

TrustSec 기반 정책을 위해 여러 ISE 클러스터를 Secure Web Appliance와 통합

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[제한 사항](#)

[네트워크 다이어그램](#)

[구성](#)

[ISE 구성](#)

[SXP 활성화](#)

[클러스터 노드에서 SXP 구성](#)

[어그리게이션 노드에서 SXP 구성](#)

[집계 노드에서 pxGrid를 활성화합니다.](#)

[pxGrid 자동 승인](#)

[네트워크 디바이스 TrustSec 설정](#)

[네트워크 디바이스 권한 부여](#)

[SGT](#)

[권한 부여 정책](#)

[ISE 어그리게이션 노드에서 ERS 활성화\(선택 사항\)](#)

[ESR 관리 그룹에 사용자 추가\(선택 사항\)](#)

[보안 웹 어플라이언스 컨피그레이션](#)

[pxGrid 인증서](#)

[Secure Web Appliance에서 SXP 및 ERS 활성화](#)

[식별 프로필](#)

[SGT 기반 암호 해독 정책](#)

[스위치 구성](#)

[AAA](#)

[트러스트섹\(TrustSec\)](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 TrustSec 구축에서 SGT 기반 웹 액세스 정책을 활용하기 위해 여러 ISE 구축의 SGT(Security Group Tag) 정보를 pxGrid를 통해 단일 Cisco Secure Web Appliance(기존의 WSA)로 전송하는 절차에 대해 설명합니다.

14.5 이전 버전에서는 Secure Web Appliance가 SGT 기반의 ID 정책을 위해 단일 ISE 클러스터와만 통합할 수 있습니다. 이 새로운 버전이 출시됨에 따라 Secure Web Appliance는 이제 여러 ISE 클러스터의 정보와 상호 운용될 수 있으며, 이 정보를 집계하는 별도의 ISE 노드가 있습니다. 이를

통해 다양한 ISE 클러스터에서 사용자 데이터를 내보낼 수 있으며 1:1 통합 없이 사용자가 사용할 수 있는 종료 지점을 자유롭게 제어할 수 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Identity Services Engine(ISE)
- 보안 웹 어플라이언스
- RADIUS 프로토콜
- 트러스트섹(TrustSec)
- pxGrid

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

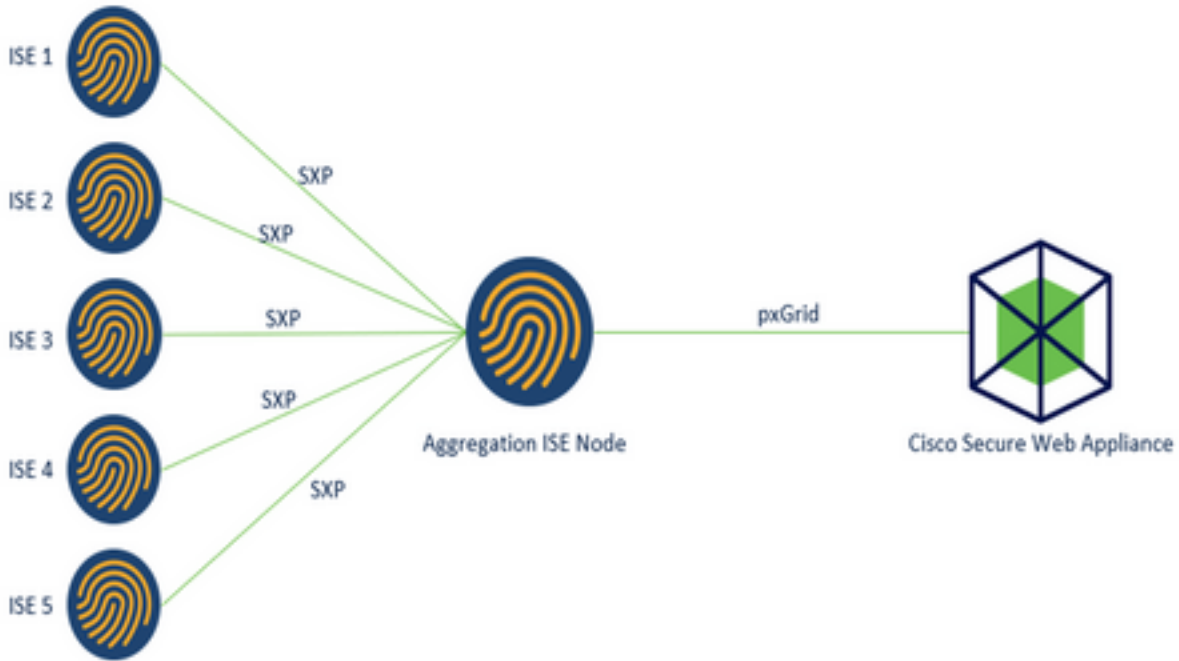
- Secure Web Appliance 14.5
- ISE 버전 3.1 P3

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.

제한 사항

1. 모든 ISE 클러스터는 SGT에 대해 균일한 매핑을 유지 관리해야 합니다.
2. ISE 어그리게이션 노드에는 나머지 ISE 클러스터의 SGT 이름/번호가 있어야 합니다.
3. Secure Web Appliance는 SGT 태그를 기반으로 정책(액세스/암호 해독/라우팅)만 식별할 수 있으며 그룹이나 사용자 이름은 식별할 수 없습니다.
4. 보고 및 추적은 SGT 기반입니다.
5. 기존 ISE/Secure Web Appliance 크기 조정 매개변수는 이 기능에 계속 적용됩니다.

네트워크 다이어그램



프로세스:

1. 최종 사용자가 네트워크에 연결하면 ISE의 권한 부여 정책에 따라 SGT를 수신합니다.
2. 다른 ISE 클러스터는 SXP를 통해 ISE 어그리게이션 노드로 SGT-IP 매핑 형식으로 이 SGT 정보를 전송합니다.
3. ISE Aggregation Node가 이 정보를 수신하여 pxGrid를 통해 단일 Secure Web Appliance와 공유합니다.
4. Secure Web Appliance는 웹 액세스 정책을 기반으로 사용자에게 액세스를 제공하기 위해 학습한 SGT 정보를 사용합니다.

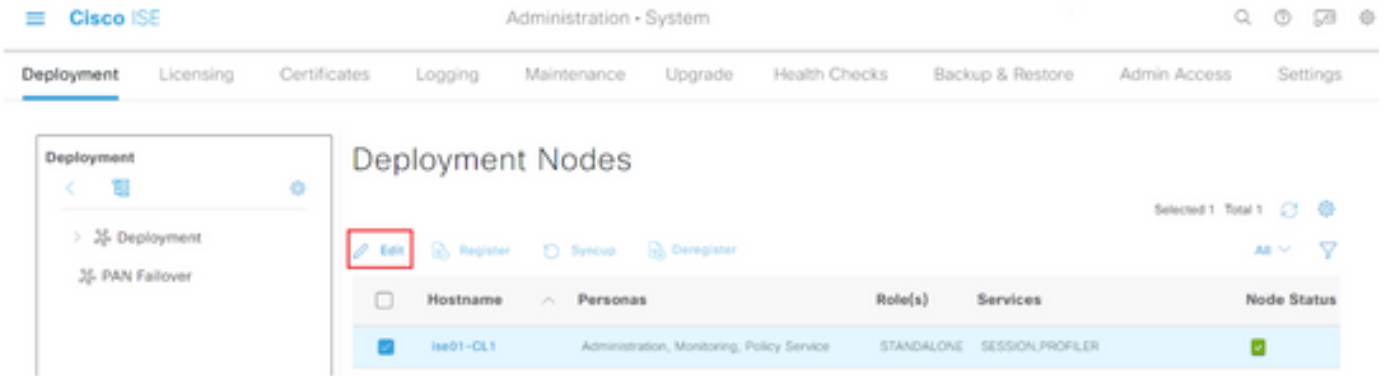
구성

ISE 구성

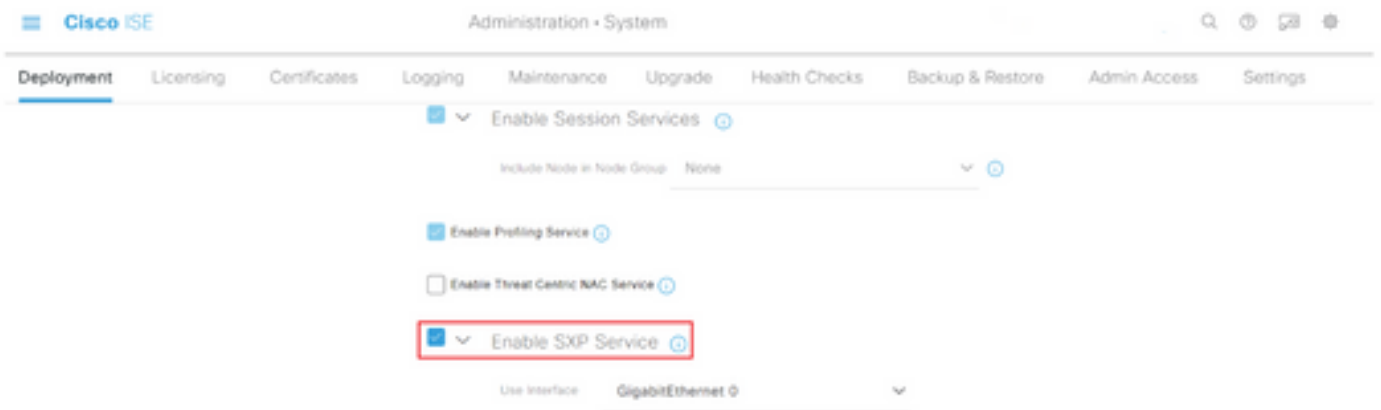
SXP 활성화

1단계. 세 개의 라인 아이콘을 선택합니다  왼쪽 상단 모서리에 있으며 Administration(관리) > System(시스템) > Deployment(구축)를 선택합니다.

