Catalyst 9800 WLC 및 ISE 서버에서 SGACL 구성 및 확인

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[구성](#)

- [네트워크 다이어그램](#)
- [설정](#)
  - [WLC 컨피그레이션](#)
  - [ISE 구성](#)
  - [Flexconnect](#)

[다음을 확인합니다.](#)

- [FlexConnect 로컬 스위칭](#)

[문제 해결](#)

소개

이 문서에서는 로컬 및 FlexConnect 모드 AP에서 SGACL 기능을 활용하도록 Catalyst 9800 및 ISE 서버에서 TrustSec을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco 9800 WLC, Cisco ISE, FlexConnect 및 TrustSec 기본 사항에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- C9800-CL v17.12.4
- ISE 3.2.0
- 9136I Access Point

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

구성

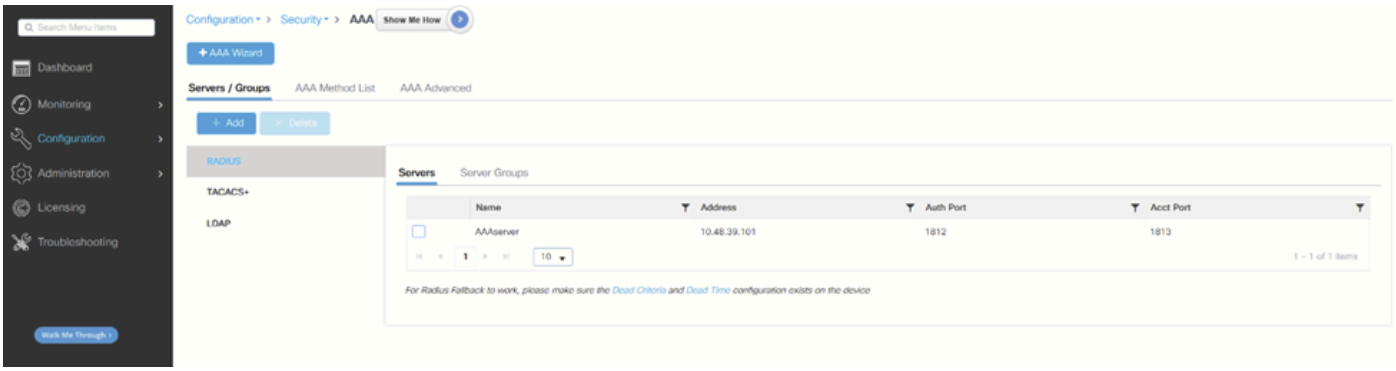
네트워크 다이어그램

네트워크 다이어그램

설정

WLC 컨피그레이션

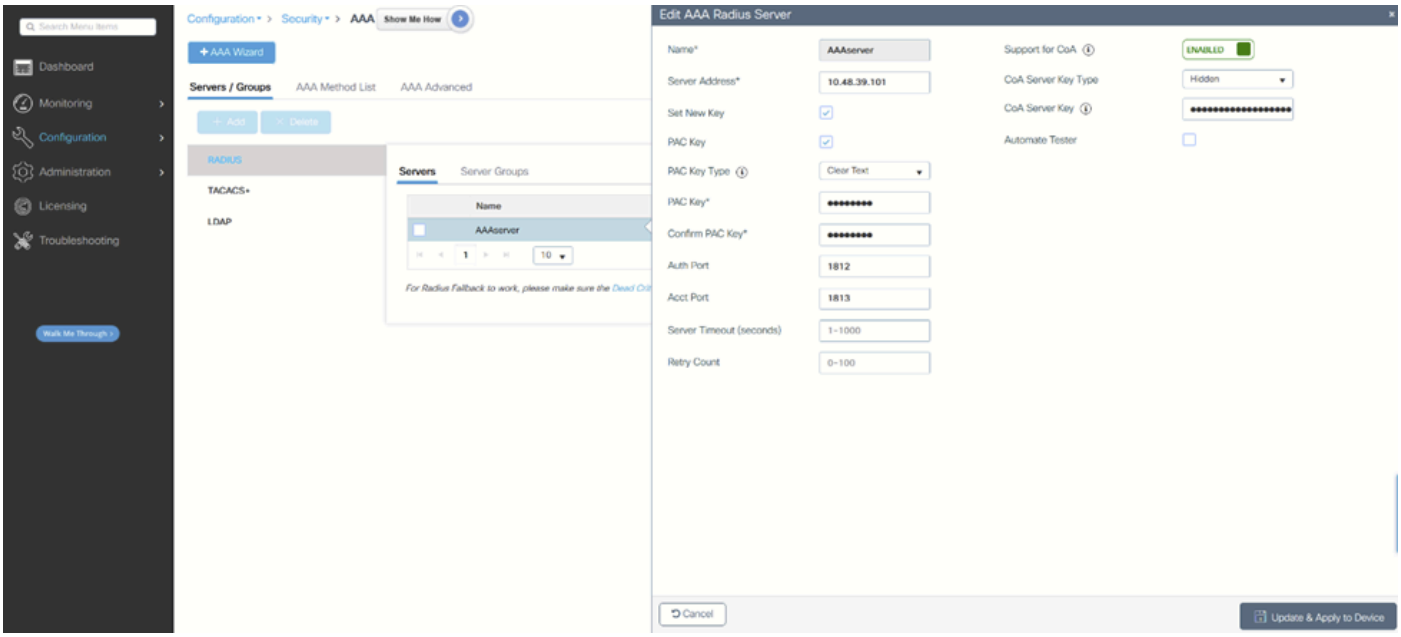
1. Configuration(컨피그레이션) > Security(보안) > AAA(AAA)에서 AAA 서버를 WLC에 추가합니다.



WLC AAA 페이지

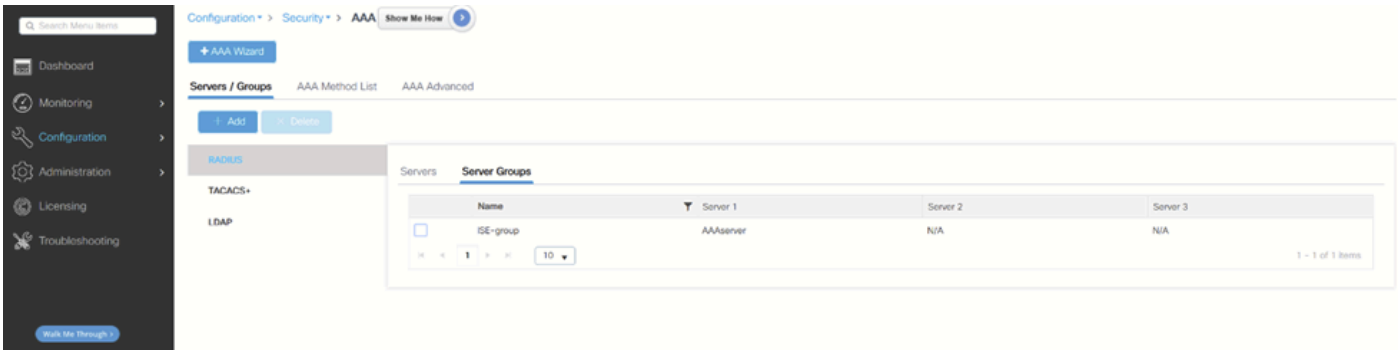
2. ISE에 디바이스를 추가할 때 여기에 있는 키 항목이 키와 일치하는지 확인합니다. CoA에 대한 지

원을 활성화하고 CoA를 사용하여 컨피그레이션 업데이트를 다운로드하려면 키를 추가합니다.



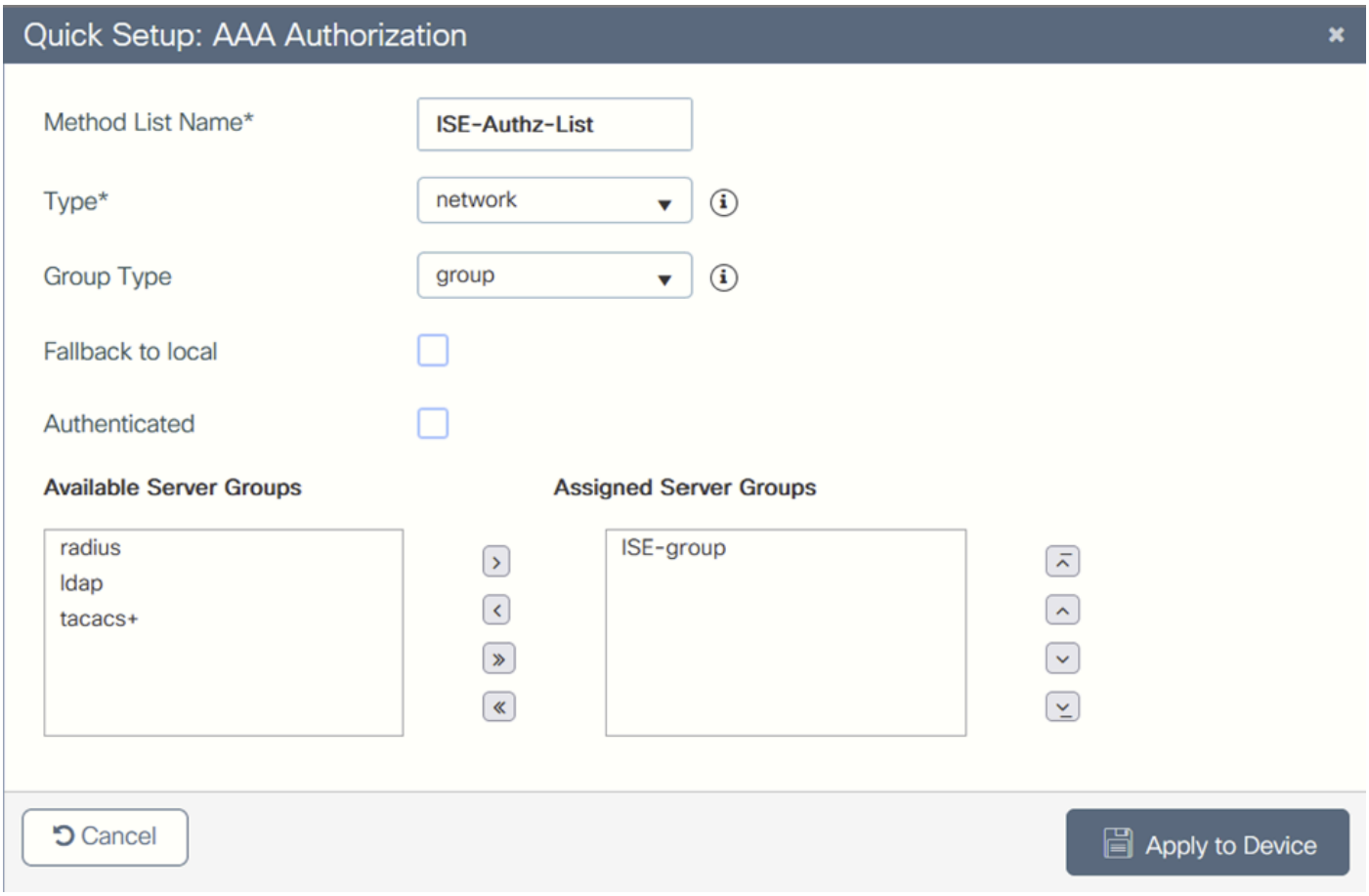
WLC 추가 AAA 서버

3. 서버 그룹을 생성합니다.

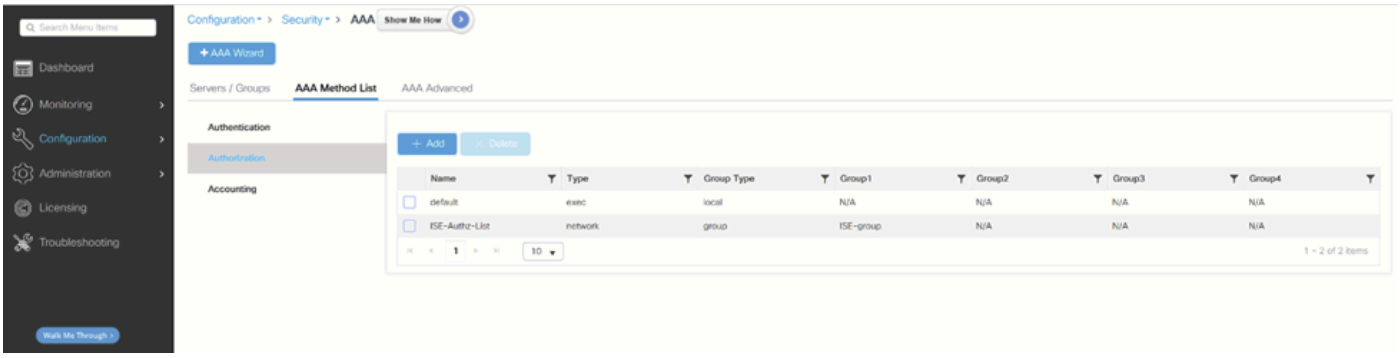


WLC 서버 그룹 추가

4. 네트워크 유형 인증 방법 목록을 추가합니다.



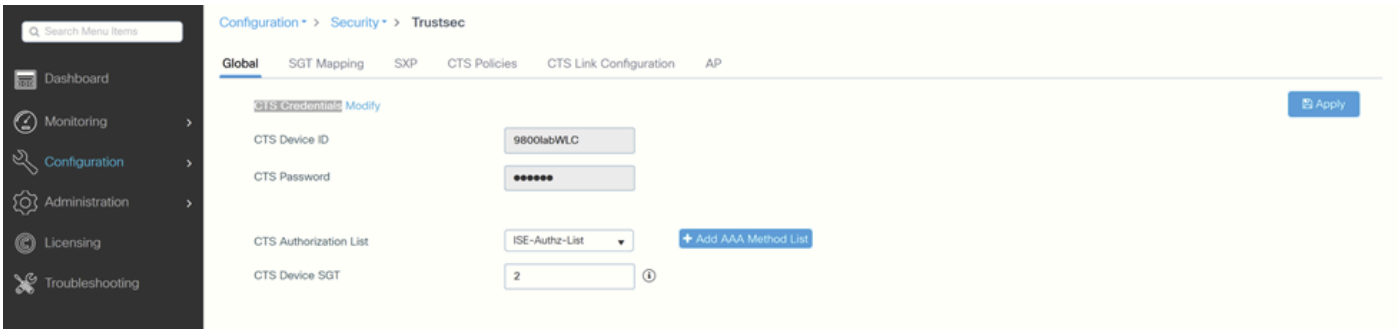
인증 방법 목록



WLC AAA 서버 그룹

5. Configuration(컨피그레이션) > Security(보안) > Trustsec으로 이동하여 CTS Device ID(CTS 디바이스 ID) 및 CTS Password(CTS 비밀번호)를 구성합니다. ISE에서 디바이스를 추가할 때 이 항목을 사용합니다.

