ISE(인라인 태깅)로 TrustSec(SGT) 구성

목차

소개

이 문서에서는 Identity Services Engine을 사용하여 Catalyst 스위치 및 무선 LAN 컨트롤러에서 TrustSec을 구성하고 확인하는 방법에 대해 설명합니다.

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco TrustSec(CTS) 구성 요소에 대한 기본 지식
- Catalyst 스위치의 CLI 구성에 대한 기본 지식
- Cisco WLC(Wireless LAN Controller)의 GUI 컨피그레이션에 대한 기본 지식
- ISE(Identity Services Engine) 컨피그레이션 경험

요구 사항

네트워크에 Cisco ISE가 구축되어 있어야 하며, 최종 사용자가 무선 또는 유선으로 연결할 때 802.1x(또는 다른 방법)를 사용하여 Cisco ISE에 인증해야 합니다. Cisco ISE는 무선 네트워크에 대한 인증 이 되면 트래픽을 SGT (Security Group Tag) 를 할당 합니다.

이 예에서 최종 사용자는 Cisco ISE BYOD(Bring Your Own Device) 포털로 리디렉션되고 인증서를 프로비저닝받므로 BYOD 포털 단계를 완료한 후 EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)를 사용하여 무선 네트워크에 안전하게 액세스할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Cisco Identity Services Engine, 버전 2.4
- Cisco Catalyst 3850 Switch, 버전 3.7.5E
- Cisco WLC, 버전 8.5.120.0
- 로컬 모드의 Cisco Aironet 무선 액세스 포인트

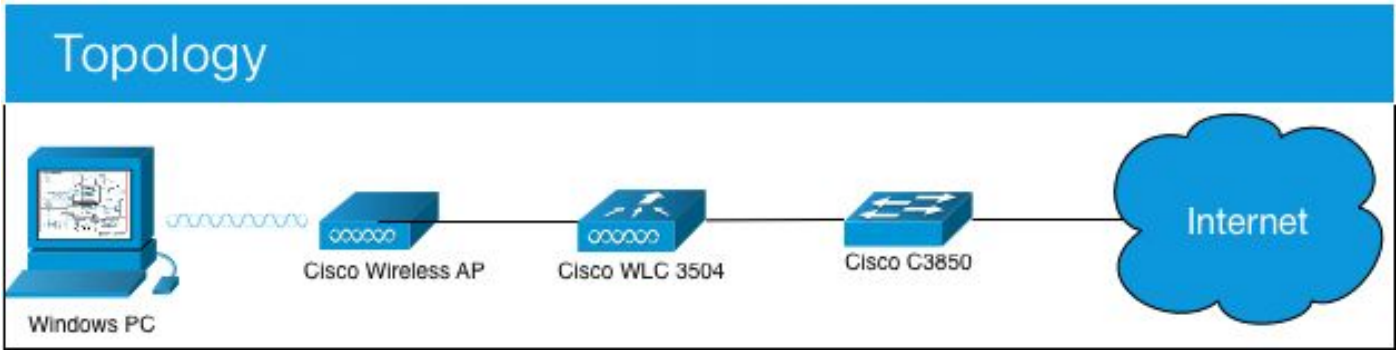
Cisco TrustSec을 구축하기 전에 Cisco Catalyst Switch 및/또는 Cisco WLC+AP 모델 + 소프트웨어 버전이 다음을 지원하는지 확인하십시오.

- TrustSec/보안 그룹 태그
- 인라인 태깅(그렇지 않은 경우, 인라인 태깅 대신 SXP를 사용할 수 있음)
- 정적 IP-SGT 매핑(필요한 경우)
- 정적 서브넷-SGT 매핑(필요한 경우)
- 정적 VLAN-SGT 매핑(필요한 경우)

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



이 예에서 WLC는 컨설턴트가 보낸 패킷인 경우 SGT 15로, 직원이 보낸 패킷인 경우 + SGT 7로 태그를 지정합니다.

SGT 15에서 SGT 8로 이동하는 경우 스위치는 해당 패킷을 거부합니다(컨설턴트는 SGT 8이라는 태그가 지정된 서버에 액세스할 수 없음).

이 스위치는 SGT 7에서 SGT 8로 이동하는 경우 이러한 패킷을 허용합니다(직원은 SGT 8이라는 태그가 지정된 서버에 액세스할 수 있음).

목표

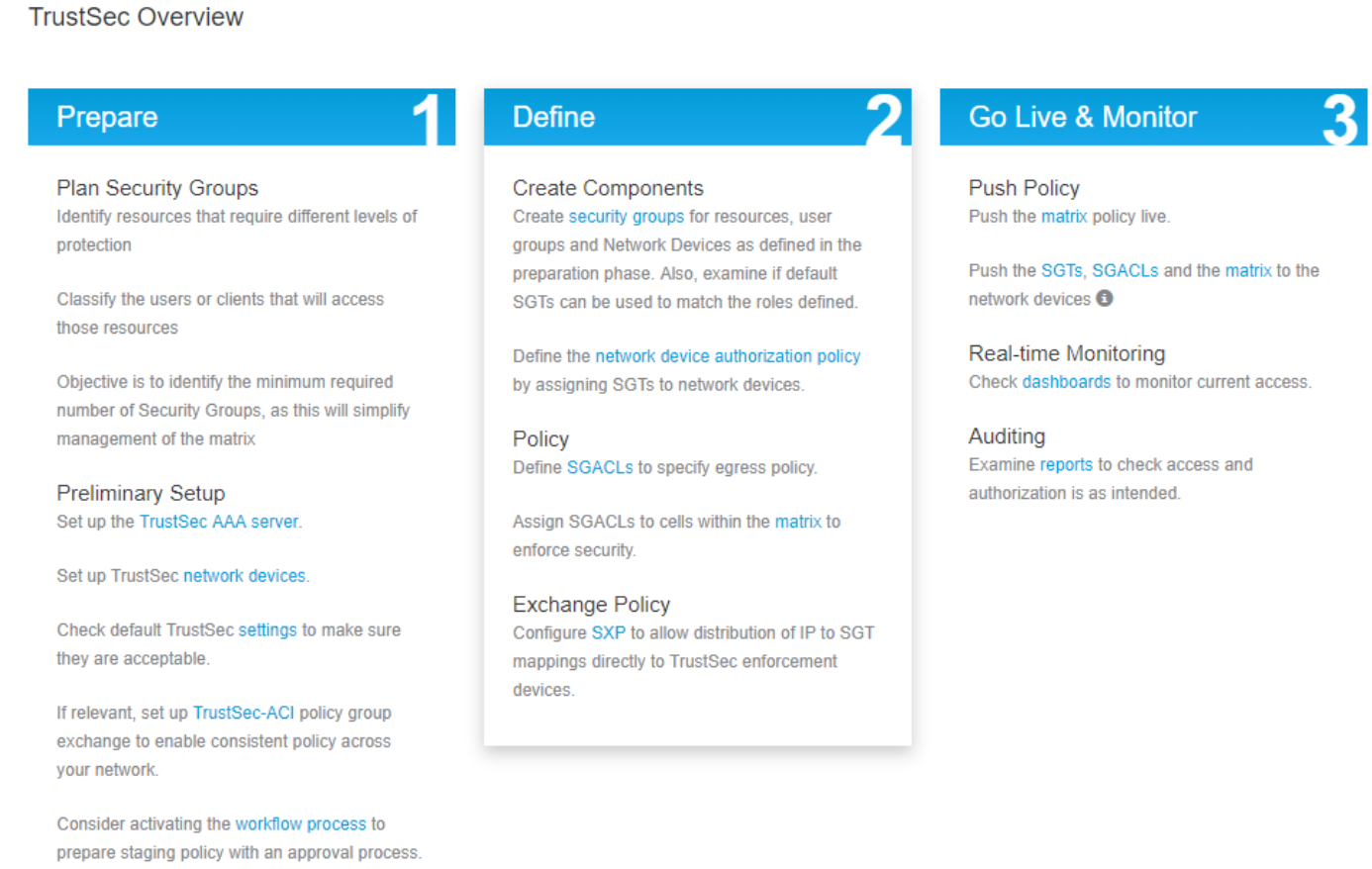
누구나 GuestSSID에 액세스할 수 있습니다.
컨설턴트가 제한된 액세스로 EmployeeSSID에 액세스하도록 허용합니다.
직원이 전체 액세스로 EmployeeSSID에 액세스하도록 허용합니다.

디바이스	IP 주소	VLAN
ISE	10.201.214.230	463
Catalyst 스위치	10.201.235.102	1115
WLC	10.201.214.229	463
액세스 포인트	10.201.214.138	455

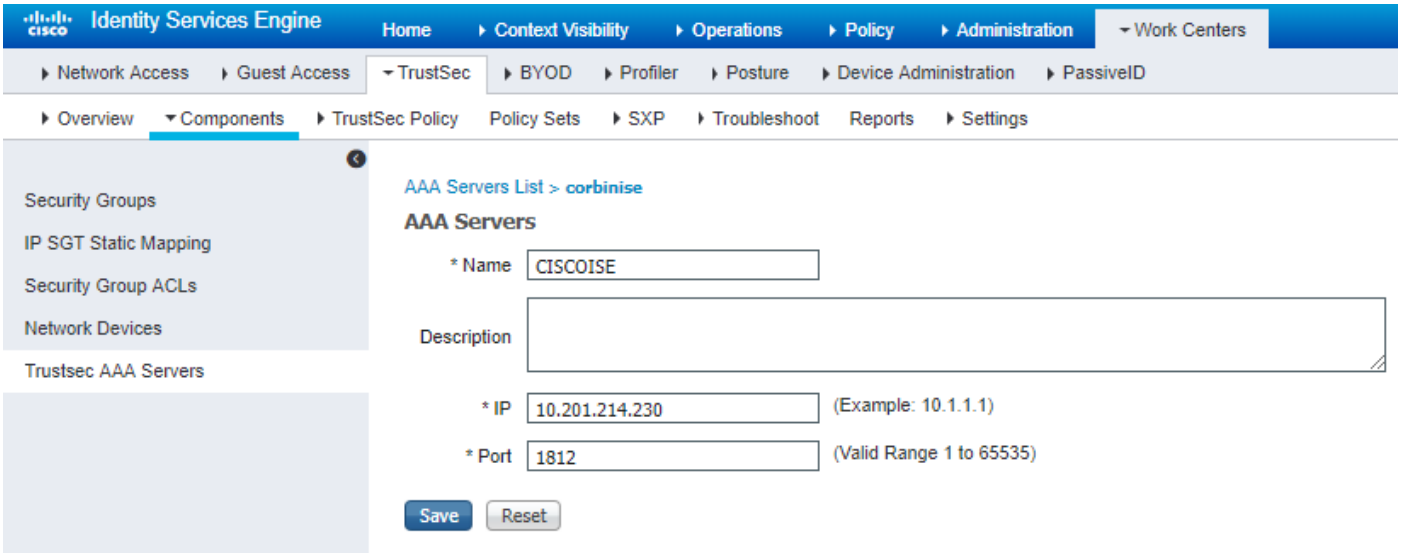
이름	사용자 이름	AD 그룹	SG	SGT
제이슨 스미스	jsmith	컨설턴트	BYOD 컨설턴트	15
샐리 스미스	스미스	직원	BYOD직원	7
해당 없음	해당 없음	해당 없음	TrustSec_장치	2