2단계. 구성할 노드를 선택하고 Edit(편집)를 클릭합니다.




3단계. SXP를 활성화하려면 Enable SXP Service(SXP 서비스 활성화) 상자를 선택합니다



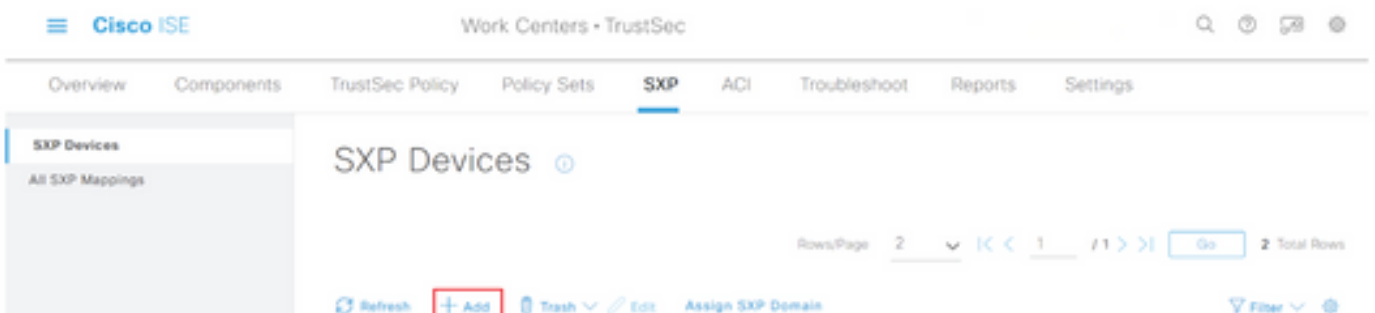
4단계. 아래로 스크롤하여 Save(저장)를 클릭합니다.

참고: 각 클러스터의 나머지 ISE 노드에 대해 모든 단계를 반복하며, 어그리게이션 노드가 포함됩니다.

클러스터 노드에서 SXP 구성

1단계. 세 개의 라인 아이콘을 선택합니다  왼쪽 위 모서리에 위치한 다음 Work Center(작업 센터) > TrustSec > SXP를 선택합니다.

2단계. +Add를 클릭하여 ISE 어그리게이션 노드를 SXP 피어로 구성합니다.



3단계. ISE 어그리게이션 노드의 Name 및 IP 주소를 정의하고 LISTENER로 피어 역할을 선택합니다

다. **Connected PSNs**(연결된 PSN)에서 **required PSNs**(필수 PSN), **required SXP Domains**(필수 SXP 도메인), **status**(상태)에서 **Enabled**(활성화됨)를 **선택한** 다음 **Password Type**(비밀번호 유형) 및 **required**(필수) **PSNversion**(버전)을 선택합니다.

The screenshot displays the Cisco ISE interface for configuring SXP devices. The breadcrumb trail is 'SXP Devices > SXP Connection'. The main content area is titled 'Add Single Device' and includes a note: 'Input fields marked with an asterisk (*) are required.' The form contains the following fields:

- Name**: ISE Aggregation node
- IP Address ***: 10.50.50.125
- Peer Role ***: LISTENER
- Connected PSNs ***: ise01-CL1

Overview Components TrustSec Policy Policy Sets **SXP** ACI

SXP Devices

All SXP Mappings

SXP Domains *
default x

Status *
Enabled

Password Type *
CUSTOM

Password

Version *
V4

▶ Advanced Settings

Cancel Save

4단계. **Save**를 클릭합니다.

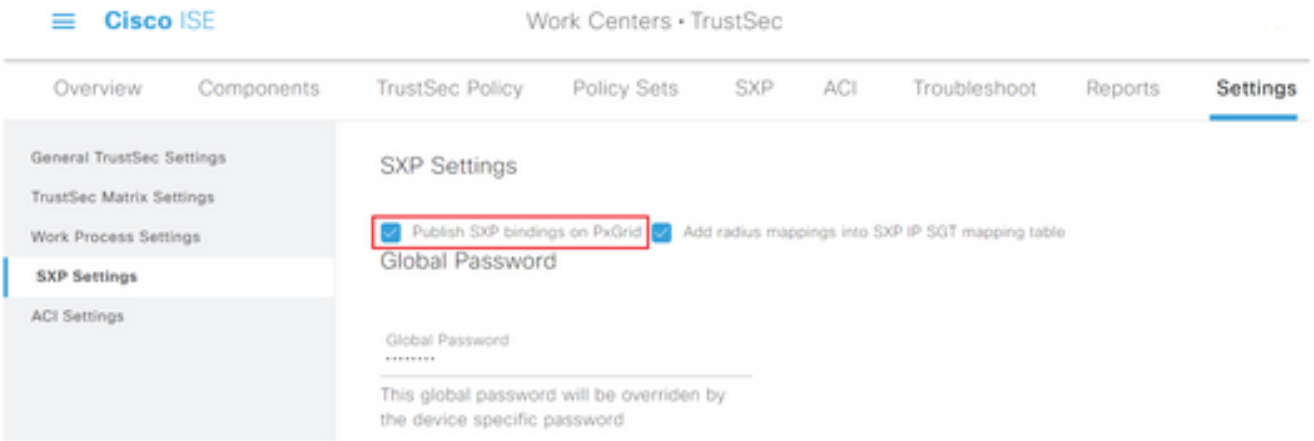
참고: 각 클러스터의 나머지 ISE 노드에 대해 모든 단계를 반복하여 어그리게이션 노드에 대한 SXP 연결을 구축합니다. 어그리게이션 노드에서 동일한 프로세스를 반복하고 피어 역할로 **SPEAKER**를 선택합니다.

어그리게이션 노드에서 SXP 구성

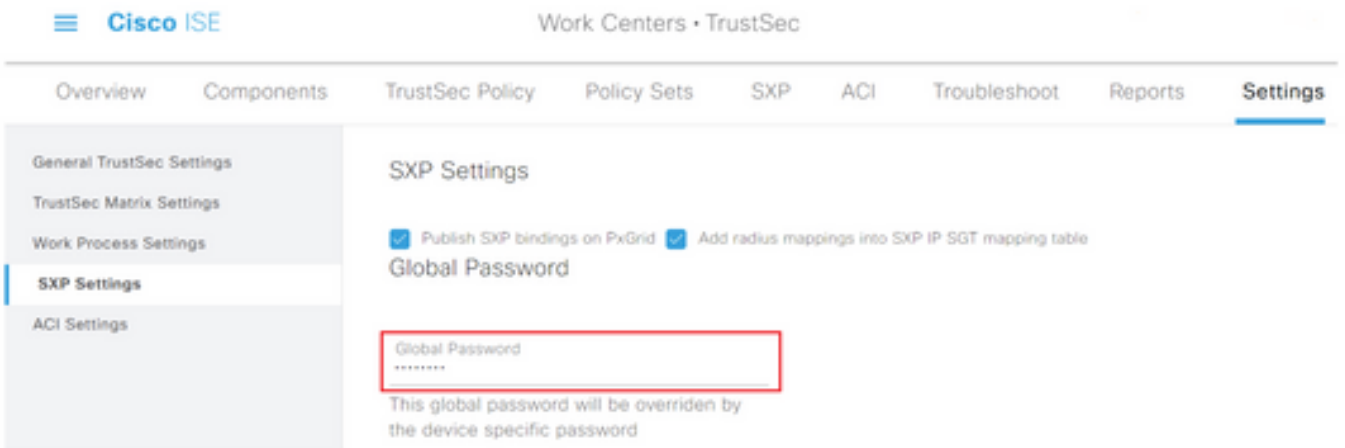
1단계. 왼쪽 상단에 있는 세 개의 회선 아이콘을 선택하고 Work Center(작업 센터) > TrustSec > **Settings(설정)**에서 선택합니다

2단계. SXP Settings(SXP 설정) **탭**을 클릭합니다

3단계. IP-SGT 매핑을 전파하려면 Publish SXP bindings on pxGrid(pxGrid에 **SXP 바인딩** 게시) **확인란**을 선택합니다.



4단계(선택 사항) Global Password(전역 비밀번호) 아래에서 SXP 설정의 기본 비밀번호를 정의합니다.

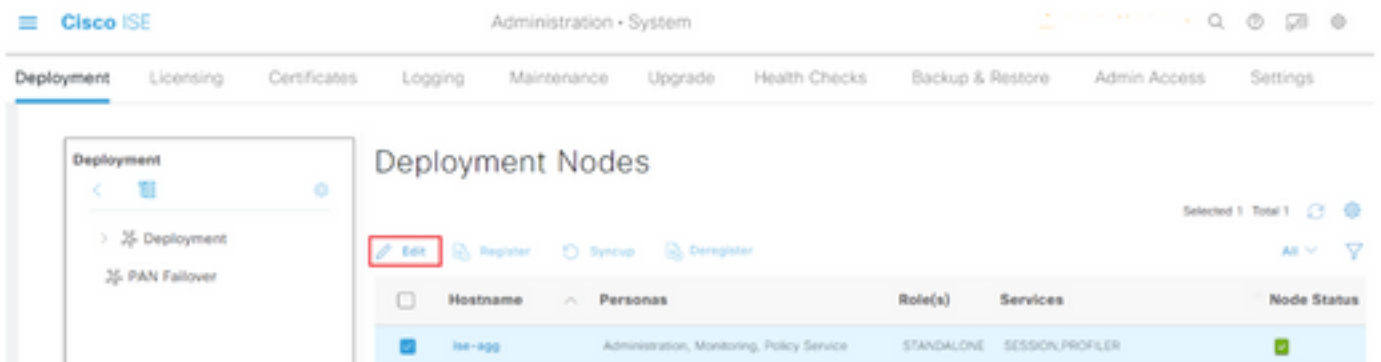


5단계. 아래로 스크롤하고 저장을 클릭합니다.