4단계에서 생성한 CTS Authorization List(CTS 권한 부여 목록)도 구성합니다.

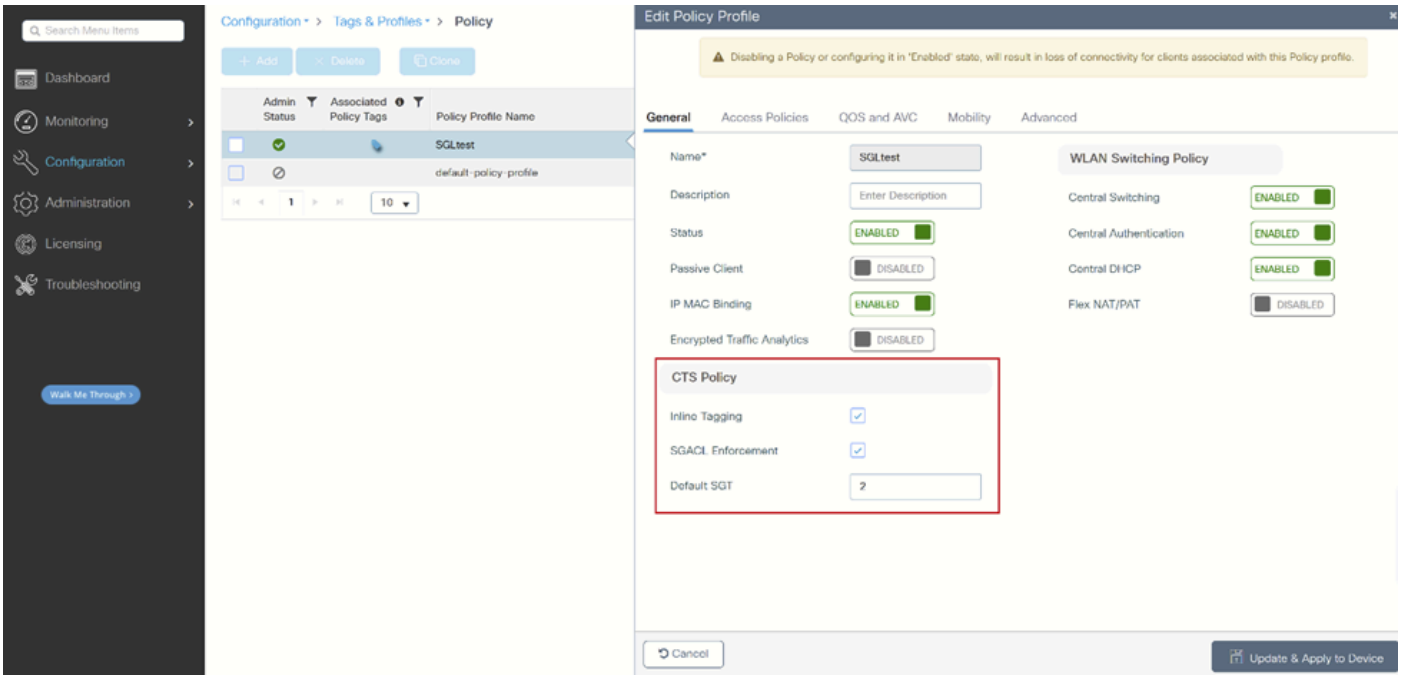


WLC 트러스트섹(TrustSec)

6. 이 예에서는 WLAN이 이미 생성되어 있고 인증 설정이 이미 구성되어 있습니다.

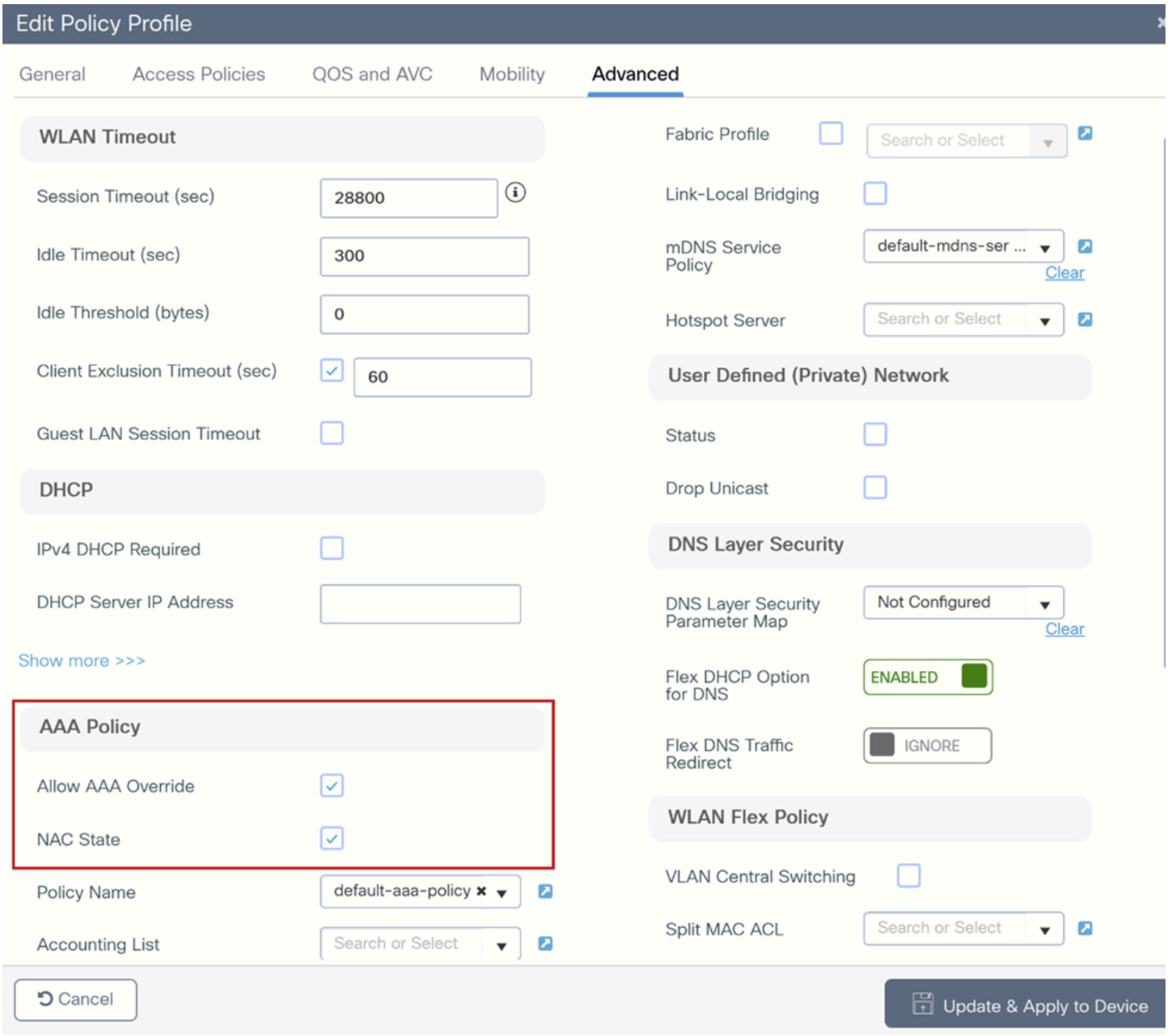
이제 SGT를 사용할 정책 프로필로 이동합니다.

i. CTS Policy(CTS 정책)에서 Inline Tagging(인라인 태깅) 및 SGACL Enforcement(SGACL 시행)를 활성화하면 Default SGT(기본 SGT)도 지정할 수 있습니다. 이 실습에서는 기본 SGT 2를 예로 들 수 있습니다.



WLC 정책 프로필

나. Advanced(고급) 탭에서 Allow AAA override and NAC state(AAA 재정의 및 NAC 상태 허용)를 활성화합니다.



WLC Policy Profile(WLC 정책 프로필) Advanced(고급) 탭

CLI에서:

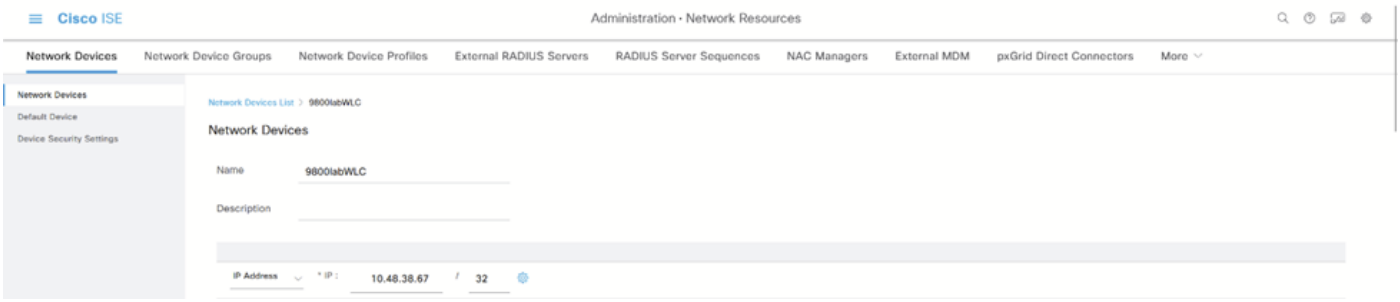
```
# configure terminal

(config)# radius server <server_name>
(config-radius-server)# address ipv4 <server_IP>
(config-radius-server)# pac key <password>

(config)# aaa server radius dynamic-author
(config-locsvr-da-radius)# client <server_IP> server-key <password>

(config)# aaa group server radius <server_group_name>
(config-sg-radius)# server name <server_name>
(config-sg-radius)# ip radius source-interface Vlan#

(config)# aaa authorization network <author_method_list> group <server_group_name>

(config)# cts authorization list <author_method_list>
```

```
(config)# wireless profile policy <policy_profile_name>
(config-wireless-policy)# shut
(config-wireless-policy)# aaa-override
(config-wireless-policy)# cts inline-tagging
(config-wireless-policy)# cts role-based enforcement
(config-wireless-policy)# cts sgt <number>
(config-wireless-policy)# no shut

# show cts credentials
CTS password is defined in keystore, device-id = 9800labWLC
```

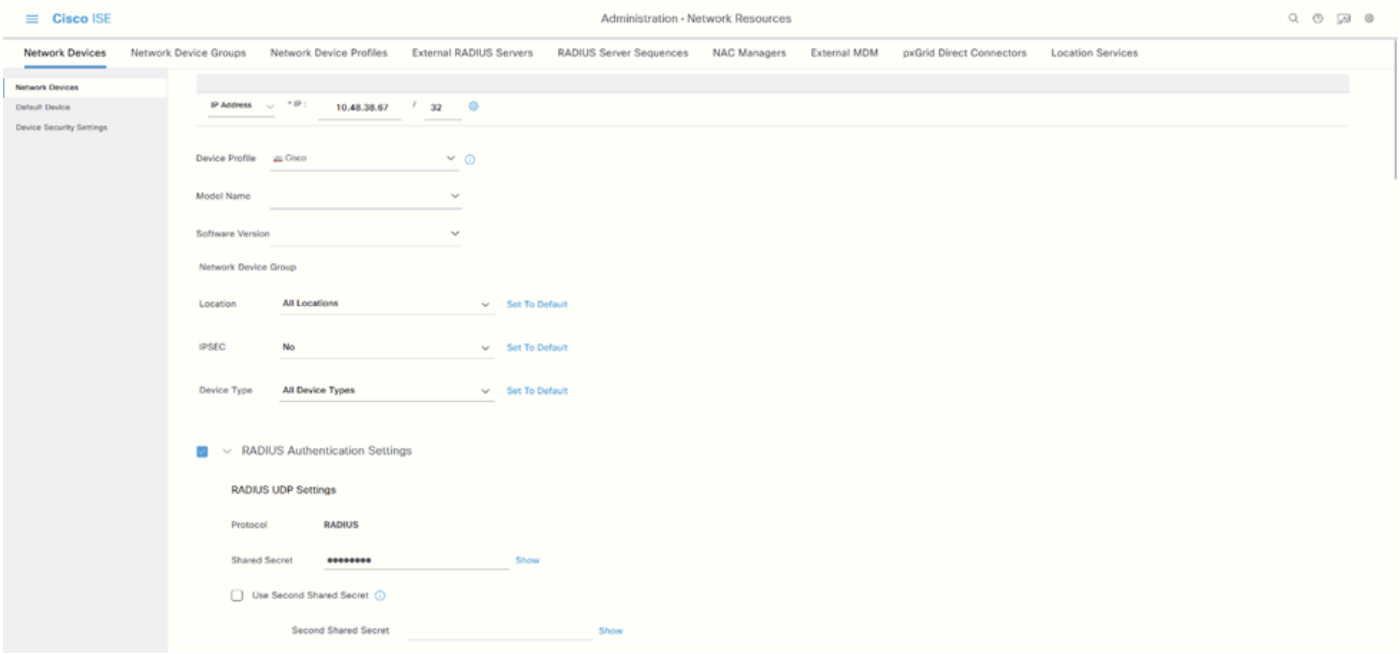
ISE 구성

1. 관리 > 네트워크 리소스 > 네트워크 장치로 이동합니다.

i. 여기에 WLC 정보를 추가합니다.