설정

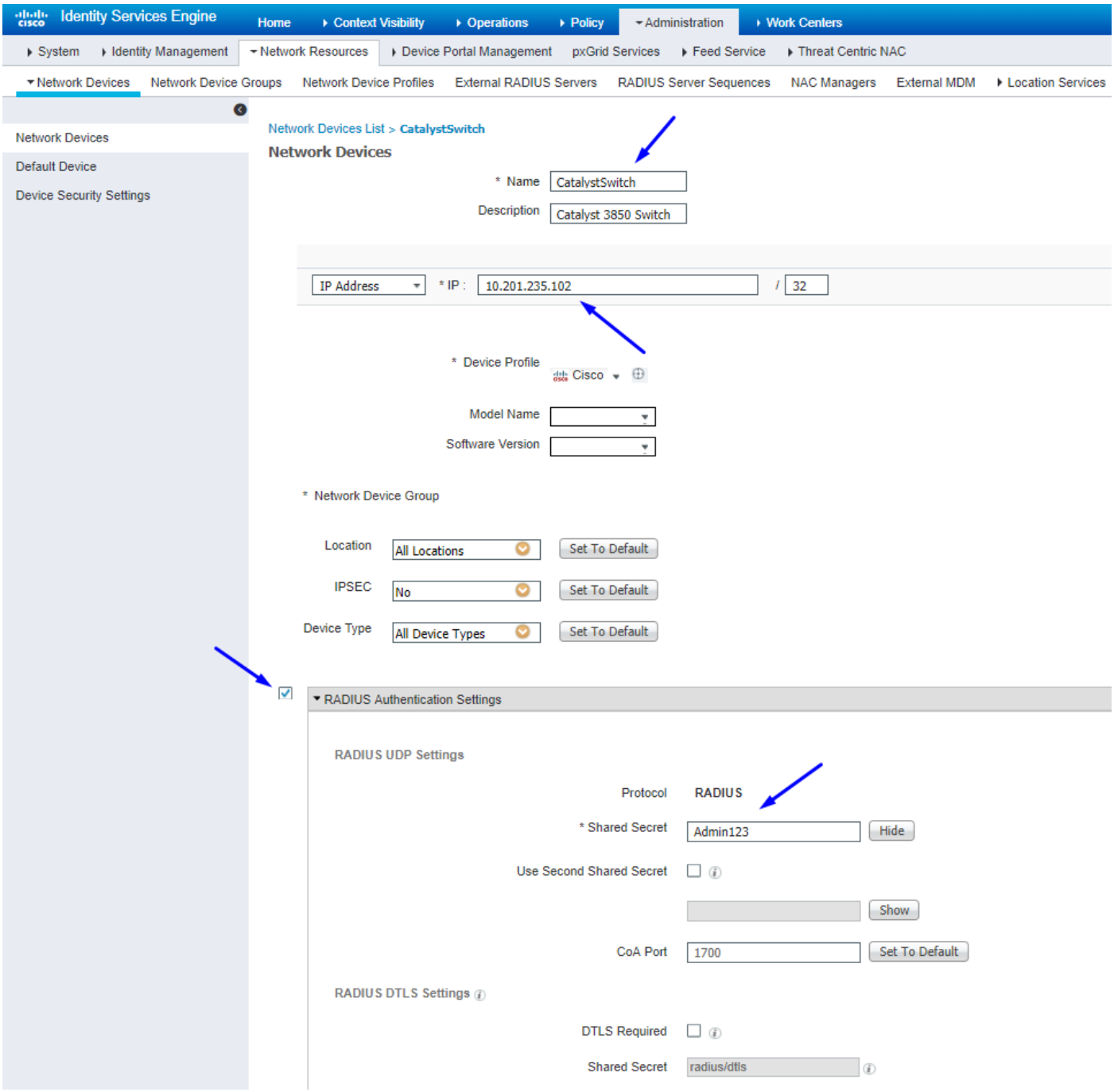
ISE에서 TrustSec 구성



Cisco ISE를 TrustSec AAA 서버로 구성

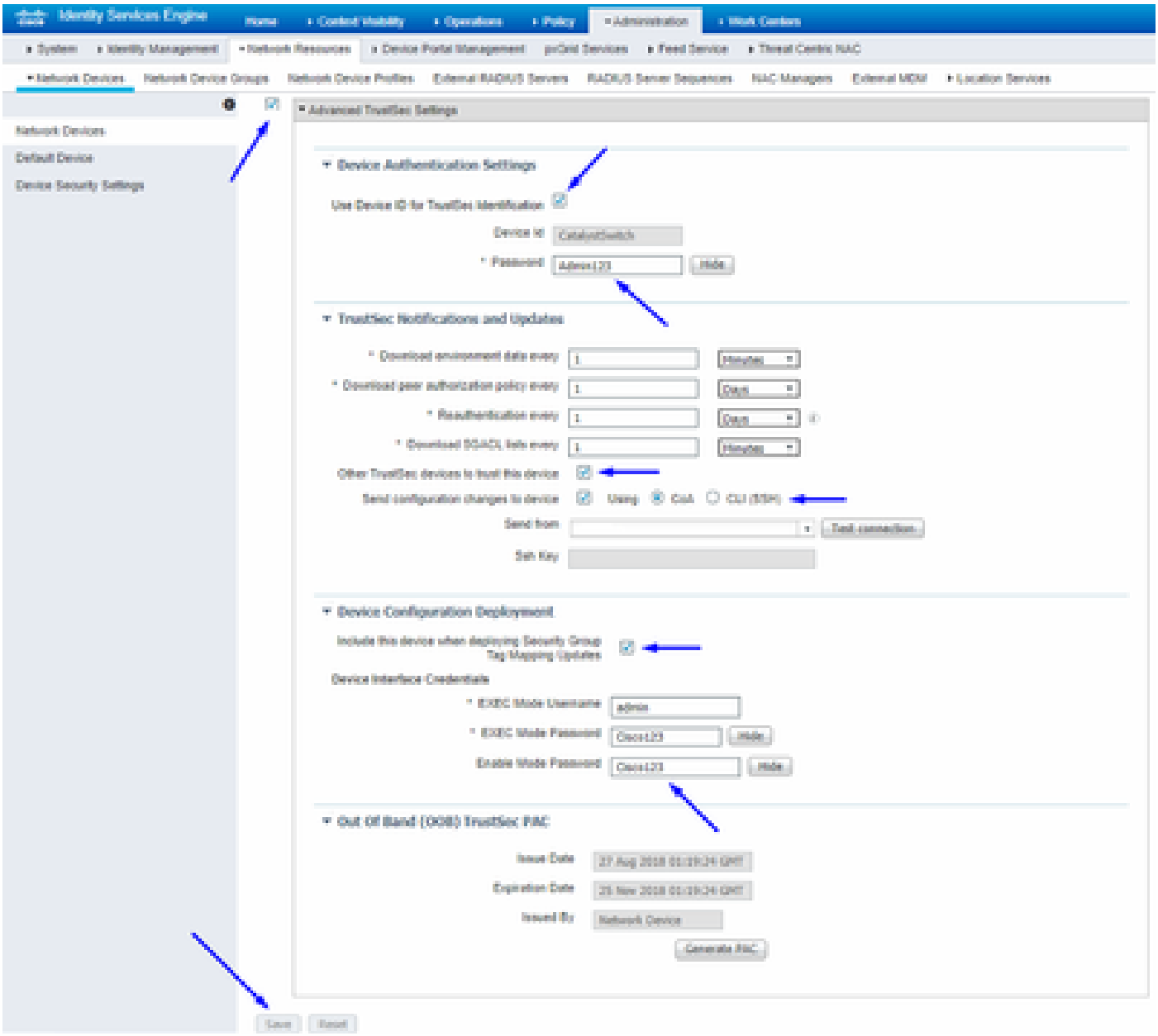


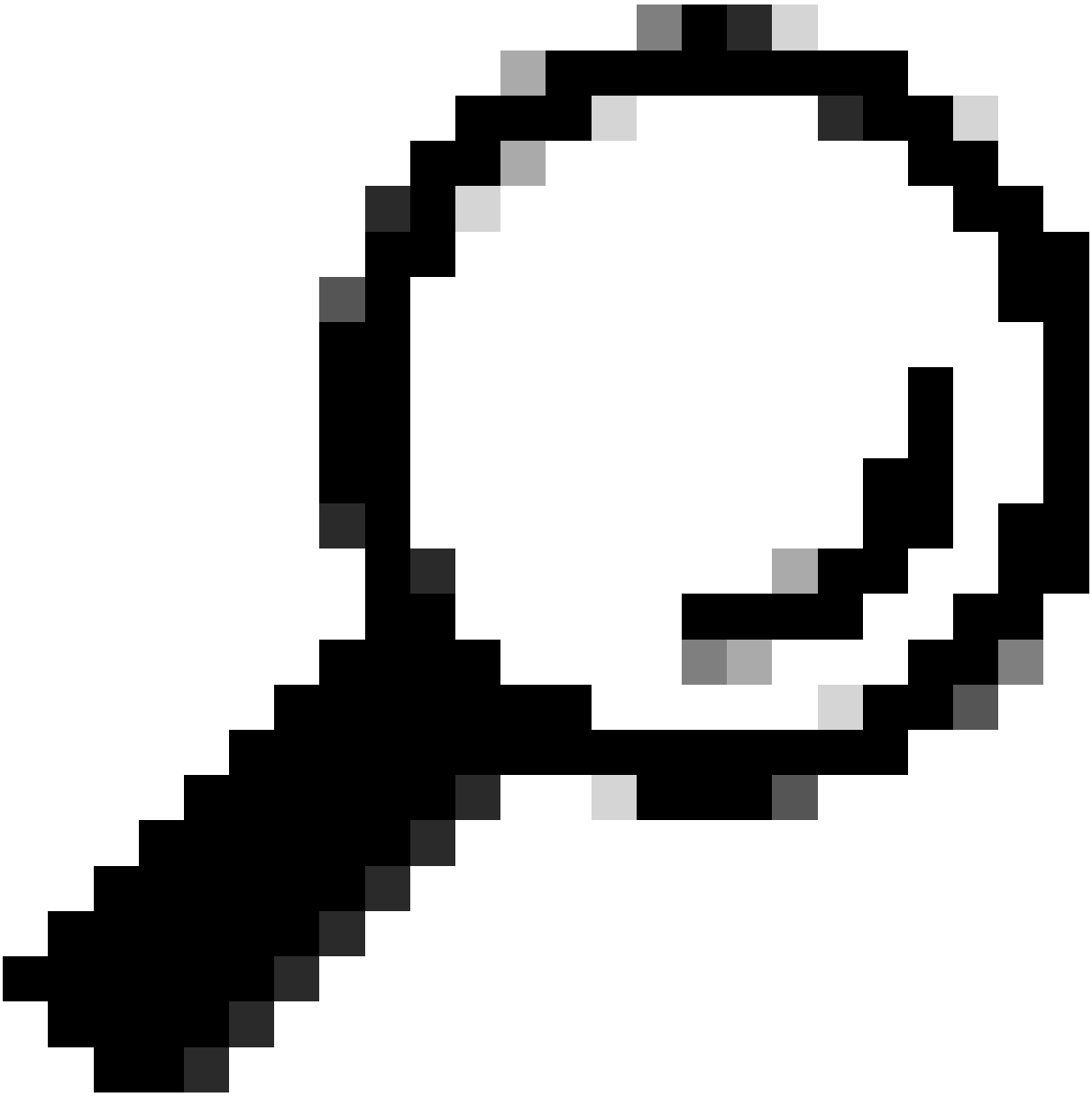
Configure 및 Verify 스위치가 Cisco ISE에서 RADIUS 디바이스로 추가되었는지 확인



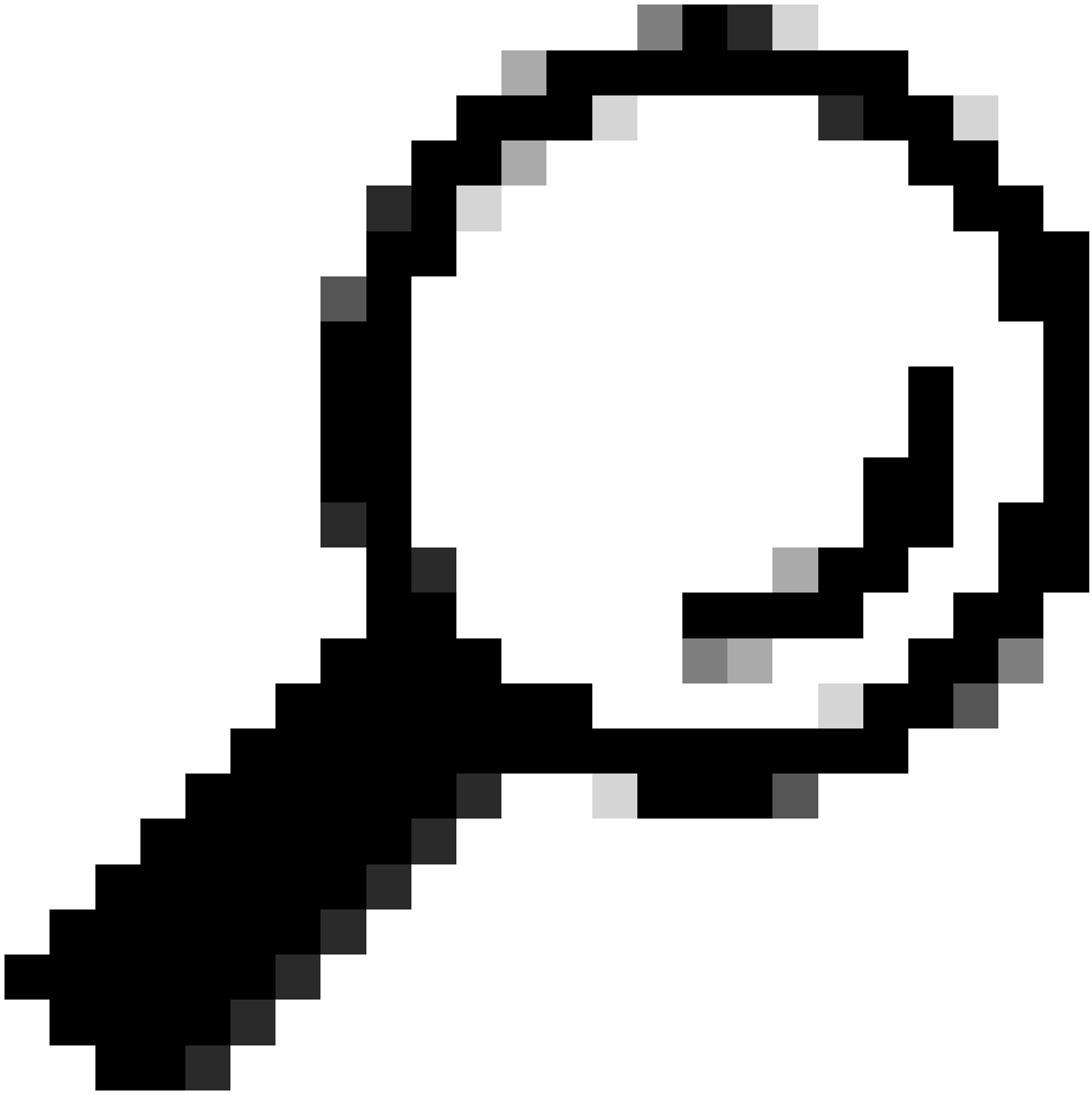
Cisco ISE에서 WLC가 TrustSec 디바이스로 추가되었는지 구성 및 확인

SSH에 대한 로그인 자격 증명을 입력합니다. 이를 통해 Cisco ISE는 스위치에 정적 IP와 SGT 매핑을 구축할 수 있습니다.
Cisco ISE 웹 GUI에서 다음 그림과 같이 이러한Work Centers > TrustSec > Components > IP SGT Static Mappings 항목을 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
External MDM
Location Services
Network Devices
Default Device
Device Security Settings
Advanced TrustSec Settings
Device Authentication Settings
Use Device ID for TrustSec Identification
Device Id
CatalystSwitch
* Password
Admin123
Hide
TrustSec Notifications and Updates
* Download environment data every
1
Minutes
* Download peer authorization policy every
1
Days
* Reauthentication every
1
Days
* Download SGACL lists every
1
Minutes
Other TrustSec devices to trust this device
Send configuration changes to device
Using
CoA
CLI (SSH)
Send from
Test Connection
Ssh Key
Device Configuration Deployment
Include this device when deploying Security Group Tag Mapping Updates
Device Interface Credentials
* EXEC Mode Username
admin
* EXEC Mode Password
Cisco123
Hide
Enable Mode Password
Cisco123
Hide
Out Of Band (OOB) TrustSec PAC
Issue Date
27 Aug 2018 01:19:24 GMT
Expiration Date
25 Nov 2018 01:19:24 GMT
Issued By
Network Device
Generate PAC
Save
Reset

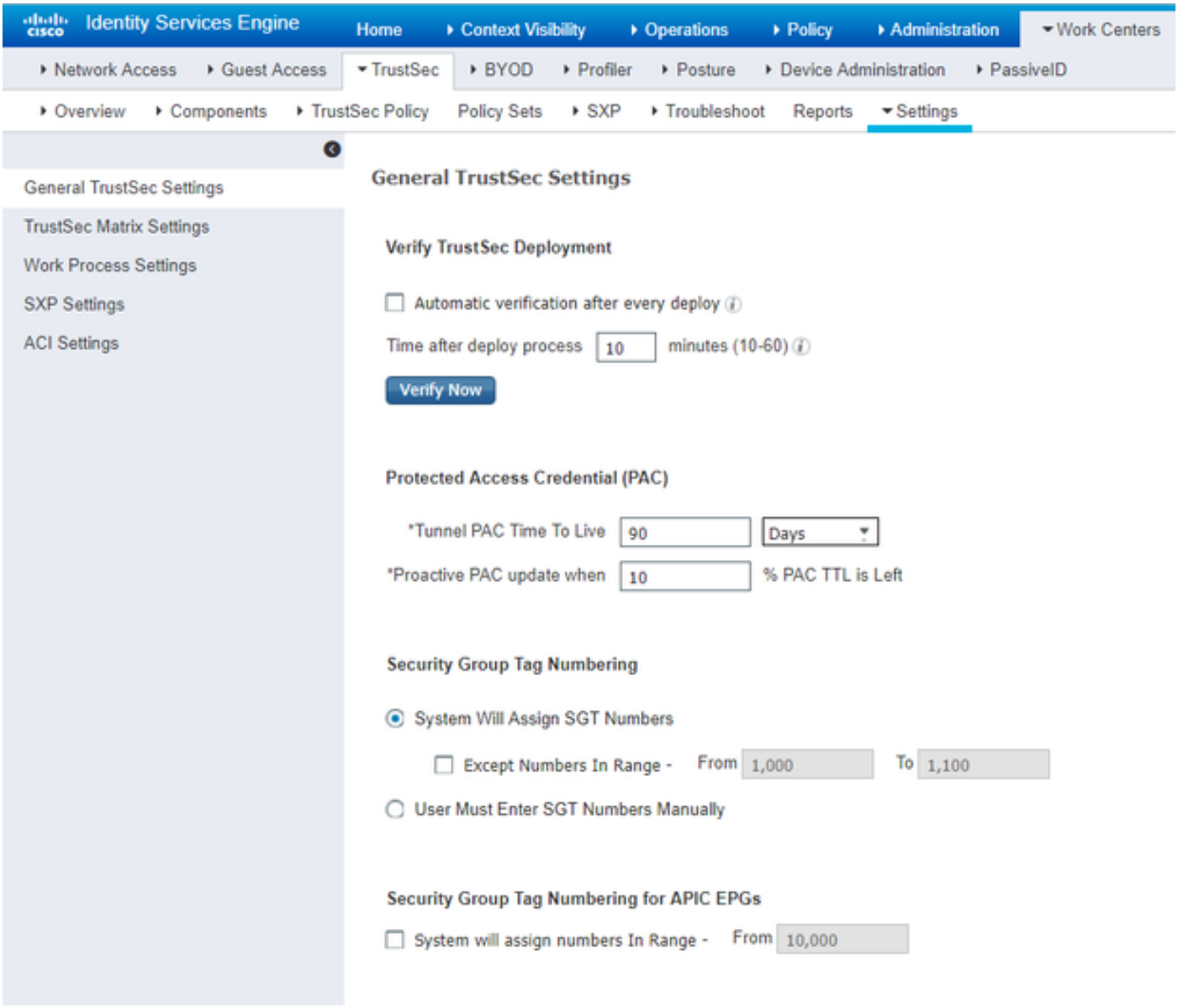


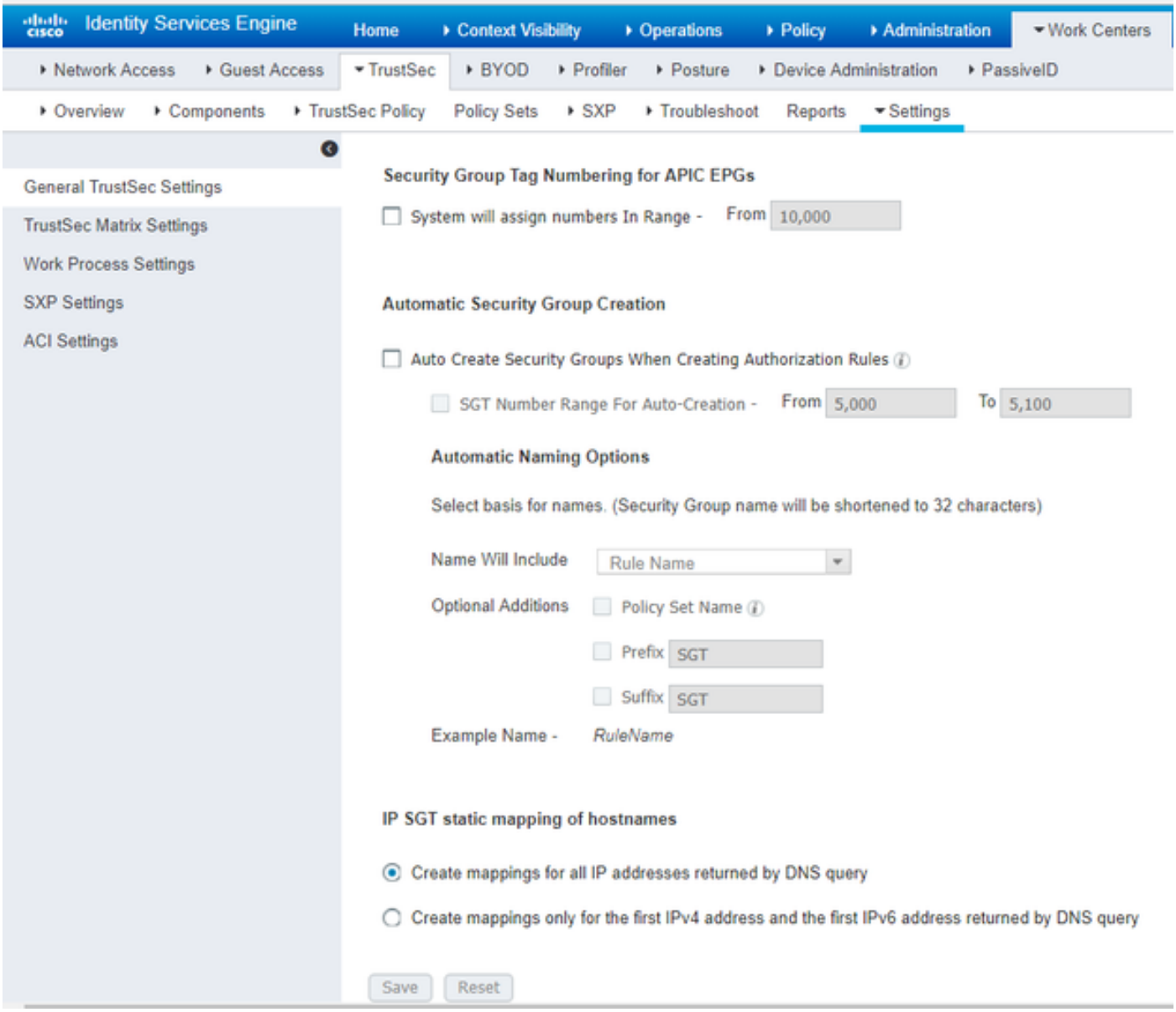
팁: Catalyst Switch에서 SSH를 아직 구성하지 않은 경우 Catalyst Switch에서 SSH(Secure Shell)를 구성하는 방법 가이드를 사용할 수 있습니다.



팁: Cisco ISE가 SSH를 통해 Catalyst Switch에 액세스하도록 활성화하지 않으려면 CLI를 대신 사용하여 Catalyst Switch에서 정적 IP와 SGT 매핑을 생성할 수 있습니다(여기 단계에 표시됨).

