ISE와 ASAv 간에 TrustSec SXP 구성

목차

소개

이 문서에서는 ISE(Identity Services Engine)와 ASAv(가상 Adaptive Security Appliance) 간 SXP(Security Group Exchange Protocol) 연결을 구성하는 방법에 대해 설명합니다.

SXP는 TrustSec에서 IP를 SGT에 TrustSec 디바이스에 매핑하는 데 사용하는 SGT(Security Group

Tag) Exchange 프로토콜입니다.SXP는 서드파티 디바이스 또는 SGT 인라인 태깅을 지원하지 않는 레거시 Cisco 디바이스를 포함한 네트워크를 TrustSec 기능을 포함하도록 개발되었습니다.SXP는 피어링 프로토콜이며, 한 디바이스는 스피커로, 다른 디바이스는 리스너로 작동합니다.SXP 스피커는 IP-SGT 바인딩을 전송할 책임이 있으며 리스너는 이러한 바인딩을 수집할 책임이 있습니다.SXP 연결은 메시지 무결성/신뢰성을 위해 TCP 포트 64999를 기본 전송 프로토콜로 사용하고 MD5를 사용합니다.

SXP는 다음 링크에서 IETF 초안으로 게시되었습니다.

https://datatracker.ietf.org/doc/draft-smith-kandula-sxp/

사전 요구 사항

요구 사항

TrustSec 호환성 매트릭스:

http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/solution-overview-listing.html