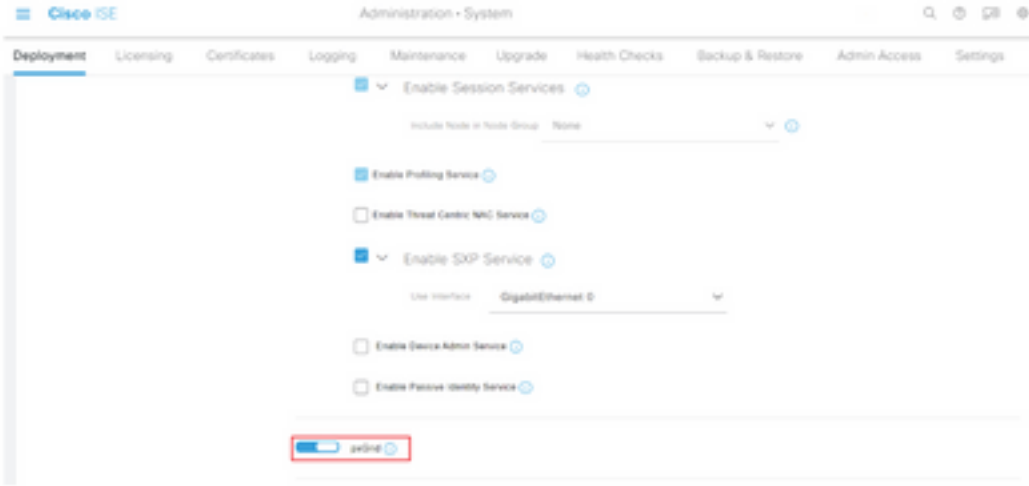
집계 노드에서 pxGrid를 활성화합니다.

1단계. 왼쪽 상단에 있는 세 개의 라인 아이콘을 선택하고 Administration(관리) > System(시스템) > Deployment(구축)를 선택합니다.

2단계. 구성할 노드를 선택하고 Edit(편집)를 클릭합니다.



3단계. pxGrid를 활성화하려면 pxGrid 옆의 버튼을 클릭합니다.

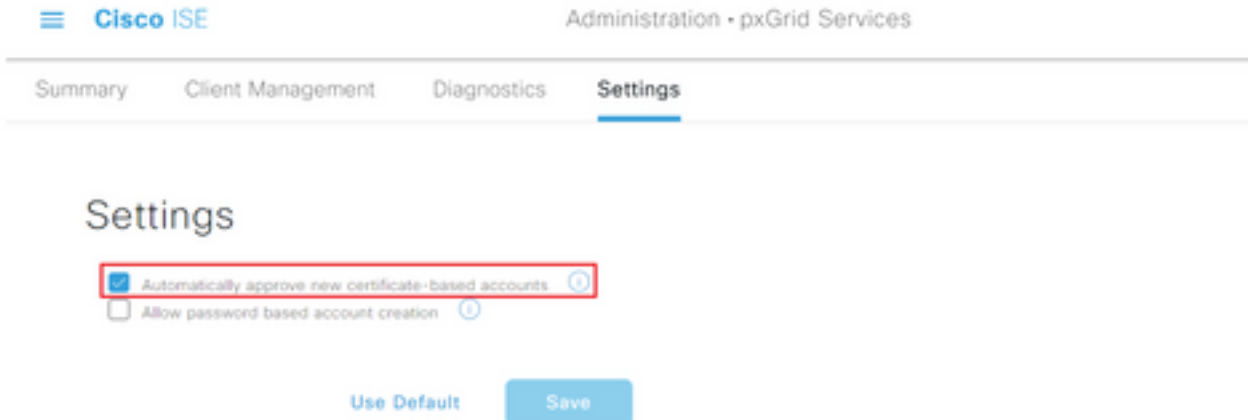


4단계. 아래로 스크롤하여 저장을 클릭합니다.

pxGrid 자동 승인

1단계. 왼쪽 상단 모서리에 있는 세 개의 회선 아이콘으로 이동하여 Administration(관리) > pxGrid Services(pxGrid 서비스) > Settings(설정)를 선택합니다.

2단계. 기본적으로 ISE는 새 pxGrid 클라이언트의 연결 요청을 자동으로 pxGrid에 승인하지 않으므로 새 인증서 기반 어카운트 자동 승인 확인란을 선택하여 해당 설정을 활성화해야 합니다.



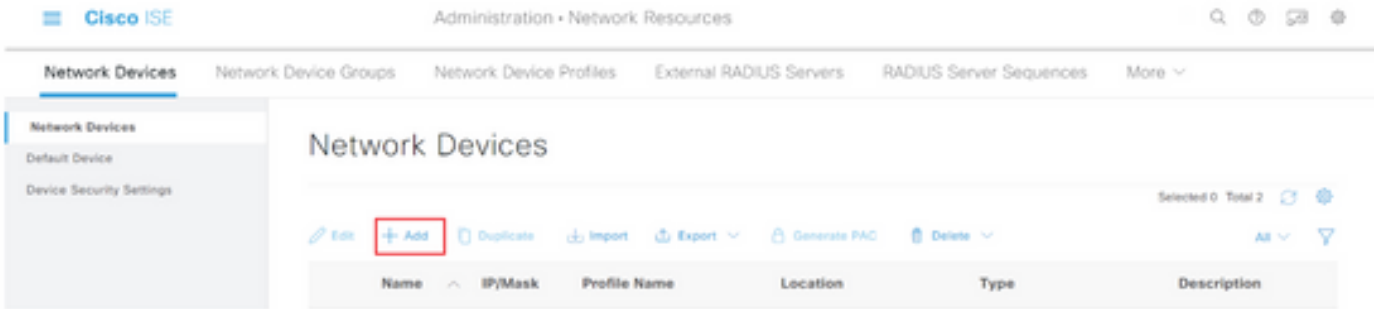
3단계. Save를 클릭합니다.

네트워크 디바이스 TrustSec 설정

Cisco ISE가 TrustSec 지원 디바이스의 요청을 처리하려면 Cisco ISE에서 이러한 TrustSec 지원 디바이스를 정의해야 합니다.

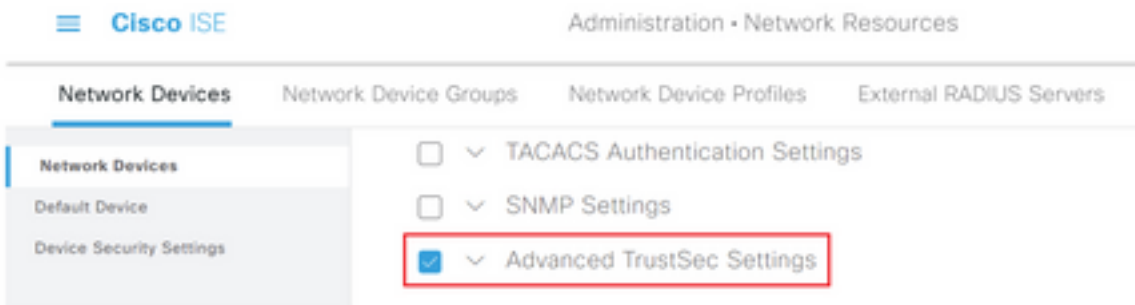
1단계. 왼쪽 상단에 있는 3개의 회선 아이콘으로 이동하여 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)를 선택합니다.

2단계. +추가를 클릭합니다.

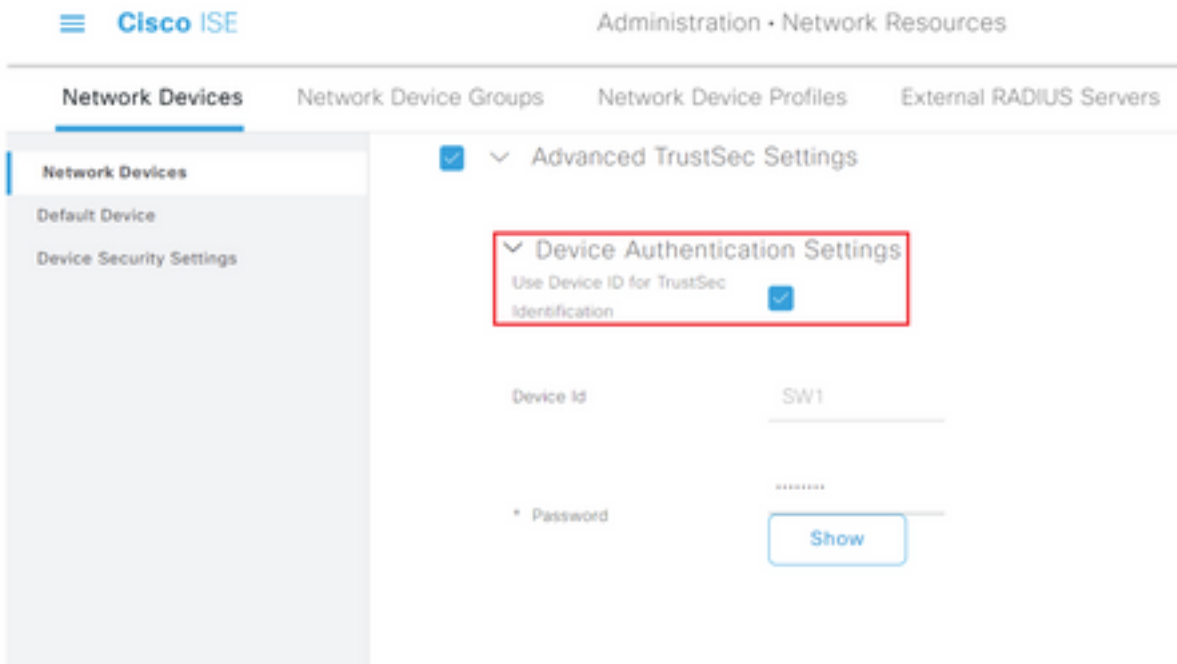


3단계. Network Devices(네트워크 디바이스) 섹션과 RADIUS Authentication Settings(RADIUS 인증 설정)에서 필요한 정보를 입력합니다.