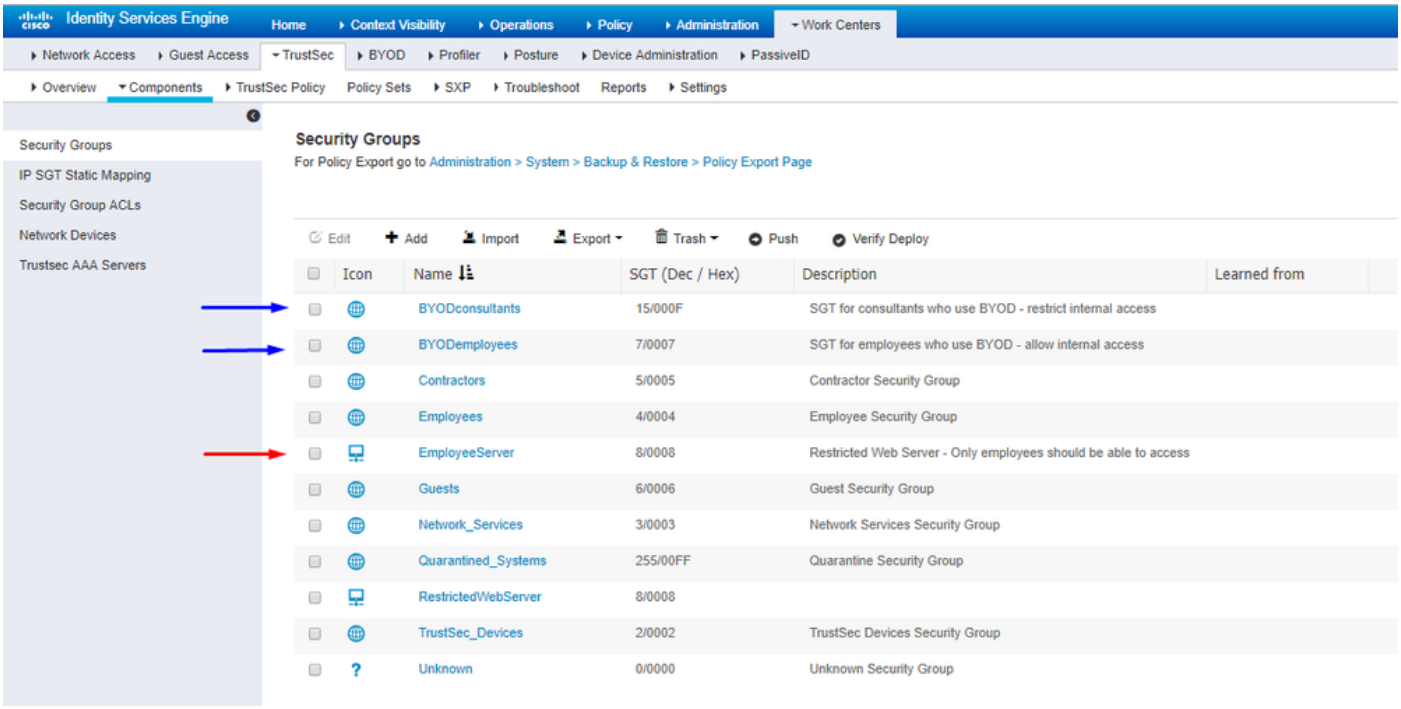
기본 TrustSec 설정을 확인하여 허용 가능한지 확인합니다(선택 사항).


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Components
TrustSec Policy
Policy Sets
SXP
Troubleshoot
Reports
Settings
General TrustSec Settings
TrustSec Matrix Settings
Work Process Settings
SXP Settings
ACI Settings
General TrustSec Settings
Verify TrustSec Deployment
Automatic verification after every deploy
Time after deploy process 10 minutes (10-60)
Verify Now
Protected Access Credential (PAC)
*Tunnel PAC Time To Live 90 Days
*Proactive PAC update when 10 % PAC TTL is Left
Security Group Tag Numbering
System Will Assign SGT Numbers
Except Numbers In Range - From 1,000 To 1,100
User Must Enter SGT Numbers Manually
Security Group Tag Numbering for APIC EPGs
System will assign numbers In Range - From 10,000



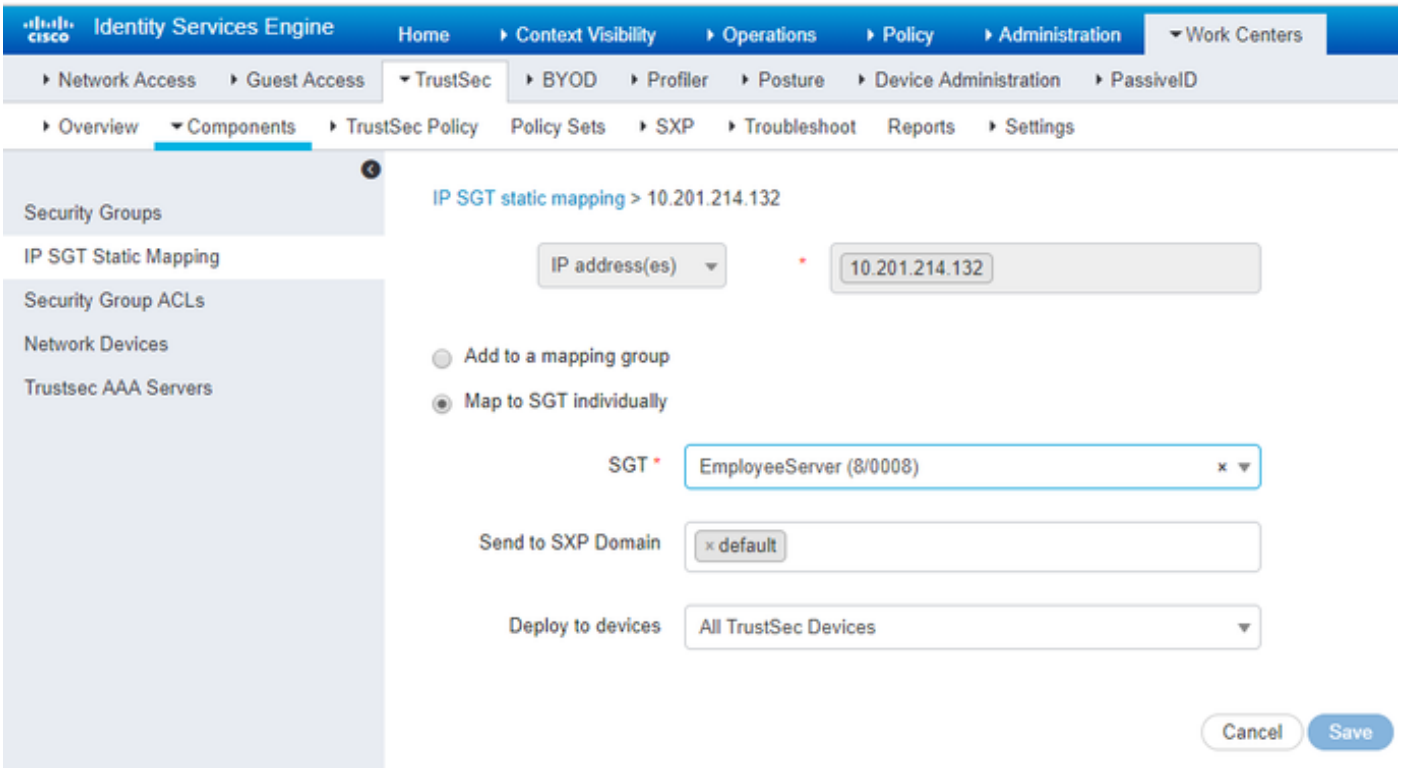
무선 사용자를 위한 보안 그룹 태그 생성

BYOD 컨설턴트용 보안 그룹 생성 - SGT 15
BYOD 직원을 위한 보안 그룹 생성 - SGT 7

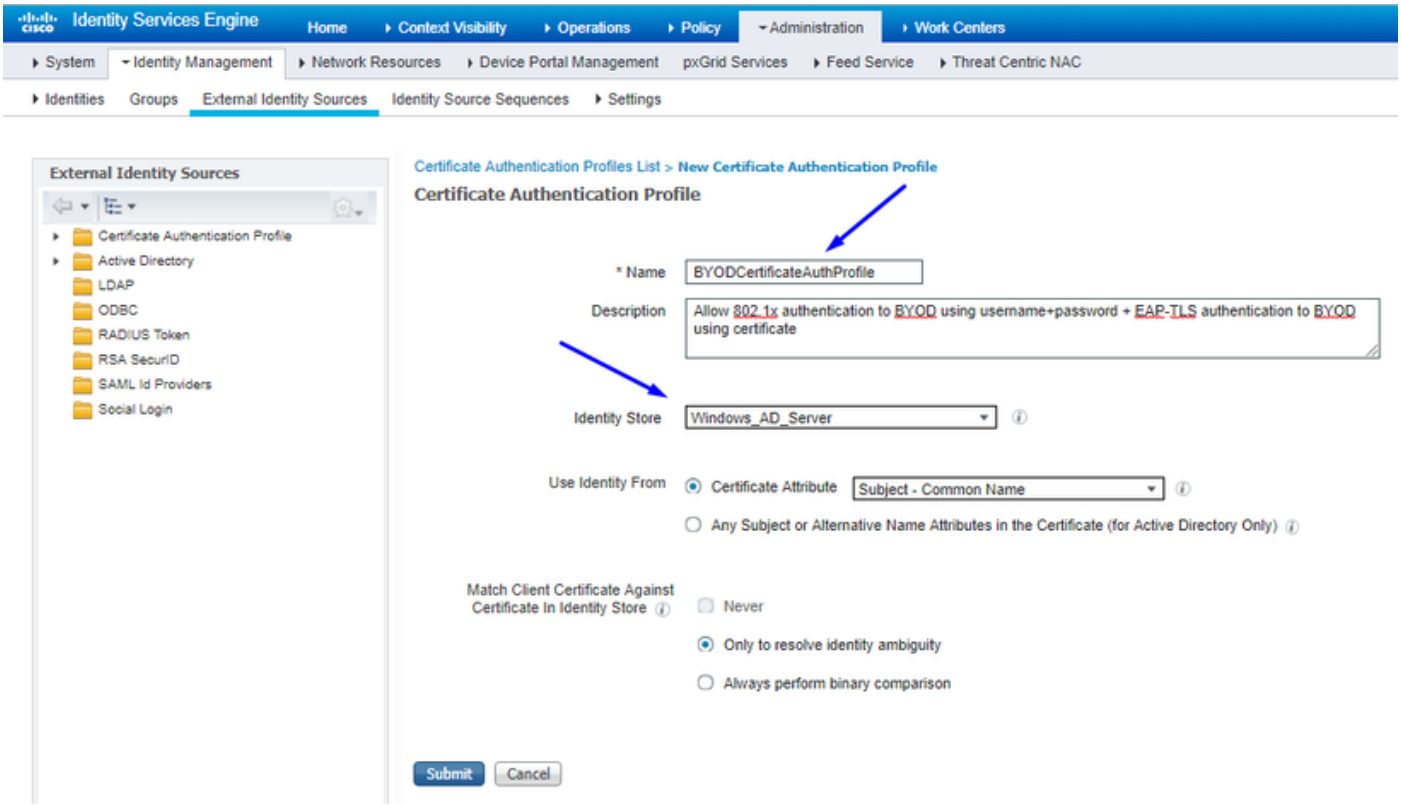


제한된 웹 서버에 대한 정적 IP-SGT 매핑 생성

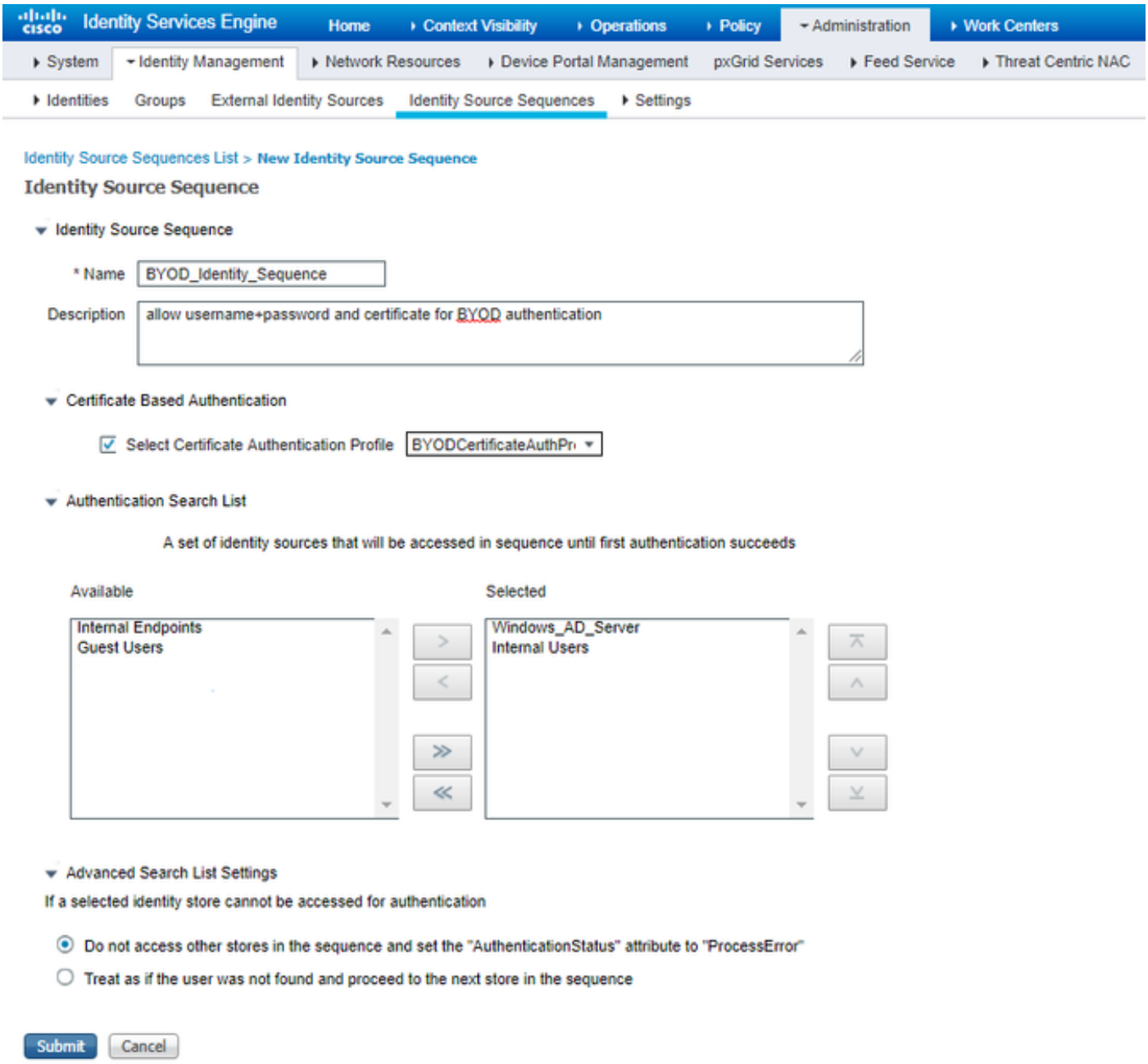
MAB(MAC Authentication Bypass), 802.1x, 프로파일 등을 사용하여 Cisco ISE에 인증하지 않는 네트워크의 다른 IP 주소 또는 서브넷에 대해 이 작업을 수행합니다.



인증서 인증 프로파일 생성

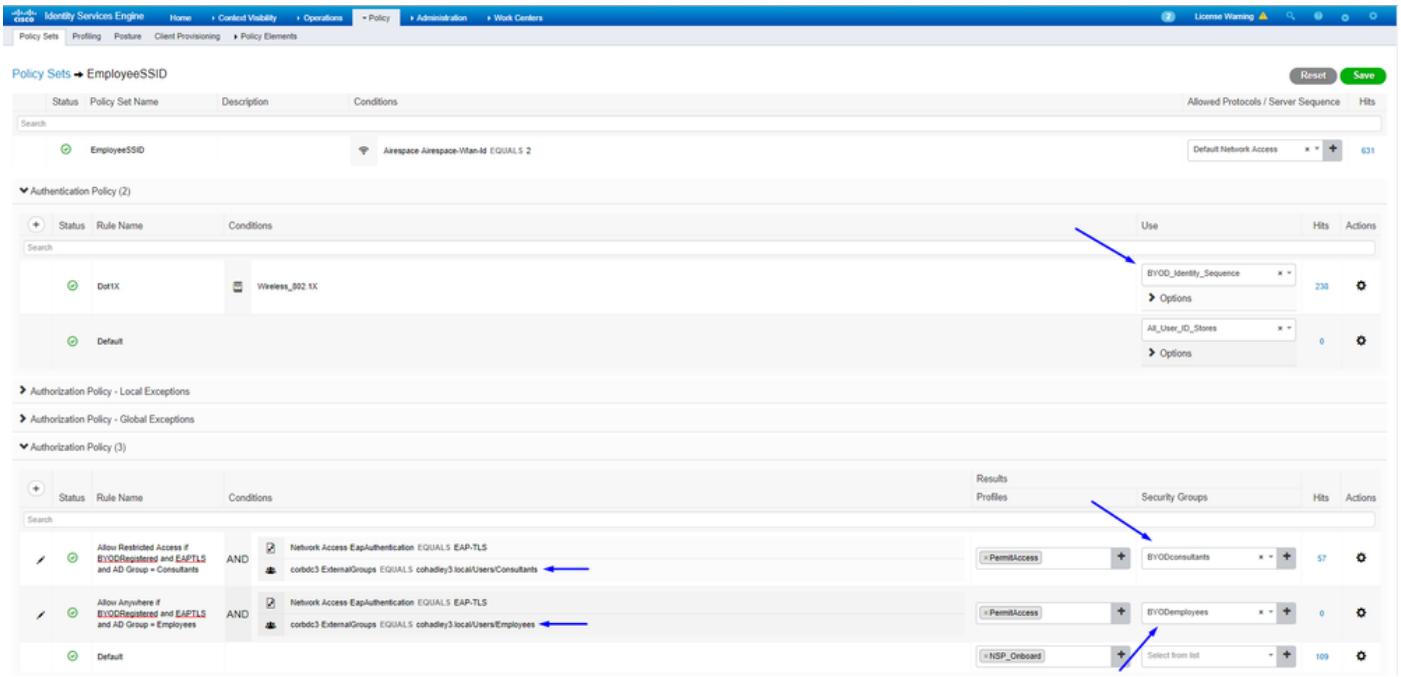


Create Identity Source Sequence with the Certificate Authentication Profile from Before(인증서 인증 프로필을 사용하여 ID 소스 시퀀스 생성)

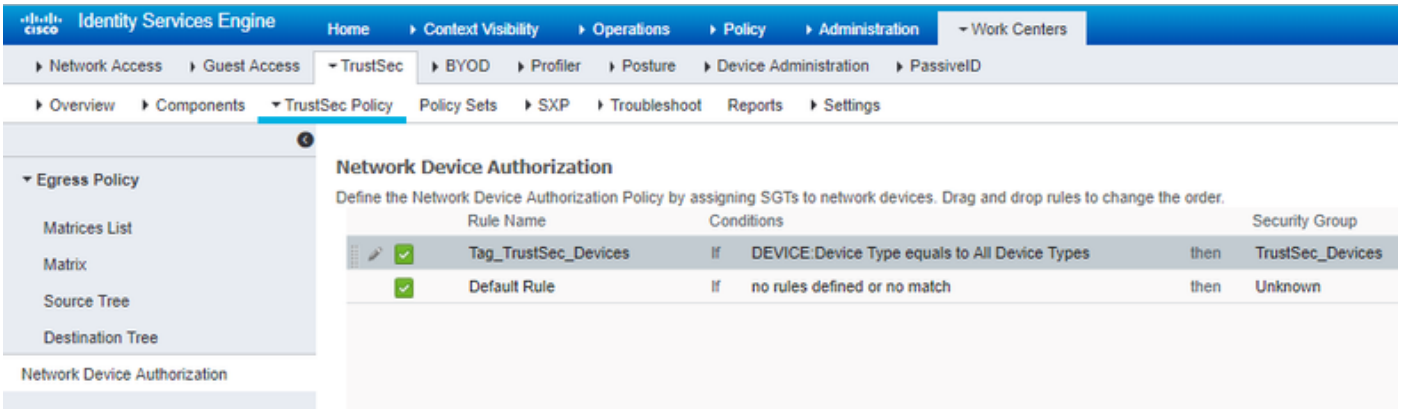


무선 사용자(직원 및 컨설턴트)에게 적절한 SGT 할당

이름	사용자 이름	AD 그룹	SG	SGT
제이슨 스미스	jsmith	컨설턴트	BYOD 컨설턴트	15
샐리 스미스	스미스	직원	BYOD직원	7
해당 없음	해당 없음	해당 없음	TrustSec_장치	2