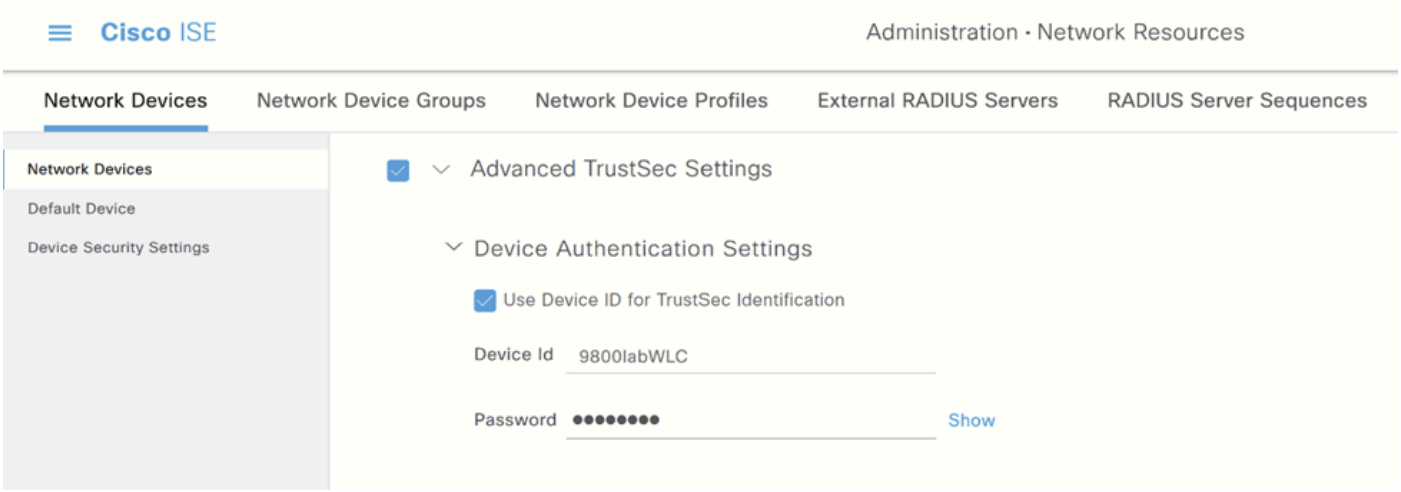


ISE 네트워크 디바이스 페이지



ISE에서 WLC RADIUS 정보 추가

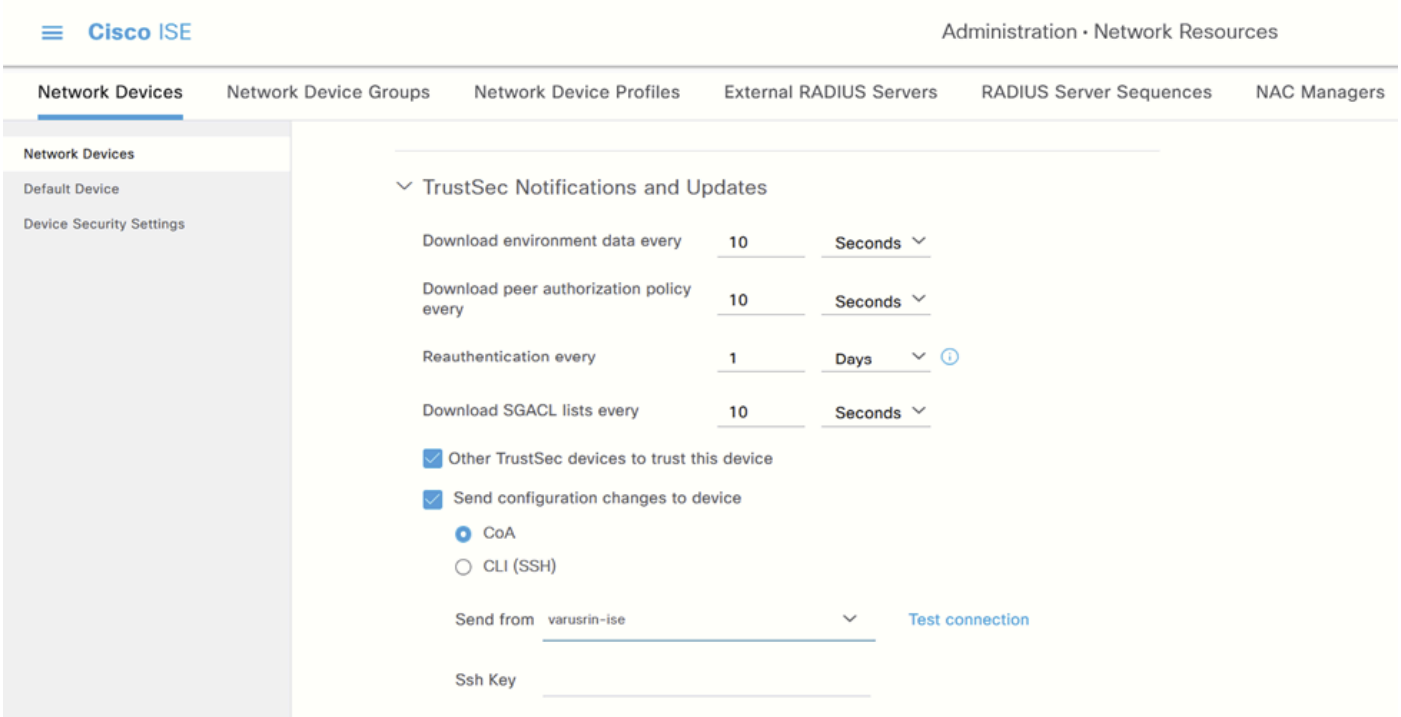
나. 아래로 스크롤하여 Advanced TrustSec Settings(고급 TrustSec 설정)를 구성하고, Use Device ID for TrustSec Identification(TrustSec 식별에 디바이스 ID 사용) 확인란을 활성화하고 비밀번호를 구성합니다.



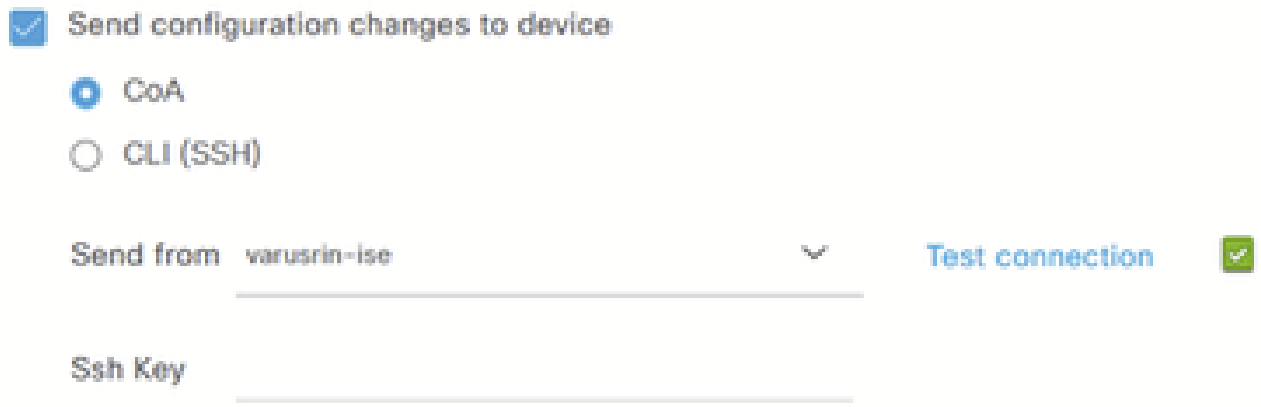
고급 TrustSec 설정

이는 WLC 컨피그레이션의 6단계에서 WLC 측의 컨피그레이션과 일치해야 합니다.

iii. 아래로 스크롤하여 TrustSec Notifications and Updates(TrustSec 알림 및 업데이트)로 이동하고 컨피그레이션 업데이트에 CoA를 사용할지 SSH를 사용할지를 구성합니다. 필요한 ISE 노드를 선택합니다.

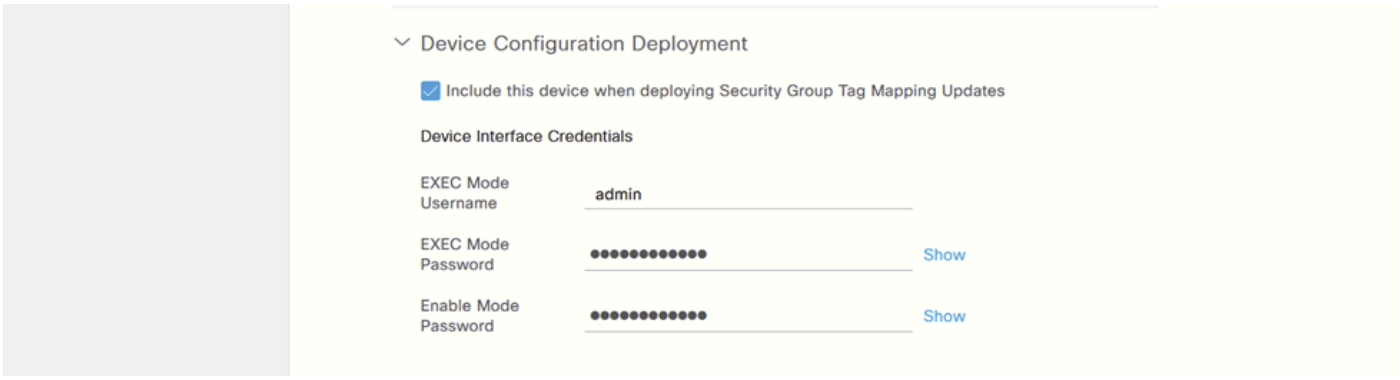


2. 연결 테스트를 눌러 연결이 설정되었는지 확인합니다. 성공하면 다음과 같은 녹색 틱 표시가 나타납니다.



연결 테스트

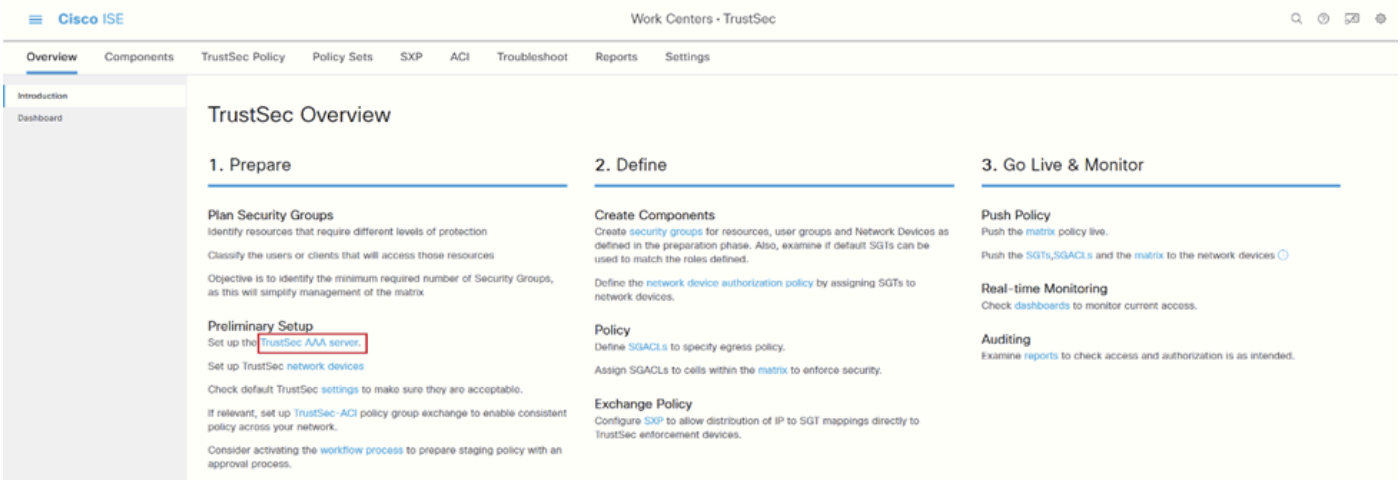
i. SGT 매핑 업데이트를 구축할 때 포함할 WLC를 아래로 스크롤하고 구성합니다. 이는 이전 단계에서 SSH 옵션을 선택한 경우 중요합니다.