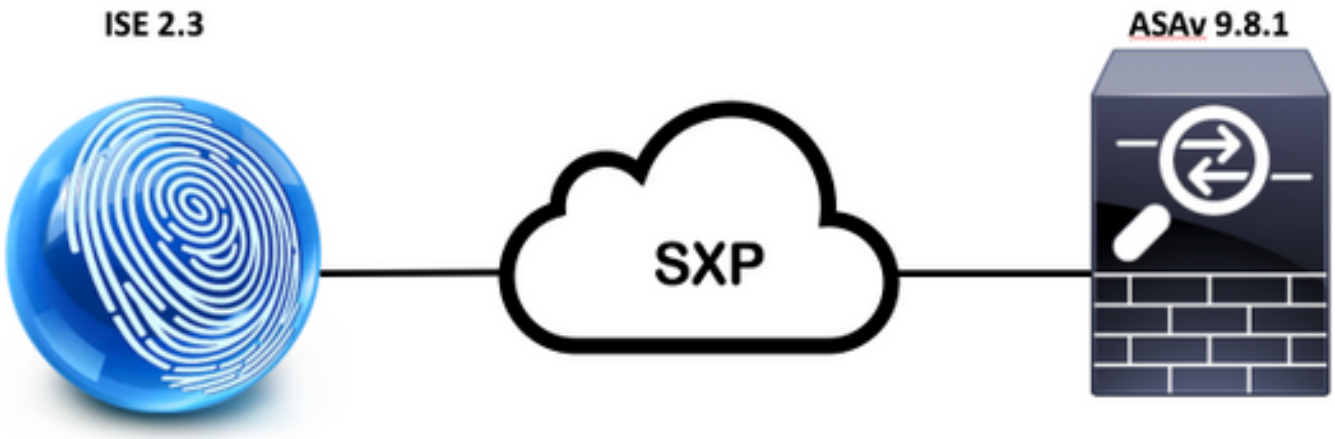
사용되는 구성 요소

ISE 2.3

ASAv 9.8.1

ASDM 7.8.1.150

네트워크 다이어그램



IP 주소

ISE:14.36.143.223

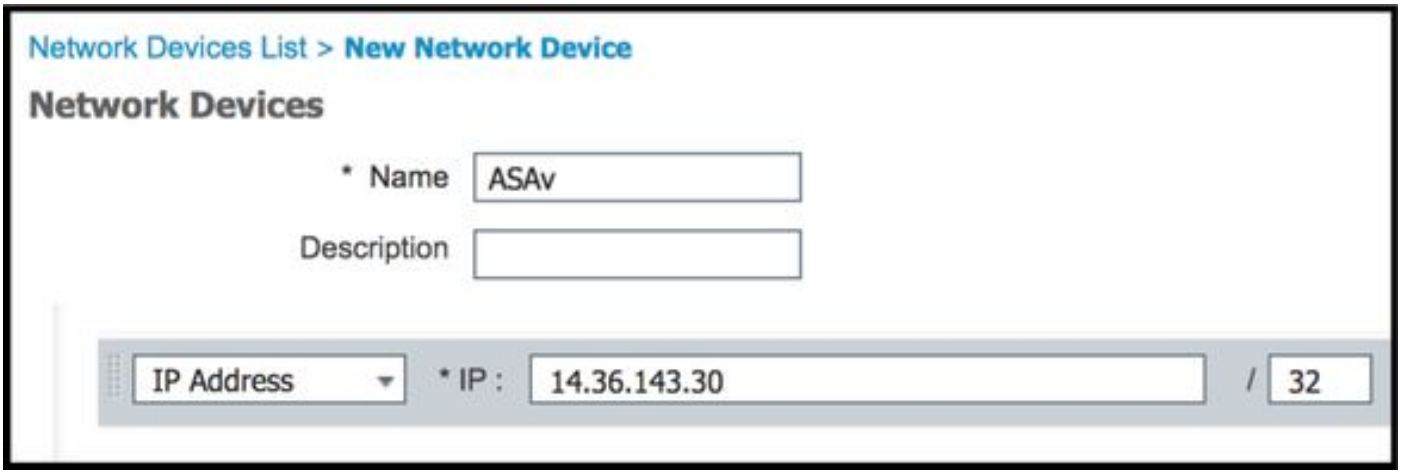
ASAv:14.36.143.30

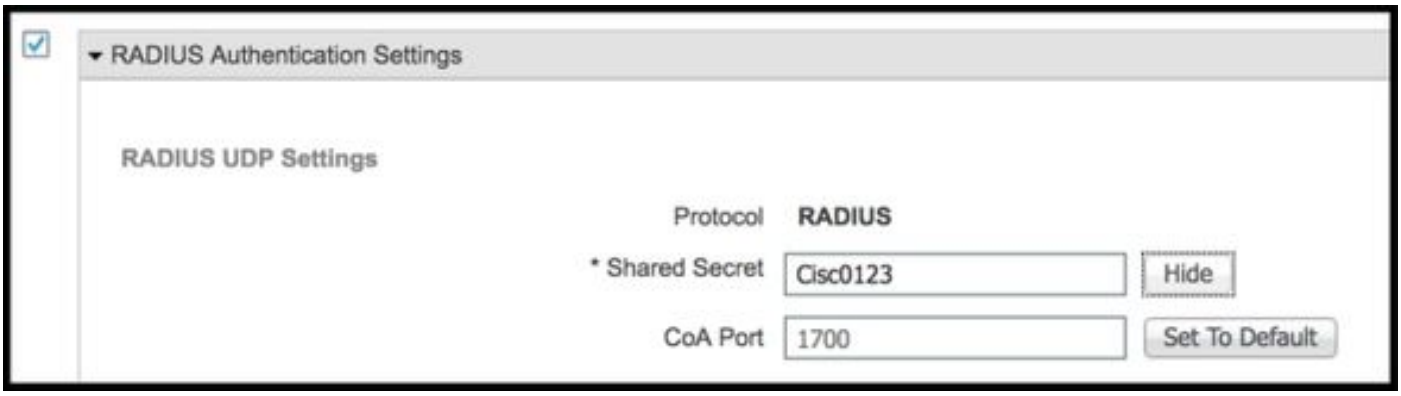