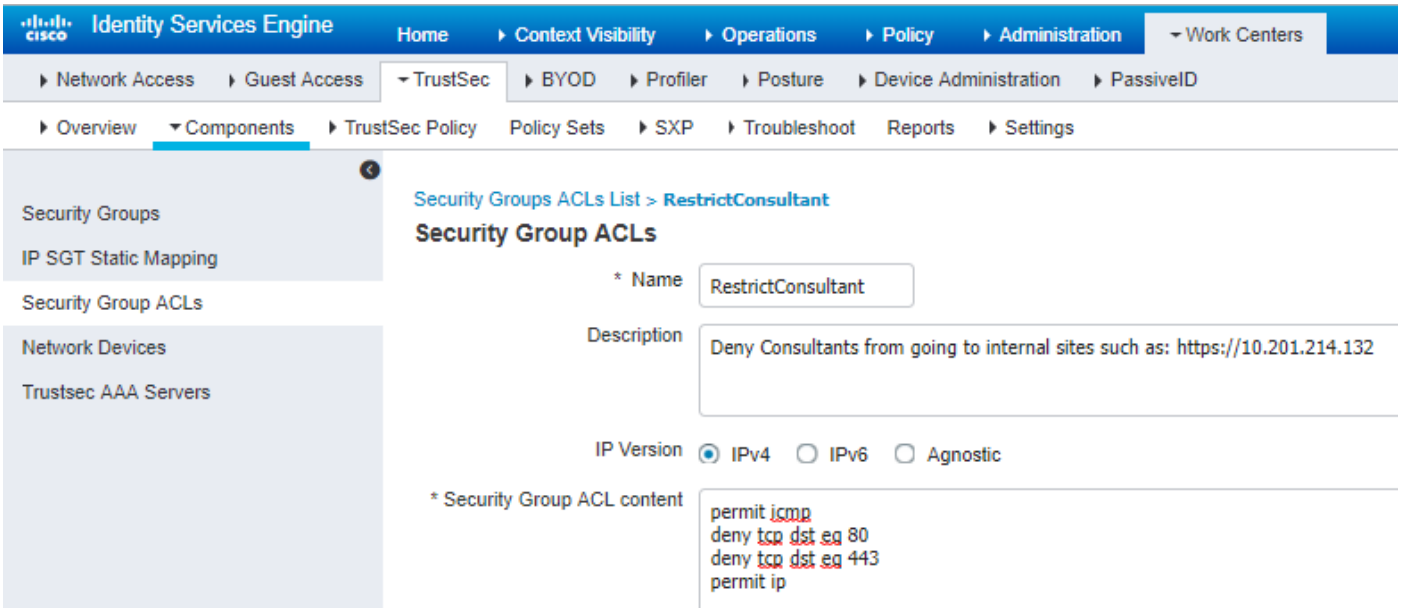


실제 디바이스(스위치 및 WLC)에 SGT 할당

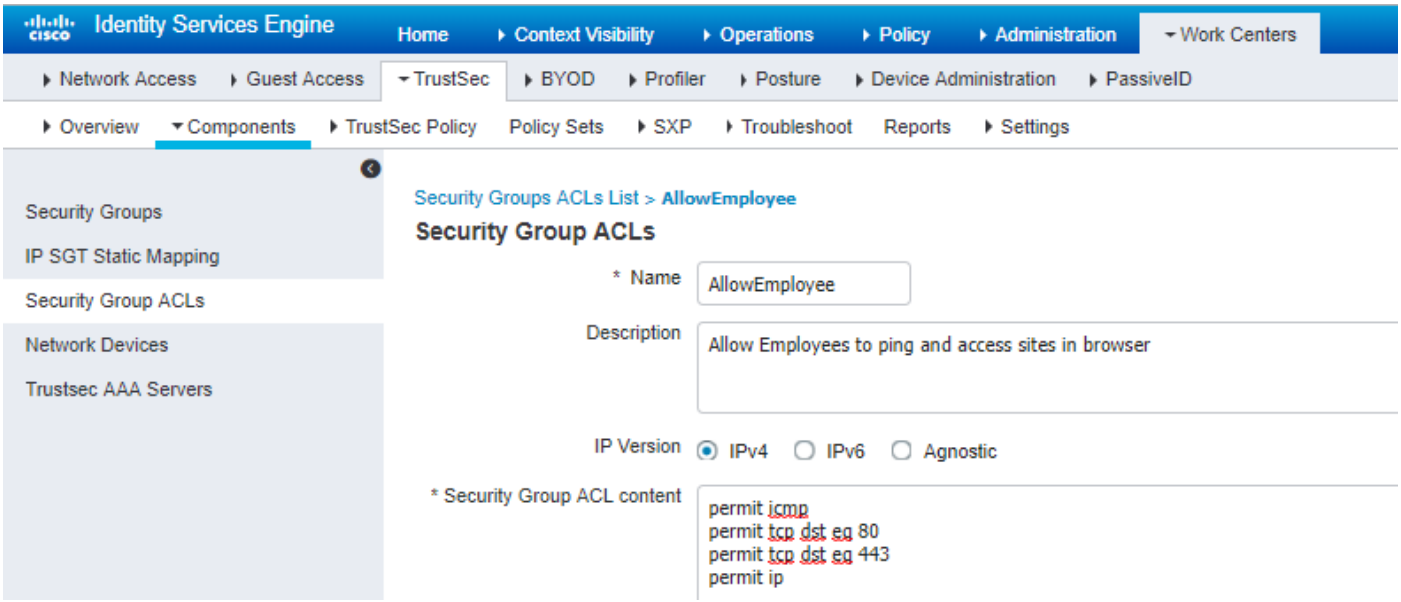


SGACL을 정의하여 이그레스 정책 지정

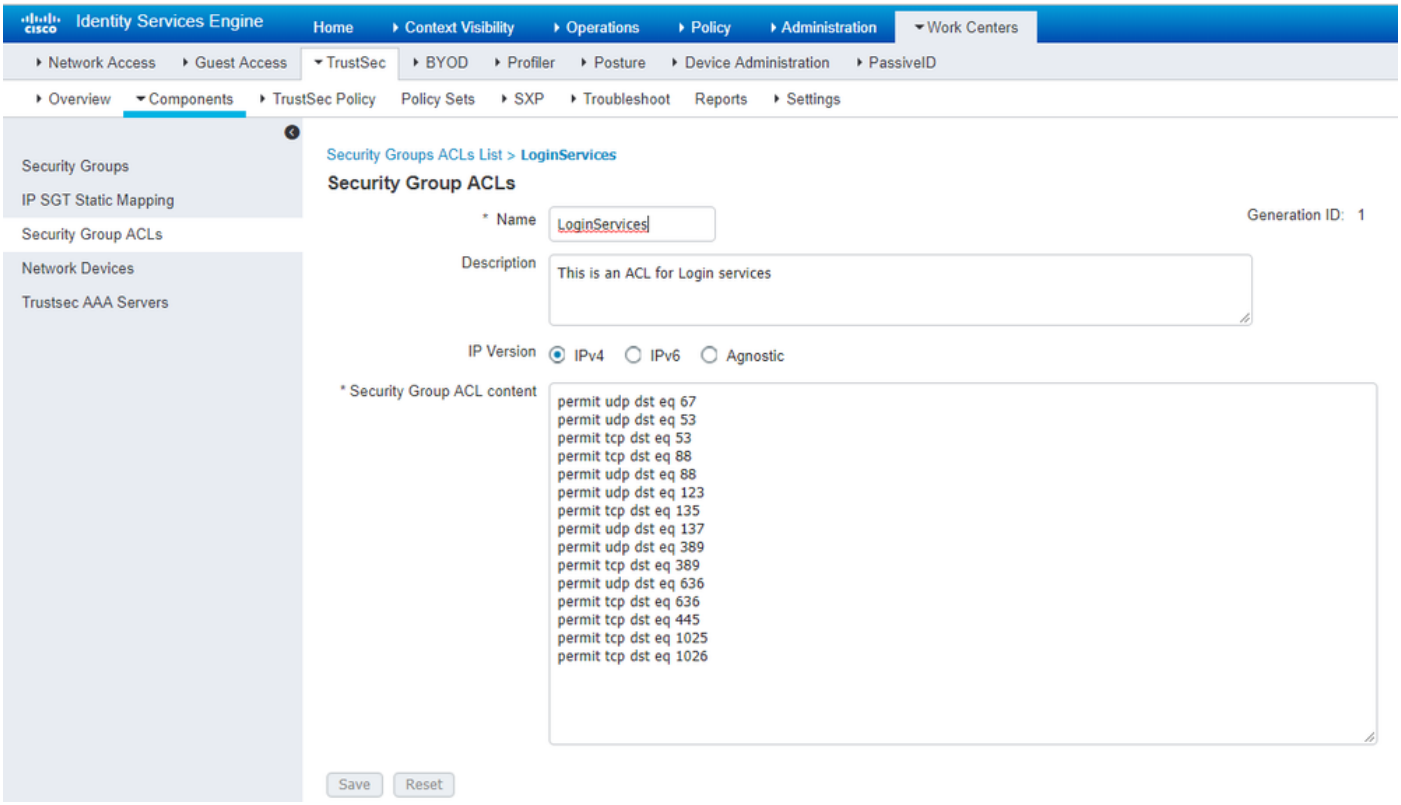
컨설턴트가 외부 어디에서나 액세스하도록 허용하되 내부 액세스는 제한합니다.



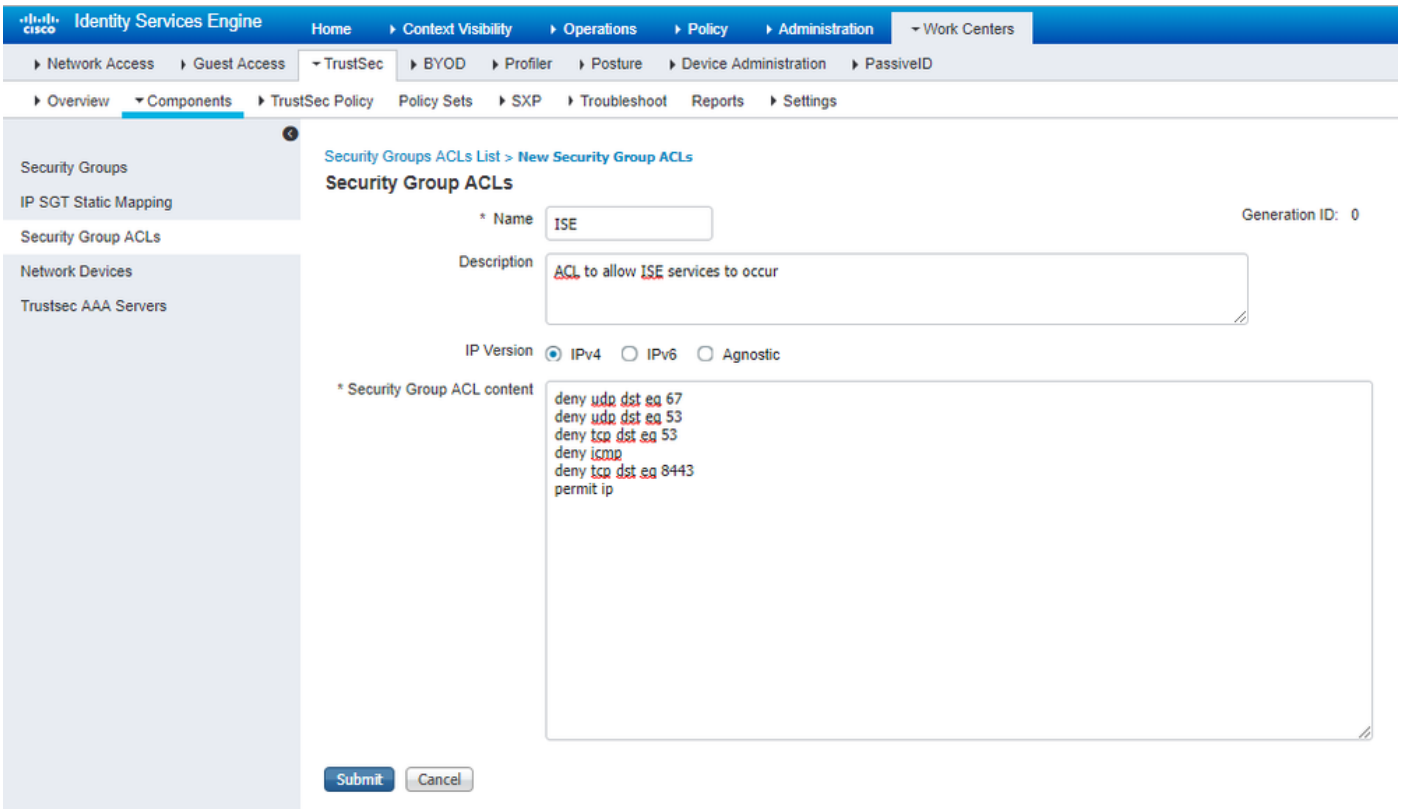
직원이 외부 및 내부 어디에서나 액세스할 수 있도록 허용:



다른 디바이스에서 기본 서비스에 액세스하도록 허용(선택 사항):



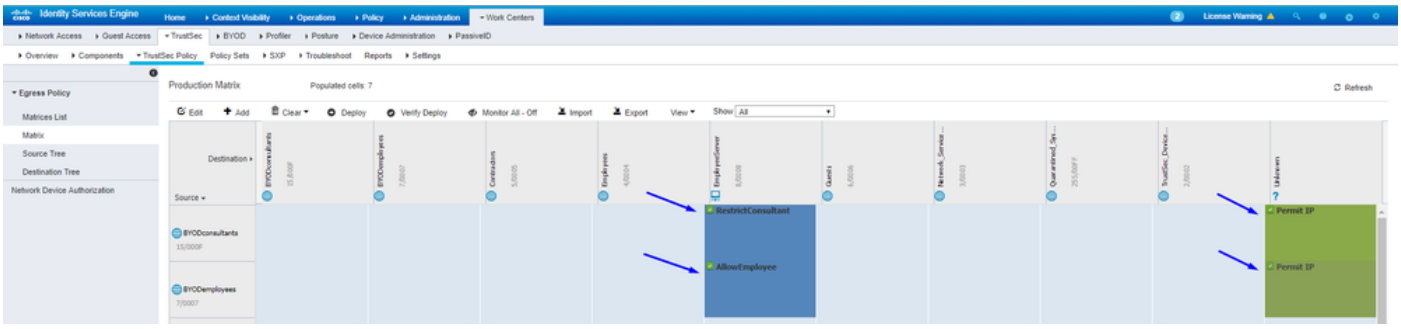
모든 최종 사용자를 Cisco ISE로 리디렉션합니다(BYOD 포털 리디렉션용). DNS, DHCP, ping 또는 WebAuth 트래픽은 Cisco ISE로 이동할 수 없으므로 포함하지 마십시오.



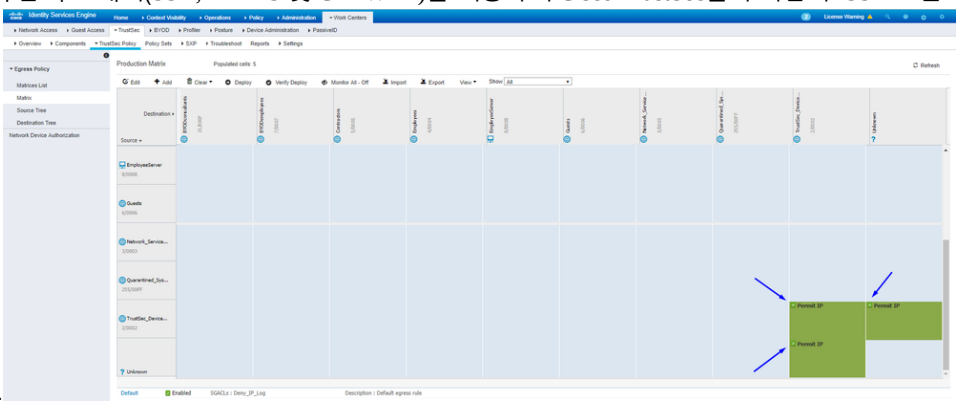
Cisco ISE의 TrustSec 정책 매트릭스에 ACL 적용

컨설턴트가 외부 어디에서나 액세스할 수 있도록 허용하지만 https://10.201.214.132과 같은 내부 웹 서버는 제한합니다.

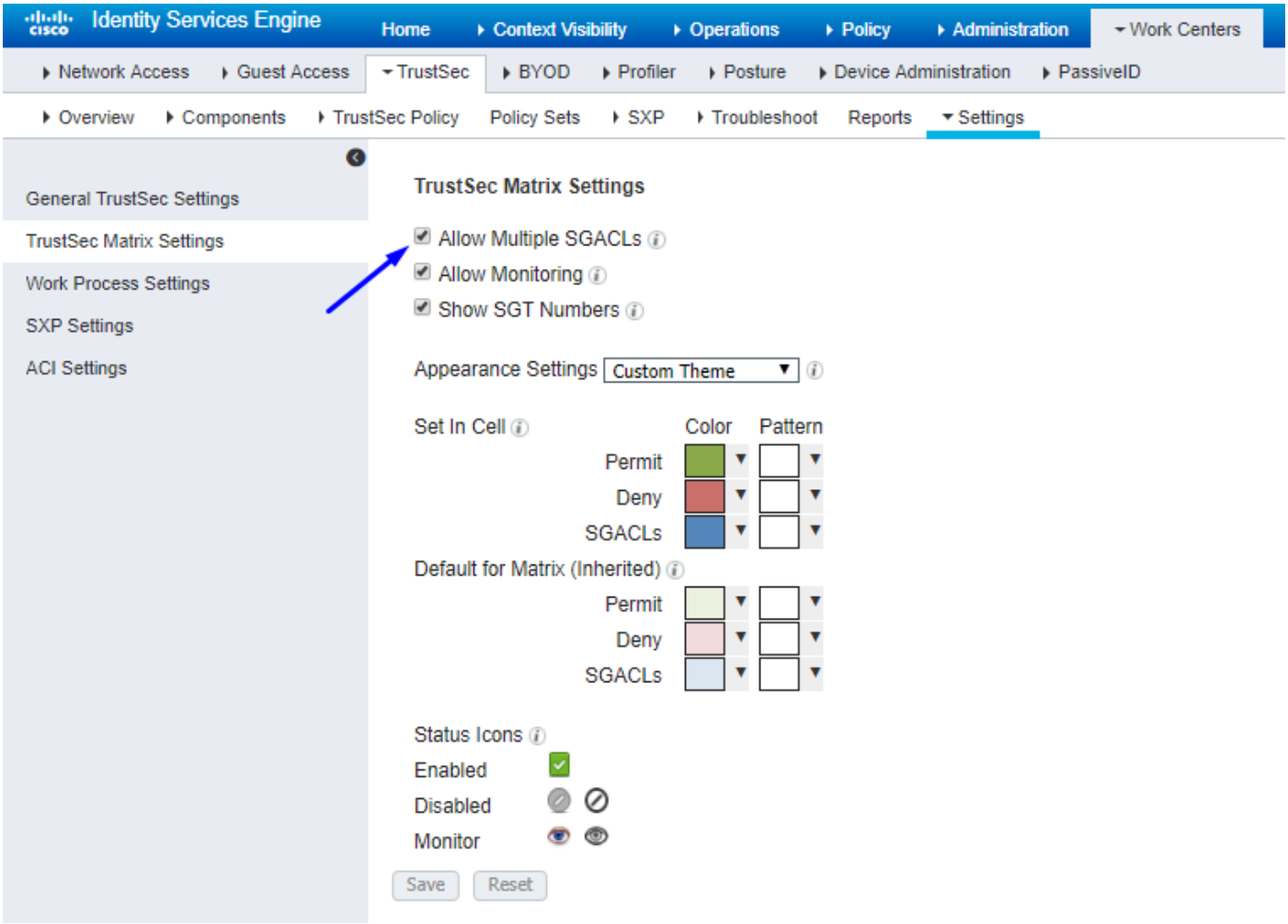
직원이 외부 어디에서나 액세스할 수 있도록 허용하고 내부 웹 서버를 허용합니다.