디바이스 컨피그레이션 구축

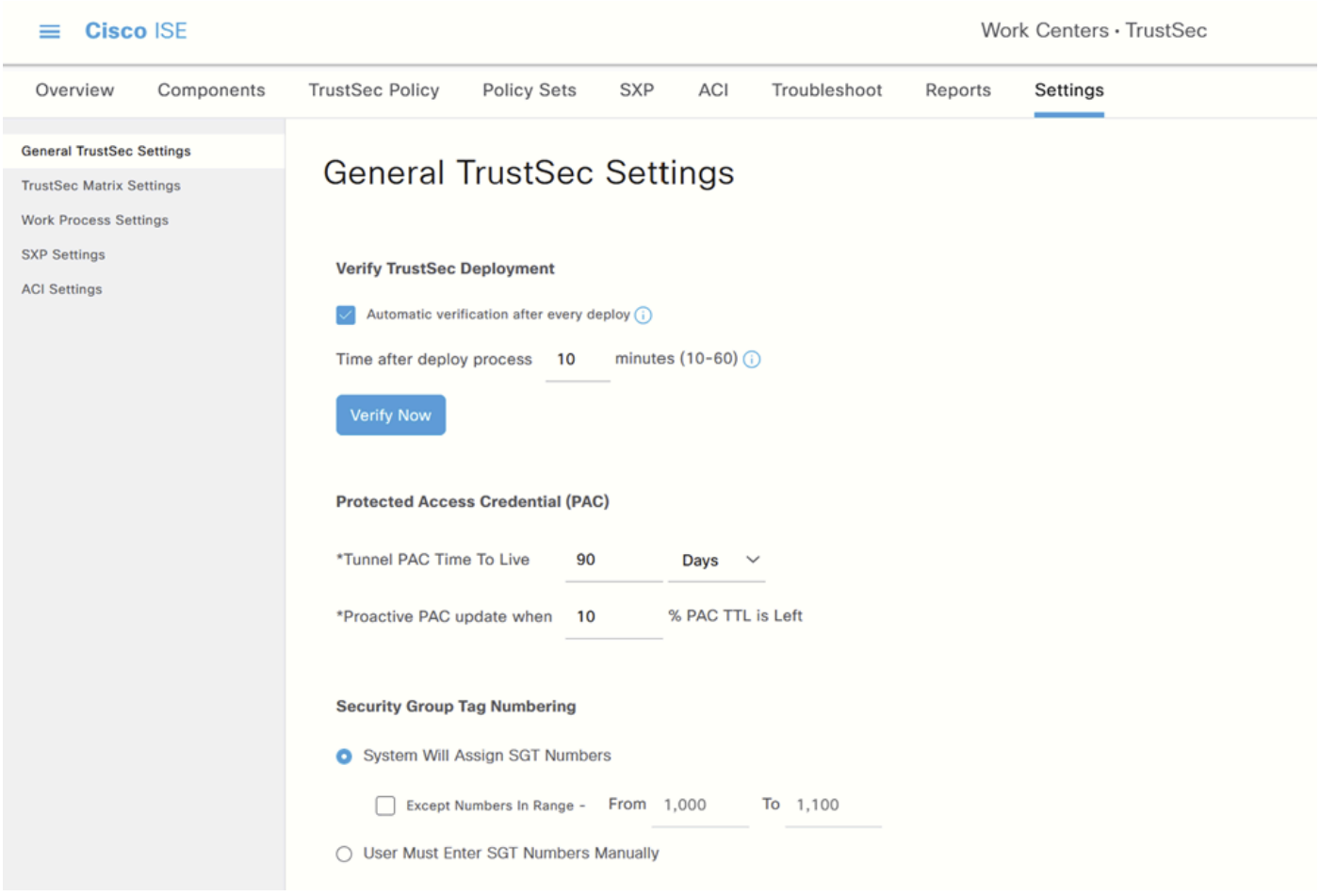
나. 설정 저장.

3. Work Centers(작업 센터) > TrustSec > Overview(개요)에서 TrustSec 구성 옵션을 사용할 수 있습니다. 사용 중인 ISE 인스턴스를 보려면 TrustSec AAA Server를 선택합니다. 여러 개의 인스턴스가 있는 경우 어떤 인스턴스가 사용되는지에 대한 자세한 내용은 Cisco Catalyst Wireless Group Based Policy(Cisco Catalyst 무선 그룹 기반 정책)를 참조하십시오.



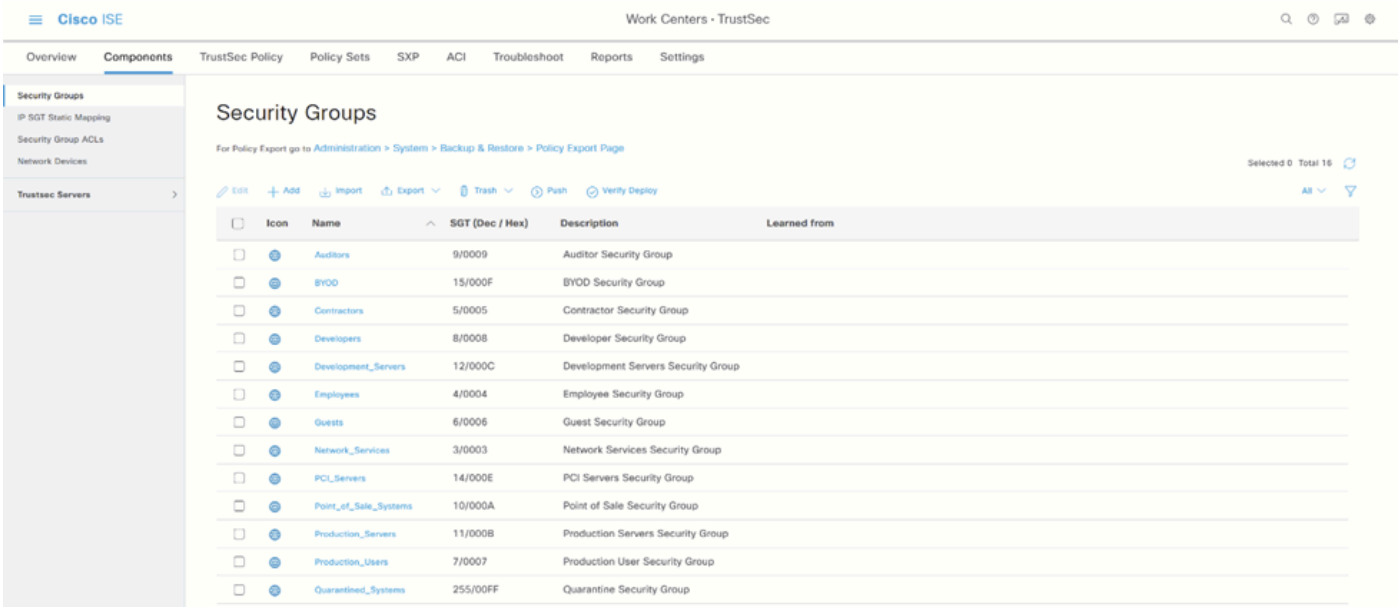
ISE TrustSec 개요

4. (선택 사항) Settings(설정) 탭으로 이동하여 원하는 경우 모든 구축 후 Automatic verification(자동 확인)을 활성화합니다.



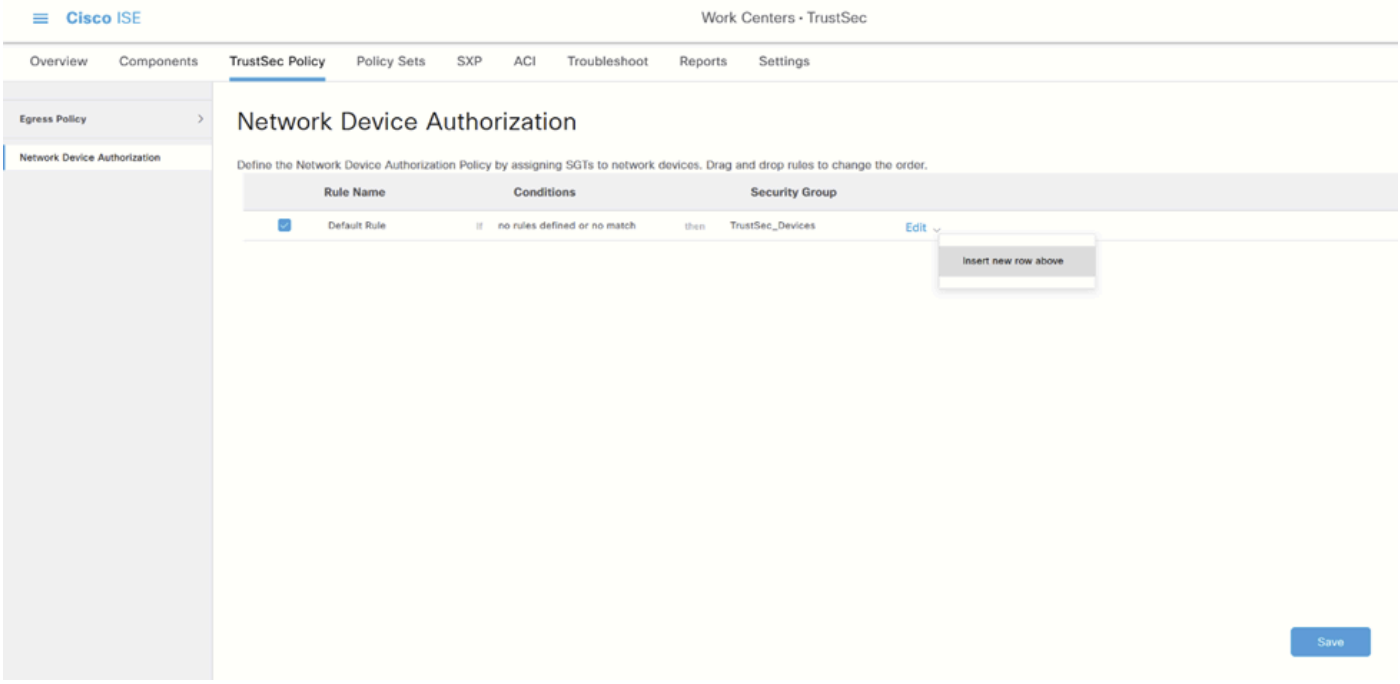
ISE TrustSec 설정

5. 요구 사항에 따라 Work Centers(작업 센터) > TrustSec > Components(구성 요소) > Security Groups(보안 그룹)에서 SGT 값을 추가하거나 편집합니다.



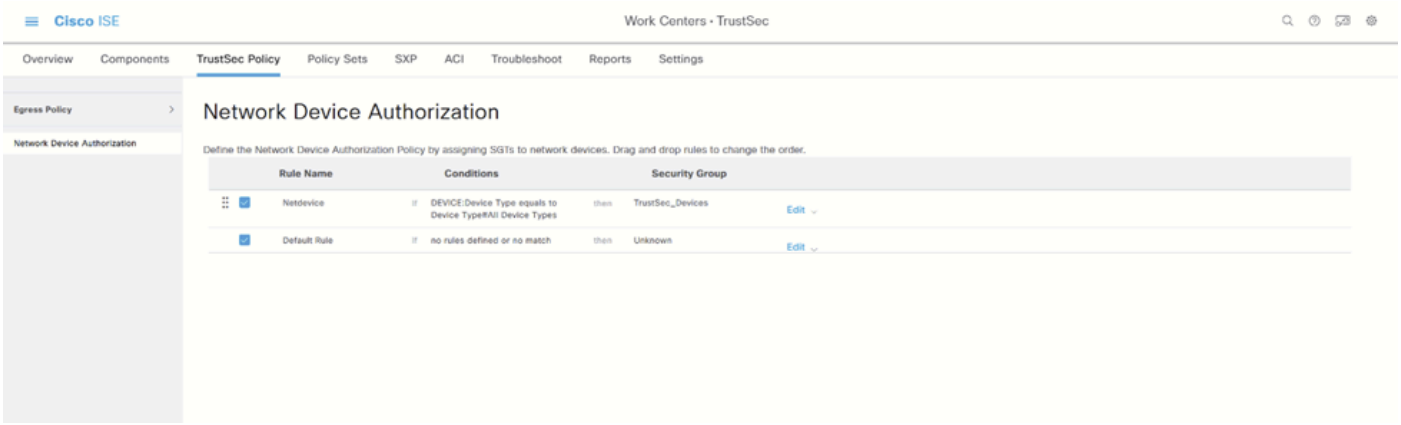
ISE 보안 그룹

6. 권한 부여 정책을 지정하려면 Work Centers(작업 센터) > TrustSec > TrustSec Policy(TrustSec 정책) > Network Device Authorization(네트워크 디바이스 권한 부여)으로 이동합니다.



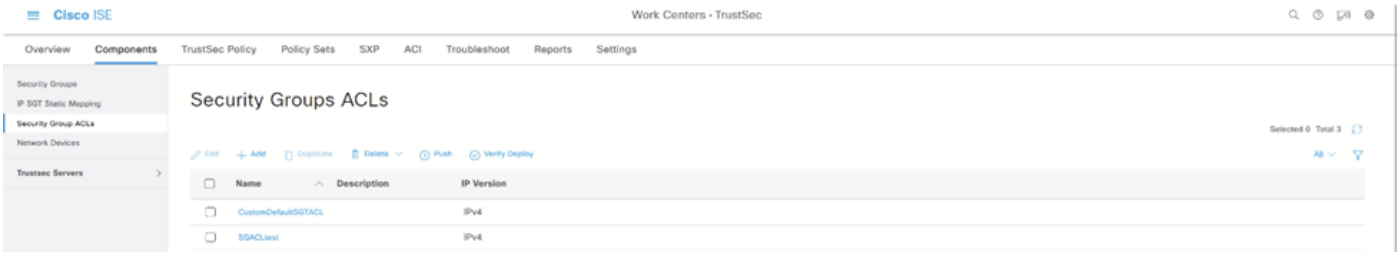
TrustSec 정책

기본값을 유지할 수 있지만 이 실습에서는 이 컨피그레이션을 예로 사용합니다.



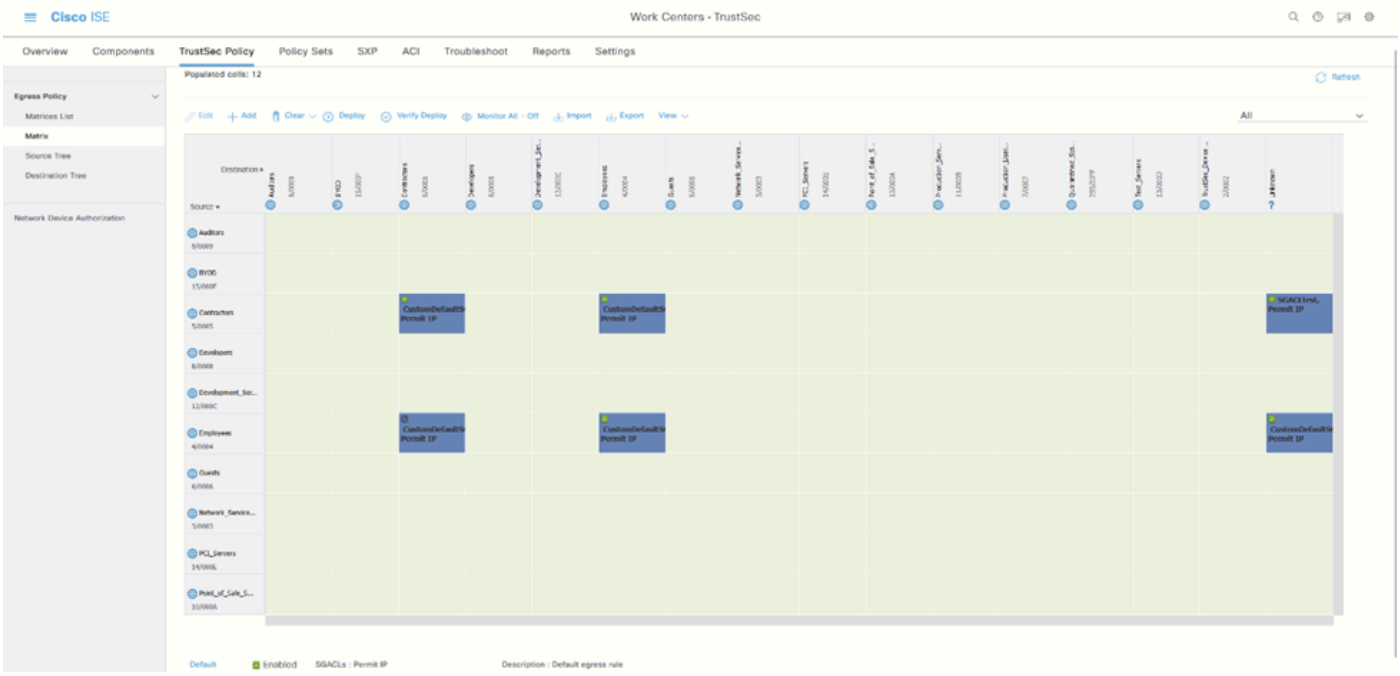
네트워크 디바이스 권한 부여

7. 구성 요소 탭에서 SGACL을 생성한 다음 보안 그룹 ACL을 생성합니다.