4단계. TrustSec 지원 디바이스를 구성하려면 Advanced TrustSec Settings 확인란을 선택합니다.



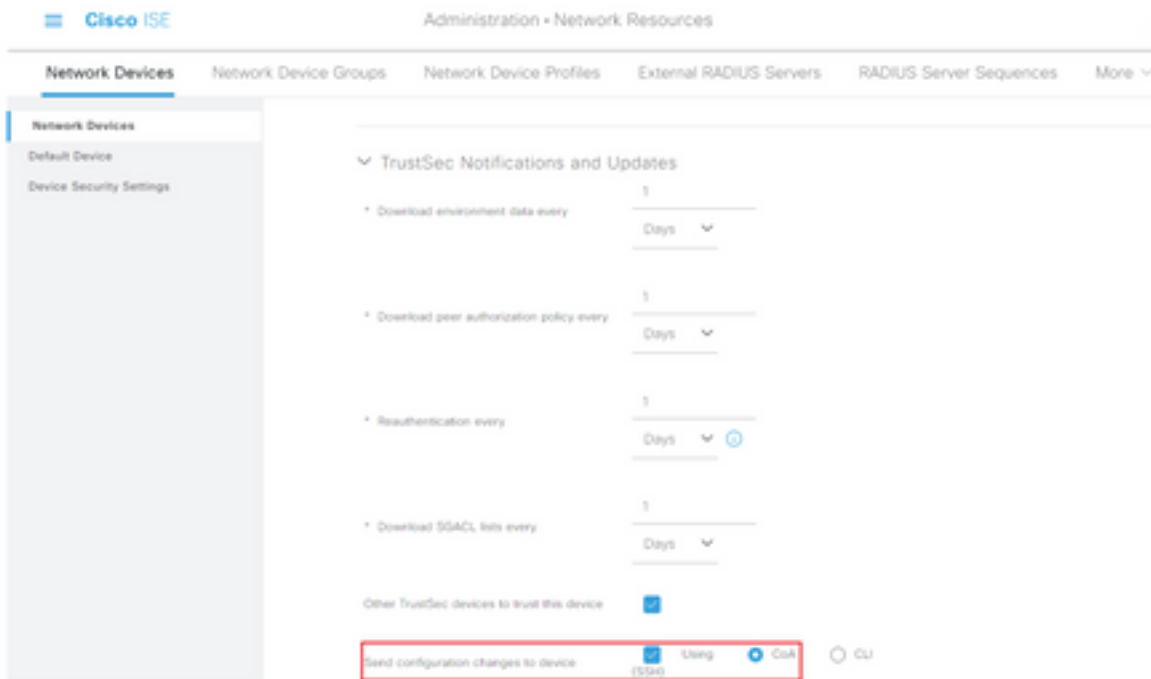
5단계. Use Device ID for TrustSec Identification(TrustSec 식별에 디바이스 ID 사용) 확인란을 클릭하여 Network Devices(네트워크 디바이스) 섹션에 나열된 디바이스 이름을 자동으로 채웁니다. Password(비밀번호) 필드에 비밀번호를 입력합니다.



참고: ID 및 비밀번호는 스위치에 나중에 구성되는 "cts credentials id <ID> password <PW>" 명령과 일치해야 합니다.

6단계. Send configuration changes to device(디바이스에 컨피그레이션 변경 사항 보내기) 확인란

을 선택하여 ISE가 디바이스에 TrustSec CoA 알림을 보낼 수 있도록 합니다.



7단계. Include this device when deploying Security Group Tag Mapping Updates(보안 그룹 태그 매핑 업데이트 구축 시 이 디바이스 포함) 확인란을 선택합니다.

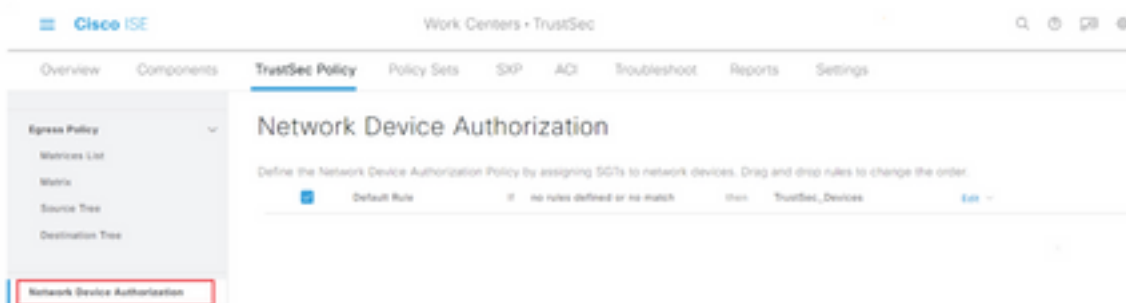
8단계. ISE가 네트워크 디바이스의 컨피그레이션을 수정하도록 하려면 EXEC Mode Username(EXEC 모드 사용자 이름) 및 EXEC Mode Password(EXEC 모드 비밀번호) 필드에 사용자 자격 증명을 입력합니다. 선택적으로, Enable Mode Password 필드에 enable 비밀번호를 입력합니다.

참고: TrustSec 도메인의 일부로 간주되는 다른 모든 NAD에 대해 이 단계를 반복합니다.

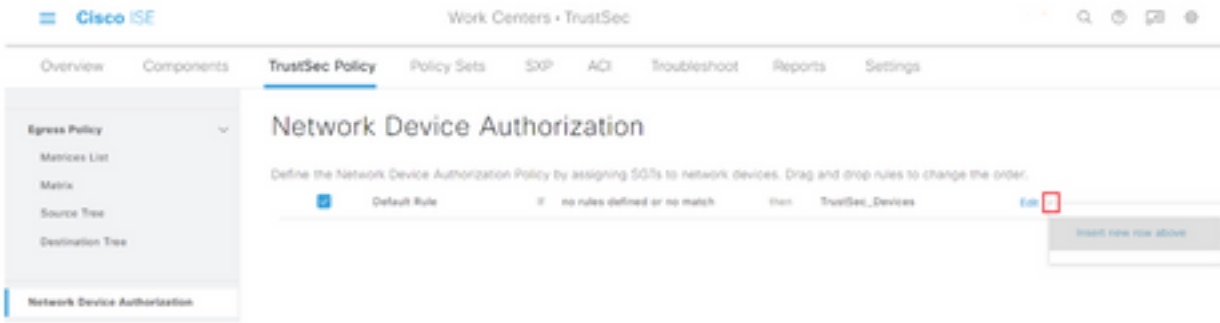
네트워크 디바이스 권한 부여

1단계. 왼쪽 상단 모서리에 있는 세 개의 라인 아이콘을 선택하고 Work Centers(작업 센터) > TrustSec > TrustSec Policy(TrustSec 정책)를 선택합니다.

2단계. 왼쪽 창에서 Network Device Authorization(네트워크 디바이스 권한 부여)을 클릭합니다.

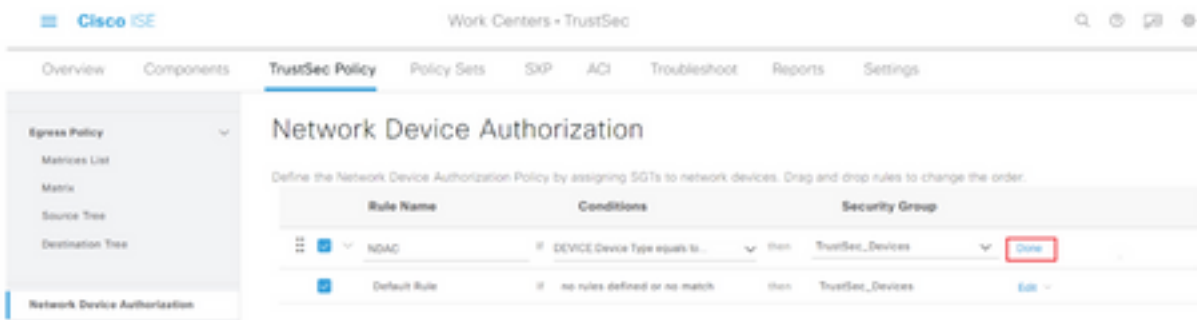


3단계. 오른쪽의 Edit and Insert new row above(편집 및 새 행 삽입) 옆에 있는 드롭다운을 사용하여 새 NDA 규칙을 만듭니다.