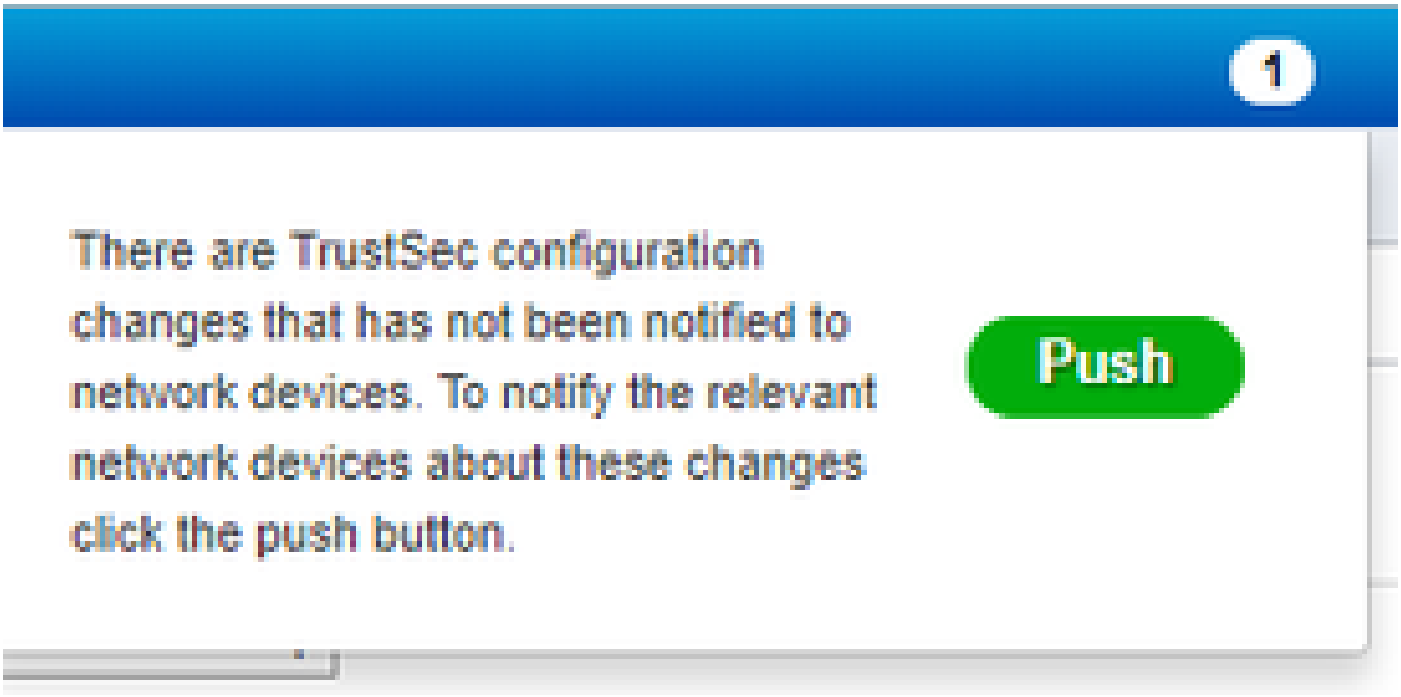
네트워크의 디바이스(스위치 및 WLC)에서 관리 트래픽(SSH, HTTPS 및 CAPWAP)을 허용하여 Cisco TrustSec을 구축한 후 SSH 또는 HTTPS 액세스가 손실되지 않도록 합니다.



Cisco ISE를 활성화하여 다음을 Allow Multiple SGACLs수행합니다.

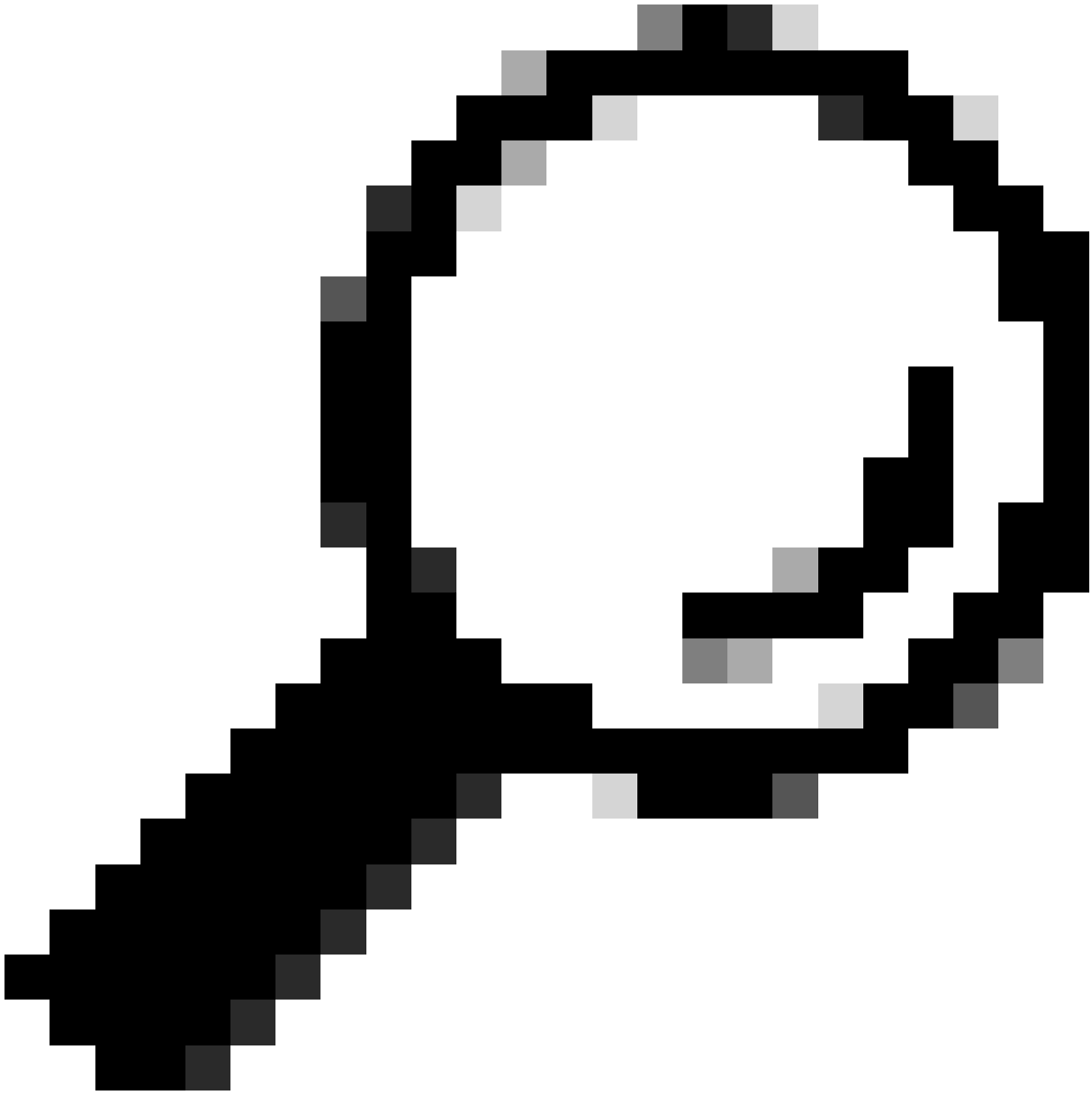


Cisco ISE의 오른쪽 상단 모서리에 있는 를 클릭하여Push 컨피그레이션을 디바이스로 푸시합니다. 이 작업은 나중에 다시 수행해야 합니다.



Catalyst 스위치에서 TrustSec 구성

Catalyst 스위치에서 AAA용 Cisco TrustSec을 사용하도록 스위치 구성



팁: 이 문서에서는 Cisco ISE에서 무선 사용자가 BYOD를 성공적으로 수행한 후 여기에 표시된 컨피그레이션을 전제로 합니다.

굵은 글꼴로 표시된 명령은 이 전에 이미 구성되었습니다(BYOD Wireless가 ISE에서 작동하기 위해).

<#root>

CatalystSwitch(config)#aaa new-model

CatalystSwitch(config)#aaa server radius policy-device

CatalystSwitch(config)#ip device tracking

CatalystSwitch(config)#radius server CISCOISE

CatalystSwitch(config-radius-server)#address ipv4 10.201.214.230 auth-port 1812 acct-port 1813

CatalystSwitch(config)#aaa group server radius AAASERVER
CatalystSwitch(config-sg-radius)#server name CISCOISE

CatalystSwitch(config)#aaa authentication dot1x default group radius
CatalystSwitch(config)#cts authorization list SGLIST
CatalystSwitch(config)#aaa authorization network SGLIST group radius

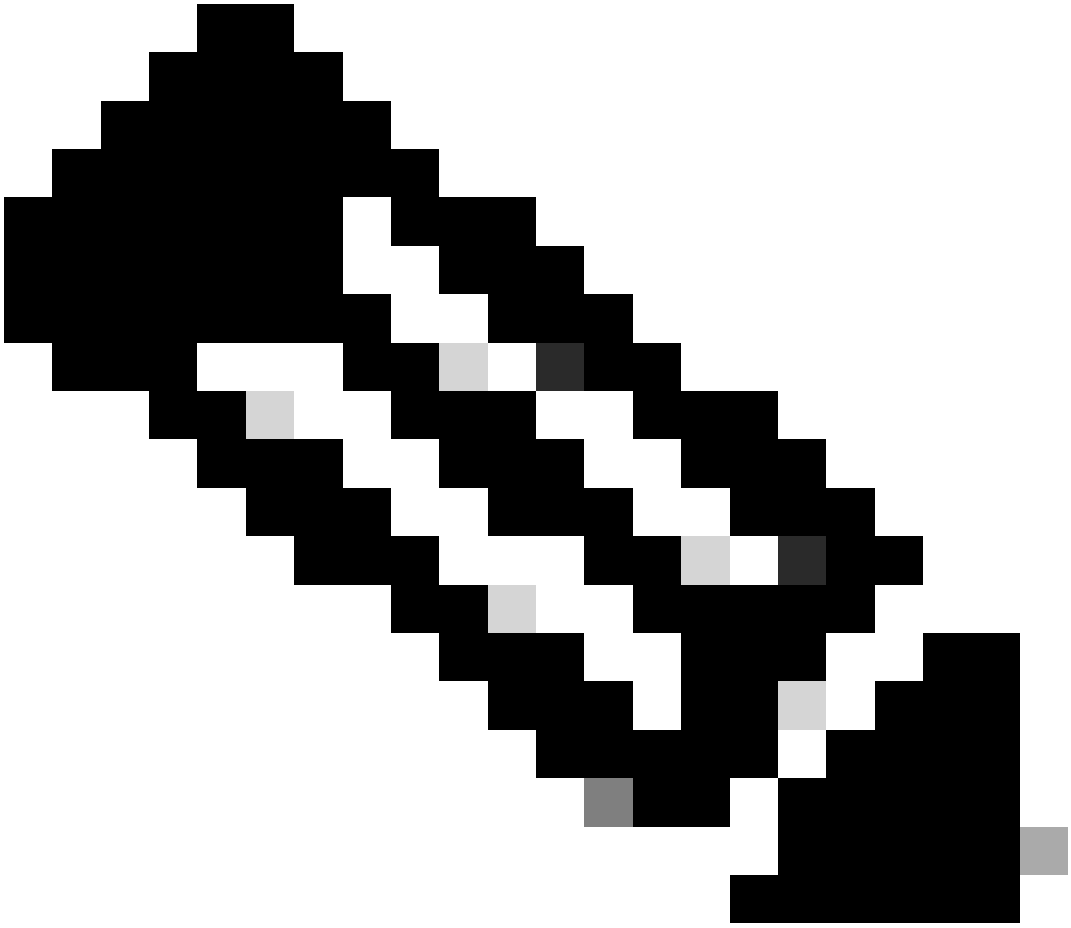
CatalystSwitch(config)#aaa authorization network default group AAASERVER

CatalystSwitch(config)#aaa authorization auth-proxy default group AAASERVER

CatalystSwitch(config)#aaa accounting dot1x default start-stop group AAASERVER

CatalystSwitch(config)#aaa server radius policy-device

CatalystSwitch(config)#aaa server radius dynamic-author
CatalystSwitch(config-locsvr-da-radius)#client 10.201.214.230 server-key Admin123



참고: PAC 키는 섹션에서 지정한 RADIUS 공유 암호와 동일해야 **Administration** > **Network Devices** > **Add Device** > **RADIUS Authentication Settings** 합니다.

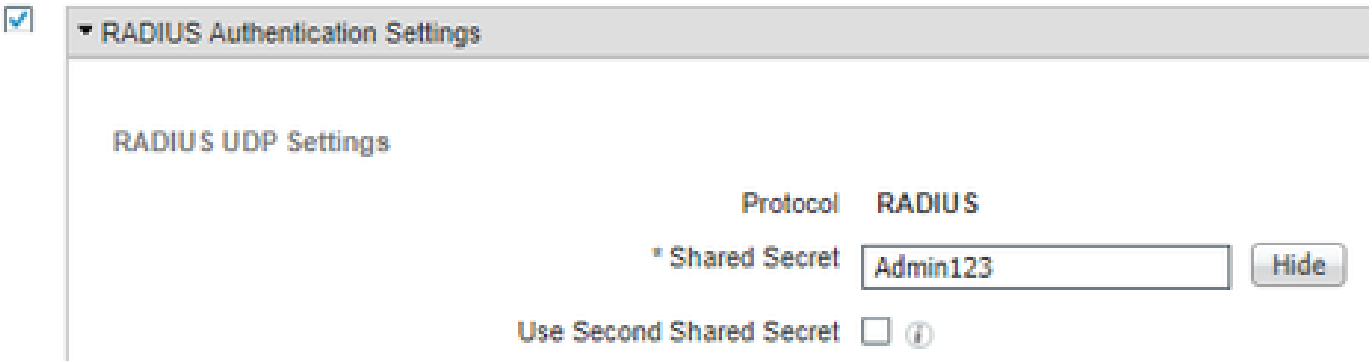
<#root>

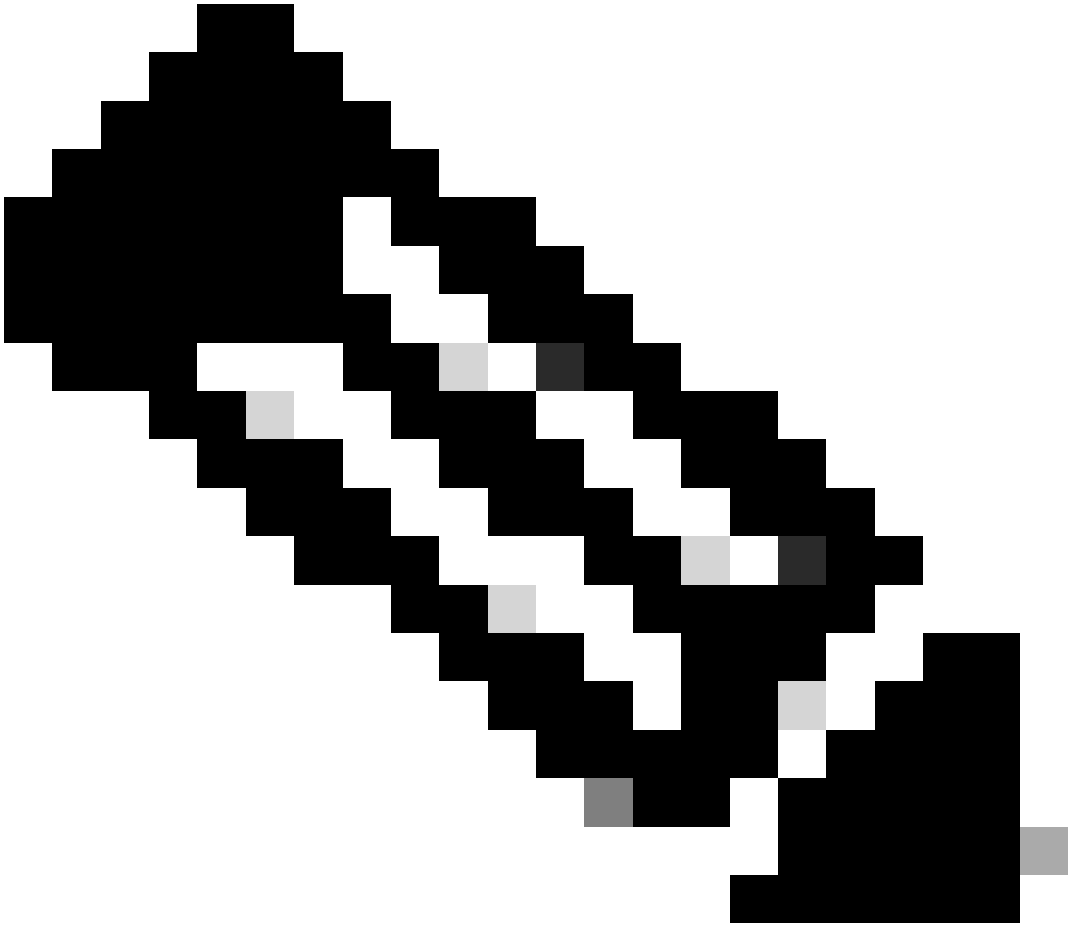
```
CatalystSwitch(config)#radius-server attribute 6 on-for-login-auth

CatalystSwitch(config)#radius-server attribute 6 support-multiple
```

```
CatalystSwitch(config)#radius-server attribute 8 include-in-access-req


CatalystSwitch(config)#radius-server attribute 25 access-request include


CatalystSwitch(config)#radius-server vsa send authentication
CatalystSwitch(config)#radius-server vsa send accounting

CatalystSwitch(config)#dot1x system-auth-control
```