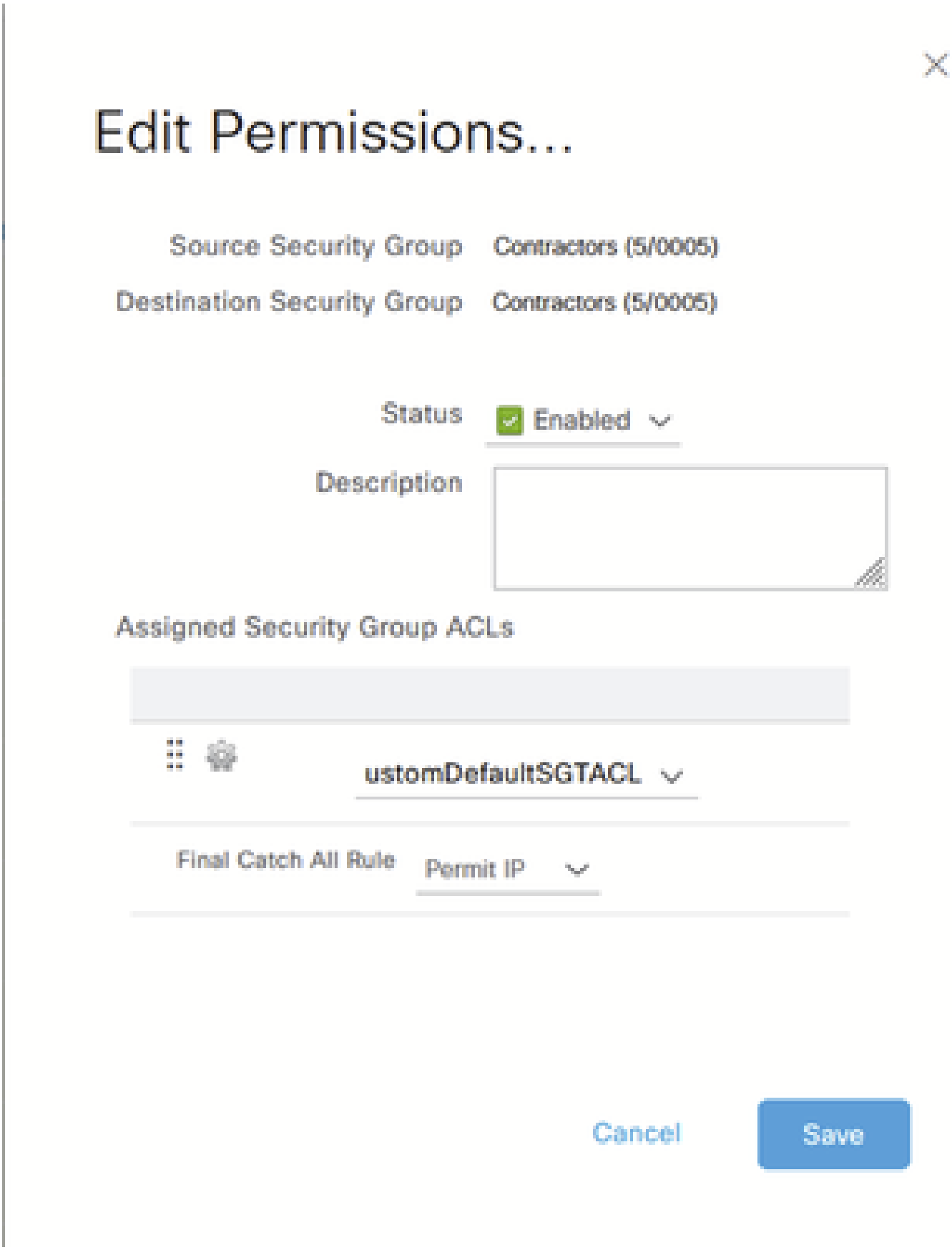
보안 그룹 ACL

8. TrustSec Policy(TrustSec 정책) 탭에서 Matrix(매트릭스) 항목을 지정하고 Matrix(매트릭스)를 지정합니다. 두 SGT가 만나는 지점을 클릭하여 Permissions(권한)를 수정할 수 있습니다.

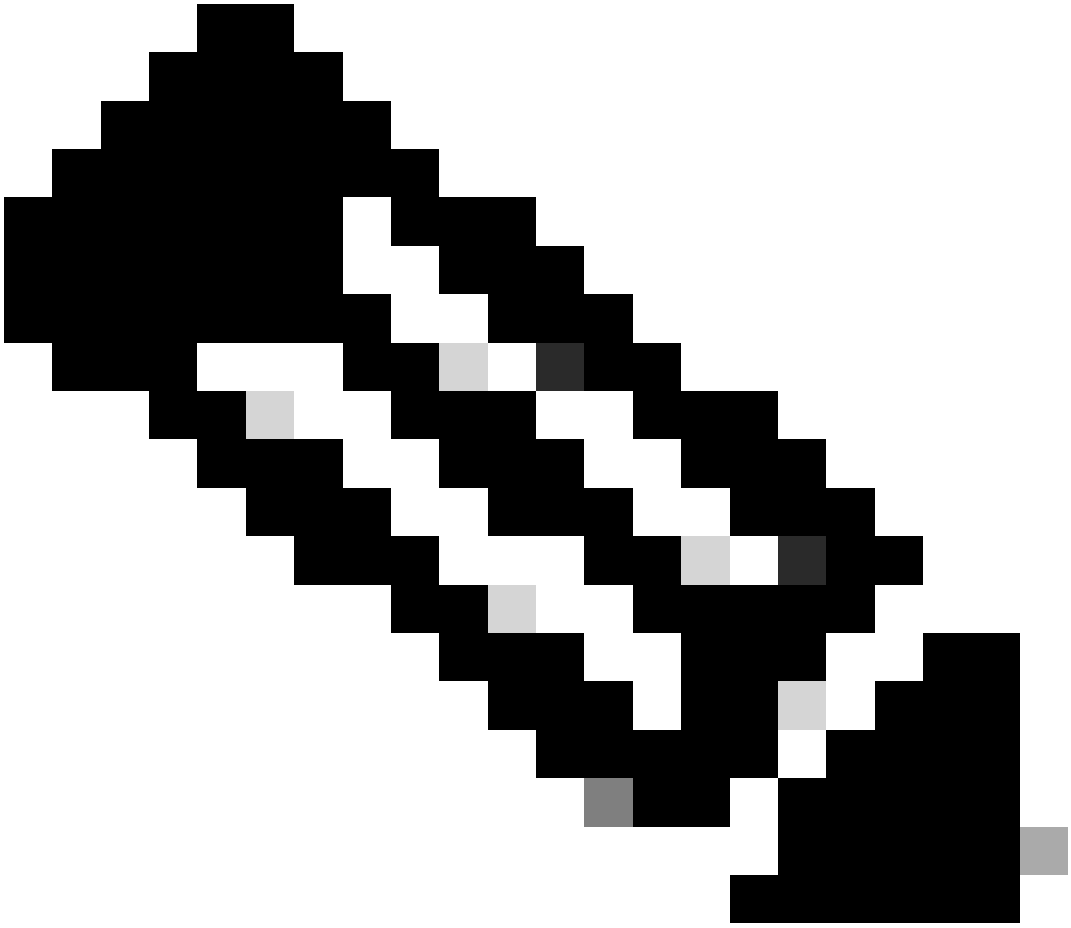


ISE TrustSec 매트릭스

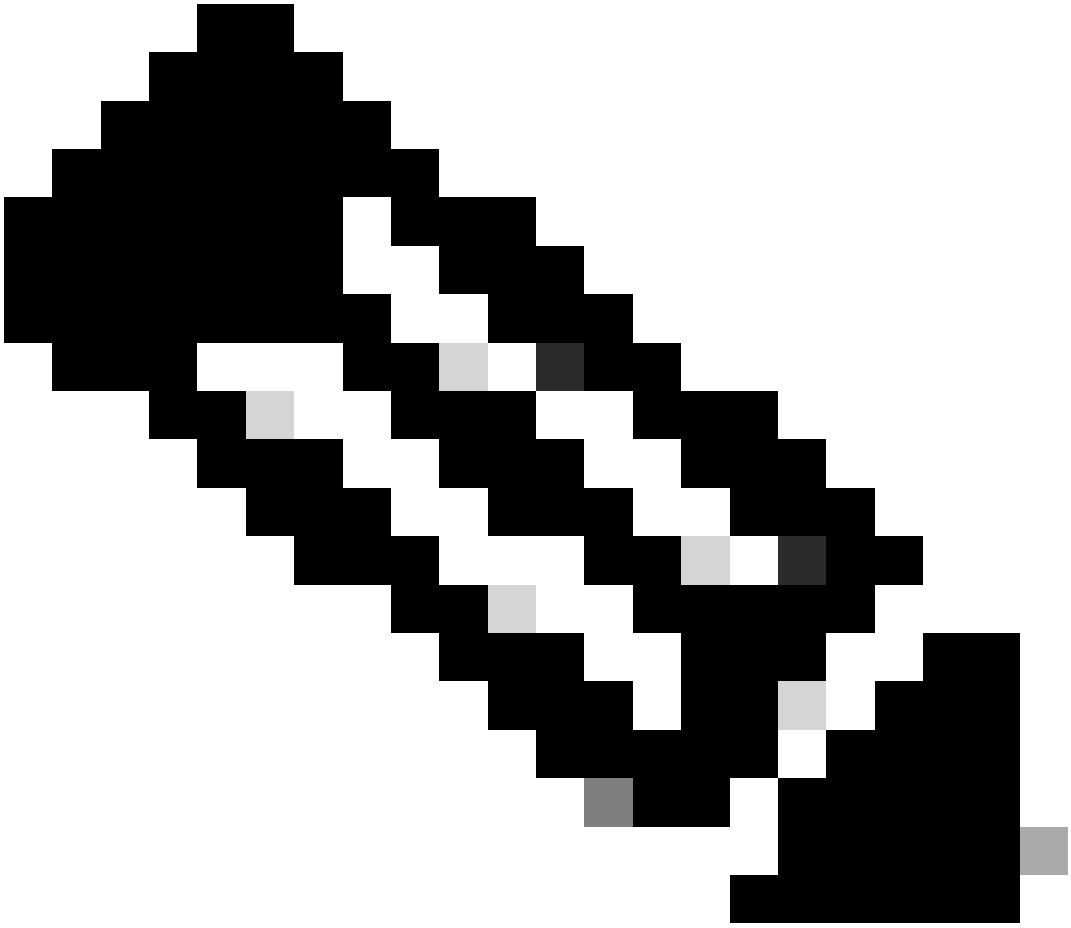
예를 들면 다음과 같습니다.


Edit Permissions...
Source Security Group
Contractors (5/0005)
Destination Security Group
Contractors (5/0005)
Status
Enabled
Description
Assigned Security Group ACLs
ustomDefaultSGTACL
Final Catch All Rule
Permit IP
Cancel
Save

권한 편집

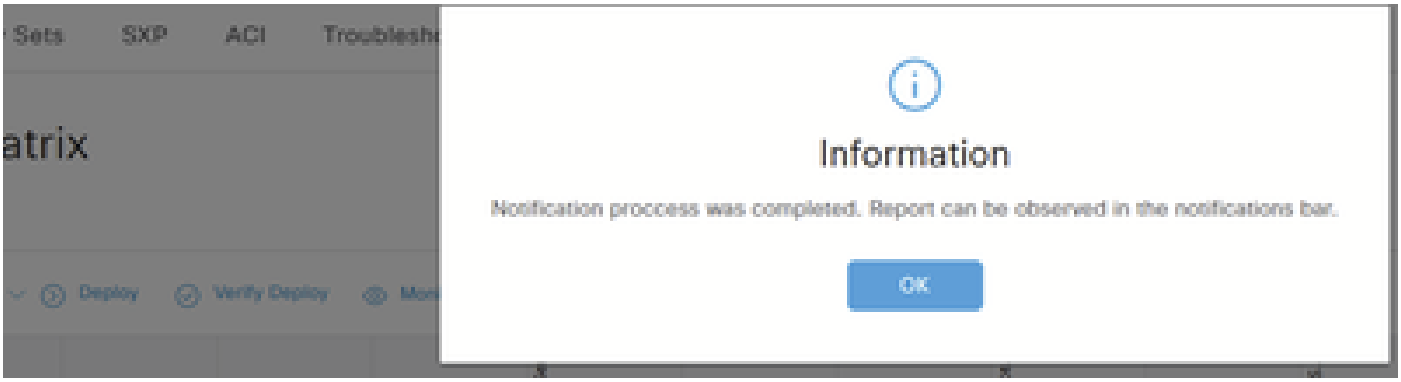


참고: 허용 목록 모델의 경우 클라이언트 디바이스에서 DHCP IP 주소를 가져오도록 DHCP 프로토콜을 명시적으로 허용한 다음 컨트롤러에 SGACL 정책을 요청해야 합니다.