4단계. Rule Name(규칙 이름), Conditions(조건)를 정의하고 Security Groups(보안 그룹) 드롭다운 목록에서 적절한 SGT를 선택합니다.

5단계. 맨 오른쪽에서 Done(완료)을 클릭합니다.



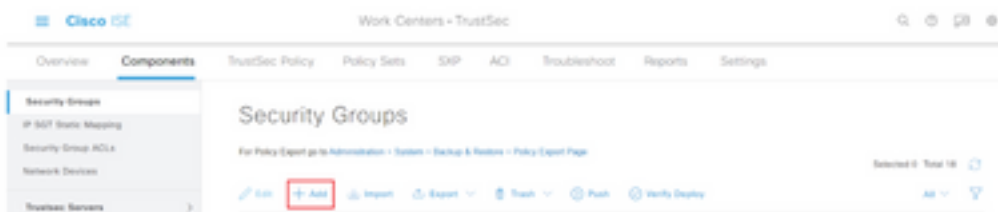
6단계. 아래로 스크롤하고 저장을 클릭합니다.

SGT

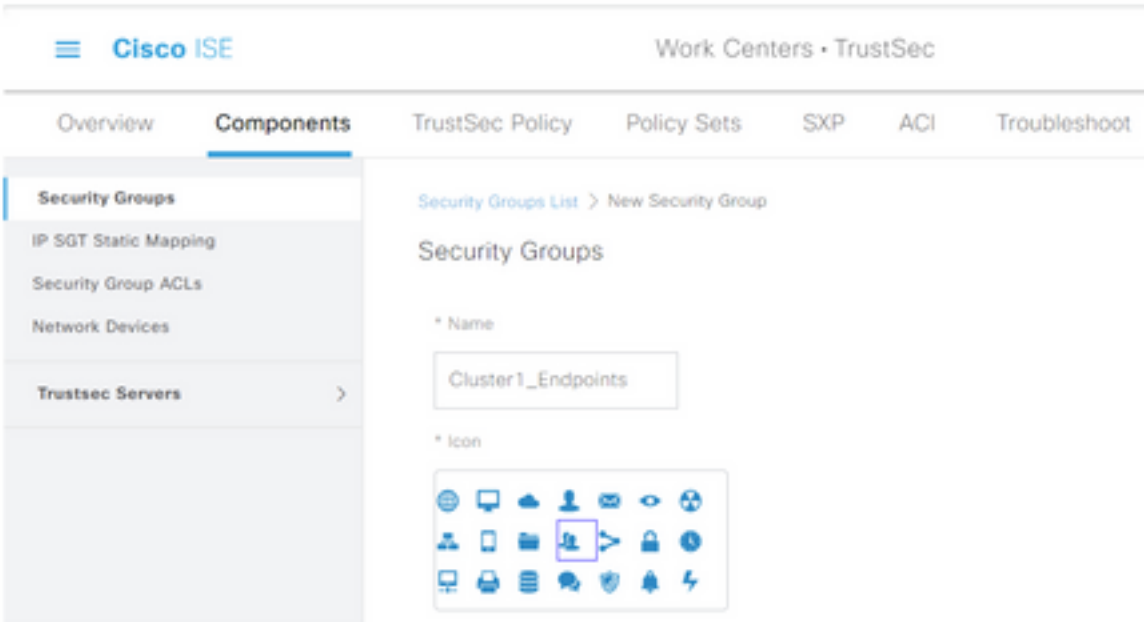
1단계. 왼쪽 상단에 있는 세 개의 라인 아이콘을 선택하고 Work Centers(작업 센터) > TrustSec > Components(구성 요소)를 선택합니다.

2단계. 왼쪽 창에서 Security Groups(보안 그룹)를 확장합니다.

3단계. 새 SGT를 생성하려면 +Add를 클릭합니다.



4단계. 이름을 입력하고 해당 필드에서 아이콘을 선택합니다.



단계 5. 필요에 따라 설명을 입력하고 태그 값을 입력합니다.

참고: 태그 값을 수동으로 입력할 수 있게 하려면 Work Centers(작업 센터) > TrustSec > Settings(설정) > General TrustSec Settings(일반 TrustSec 설정)로 이동하고 **Security Group Tag Numbering(보안 그룹 태그 번호 지정)**에서 **User Must Enter SGT Number Manually(사용자가 수동으로 SGT 번호를 입력해야 함)** 옵션을 선택합니다.

6단계. 아래로 스크롤하고 Submit(제출)을 클릭합니다.

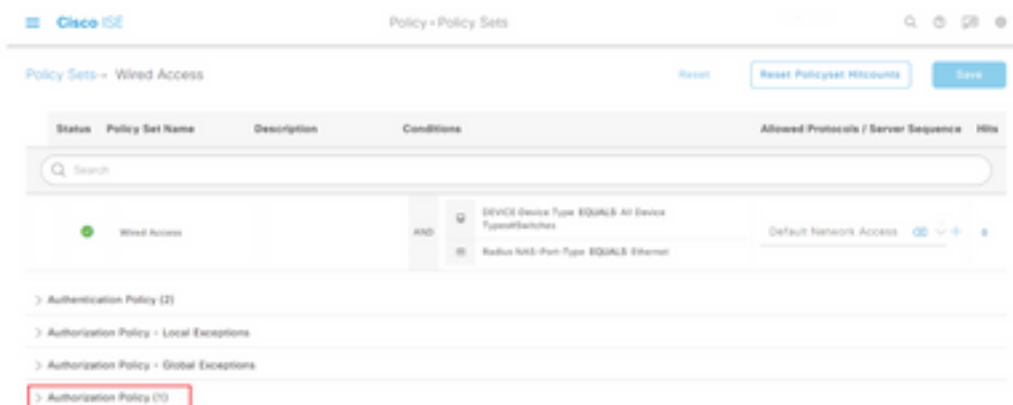
참고: 모든 필수 SGT에 대해 이 단계를 반복합니다.

권한 부여 정책

1단계. 왼쪽 상단 모서리에 있는 세 개의 라인 아이콘을 선택하고 Policy(정책) > Policy Sets(정책 집합)를 선택합니다.

2단계. 적절한 정책 집합을 선택합니다.

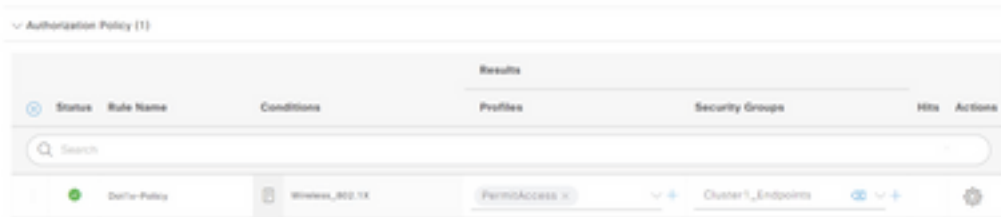
3단계. 정책 집합에서 Authorization Policy(권한 부여 정책)를 확장합니다.



4단계. 다음 중 하나를 클릭합니다.  버튼을 클릭하여 권한 부여 정책을 생성합니다.



5단계. 필수 규칙 이름, 조건 및 프로파일을 정의하고 Security Groups(보안 그룹) 아래의 드롭다운 목록에서 적절한 SGT를 선택합니다.



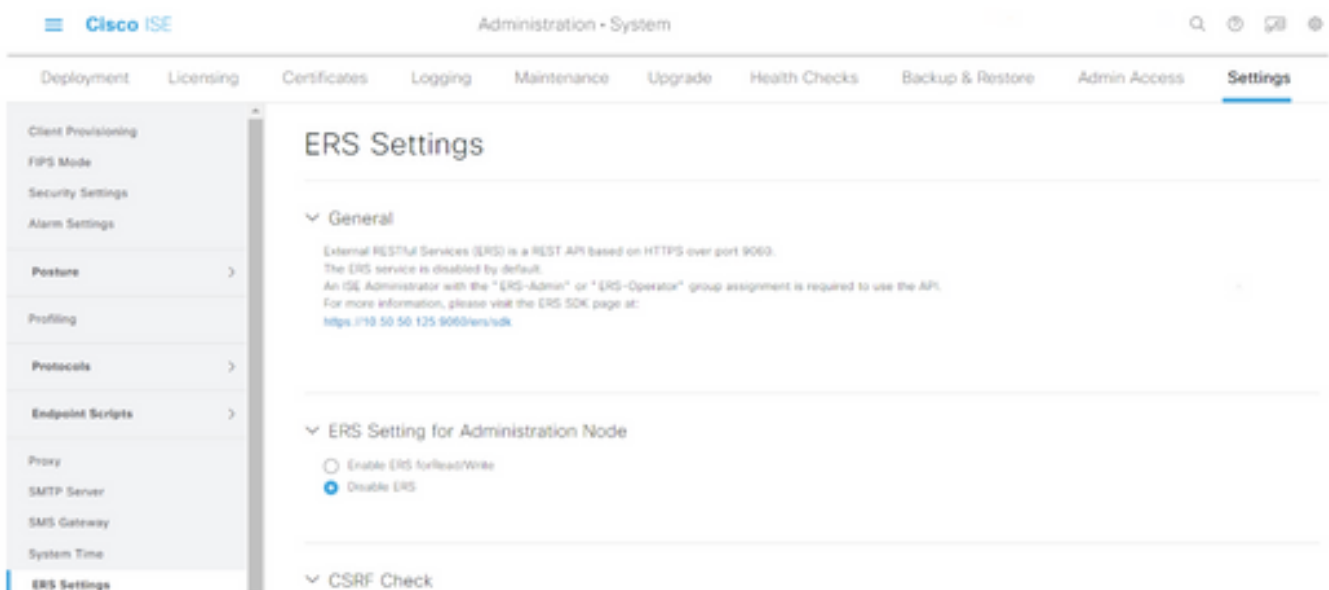
6단계. Save를 클릭합니다.