Cisco ISE에 대한 스위치를 인증 하기 위해 RADIUS 서버 아래에 PAC 키를 구성 합니다

CatalystSwitch(config)#radius server CISCOISE
CatalystSwitch(config-radius-server)#address ipv4 10.201.214.230 auth-port 1812 acct-port 1813
CatalystSwitch(config-radius-server)#pac key Admin123

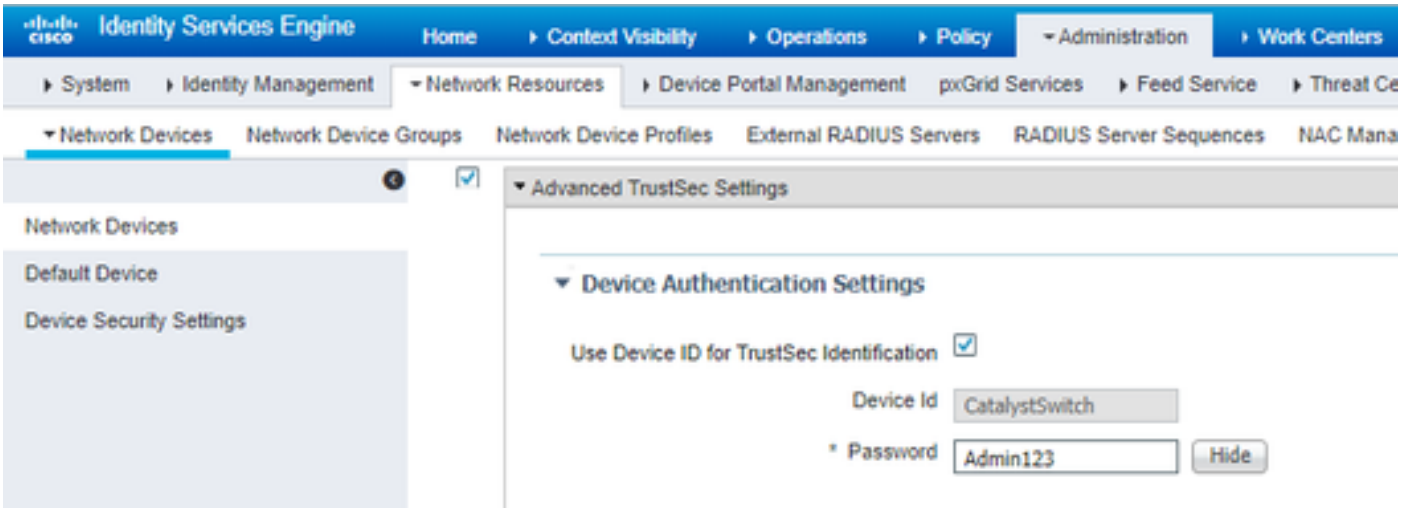


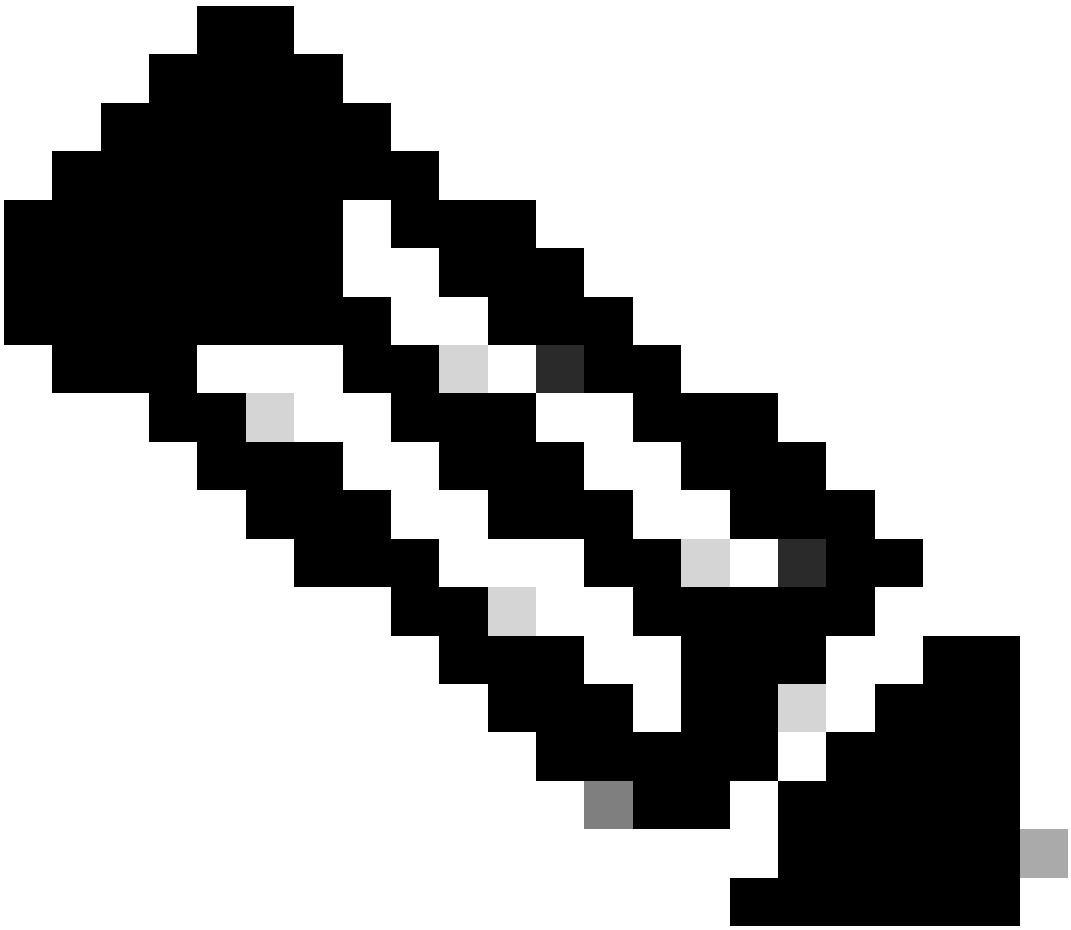


참고: PAC 키는 Cisco ISE의 **Administration > Network Devices > Add Device > RADIUS Authentication Settings** 섹션(화면 캡처에 나와 있는 것처럼)에서 지정한 RADIUS 공유 암호와 동일해야 합니다.

Cisco ISE에 대한 스위치를 인증 하기 위해 CTS 자격 증명 구성

CatalystSwitch#cts credentials id CatalystSwitch password Admin123





참고: CTS 자격 증명은 CTS 자격 증명에서 지정한 장치 ID + 암호와 동일해야 합니다. CTS 자격 증명은 Cisco ISE의 Administration > Network Devices > Add Device > Advanced TrustSec Settings 섹션(화면 캡처에 표시됨)에서 지정한 장치 ID

+ 암호와 동일해야 합니다.

그런 다음 PAC를 새로고침하여 Cisco ISE에 다시 연결합니다.

```
CatalystSwitch(config)#radius server CISCOISE
CatalystSwitch(config-radius-server)#exit
 Request successfully sent to PAC Provisioning driver.
```

Catalyst 스위치에서 CTS Globally 활성화

```
CatalystSwitch(config)#cts role-based enforcement
CatalystSwitch(config)#cts role-based enforcement vlan-list 1115 (choose the vlan that your end user devices are on only)
```

제한된 웹 서버에 대해 정적 IP에서 SGT로의 매핑 설정(선택 사항)

이 제한된 웹 서버는 인증을 위해 ISE를 통과하지 않으므로 Cisco의 여러 웹 서버 중 하나인 스위치 CLI 또는 ISE 웹 GUI를 사용하여 수동으로 태그를 지정해야 합니다.

```
CatalystSwitch(config)#cts role-based sgt-map 10.201.214.132 sgt 8
```

Catalyst 스위치에서 TrustSec 확인

```
CatalystSwitch#show cts pac
 AID: EF2E1222E67EB4630A8B22D1FF0216C1
 PAC-Info:
 PAC-type = Cisco Trustsec
 AID: EF2E1222E67EB4630A8B22D1FF0216C1
 I-ID: CatalystSwitch
 A-ID-Info: Identity Services Engine
 Credential Lifetime: 23:43:14 UTC Nov 24 2018
 PAC-Opaque: 000200B800030001000400010EF2E1222E67EB4630A8B22D1FF0216C10006009C0003010025D40D409A0DDAF352A3F1A9884AC3F6
 Refresh timer is set for 12w5d
```

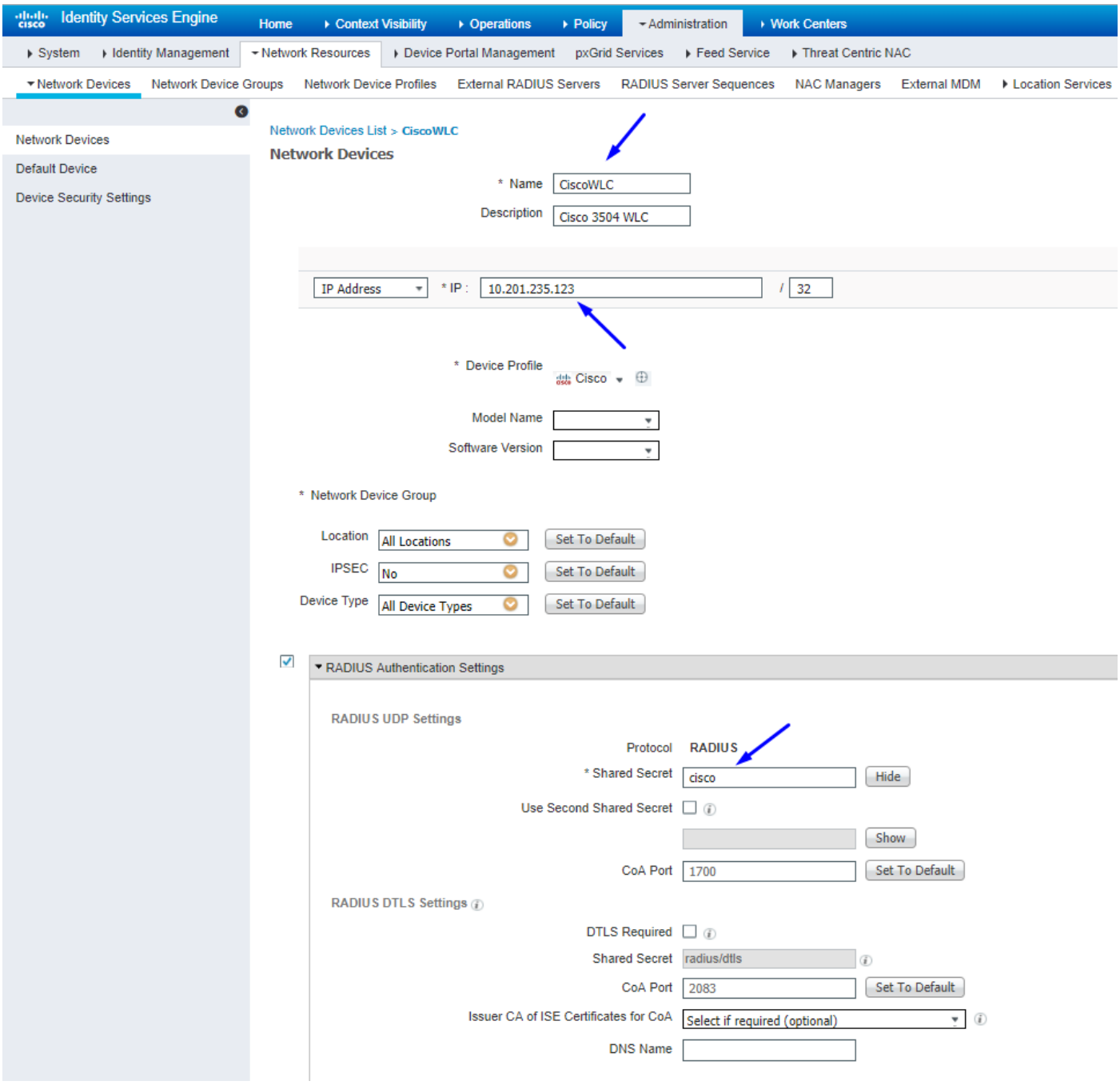
```
CatalystSwitch#cts refresh environment-data
Environment data download in progress
```

```
CatalystSwitch#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 2-02:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.201.214.230, port 1812, A-ID EF2E1222E67EB4630A8B22D1FF0216C1
 Status = ALIVE flag(0x11)
 auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
 0001-31 :
 0-00:Unknown
 2-00:TrustSec_Devices
 3-00:Network_Services
 4-00:Employees
 5-00:Contractors
 6-00:Guests
 7-00:BYODemployees
 8-00:EmployeeServer
 15-00:BYODconsultants
 255-00:Quarantined_Systems
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 86400 secs
Last update time = 16:04:29 UTC Sat Aug 25 2018
Env-data expires in 0:23:57:01 (dd:hr:mm:sec)
Env-data refreshes in 0:23:57:01 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