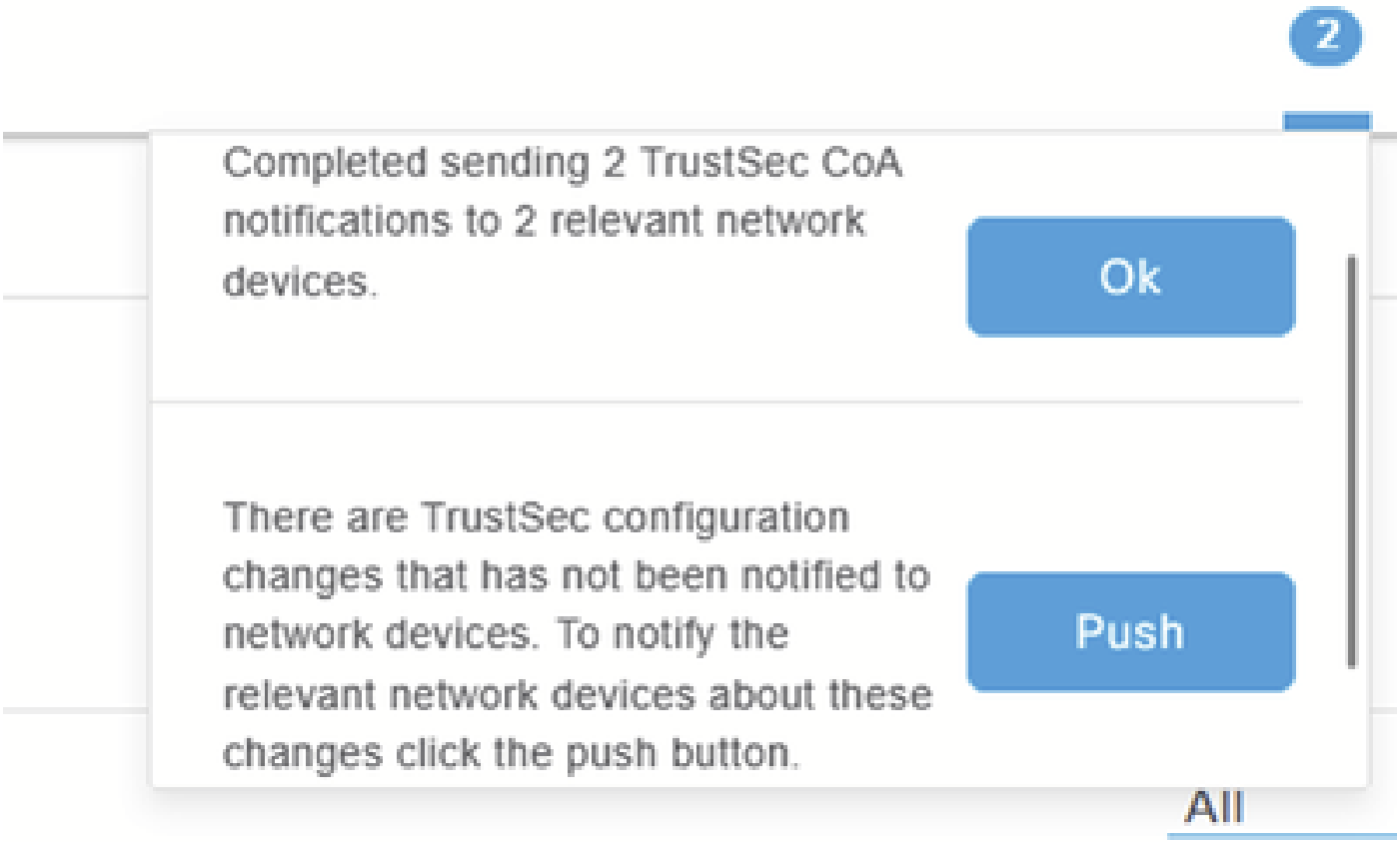


참고: TrustSec 매트릭스에서 TrustSec 정책 "unknown to unknown(알 수 없음 - 알 수 없음)"이 거부된 경우 클라이언트에는 SGT 값이 0으로 표시되고 DHCP 클라이언트에는 APIPA(Automatic Private IP Addressing) 주소가 표시됩니다.
TrustSec 매트릭스에서 TrustSec 정책 "unknown to unknown(알 수 없음 - 알 수 없음)"이 허용되면 클라이언트는 올바른 SGT 값을 받고 DHCP 클라이언트는 IP 주소를 받습니다.

9. 구축을 클릭합니다. 그러면 다음과 같은 메시지와 알림이 생성됩니다.



구축

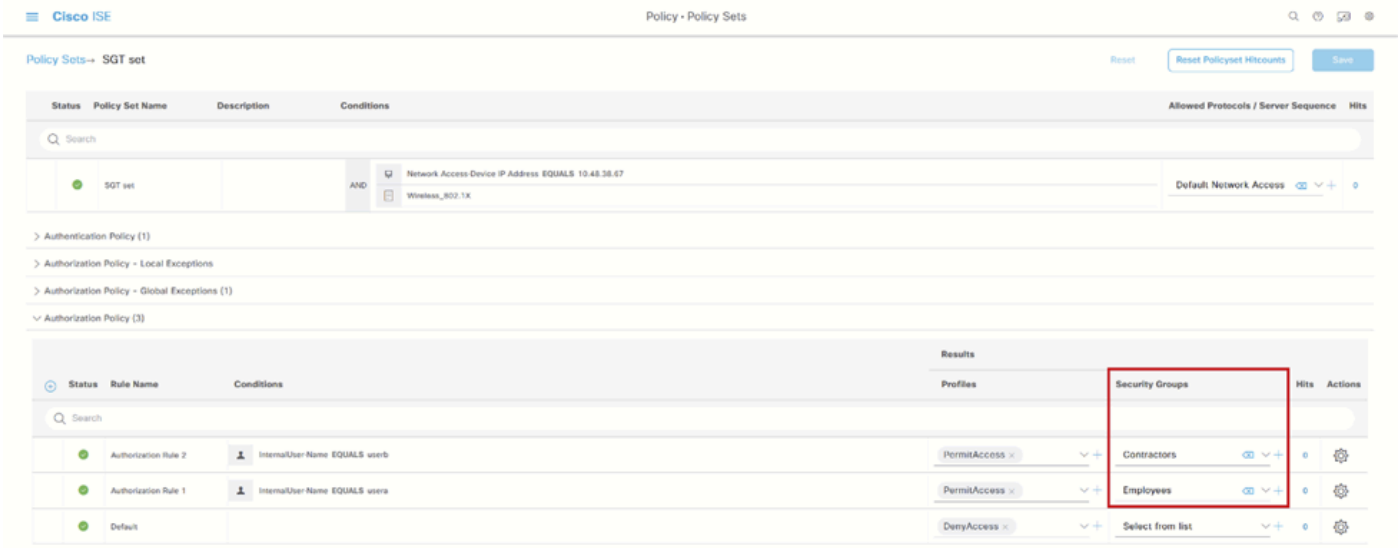


알림 배포

10. Policy(정책) > Policy Sets(정책 세트) 아래에서 WLAN에 사용되는 Policy Set(정책 세트)로 이동합니다.

ISE 정책 집합

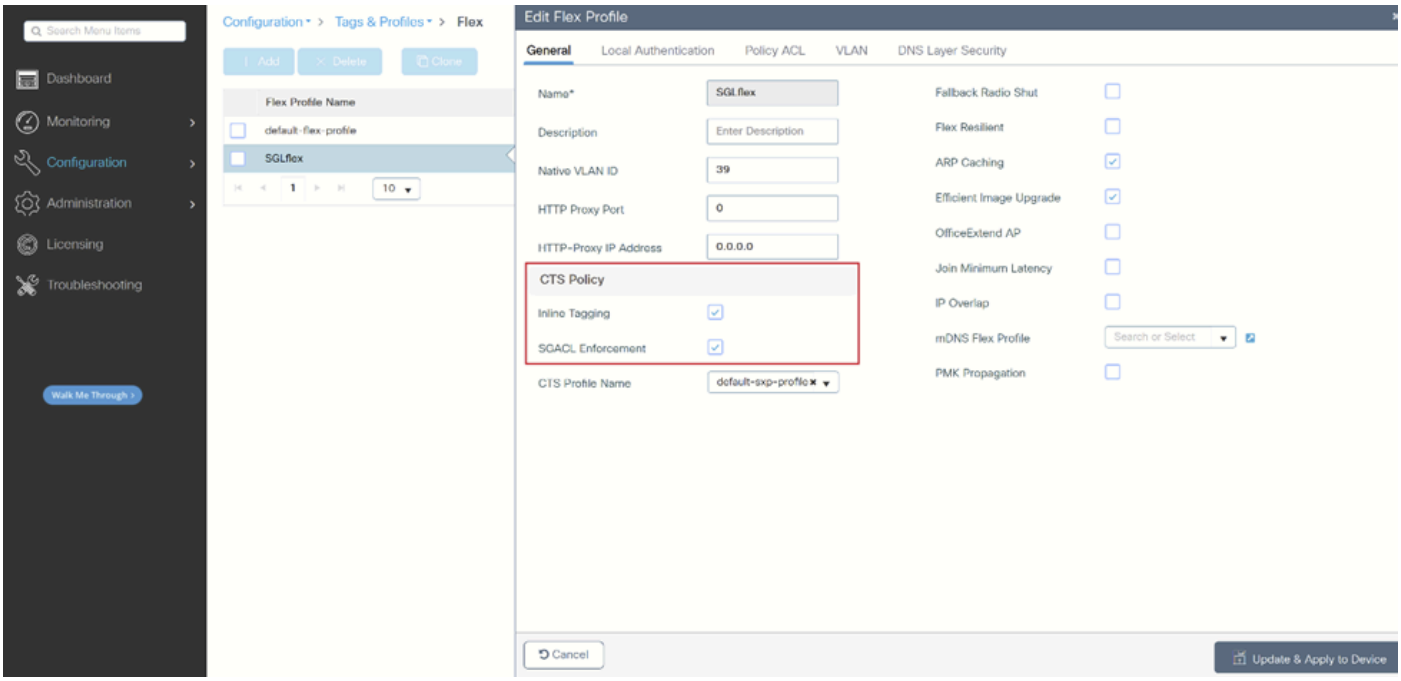
이 실습에서는 사용자별 SGT를 정의하며, Security Groups(보안 그룹) 필드 아래에서 SGT를 선택합니다.



ISE 보안 그룹

Flexconnect

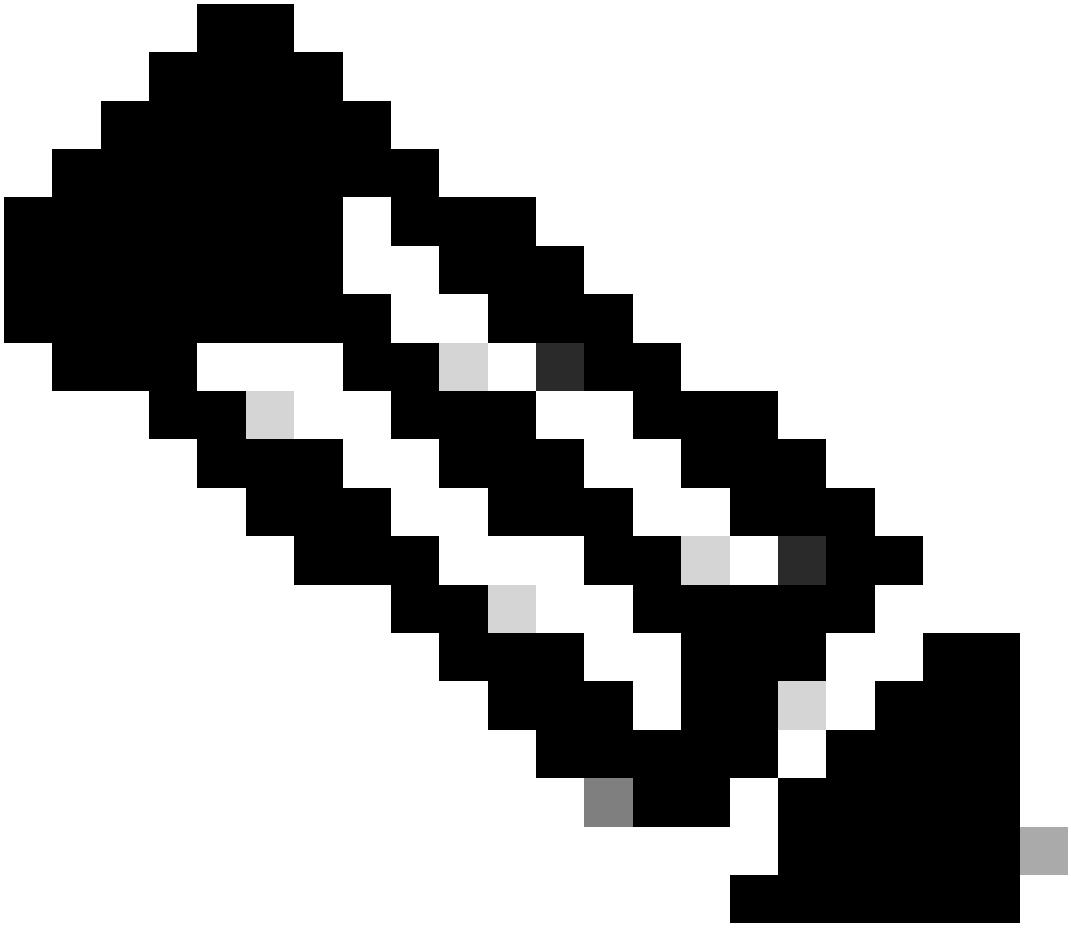
Configuration(컨피그레이션) > Tags & Policies(태그 및 정책) > Flex(Flex)의 Flex Profile(Flex 프로필)에서 인라인 태깅 및 SGACL Enforcement(SGACL 시행)를 활성화합니다.