ISE 어그리게이션 노드에서 ERS 활성화(선택 사항)

외부 RESTful API 서비스(ERS)는 WSA에서 그룹 정보를 쿼리할 수 있는 API입니다. ERS 서비스는 ISE에서 기본적으로 비활성화되어 있습니다. 활성화된 클라이언트는 ISE 노드에서 ERS 관리자 그룹의 멤버로 인증될 경우 API를 쿼리할 수 있습니다. ISE에서 서비스를 활성화하고 올바른 그룹에 계정을 추가하려면 다음 단계를 수행합니다.

1단계. 왼쪽 상단에 있는 세 개의 라인 아이콘을 선택하고 Administration(관리) > System(시스템) > Settings(설정)에서 선택합니다.

2단계. 왼쪽 창에서 ERS Settings(ERS 설정)를 클릭합니다.



3단계. Enable ERS for Read/Write(읽기/쓰기에 ERS 활성화) 옵션을 선택합니다.

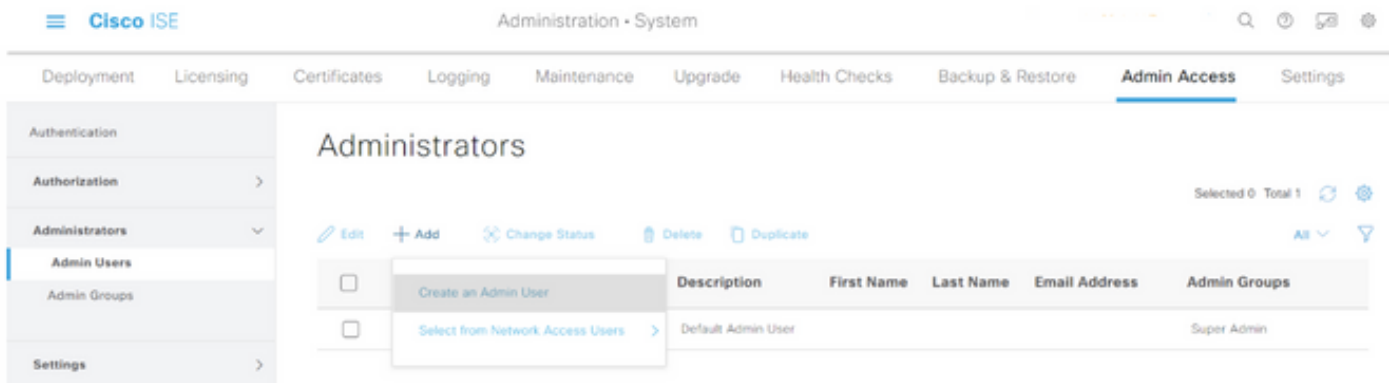
4단계. Save(저장)를 클릭하고 OK(확인)를 클릭합니다.

ESR 관리 그룹에 사용자 추가(선택 사항)

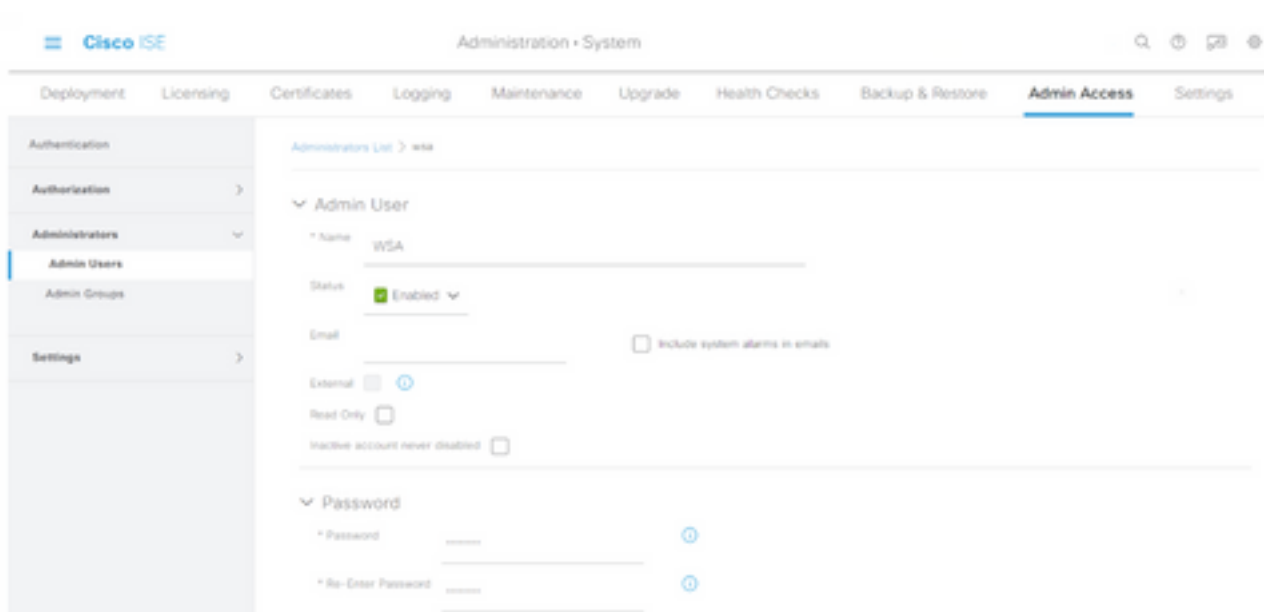
1단계. 왼쪽 상단에 있는 세 개의 회선 아이콘을 선택하고 Administration(관리) > System(시스템) > Admin Access(관리자 액세스)를 선택합니다

2단계. 왼쪽 창에서 Administrators(관리자)를 확장하고 Admin Users(사용자 관리)를 클릭합니다.

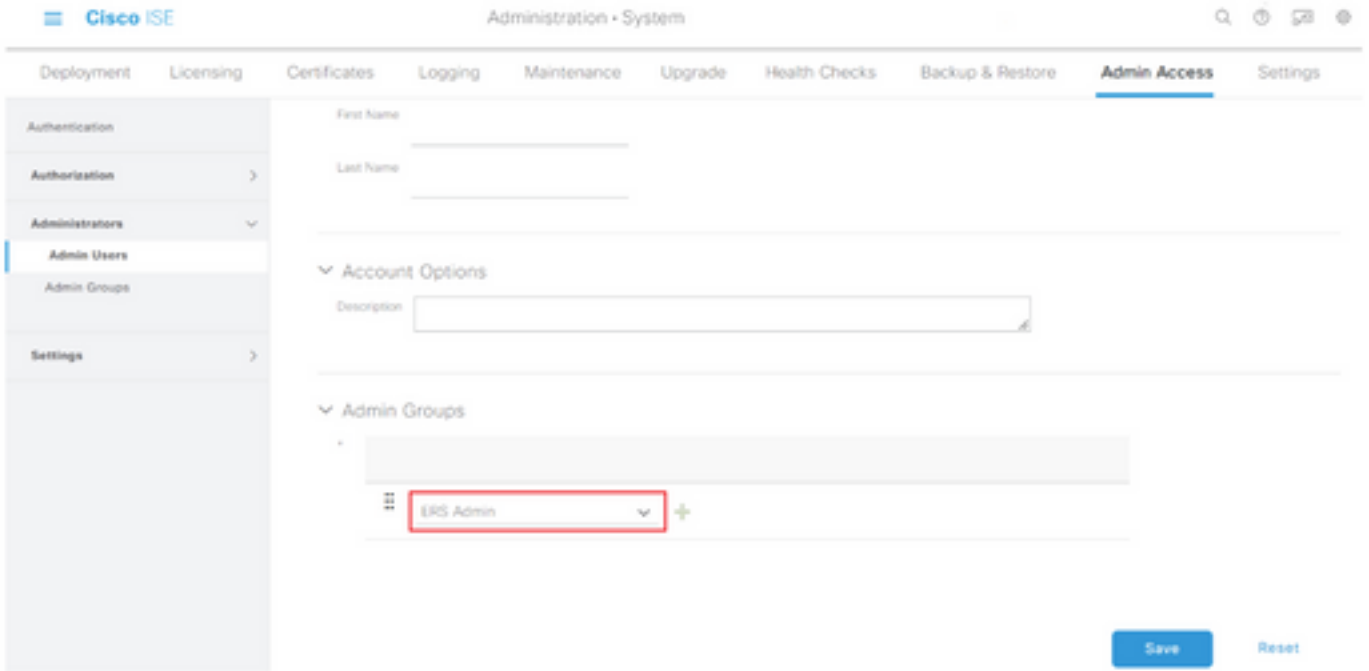
3단계. +Add를 클릭하고 드롭다운에서 Admin User를 선택합니다.



4단계. 해당 필드에 사용자 이름과 비밀번호를 입력합니다.



5단계. Admin Groups(관리자 그룹) 필드에서 드롭다운을 사용하여 ERS Admin(ERS 관리자)을 선택합니다.