```
CatalystSwitch#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address SGT Source
============================================
10.201.214.132 8 CLI
10.201.235.102 2 INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of CLI bindings = 1
Total number of INTERNAL bindings = 1
Total number of active bindings = 2
```

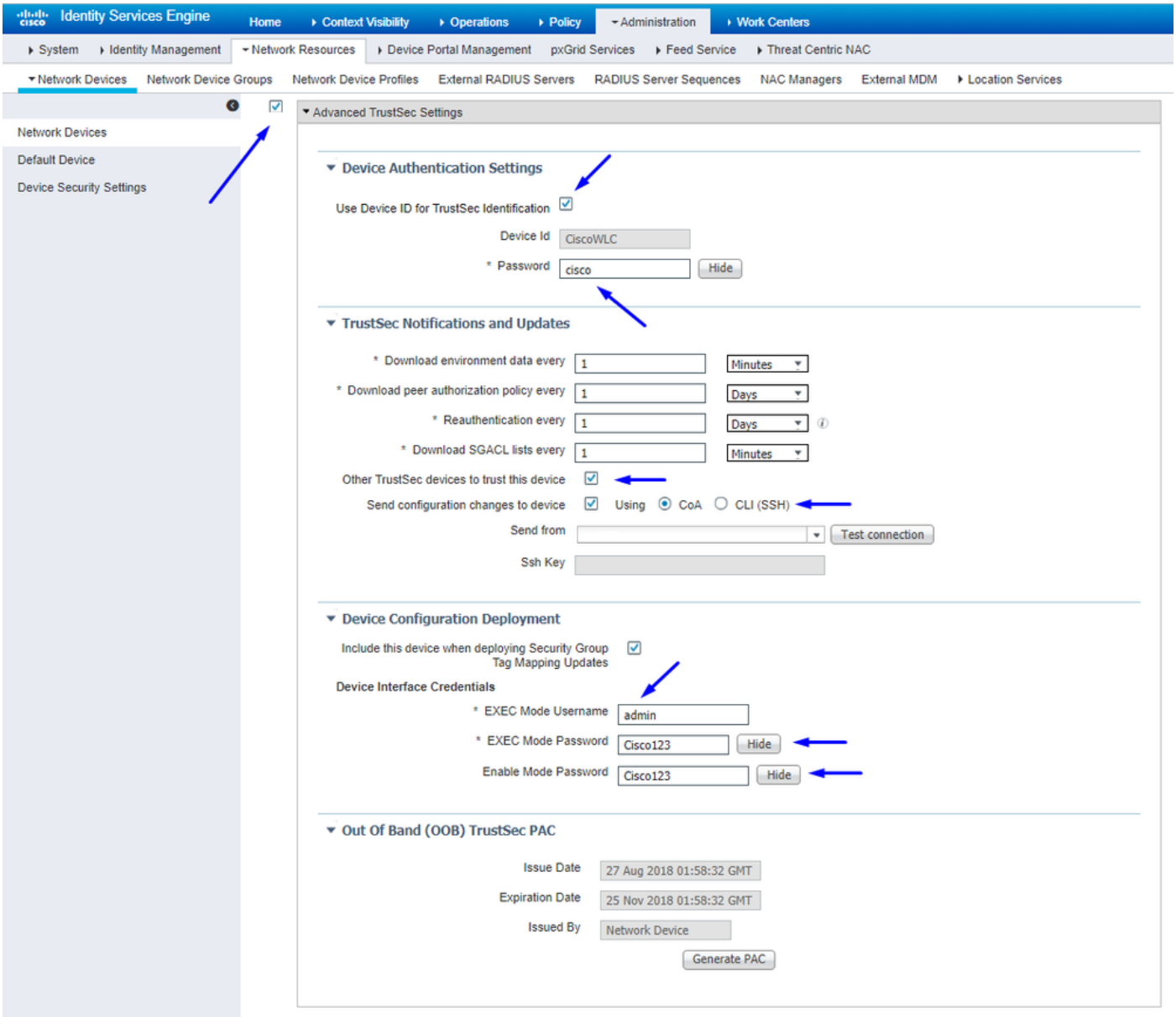
WLC에서 TrustSec 구성

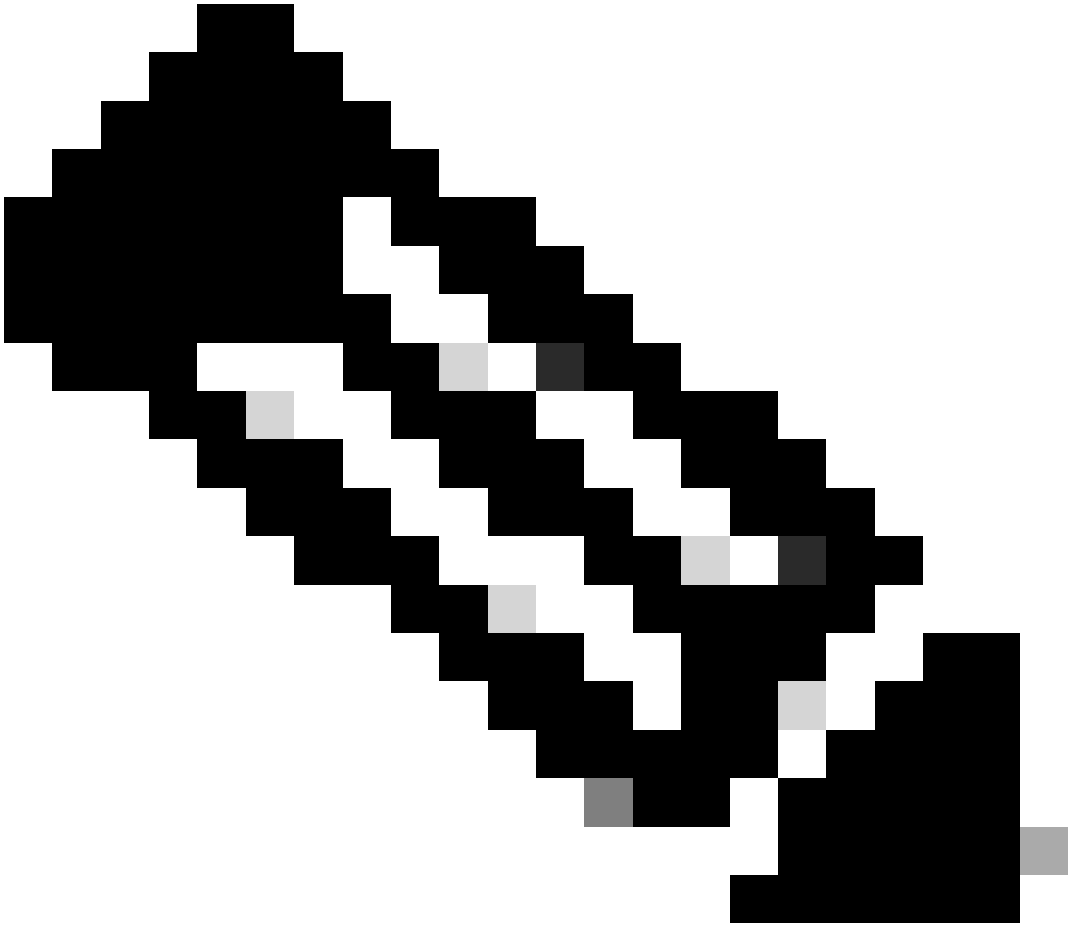
Cisco ISE에서 WLC가 RADIUS 디바이스로 추가되었는지 구성 및 확인



Cisco ISE에서 WLC가 TrustSec 디바이스로 추가되었는지 구성 및 확인

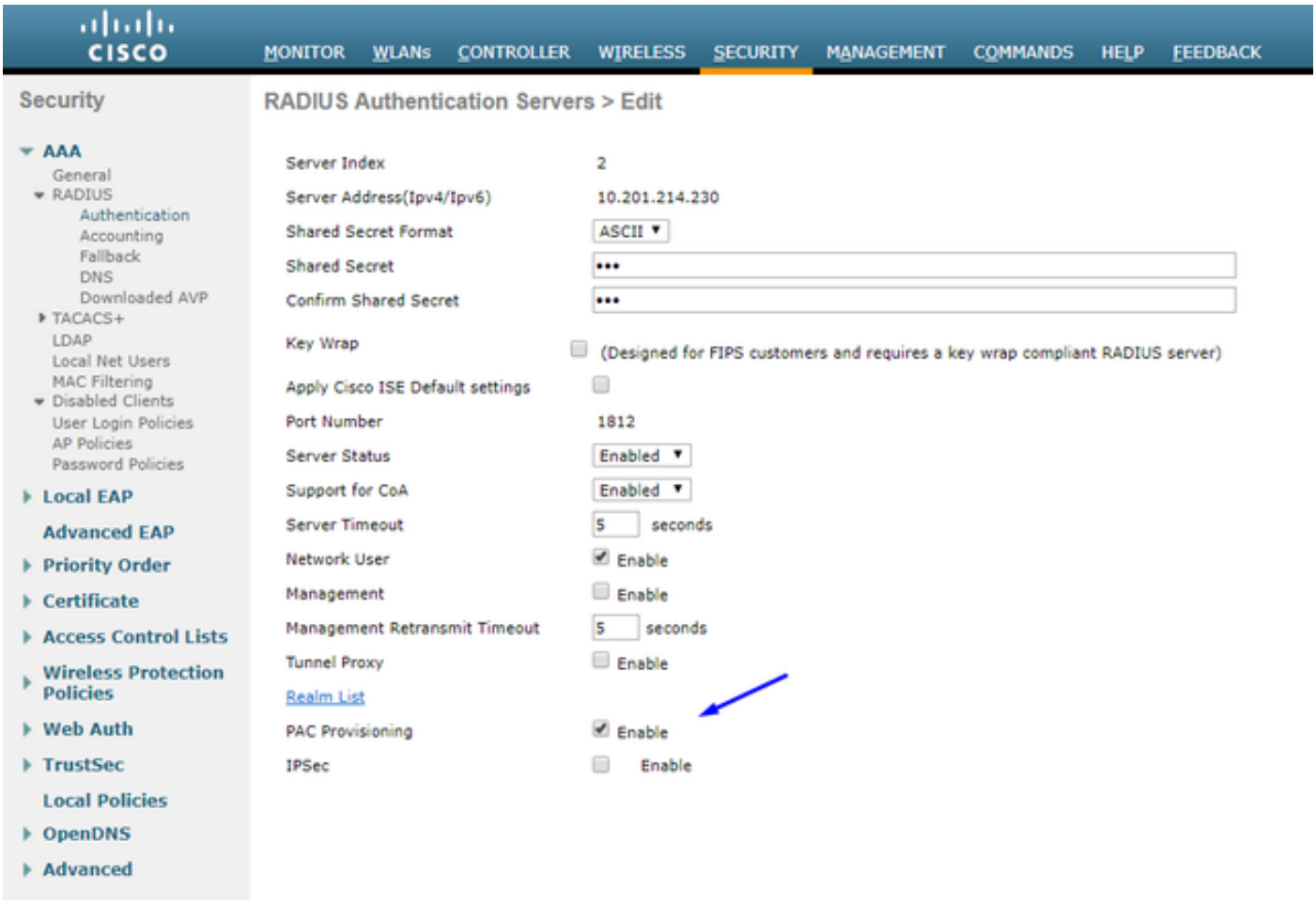
이 단계를 통해 Cisco ISE는 WLC에 정적 IP에서 SGT 매핑으로 구축할 수 있습니다. 이전 단계에서 Cisco ISE 웹 GUI의 **Work Centers(작업 센터) > TrustSec > Components(구성 요소) > IP SGT Static Mappings(IP SGT 정적 매핑)**에서 이러한 매핑을 생성했습니다.


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
External MDM
Location Services
Network Devices
Default Device
Device Security Settings
Advanced TrustSec Settings
Device Authentication Settings
Use Device ID for TrustSec Identification
Device Id
CiscoWLC
* Password
cisco
Hide
TrustSec Notifications and Updates
* Download environment data every
1
Minutes
* Download peer authorization policy every
1
Days
* Reauthentication every
1
Days
* Download SGACL lists every
1
Minutes
Other TrustSec devices to trust this device
Send configuration changes to device
Using
CoA
CLI (SSH)
Send from
Test connection
Ssh Key
Device Configuration Deployment
Include this device when deploying Security Group Tag Mapping Updates
Device Interface Credentials
* EXEC Mode Username
admin
* EXEC Mode Password
Cisco123
Hide
Enable Mode Password
Cisco123
Hide
Out Of Band (OOB) TrustSec PAC
Issue Date
27 Aug 2018 01:58:32 GMT
Expiration Date
25 Nov 2018 01:58:32 GMT
Issued By
Network Device
Generate PAC

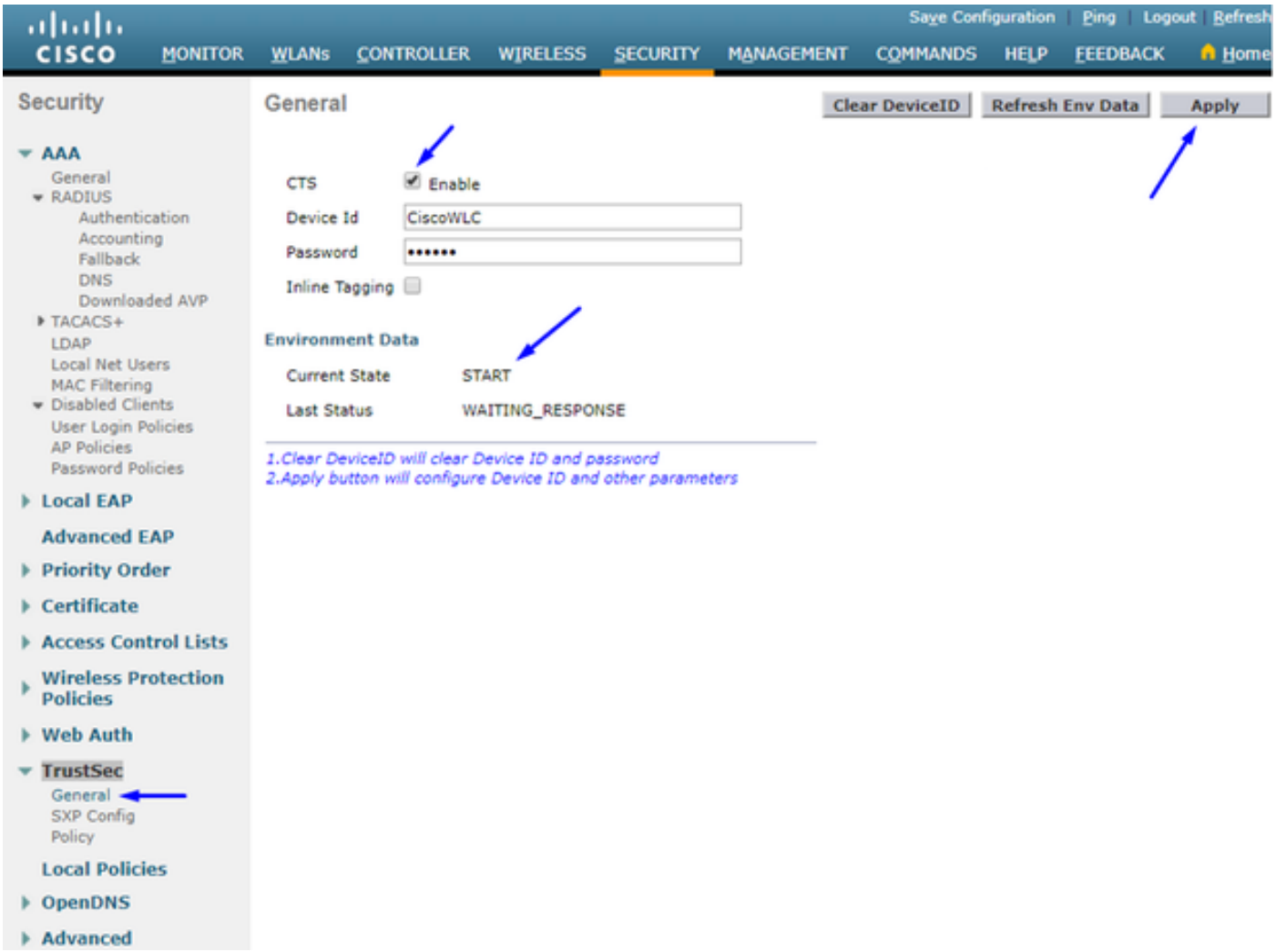


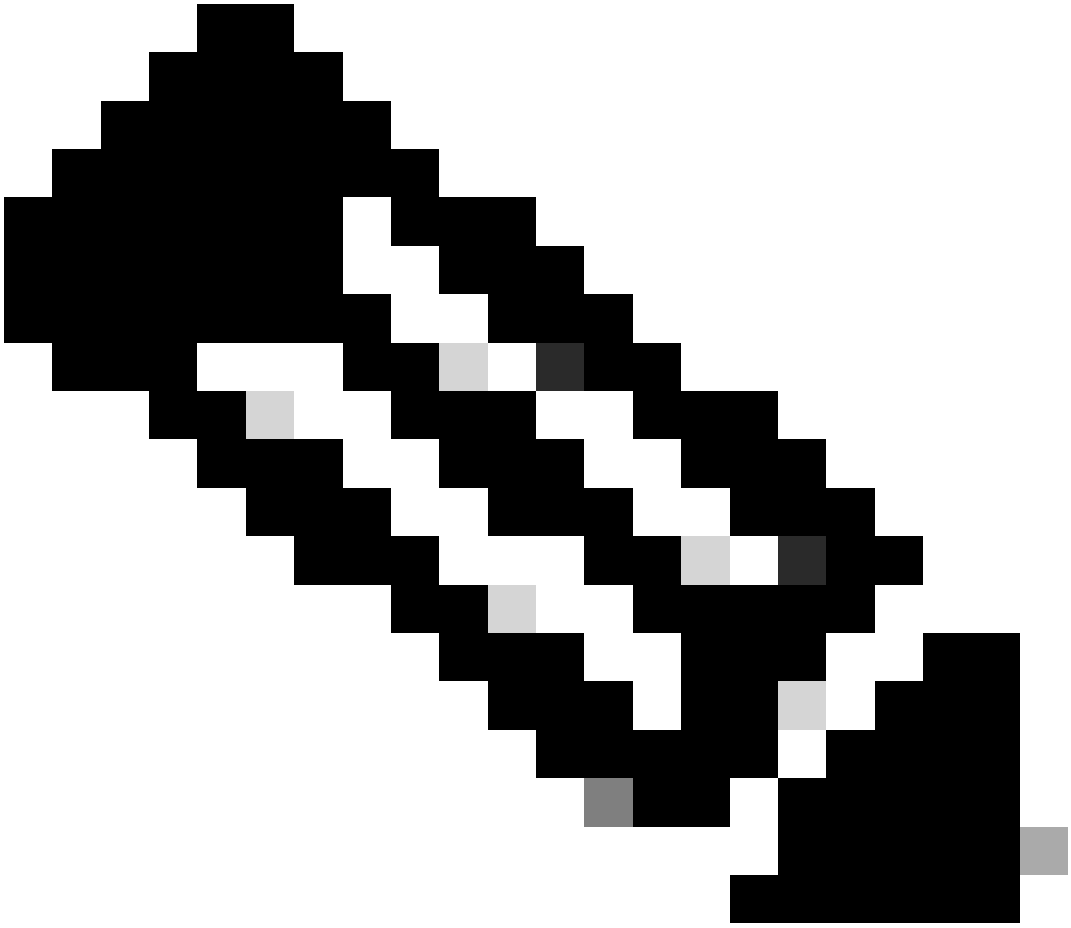
참고: 이 Device ld 와 Password 이후의 WLC 웹 UI에서Security > TrustSec > General 이를 사용합니다.

WLC의 PAC 프로비저닝 활성화



WLC에서 TrustSec 사용

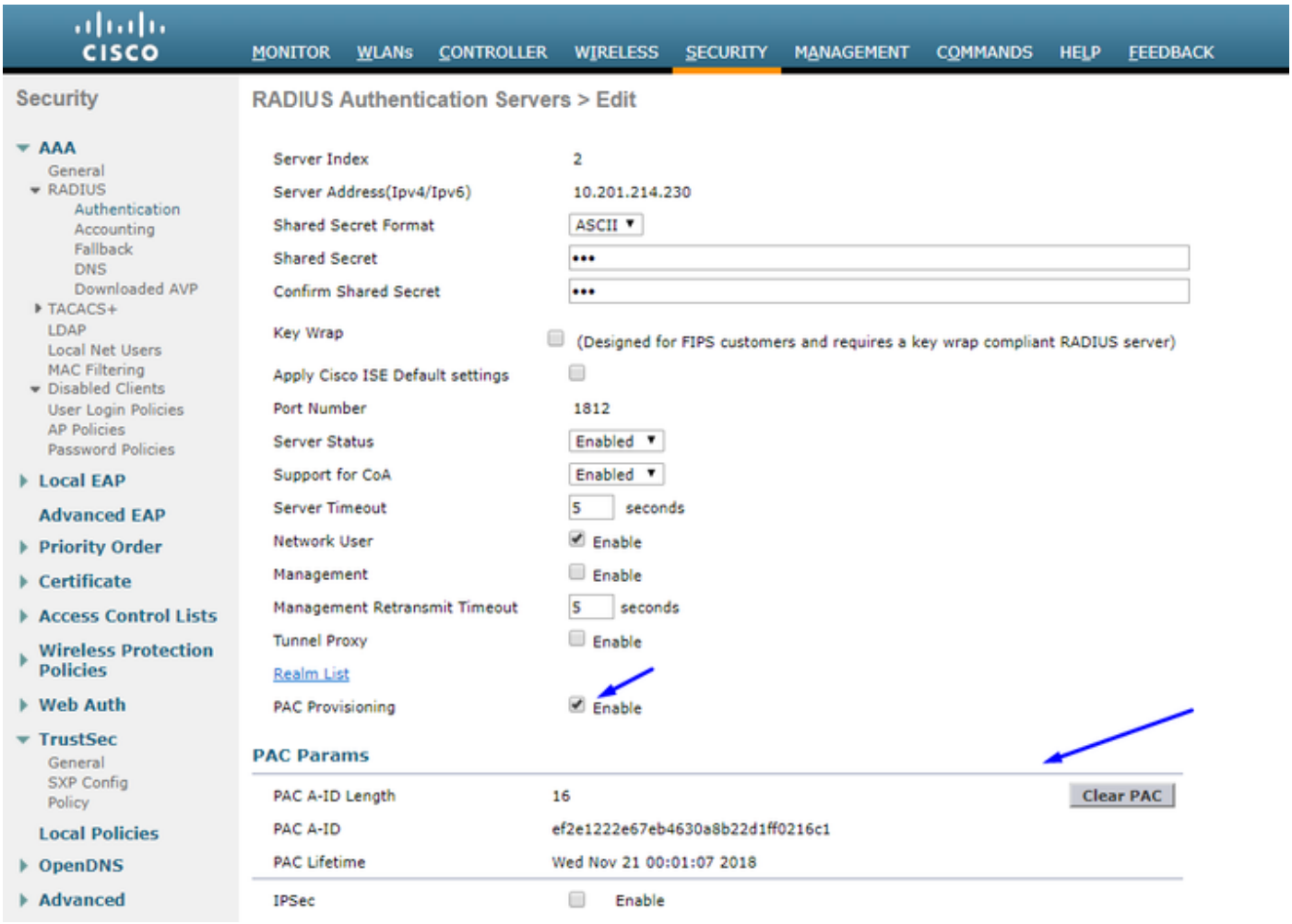

Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
TrustSec
General
SXP Config
Policy
Local Policies
OpenDNS
Advanced
General
Clear DeviceID
Refresh Env Data
Apply
CTS
Enable
Device Id
CiscoWLC
Password
Inline Tagging
Environment Data
Current State
START
Last Status
WAITING_RESPONSE
1.Clear DeviceID will clear Device ID and password
2.Apply button will configure Device ID and other parameters



참고: CTS Device Id 및 Password 는 Cisco ISE의 섹션에서 Device Id Password 지정한 Administration > Network Devices > Add Device > Advanced TrustSec Settings와 같아야 합니다.

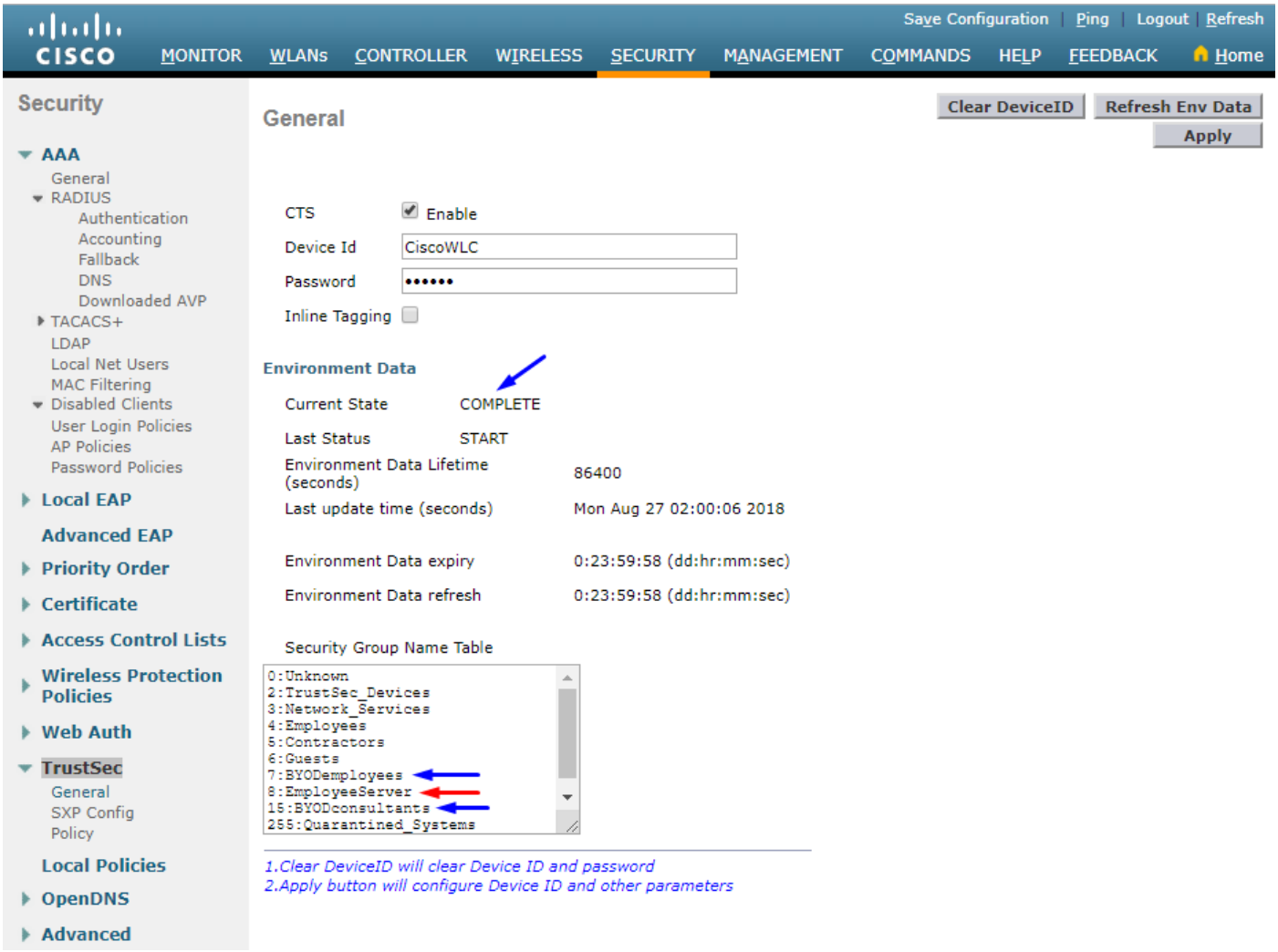
PAC가 WLC에 프로비저닝되었는지 확인

다음을 클릭하면 WLC에 PAC가 성공적으로 Refresh Env Data 프로비저닝된 것을 확인할 수 있습니다(이 단계에서 수행).



Cisco ISE에서 WLC로 CTS 환경 데이터 다운로드

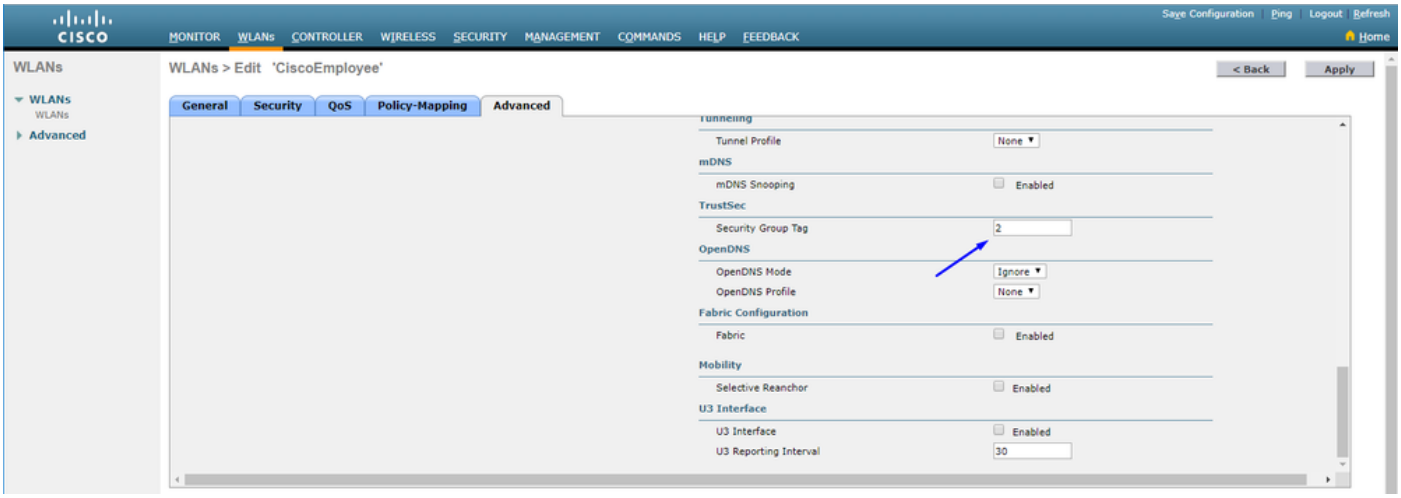
를 클릭하면 Refresh Env Data WLC에서 SGT를 다운로드합니다.



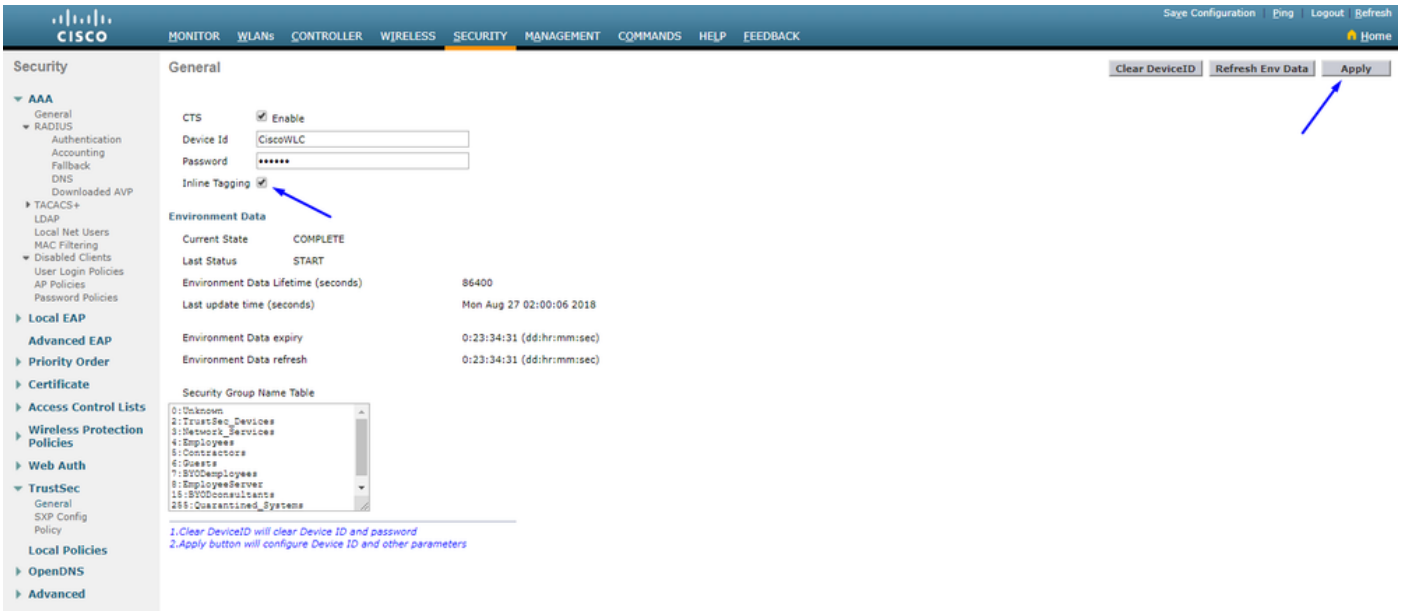
SGACL 다운로드 및 트래픽에 대한 시행 활성화

WLC 및 액세스 포인트에 SGT 2개 할당(TrustSec_Devices)

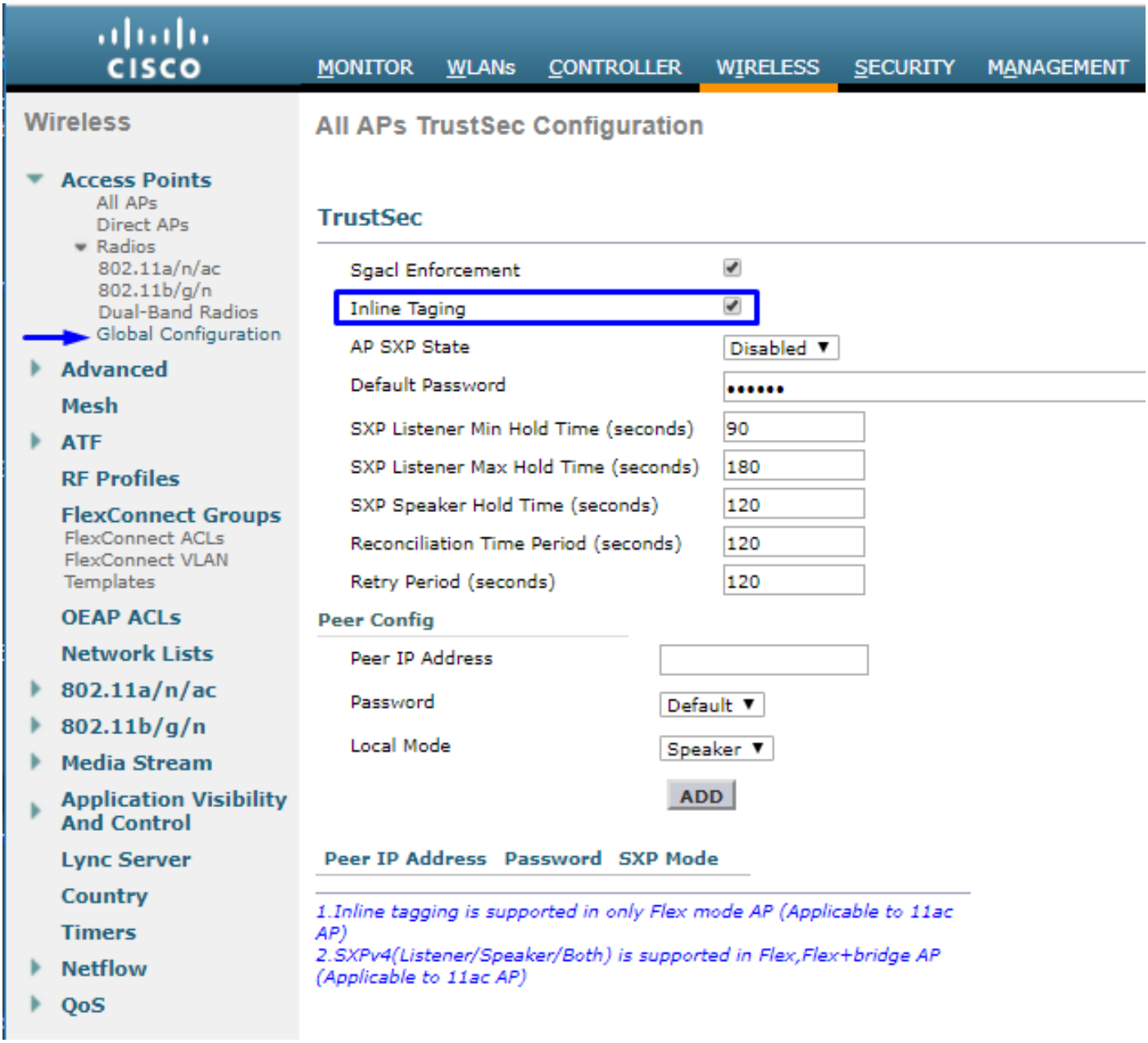
스위치를 통해 WLC + AP로/로부터 트래픽(SSH, HTTPS 및 CAPWAP)을 허용하기 위해 WLC + WLAN에 SGT 2(TrustSec_Devices)를 지정합니다.



WLC에서 인라인 태깅 사용



아래에서 **Wireless** > **Access Points** > **Global Configuration** 아래로 스크롤하여 를 **TrustSec Config**선택합니다.



Catalyst 스위치에서 인라인 태깅 활성화

<#root>

CatalystSwitch(config)#interface TenGigabitEthernet1/0/48

CatalystSwitch(config-if)#description goestoWLC

CatalystSwitch(config-if)#switchport trunk native vlan 15

CatalystSwitch(config-if)#switchport trunk allowed vlan 15,455,463,1115

CatalystSwitch(config-if)#switchport mode trunk

