

TACACS+를 사용하는 Cisco WLC의 디바이스 관리

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[1단계. 디바이스 관리 라이선스를 확인합니다.](#)

[2단계. ISE PSN 노드에서 디바이스 관리를 활성화합니다.](#)

[3단계. 네트워크 장치 그룹을 만듭니다.](#)

[4단계. WLC를 네트워크 디바이스로 추가합니다.](#)

[5단계. WLC에 대한 TACACS 프로파일을 생성합니다.](#)

[6단계. 정책 세트를 생성합니다.](#)

[7단계. 인증 및 권한 부여 정책을 생성합니다.](#)

[8단계. 디바이스 관리를 위한 WLC를 구성합니다.](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 ISE(Identity Service Engine)를 사용하여 Cisco WLC(Wireless LAN Controller)의 디바이스 관리를 위해 TACACS+를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE(Identity Service Engine)에 대한 기본 지식
- Cisco WLC(Wireless LAN Controller)에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Service Engine 2.4
- Cisco Wireless LAN Controller 8.5.135

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

구성

1단계. 디바이스 관리 라이선스를 확인합니다.

Administration(관리) > System(시스템) > Licensing(라이선싱) 탭으로 이동하고 이미지에 표시된 대로 Device Admin 라이선스가 설치되었는지 확인합니다.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services

Deployment > Licensing > Certificates > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings

Licensing Method

✔ Traditional Licensing is currently in use.

Click below to switch to Cisco Smart Licensing

Cisco Smart Licensing

License Usage How are licenses consumed?

Current Usage Usage Over Time

Base 0 Licensed : 100 (Consumed : 0)

Plus

Apex

Updated : Aug 20, 2019 09:30:00 UTC

Licenses How do I register, modify or lookup my licenses?

License File	Quantity	Term	Expiration Date
POSITRONFEAT20190820025931403.lic			
Base	100	Term	19-Aug-2020 (365 days remaining)
POSITRONFEAT20190820025911402.lic			
Device Admin	50	Term	19-Aug-2020 (365 days remaining)

참고: ISE에서 TACACS+ 기능을 사용하려면 디바이스 관리자 라이선스가 필요합니다.

2단계. ISE PSN 노드에서 디바이스 관리를 활성화합니다.

Work Centers(작업 센터) > Device Administration(디바이스 관리) > Overview(개요)로 이동하고 Deployment(구축) 탭, Select the Specific PSN Node(특정 PSN 노드 선택) 라디오 버튼을 클릭합니다. ISE 노드에서 확인란을 선택하고 이미지에 표시된 대로 저장을 클릭하여 디바이스 관리를 활성화합니다.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > Device Administration > PassiveID

Overview > Identities User Identity Groups Ext Id Sources > Network Resources > Policy Elements Device Admin Policy Sets Reports Settings

Introduction
TACACS Livelog
Deployment

Device Administration Deployment

Activate ISE Nodes for Device Administration

None
 All Policy Service Nodes
 Specific Nodes

ISE Nodes
 ISE-PSN.panlab.local

Only ISE Nodes with Policy Service are displayed.

TACACS Ports * 49 ⓘ

Save Reset

3단계. 네트워크 장치 그룹을 만듭니다.

ISE에서 WLC를 네트워크 디바이스로 추가하려면 다음 이미지에 표시된 대로 Administration(관리) > Network Resources(네트워크 리소스) > Network Device Groups(네트워크 디바이스 그룹) > All Device Types(모든 디바이스 유형)로 이동하여 WLC에 대한 새 그룹을 생성합니다.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management pxGrid Services > Feed Service > Threat Centric NAC

Network Devices > Network Device Groups > Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers Ex

Network Device Groups

All Groups > Choose group ▾

Refresh + Add Duplicate Edit Trash Show group members Import Export ▾ Flat Table Expand

Name	Description
<input type="checkbox"/> All Device Types	All Device Types
<input type="checkbox"/> All Locations	All Locations
<input type="checkbox"/> Is IPSEC Device	Is this a RADIUS over IPSEC Device

Add Group

Name *

WLC

Description

Parent Group *

All Device Types

Cancel

Save

4단계. WLC를 네트워크 디바이스로 추가합니다.

Work Centers(작업 센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다. Add(추가)를 클릭하고 Name, IP Address(이름, IP 주소)를 제공하고 Device type as WLC(디바이스 유형)를 선택하고 TACACS+ Authentication Settings(TACACS+ 인증 설정) 확인란을 선택한 후 이미지에 표시된 대로 Shared Secret(공유 암호) 키를 제공합니다.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management pxGrid Services

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences

Network Devices

Default Device

Device Security Settings

Network Devices List > New Network Device

Network Devices

* Name FloorWLC

Description

IP Address * IP : 10.106.37.180 / 32

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Location All Locations Set To Default

IPSEC Is IPSEC Device Set To Default

Device Type WLC Set To Default

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret Show

Enable Single Connect Mode

Legacy Cisco Device
 TACACS Draft Compliance Single Connect Support

SNMP Settings

5단계. WLC에 대한 TACACS 프로파일을 생성합니다.

Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Profiles(TACACS 프로파일)로 이동합니다. Add(추가)를 클릭하고 Name(이름)을 입력합니다. 작업 속성 보기 탭에서 공통 작업 유형에 대해 WLC를 선택합니다. 기본 프로파일이 있으며 이 프로파일에서 이미지에 표시된 대로 사용자에 대한 제한적 액세스를 허용하도록 모니터를 선택합니다.

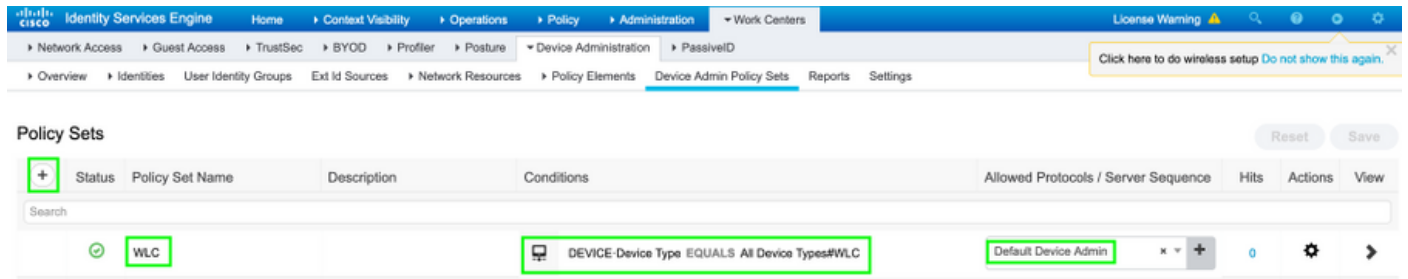
The screenshot shows the Cisco ISE configuration interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The page title is 'TACACS Profiles > WLC MONITOR'. The 'TACACS Profile' section shows 'Name: WLC MONITOR' and 'Description: WLC MONITOR'. Below this, there are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under 'Common Tasks', the 'Common Task Type' is set to 'WLC'. The task type options are: All, Monitor (selected), Lobby, and Selected. There are also checkboxes for WLAN, Controller, Wireless, Security, Management, and Commands. A note states: 'The configured options give a mgmtRole Debug value of: 0x0'. The 'Custom Attributes' section is empty.

이미지에 표시된 대로 사용자에게 대한 전체 액세스를 허용하는 또 다른 기본 프로파일 **All**이 있습니다.

The screenshot shows the Cisco ISE configuration interface for a different TACACS profile. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The page title is 'TACACS Profiles > WLC ALL'. The 'TACACS Profile' section shows 'Name: WLC ALL' and 'Description: WLC ALL'. Below this, there are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under 'Common Tasks', the 'Common Task Type' is set to 'WLC'. The task type options are: All (selected), Monitor, Lobby, and Selected. There are also checkboxes for WLAN, Controller, Wireless, Security, Management, and Commands. A note states: 'The configured options give a mgmtRole Debug value of: 0xffffffff'. The 'Custom Attributes' section is empty.

6단계. 정책 세트를 생성합니다.

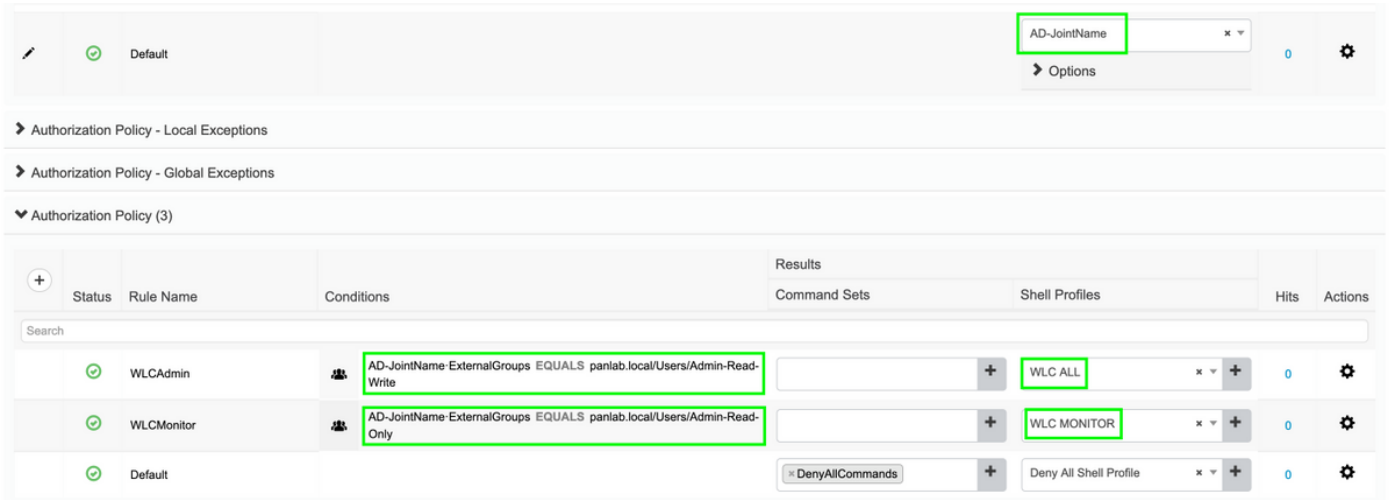
Work centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 세트)로 이동합니다. (+)를 클릭하고 정책 세트에 이름을 지정합니다. 정책 조건에서 Device Type(디바이스 유형)을 WLC로 선택합니다. 허용되는 프로토콜은 이미지에 표시된 대로 Default Device Admin(기본 디바이스 관리자)이 될 수 있습니다.