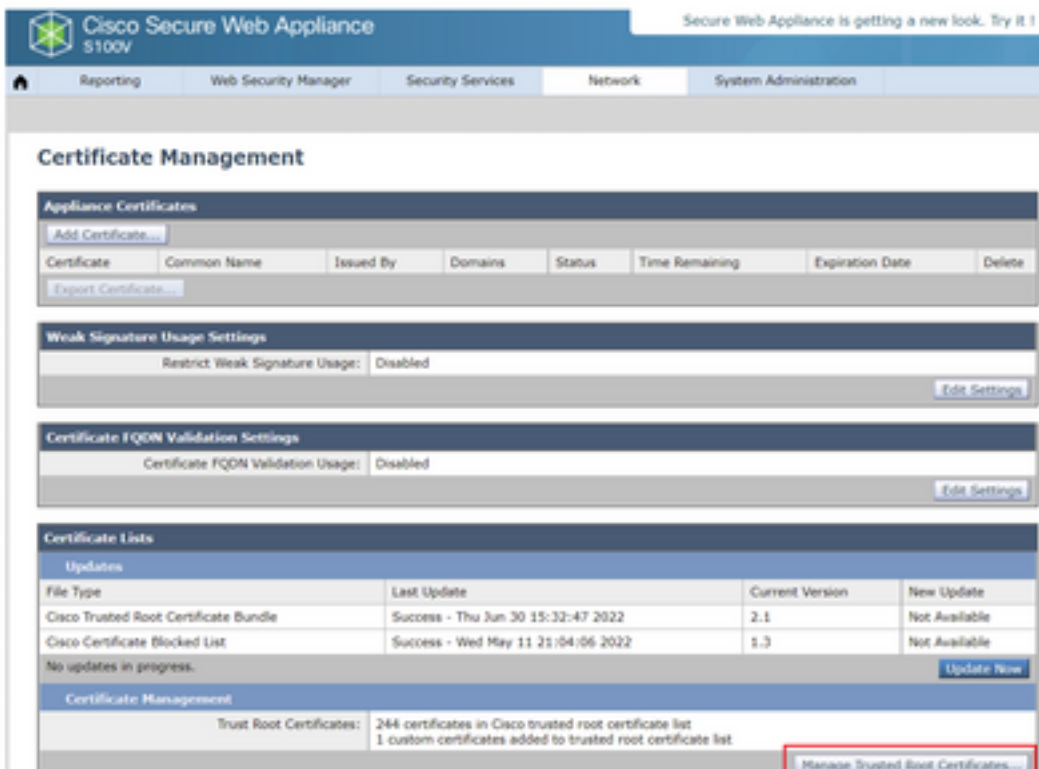
6단계. Save를 클릭합니다.

보안 웹 어플라이언스 컨피그레이션

루트 인증서

통합 설계에서 내부 인증 기관을 WSA와 ISE 간 연결에 대한 트러스트 루트로 사용하는 경우 이 루트 인증서를 두 어플라이언스 모두에 설치해야 합니다.

1단계. Network(네트워크) > Certificate Management(인증서 관리)로 이동하고 Manage Trusted Root Certificates(신뢰할 수 있는 루트 인증서 관리)를 클릭하여 CA 인증서를 추가합니다.



2단계. Import(가져오기)를 클릭합니다.



3단계. Choose File(파일 선택)을 클릭하여 생성된 루트 CA를 찾은 다음 Submit(제출)을 클릭합니다.

4단계. Submit을 다시 클릭합니다.

5단계. 오른쪽 상단 모서리에서 Commit Changes(변경 사항 커밋)를 클릭합니다.



6단계. Commit Changes(변경 사항 커밋)를 다시 클릭합니다.

pxGrid 인증서

WSA에서는 pxGrid에서 사용할 키 쌍 및 인증서 생성이 ISE 서비스 컨피그레이션의 일부로 완료됩니다.

1단계. Network(네트워크) > Identity Service Engine으로 이동합니다.

2단계. Enable and Edit Settings(설정 활성화 및 편집)를 클릭합니다.

3단계. Choose File(파일 선택)을 클릭하여 생성된 루트 CA를 찾고 Upload File(파일 업로드)을 클릭합니다.



참고: 일반적인 컨피그레이션 오류는 이 섹션에서 ISE pxGrid 인증서를 업로드하는 것입니다. 루트 CA 인증서는 ISE pxGrid Node Certificate 필드에 업로드해야 합니다.

4단계. Web Appliance Client Certificate(웹 어플라이언스 클라이언트 인증서) 섹션에서 Use Generated Certificate and Key(생성된 인증서 및 키 사용)를 선택합니다.



5단계. Generate New Certificate and Key(새 인증서 및 키 생성) 버튼을 클릭하고 필수 인증서 필드를 완료합니다.

6단계. Download Certificate Signing Request(인증서 서명 요청 다운로드)를 클릭합니다.

참고: ISE 컨피그레이션에 변경 사항을 커밋하려면 **Submit**(제출) 버튼을 선택하는 것이 좋습니다. 변경 사항이 제출되기 전에 세션이 시간 초과될 경우, CSR이 다운로드되었더라도 생성된 키와 인증서가 손실될 수 있습니다.

7단계. CA로 CSR에 서명한 후 Choose File(파일 선택)을 클릭하여 인증서를 찾습니다.

Web Appliance Client Certificate: For secure communication between the Web Appliance and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.

Use Uploaded Certificate and Key

Certificate:

Key:

Key is Encrypted

No certificate has been uploaded.

Use Generated Certificate and Key

Common name: wsa.securitylab.net
 Organization: Cisco
 Organizational Unit: Security
 Country: SE
 Expiration Date: May 10 19:19:26 2024 GMT
 Basic Constraints: Not Critical

[Download Certificate...](#) | [Download Certificate Signing Request...](#)

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate:

8단계. 파일 업로드를 클릭합니다.

9단계. 제출 및 커밋

Secure Web Appliance에서 SXP 및 ERS 활성화

1단계. SXP와 ERS 모두의 Enable(활성화) 버튼을 클릭합니다.

ISE SOAP Exchange Protocol (SXP) Service: Enabling the service, Web Appliance will retrieve SXP Binding Topic from ISE Services.

Enable ISE External Restful Service (ERS)

The Web Appliance retrieves Active Directory groups, and local ISE groups from ISE using the ERS. If you are configuring the Web Appliance's policies using Active Directory groups, or in combination with Secure Group Type (SGT), you should enable ERS.

2단계. ERS Administrator Credentials(ERS 관리자 자격 증명) 필드에 ISE에 구성된 사용자 정보를 입력합니다.

3단계. 이전에 구성한 정보를 상속하려면 ISE pxGrid 노드와 동일한 서버 이름의 확인란을 선택합니다. 그렇지 않은 경우 필요한 정보를 입력합니다.

Enable ISE External Restful Service (ERS)

ERS Administrator Credentials

Username:

Password:

ERS Servers

Server name same as ISE pxGrid Nodes

Primary: (Hostname or IPv4 address)

Secondary (Optional): (Hostname or IPv4 address)

Port: (Enter the port number specified for ERS in ISE)

4단계. 제출 및 커밋

식별 프로필

WSA 정책에서 보안 그룹 태그 또는 ISE 그룹 정보를 사용하려면 먼저 사용자를 투명하게 식별하기 위한 수단으로 ISE를 활용하는 식별 프로필을 생성해야 합니다.

1단계. Web Security Manager > Authentication > Identification Profiles로 이동합니다.

2단계. Add Identification Profile(식별 프로필 추가)을 클릭합니다.

3단계. 이름과 내용(선택적)을 입력합니다.

4단계. Identification and Authentication(식별 및 인증) 섹션에서 드롭다운을 사용하여 Transparently identify users with ISE(ISE로 투명하게 사용자 식별)를 선택합니다.

Identification Profiles: Add Profile

Client / User Identification Profile Settings

Enable Identification Profile

Name: ISE Profile
(e.g. my IT Profile)

Description: Identification profile for ISE integration.
(Maximum allowed characters 256)

Insert Above: 2 (Global Profile)

User Identification Method

Identification and Authentication: Transparently identify users with ISE

Fallback to Authentication Realm or Guest Privileges: Support Guest Privileges

Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by Subnet:

Define Members by Protocol: HTTP/HTTPS

Advanced Define additional group membership criteria.

5단계. 제출 및 커밋

SGT 기반 암호 해독 정책

1단계. Web Security Manager > Web Policies > Decryption Policies로 이동합니다.

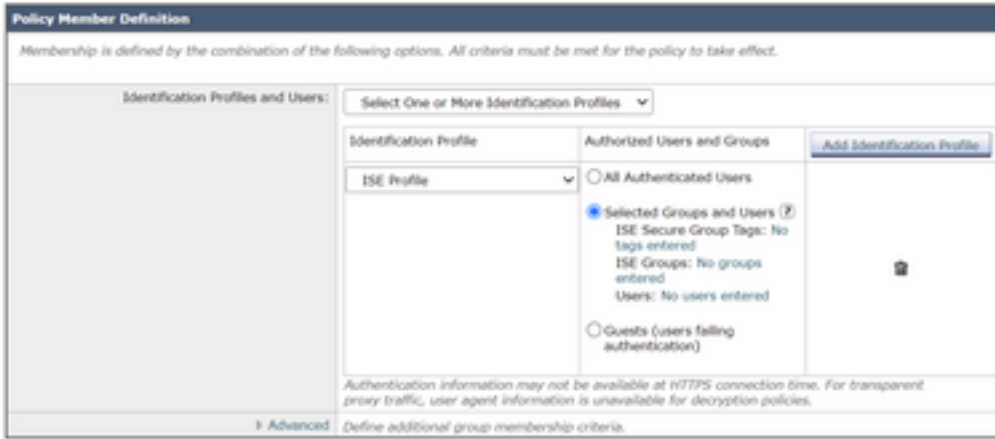
2단계. Add Policy(정책 추가)를 클릭합니다.

