기 위해 Details를 클릭할 수도 있습니다.

								Launch Interact	live Yanwar 🗄
Showing Page	a 1 of 1			I Geto	Page: Go				
AAA Protocol > RAD	IUS Authenticati	on							
Authentication Status : Date :	Pass or Pail January 29, 2012 ()	Last 30 Minutes I	LastHouri Last 12 Hours (70	iday i <u>Yeaferdar</u> i <u>Last 7 Dav</u>	s (Last 30 Davs)				
Generated on January 2	29, 2012 9:15:01 FM	EST							
Reload	t + Click for details	9 -mouse ove	r item for additional informa	tian					
Logged At	RADUS NAS Status Falur	Details User	name MACIP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Ge
Jan 25.12 9 11 12 966	PM 👻	S 3502v	CC-EF-48-FA-53-19	Default Network Access	EAP-FAST (EAP-MSCHAP\2)	3560-Switch-LAP	192.168.153.10	GigabitEthemet0'11	

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- <u>Cisco Secure Access Control System</u>
- <u>기술 지원 및 문서 Cisco Systems</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.