7단계. 인증 및 권한 부여 정책을 생성합니다.

이 문서에서 두 개의 샘플 그룹 Admin-Read-Write 및 Admin-Read-Only가 각각 Active Directory에 구성되고 각 그룹 admin1에 속한 한 사용자가 admin2로 구성됩니다. Active Directory는 AD-JointName이라는 연결점을 통해 ISE와 통합됩니다.

이미지에 표시된 대로 두 개의 권한 부여 정책을 생성합니다.



8단계. 디바이스 관리를 위한 WLC를 구성합니다.

Security(보안) > AAA > TACACS로 이동하고 New(새로 만들기)를 클릭하고 이미지에 표시된 대로 Authentication, Accounting server(인증, 어카운팅 서버)를 추가합니다.

CISCO MONITOR WLANS CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMM

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - Authentication**
 - Accounting
 - Authorization
 - Fallback
 - DNS

TACACS+ Authentication Servers > New

Server Index (Priority) 1

Server IP Address(Ipv4/Ipv6) 10.106.37.180

Shared Secret Format ASCII

Shared Secret

Confirm Shared Secret

Port Number 49

Server Status Enabled

Server Timeout 5 seconds

CISCO MONITOR WLANS CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - Authentication
 - Accounting**
 - Authorization
 - Fallback
 - DNS

TACACS+ Accounting Servers > New

Server Index (Priority) 1

Server IP Address(Ipv4/Ipv6) 10.106.37.180

Shared Secret Format ASCII

Shared Secret

Confirm Shared Secret

Port Number 49

Server Status Enabled

Server Timeout 5 seconds

이미지에 표시된 대로 우선 순위 순서를 변경하고 TACACS+를 위쪽에서 아래쪽으로 설정하고 Local을 아래쪽으로 설정합니다.

CISCO MONITOR WLANS CONTROLLER WIRELESS **SECURITY** MANAGEMENT CO

Security

- AAA
- Local EAP
- Advanced EAP
- Priority Order**
 - Management User**
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth

Priority Order > Management User

Authentication

Not Used

RADIUS > <

Order Used for Authentication

TACACS+ LOCAL Up Down

If LOCAL is selected as second priority then user will be authenticated against LOCAL only if first priority is unreachable.

주의:현재 WLC GUI 세션을 닫지 마십시오.다른 웹 브라우저에서 WLC GUI를 열고 TACACS+ 자격 증명으로 로그인하는지 여부를 확인하는 것이 좋습니다.그렇지 않은 경우 TCP 포트 49에서 ISE 노드에 대한 컨피그레이션 및 연결을 확인합니다.

다음을 확인합니다.

Operations(작업) > TACACS > Live logs(라이브 로그)로 이동하고 라이브 로그를 모니터링합니다. 이미지에 표시된 대로 WLC GUI를 열고 Active Directory 사용자 자격 증명으로 로그인합니다.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Network Device ...
Oct 03, 2019 03:15:55.969 PM	✓		admin2	Authorization		WLC >> WLCAdmin	FloorWLC
Oct 03, 2019 03:15:55.938 PM	✓		admin2	Authentication	WLC >> Default		FloorWLC
Oct 03, 2019 03:15:39.298 PM	✓		admin1	Authorization		WLC >> WLCMonitor	FloorWLC
Oct 03, 2019 03:15:39.268 PM	✓		admin1	Authentication	WLC >> Default		FloorWLC

Last Updated: Thu Oct 03 2019 15:16:26 GMT+0530 (India Standard Time)

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.