WLC Flex 프로파일

CLI에서:

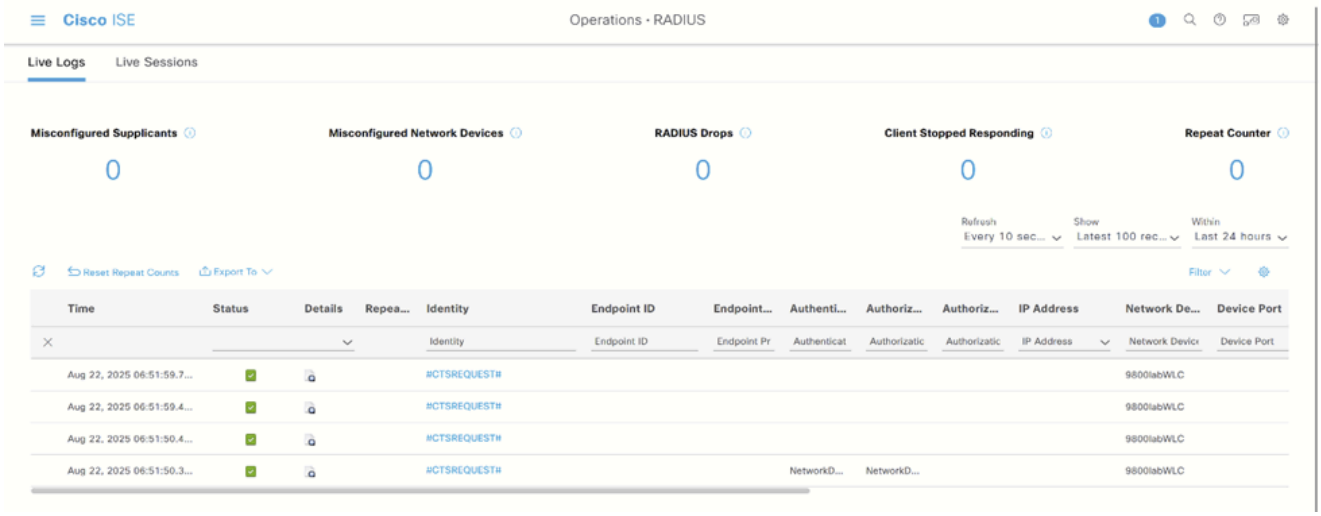
```
# configure terminal

(config)# wireless profile flex SGLflex
(config-wireless-flex-profile)# cts inline-tagging
(config-wireless-flex-profile)# cts role-based enforcement
```



참고: WLC가 HA-SSO에 있는 경우 FlexConnect AP의 SGACL은 지원되지 않습니다. Cisco 버그 ID CSCwn85468. 17.19에 추가됩니다.

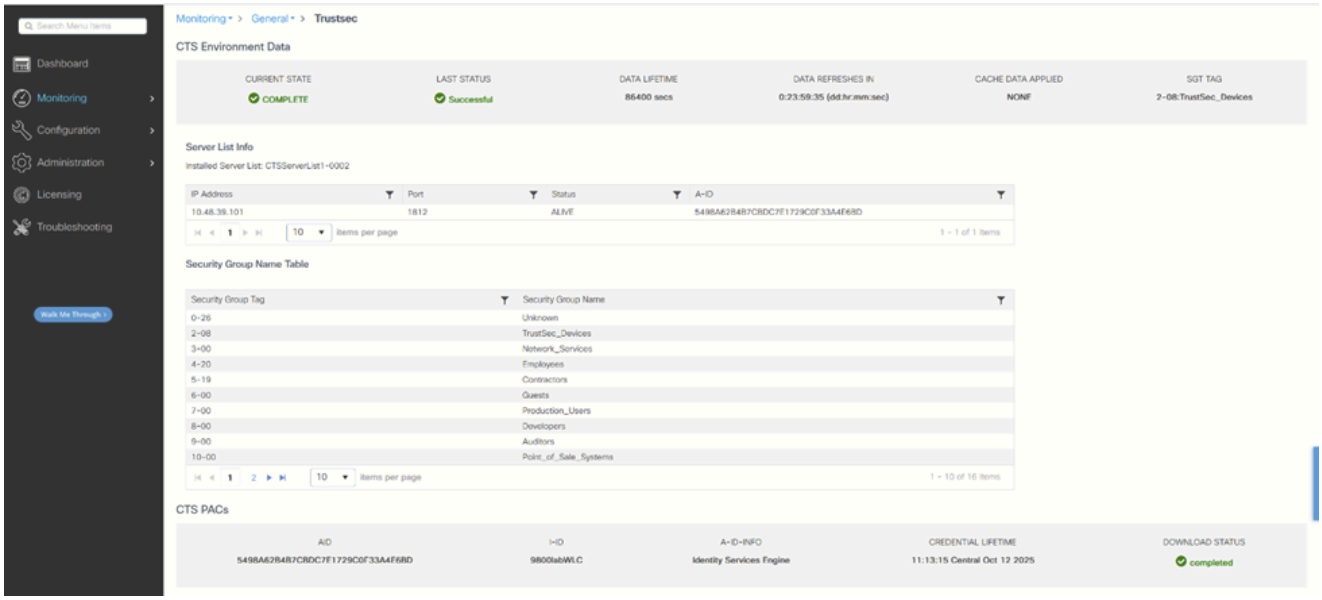
다음을 확인합니다.

1. ISE에서 Operations(운영) > RADIUS > Live Logs(라이브 로그) 아래에서 성공적인 CTS 요청을 확인해야 합니다.



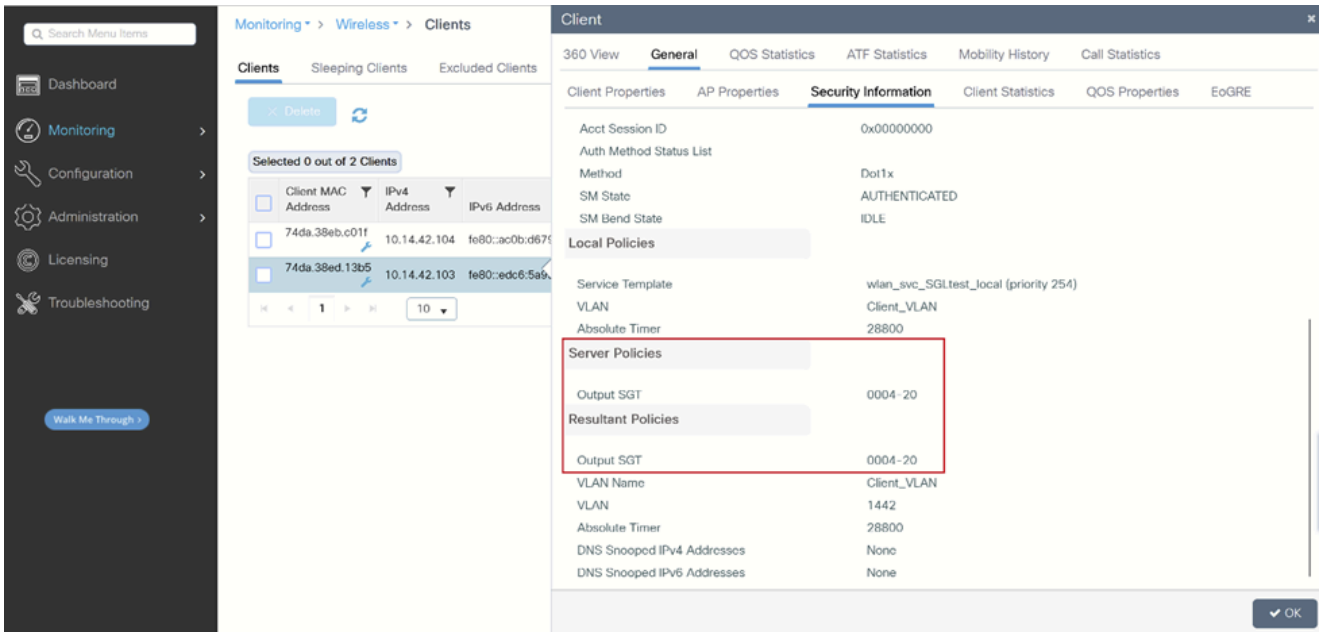
ISE RADIUS 라이브 로그

2. 연결이 설정되었고 WLC의 Monitoring(모니터링) > General(일반) > Trustsec에서 SGT가 다운로드되었는지 확인할 수 있습니다.



WLC TrustSec 모니터링

3. 클라이언트를 연결할 때 할당된 SGT가 Monitoring(모니터링) > Wireless(무선) > Clients(클라이언트) 아래에 표시되며, 확인할 클라이언트를 선택하고 General(일반) > Security information(보안 정보) 탭으로 이동합니다.



WLC 클라이언트 모니터링

CLI에서:

- 클라이언트를 연결하기 전에 WLC 출력에서 다음 사항을 확인할 수 있습니다. 알 수 없는 SGT와 관련된 권한만 표시됩니다.

```
<#root>

#

show cts role-based sgt-map all


Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.14.12.110            2       INTERNAL
10.48.39.55             2       INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of INTERNAL bindings = 2
Total number of active   bindings = 2

Active IPv6-SGT Bindings Information

IP Address                                SGT     Source
============================================================


<#root>

#
```

show cts role-based permissions

```
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group Unknown:
        SGACLtest-03
        Permit IP-00
IPv4 Role-based permissions from group 2:TrustSec_Devices to group Unknown:
        CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 4:Employees to group Unknown:
        CustomDefaultSGTACL-03
        Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group Unknown:
        SGACLtest-03
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group 2:TrustSec_Devices:
        CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 2:TrustSec_Devices to group 2:TrustSec_Devices:
        SGT32-06
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

- 클라이언트를 연결할 때 RA 추적에서 이러한 로그를 관찰할 수 있으며, SGT는 AAA에서 적용됩니다.

<#root>

```
2025/08/14 08:44:47.072771984 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info): [ Applied attribute :
2025/08/14 08:44:47.072786402 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info): [ Applied attribute :
2025/08/14 08:44:47.072788080 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info):
```

[Applied attribute : security-group-tag   0 "0004-20"]

```
2025/08/14 08:44:47.072809490 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info): [ Applied attribute :bs
2025/08/14 08:44:47.072811627 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info): [ Applied attribute :
2025/08/14 08:44:47.072824202 {wncd_x_R0-0}{1}: [auth-mgr] [15596]: (info): [0000.0000.0000:unknown]  R
2025/08/14 08:44:47.072829794 {wncd_x_R0-0}{1}: [ewlc-qos-client] [15596]: (info): MAC: 74da.38ed.13b5
2025/08/14 08:44:47.072860963 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [15596]: (debug): Managed client RUN
2025/08/14 08:44:47.072905375 {wncd_x_R0-0}{1}: [client-orch-state] [15596]: (note): MAC: 74da.38ed.13b
```

- 클라이언트에 할당된 SGT를 표시할 CLI에서 show wireless client mac-address <client_MAC_address> detail 명령을 사용합니다.

<#root>

```
#show wireless client mac-address 74da.38ed.13b5 detail

Client MAC Address : 74da.38ed.13b5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 10.14.42.103
```

```
…
  Auth Method Status List
        Method : Dot1x
                SM State         : AUTHENTICATED
                SM Bend State    : IDLE
  Local Policies:
        Service Template : wlan_svc_SGLtest_local (priority 254)
                VLAN             : Client_VLAN
                Absolute-Timer   : 28800
  Server Policies:


       Output SGT       : 0004-20


  Resultant Policies:


Output SGT       : 0004-20


                VLAN Name        : Client_VLAN
                VLAN             : 1442
                Absolute-Timer   : 28800
…
```

- SGT 4에서 하나의 클라이언트를 연결한 후 SGT 4에 대한 권한이 표시됩니다. 사용 권한은 클라이언트가 연결되고 SGT가 할당된 후에 추가됩니다.

<#root>

#

show cts role-based permissions

```
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group Unknown:
        SGACLtest-03
        Permit IP-00
IPv4 Role-based permissions from group 2:TrustSec_Devices to group Unknown:
        CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 4:Employees to group Unknown:
        CustomDefaultSGTACL-03
        Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group Unknown:
        SGACLtest-03
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group 2:TrustSec_Devices:
        CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 2:TrustSec_Devices to group 2:TrustSec_Devices:
        SGT32-06
```

IPv4 Role-based permissions from group Unknown to group 4:Employees:

CustomDefaultSGTACL-03

Permit IP-00

IPv4 Role-based permissions from group 4:Employees to group 4:Employees:

CustomDefaultSGTACL-03

Permit IP-00

IPv4 Role-based permissions from group 5:Contractors to group 4:Employees:

CustomDefaultSGTACL-03

Permit IP-00

```
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

<#root>

#

show cts role-based sgt-map all

```
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.14.12.110            2       INTERNAL
10.14.42.103            4       LOCAL
10.48.39.55             2       INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of INTERNAL bindings = 2
Total number of active   bindings = 3

Active IPv6-SGT Bindings Information

IP Address                                  SGT     Source
============================================================
```

- SGT 4와 SGT 5의 두 클라이언트를 연결한 후:

<#root>

```
#
show cts role-based sgt-map all


Active IPv4-SGT Bindings Information

IP Address              SGT     Source
========================================
10.14.12.110            2       INTERNAL
10.14.42.103            4       LOCAL
10.14.42.104            5       LOCAL
10.48.39.55             2       INTERNAL

IP-SGT Active Bindings Summary
========================================
Total number of LOCAL    bindings = 2
Total number of INTERNAL bindings = 2
Total number of active   bindings = 4

Active IPv6-SGT Bindings Information

IP Address                                  SGT     Source
============================================================
```

- 이제 SGT 5의 권한이 추가된 것을 확인할 수 있습니다.