```
CatalystSwitch(config-if)#cts role-based enforcement
CatalystSwitch(config-if)#cts manual
CatalystSwitch(config-if-cts-manual)#policy static sgt 2 trusted
```

다음을 확인합니다.

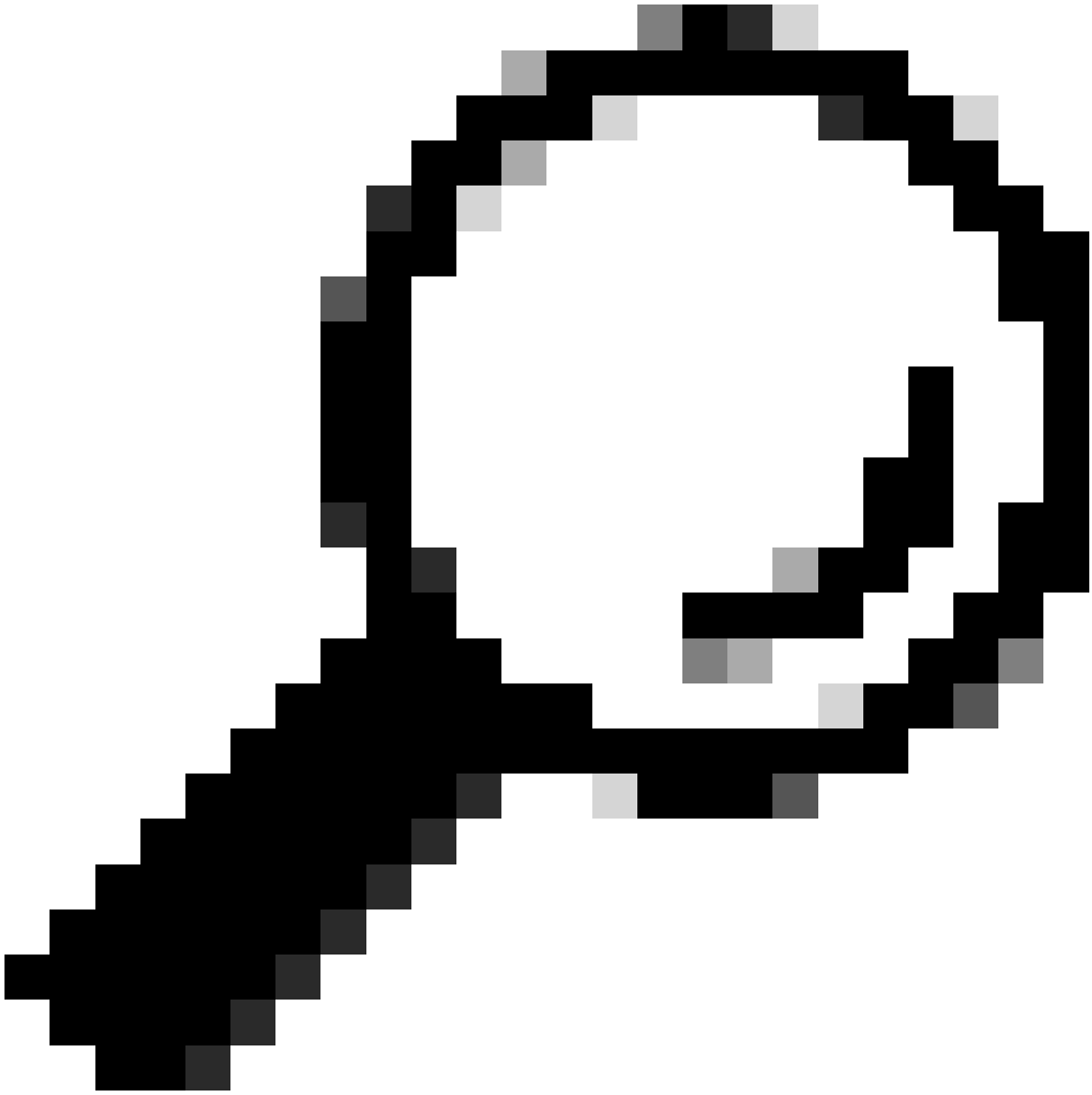
CatalystSwitch#show platform acl counters 하드웨어 | SGACL 포함

이그레스 IPv4 SGACL 삭제(454): 10프레임

이그레스 IPv6 SGACL 삭제(455): 0 프레임

이그레스 IPv4 SGACL 셀 삭제(456): 0 프레임

이그레스 IPv6 SGACL 셀 삭제(457): 0 프레임



팁: Cisco ASR, Nexus 또는 Cisco ASA를 대신 사용하는 경우 여기에 나열된 문서를 통해 SGT 태그가 적용되었는지 확인할 수 있습니다. TrustSec 문제 해결 가이드.

사용자 이름 jsmith 비밀번호 Admin123으로 무선 인증 - 스위치에 거부 ACL이 있습니다.

This site can't be reached

10.201.214.132 took too long to respond.

Try:

Checking the connection

ERR_CONNECTION_TIMED_OUT

RELOAD

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.