3단계. 이름과 내용(선택적)을 입력합니다.

4단계. Identification Profiles and Users(식별 프로필 및 사용자) 섹션에서 드롭다운을 사용하여 Select One or More Identification Profiles(하나 이상의 식별 프로필 선택)를 선택합니다.

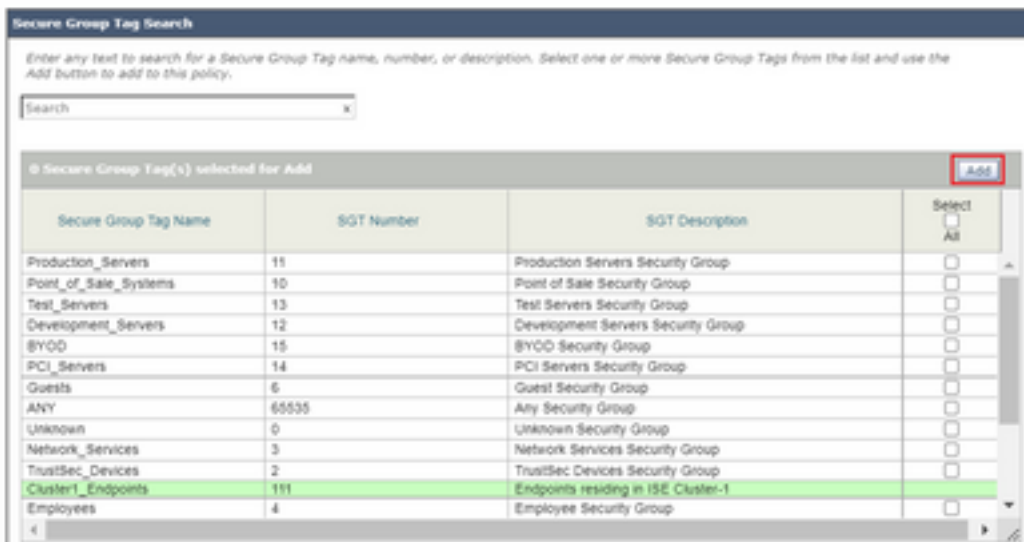
5단계. Identification Profiles(식별 프로필) 섹션에서 드롭다운을 사용하여 ISE 식별 프로필의 이름을 선택합니다.

6단계. Authorized Users and Groups(인증된 사용자 및 그룹) 섹션에서 Selected Groups and Users(선택된 그룹 및 사용자)를 선택합니다.



7단계. ISE Secure Group Tags 옆의 하이퍼링크를 클릭합니다.

8단계. Secure Group Tag Search(Secure Group Tag 검색) 섹션에서 원하는 SGT 오른쪽에 있는 확인란을 선택하고 Add(추가)를 클릭합니다.



9단계. Done(완료)을 클릭하여 돌아갑니다.

10단계. 제출 및 커밋

스위치 구성

AAA

```

aaa new-model

aaa group server radius ISE
  server name ise01-cl1
  server name ise02-cl1
  ip radius source-interface Vlan50

aaa authentication dot1x default group ISE
aaa authorization network ISE group ISE
aaa accounting update newinfo periodic 2440
aaa accounting dot1x default start-stop group ISE

aaa server radius dynamic-author
  client 10.50.50.120 server-key Cisco123
  client 10.50.50.121 server-key Cisco123
  auth-type any

radius server ise01-cl1
  address ipv4 10.50.50.121 auth-port 1812 acct-port 1813
  pac key Cisco123
radius server ise02-cl1
  address ipv4 10.50.50.120 auth-port 1812 acct-port 1813
  pac key Cisco123

```

트러스트섹(TrustSec)

```

cts credentials id SW1 password Cisco123 (This is configured in Privileged EXEC Mode)
cts role-based enforcement

```

```

aaa authorization network cts-list group ISE
cts authorization list cts-list

```

다음을 확인합니다.

ISE에서 엔드포인트로의 SGT 할당

인증 및 권한 부여가 성공한 후 SGT가 할당된 ISE 클러스터 1의 엔드포인트를 볼 수 있습니다.

| Identity | Endpoint ID | Endpoint Profile | Authorization Policy | Authorization Policy | Authorization Profile | IP Address | Security Group | Server |
|----------|-------------|------------------|----------------------|----------------------|-----------------------|------------|--------------------|-----------|
| ... | ... | ... | ... | ... | ... | ... | Cluster_1_Endpoint | ise01-cl1 |

인증 및 권한 부여가 성공한 후 SGT가 할당된 ISE 클러스터 2의 엔드포인트를 볼 수 있습니다.

| Identity | Endpoint ID | Endpoint Profile | Authorization Policy | Authorization Policy | Authorization Profile | IP Address | Security Group | Server |
|----------|-------------|------------------|----------------------|----------------------|-----------------------|------------|--------------------|-----------|
| ... | ... | ... | ... | ... | ... | ... | Cluster_2_Endpoint | ise02-cl1 |

SXP 매핑

클러스터 ISE 노드와 ISE 어그리게이션 노드 간에 SXP 통신이 활성화되므로 ISE 어그리게이션에서 SXP를 통해 이러한 SGT-IP 매핑을 학습합니다.

| IP Address | SGT | VN | Learned From | Learned By | SXP Domain | PDNs Involved |
|--------------|-----------------------------|----|--------------------------|------------|------------|---------------|
| 10.50.50.112 | TrustSec_Device (20000) | | 10.50.50.121, 10.50.50.5 | SXP | default | 10.50.50.5 |
| 10.50.50.112 | TrustSec_Device (20000) | | 10.50.50.121, 10.50.50.7 | SXP | default | 10.50.50.7 |
| 10.50.50.121 | Cluster_Endpoints (1110000) | | 10.50.50.121, 10.50.50.5 | SXP | default | 10.50.50.5 |
| 10.50.50.121 | Cluster_Endpoints (1110000) | | 10.50.50.121, 10.50.50.7 | SXP | default | 10.50.50.7 |

다른 ISE 클러스터의 이러한 SXP 매핑은 ISE 어그리게이션 노드를 통해 pxGrid를 통해 WSA로 전송됩니다.

```

wsa2.securitylab.net> isedata
Choose the operation you want to perform:
- STATISTICS - Show the ISE server status and ISE statistics.
- CACHE - Show the ISE cache or check an IP address.
- SGTs - Show the ISE Secure Group Tag (SGT) table.
- GROUPS - Show the ISE Groups table.
[ ]> cache

Choose the operation you want to perform:
- SHOW - Show the ISE IP cache.
- CHECKIP - Query the local ISE cache for an IP address
[ ]> show
IP                username                                     SGT#  Port Range
10.50.50.13       isesxp_10.50.50.122_sgt222_10.50.50.13    222   -
10.50.50.12       isesxp_10.50.50.121_sgt111_10.50.50.12    111   -
  
```

SGT 기반 정책 시행

여기에서 서로 다른 엔드포인트가 해당 정책과 일치하고 트래픽이 SGT를 기반으로 차단됨을 확인할 수 있습니다.

ISE 클러스터 1에 속하는 엔드포인트

This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site (<https://bbc.com/>) has been blocked.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

```

Date: Thu, 14 Jul 2022 14:28:16 CEST
Username: isesxp_10.50.50.121_sgt111_10.50.50.12
Source IP: 10.50.50.12
URL: GET https://bbc.com/
Category: Block URLs CL1
Reason: UNKNOWN
Notification: BLOCK_DEST
  
```

| Time (GMT +02:00) | Website (source) | Display All Details... | Disposition | Bandwidth | User / Client IP |
|----------------------|---|------------------------|-----------------|-----------|--|
| 14 Jul 2022 14:28:17 | https://bbc.com/443/television CONTENT TYPE: - URL CATEGORY: Block URLs CL1 DESTINATION IP: DETAILS: Decryption Policy: 'ISE_Cluster1', WBSA: No Score, Malware Analytics File Verdict: - | | Block - URL Cat | 0B | isesxp_10.50.50.121_sgt111_10.50.50.12 (Identified by ISE) 10.50.50.12 |

ISE 클러스터 2에 속하는 엔드포인트

This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site (https://www.facebook.com/) has been blocked.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Thu, 14 Jul 2022 14:23:58 CEST
Username: isesxp_10.50.50.122_sgt222_10.50.50.13
Source IP: 10.50.50.13
URL: GET https://www.facebook.com/
Category: Block URLs CL2
Reason: UNKNOWN
Notification: BLOCK_DEST

| Time (GMT +02:00) | Website (count) | Disposition | Bandwidth | User / Client IP |
|----------------------|--|-----------------|-----------|--|
| 14 Jul 2022 14:23:58 | https://www.facebook.com/43/revision/ice CONTENT TYPE: - URL CATEGORY: Block URLs CL2 DESTINATION IP: - DETAILS: Decryption Policy: 'ISE_Cluster2', WSRB: No Score, Malware Analysis File Verdict: - | Block - URL Cat | 0B | isesxp_10.50.50.122_sgt222_10.50.50.13 (Identified by ISE) 10.50.50.13 |

관련 정보

- [Web Security Appliance 및 Identity Service Engine 통합 설명서](#)
- [TrustSec 인식 서비스를 위한 ISE와의 WSA 통합 구성](#)
- [Cisco Identity Services Engine 관리자 가이드, 릴리스 3.1](#)
- [AsyncOS 14.5 for Cisco Secure Web Appliance 사용 설명서](#)