<#root>

```
#
show cts role-based permissions


IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group Unknown:
        SGACLtest-03
        Permit IP-00
IPv4 Role-based permissions from group 2:TrustSec_Devices to group Unknown:
        CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 4:Employees to group Unknown:
        CustomDefaultSGTACL-03
        Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group Unknown:
        SGACLtest-03
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group 2:TrustSec_Devices:
        CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 2:TrustSec_Devices to group 2:TrustSec_Devices:
        SGT32-06
IPv4 Role-based permissions from group Unknown to group 4:Employees:
        CustomDefaultSGTACL-03
        Permit IP-00
IPv4 Role-based permissions from group 4:Employees to group 4:Employees:
        CustomDefaultSGTACL-03
        Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group 4:Employees:
        CustomDefaultSGTACL-03
```

```
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group 5:Contractors:

        SGACLtest-03

        Permit IP-00

IPv4 Role-based permissions from group 4:Employees to group 5:Contractors:

        CustomDefaultSGTACL-03

        Permit IP-00

IPv4 Role-based permissions from group 5:Contractors to group 5:Contractors:

        CustomDefaultSGTACL-03

        Permit IP-00

RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

- ACL은 WLC에서 "다운로드됨"으로 표시됩니다.

<#root>

#

show ip access-lists

```
Role-based IP access list CustomDefaultSGTACL-03 (downloaded)
    10 permit udp src eq bootps (12 matches)
    20 permit udp src eq bootpc
    30 permit ip
Extended IP access list IP-Adm-V4-Int-ACL-global
    10 permit tcp any any eq www
    20 permit tcp any any eq 443
Role-based IP access list Permit IP-00 (downloaded)
    10 permit ip
Role-based IP access list SGACLtest-03 (downloaded)
    10 permit udp src eq bootps (18 matches)
    20 permit udp src eq bootpc
    30 permit udp dst eq bootps
    40 permit udp dst eq bootpc
```

```
    50 permit ip
Role-based IP access list SGT32-06 (downloaded)
    10 permit ip
Extended IP access list implicit_deny
    10 deny ip any any
Extended IP access list implicit_permit
    10 permit ip any any
Extended IP access list meraki-fqdn-dns
Extended IP access list preauth_v4
    10 permit udp any any eq domain
    20 permit tcp any any eq domain
    30 permit udp any eq bootps any
    40 permit udp any any eq bootpc
    50 permit udp any eq bootpc any
    60 deny ip any any
```

FlexConnect 로컬 스위칭

- 클라이언트를 AP에 연결하기 전의 WLC 출력입니다.

<#root>

#

show cts ap sgt-info

```
Number of SGTs referred by the AP.............: 4

SGT               PolicyPushedToAP       No.of Clients
-----------------------------------------------------------
UNKNOWN(0)        NO                     0
2                 NO                     1
DEFAULT(65535)    YES                    0
```

- AP CLI에서, 클라이언트를 AP에 연결하기 전에 출력되는 권한:

```
AP#show cts role-based permissions
IPv4 role-based permissions:
SGT DGT ACL
65535 65535 Permit_IP

IPv6 role-based permissions:
SGT DGT ACL
65535 65535 Permit_IP
```

- 이러한 AP 디버그는 클라이언트가 연결되어 흐름을 표시하는 동안 수행됩니다.

<#root>

```
[*08/14/2025 09:45:40.8504] CLSM[74:DA:38:ED:13:B5]: US Auth(b0) seq 2599 IF 72 slot 0 vap 0 len 30 sta
[*08/14/2025 09:45:40.8507] CLSM[74:DA:38:ED:13:B5]: DS Auth len 30 slot 0 vap 0
[*08/14/2025 09:45:40.8509] CLSM[74:DA:38:ED:13:B5]: Driver send mgmt frame success Radio 0 Vap 0
[*08/14/2025 09:45:40.8509] CLSM[74:DA:38:ED:13:B5]: client moved from UNASSOC to AUTH
[*08/14/2025 09:45:40.8660] CLSM[74:DA:38:ED:13:B5]: US Assoc Req(0) seq 2600 IF 72 slot 0 vap 0 len 17
...
[*08/14/2025 09:45:40.8782] CLSM[74:DA:38:ED:13:B5]: client moved from ASSOC to 8021X
[*08/14/2025 09:45:40.8783] CLSM[74:DA:38:ED:13:B5]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc
[*08/14/2025 09:45:40.8784] CLSM[74:DA:38:ED:13:B5]:
```

SGT Data sent: 74:DA:38:ED:13:B5 0 0

!--- The client initiates the connection and it's directly put under the SGT 0.

<#root>

```
[*08/14/2025 09:45:40.8800] CLSM[74:DA:38:ED:13:B5]: ADD_CENTRAL_AUTH_INFO_MOBILE Payload
[*08/14/2025 09:45:40.8801] CLSM[74:DA:38:ED:13:B5]: msAssocTypeFlags: 2 apfMsEntryType: 2 eap_type: 0
[*08/14/2025 09:45:40.8807] CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENTCAPABILITYPAYLOAD: capbaility:
[*08/14/2025 09:45:40.8812] CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENT_TYPE_PAYLOAD: Client Type : 0
[*08/14/2025 09:45:41.5130] CLSM[74:DA:38:ED:13:B5]: ADD_MOBILE AID 1
[*08/14/2025 09:45:41.5135] CLSM[74:DA:38:ED:13:B5]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*08/14/2025 09:45:41.5139] chatter: 74:DA:38:ED:13:B5: web_auth status 1
[*08/14/2025 09:45:41.5140] CLSM[74:DA:38:ED:13:B5]: client moved from 8021X to
```

IPLEARN_PENDING

!--- The client must get an IP address through DHCP.

<#root>

```
[*08/14/2025 09:45:41.5144] CLSM[74:DA:38:ED:13:B5]: ADD_CENTRAL_AUTH_INFO_MOBILE Payload
[*08/14/2025 09:45:41.5144] CLSM[74:DA:38:ED:13:B5]: msAssocTypeFlags: 2 apfMsEntryType: 2 eap_type: 25
[*08/14/2025 09:45:41.5150] CLSM[74:DA:38:ED:13:B5]: TLV_FLEX_CENTRAL_AUTH_STA_PAYLOAD
[*08/14/2025 09:45:41.5155] CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENTCAPABILITYPAYLOAD: capbaility:
[*08/14/2025 09:45:41.5161] CLSM[74:DA:38:ED:13:B5]:
```

SGT Data sent: 74:DA:38:ED:13:B5 4 0

!--- Afterwards, the assigned SGT for that client is going to be applied accordingly.

<#root>

[*08/14/2025 09:45:41.5163] CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENT_TYPE_PAYLOAD: Client Type : 0
[*08/14/2025 09:45:41.6476] chatter: find_insert_client:3313
[*08/14/2025 09:45:41.6476] chatter: Update IP from 0.0.0.0 to 10.14.42.103
[*08/14/2025 09:45:41.6477] chatter:

Update ipsgt: IPV4 client(74:DA:38:ED:13:B5) - [10.14.42.103]

!--- Associated IP & SGT is going to be added into mapping table.

<#root>

[*08/14/2025 09:45:41.6477] chatter: Update ipsgt IPV6 client(74:DA:38:ED:13:B5) - [fe80::edc6:5a93:ada
[*08/14/2025 09:45:41.6481] CLSM[74:DA:38:ED:13:B5]: Authorize succeeded to radio intf apr0v0
[*08/14/2025 09:45:41.6490] chatter: 74:DA:38:ED:13:B5: web_auth status 1
[*08/14/2025 09:45:41.6492] CLSM[74:DA:38:ED:13:B5]: client moved from IPLEARN_PENDING to

FWD

<#root>

!--- Then for the IP-SGT mapping entry in the mapping table, SGACL policy for those SGTs is requested.
!--- This is a snippet of the AP debugs showing one of the ACLs:

CLSM[74:DA:38:ED:13:B5]: SGT Data sent: 74:DA:38:ED:13:B5 4 0
CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENT_TYPE_PAYLOAD: Client Type : 0
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 165 len 148
....TLV: TLV_CTS_RBACL_DELETE(1434), level: 0, seq: 0, nested: true
....TLV: TLV_CTS_RBACL_DELETE(1437), level: 1, seq: 0, nested: false
TLV_CTS_RBACL_DELETE received
ACL Name:CustomDefaultSGTACL
....TLV: TLV_CTS_RBACL_ADD(1433), level: 0, seq: 0, nested: true
....TLV: TLV_CTS_RBACL_ADD(1437), level: 1, seq: 0, nested: false
....TLV: TLV_CTS_RBACL_ADD(1438), level: 1, seq: 1, nested: false
....TLV: TLV_CTS_RBACL_ADD(1439), level: 1, seq: 2, nested: false
....TLV: TLV_CTS_RBACL_ADD(1439), level: 1, seq: 3, nested: false
....TLV: TLV_CTS_RBACL_ADD(1439), level: 1, seq: 4, nested: false
TLV_CTS_RBACL_ADD received

ACL Name:CustomDefaultSGTACL

ACL Type:1

ACE entry:permit udp src eq bootps

ACE entry:permit udp src eq bootpc

ACE entry:permit ip

```
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
…
```

- WLC CLI에서 SGT 4에 하나의 클라이언트를 연결할 때:

<#root>

#

show cts ap sgt-info

```
Number of SGTs referred by the AP.............: 4

SGT                PolicyPushedToAP       No.of Clients
-------------------------------------------------------------
UNKNOWN(0)         NO                     0
2                  NO                     1
4                  YES                    1
DEFAULT(65535)     YES                    0
```

- AP CLI에서:
  같은 것을 볼 수 있는데 SGT 4와 관련된 권한만 추가됩니다.

```
AP#show cts role-based permissions
IPv4 role-based permissions:
SGT DGT ACL
0 4 Permit_IP, CustomDefaultSGTACL
4 4 Permit_IP, CustomDefaultSGTACL
5 4 Permit_IP, CustomDefaultSGTACL
65535 65535 Permit_IP

IPv6 role-based permissions:
SGT DGT ACL
0 4 Permit_IP
4 4 Permit_IP
5 4 Permit_IP
```

```
65535 65535 Permit_IP
```

- SGT 5에서 두 번째 클라이언트를 연결할 때 WLC CLI에서 다음을 수행합니다.

```
<#root>

#

show cts ap sgt-info

Number of SGTs referred by the AP.............: 5

SGT               PolicyPushedToAP       No.of Clients
-----------------------------------------------------------
UNKNOWN(0)        NO                     0
2                 NO                     1
4                 YES                    1
5                 YES                    1
DEFAULT(65535)    YES                    0
```

- AP 출력:

```
<#root>

AP#

show flexconnect client

Flexconnect Clients:
              mac radio vap aid state       encr aaa-vlan aaa-acl aaa-ipv6-acl assoc    auth switching
SGT

74:DA:38:EB:C0:1F     0   0   1   FWD AES_CCM128     none    none         none Local Central     Local
5

74:DA:38:ED:13:B5     0   0   2   FWD AES_CCM128     none    none         none Local Central     Local
4

<#root>

AP#
```

show cts role-based sgt-map all

```
Active IPv4-SGT Bindings Information
          IP SGT SOURCE
10.14.42.103   4  LOCAL
10.14.42.104   5  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2

Active IPv6-SGT Bindings Information
                       IP SGT SOURCE
 fe80::ac0b:d679:e356:a17   5  LOCAL
fe80::edc6:5a93:adab:fff6   4  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
```

<#root>

AP#

show cts role-based permissions

```
IPv4 role-based permissions:
  SGT   DGT                              ACL
    0     4 Permit_IP, CustomDefaultSGTACL
    4     4 Permit_IP, CustomDefaultSGTACL
    5     4 Permit_IP, CustomDefaultSGTACL
    0     5           Permit_IP, SGACLtest
    4     5 Permit_IP, CustomDefaultSGTACL
    5     5 Permit_IP, CustomDefaultSGTACL
65535 65535 Permit_IP, CustomDefaultSGTACL

IPv6 role-based permissions:
  SGT   DGT       ACL
    0     4 Permit_IP
    4     4 Permit_IP
    5     4 Permit_IP
    0     5 Permit_IP
    4     5 Permit_IP
    5     5 Permit_IP
65535 65535 Permit_IP
```

<#root>

AP#

show cts access-lists

```
IPv4 role-based ACL:
SGACLtest
```

```
        rule 0: allow true && ip proto 17 && ( src port 67 )
        rule 1: allow true && ip proto 17 && ( src port 68 )
        rule 2: allow true && ip proto 17 && ( dst port 67 )
        rule 3: allow true && ip proto 17 && ( dst port 68 )
        rule 4: allow true
CustomDefaultSGTACL
        rule 0: allow true && ip proto 17 && ( src port 67 )
        rule 1: allow true && ip proto 17 && ( src port 68 )
        rule 2: allow true
Permit_IP
        rule 0: allow true

IPv6 role-based ACL:
Permit_IP
        rule 0: allow true
```

<#root>

AP#

show cts role-based sgt-map summary

```
        -IPv4-
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2

        -IPv6-
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
```

문제 해결

- WLC CLI에서:

cts 프로비저닝 표시

cts 역할 기반 권한 표시

ip 액세스 목록 표시

show cts ap sgt-info <ap_name>

- AP에서:

show cts role-based sgt-map all

cts 역할 기반 권한 표시

show cts access-lists <acl-name>

show cts role-based sgt-map 요약

cts 액세스 목록 표시

flexconnect 클라이언트 표시

cts 역할 기반 카운터 지우기

cts 역할 기반 카운터 표시

- AP 디버깅:

- CTS 패킷 레벨 시행 디버깅을 활성화합니다.

cts 시행 디버그

학기 월

- CAPWAP ACL 이벤트 및 페이로드 관련 정보를 확인하려면

debug dot11 client access-list <client-mac-addr>

debug capwap 클라이언트 acl

debug capwap 클라이언트 페이로드

디버그 capwap 클라이언트 오류

dot11 클라이언트 관리 정보 디버그

dot11 클라이언트 관리 중요 디버그

debug dot11 클라이언트 관리 오류

dot11 클라이언트 관리 이벤트 디버그

디버그 일반 데이터 경로 client_ip_table/debug_acl

디버그 일반 데이터 경로 client_ip_table/debug

디버그 일반 데이터 경로 sgacl/디버그

디버그 일반 데이터 경로 sgacl/debug_sgt

디버그 일반 데이터 경로 sgacl/debug_protocol

디버그 일반 데이터 경로 sgacl/debug_permission

학기 월

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 번역 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.