초기 컨피그레이션

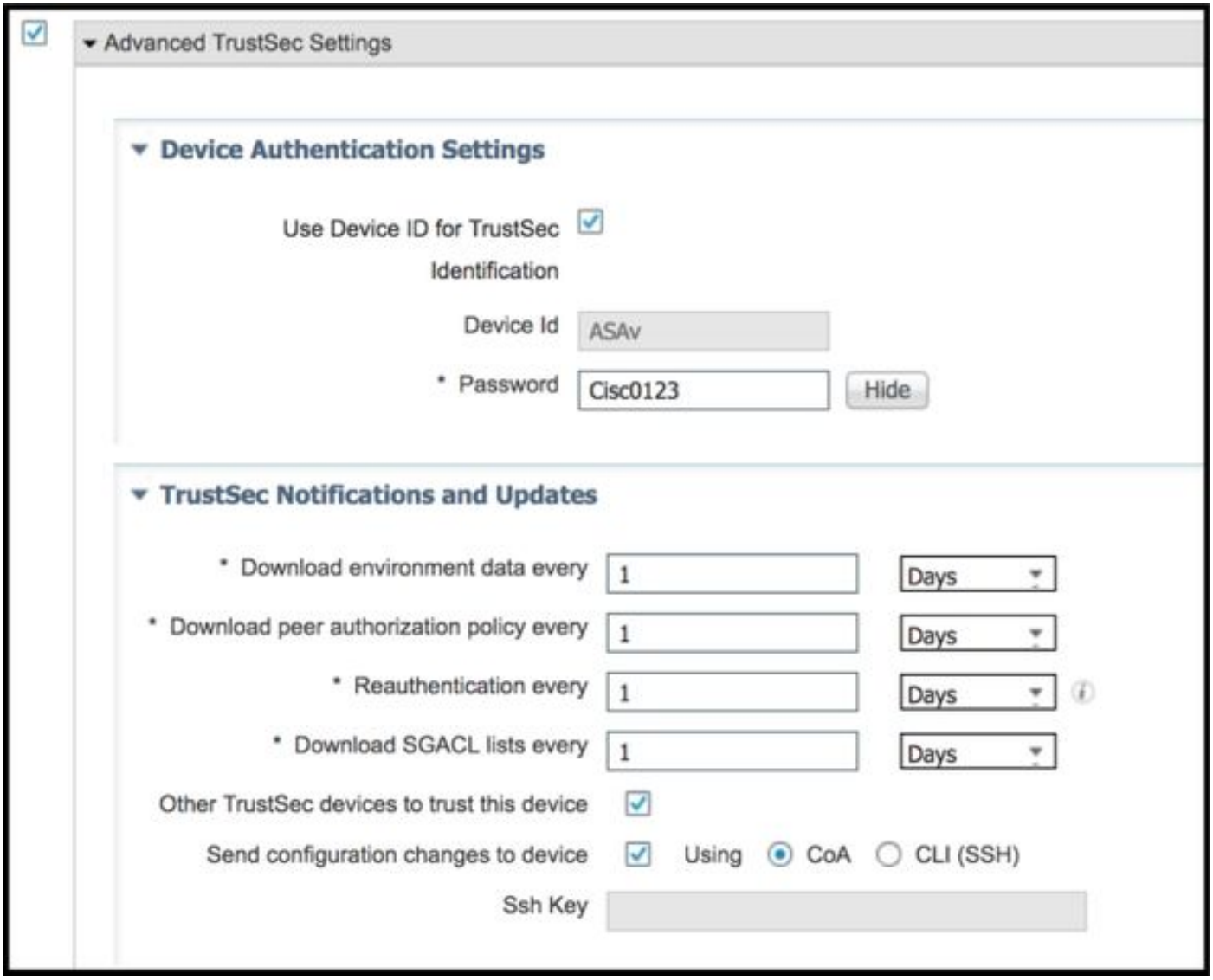
ISE 네트워크 디바이스

ASA를 네트워크 디바이스로 등록

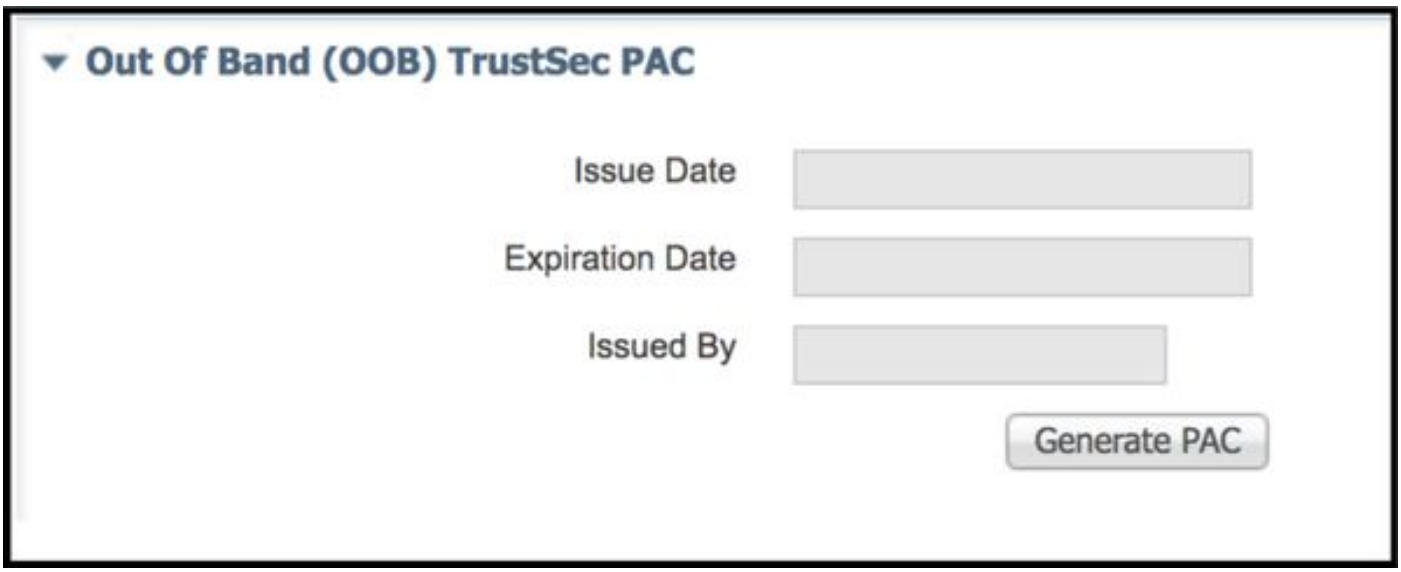
WorkCenters(작업 센터) > TrustSec > Components(구성 요소) > Network Devices(네트워크 디바이스) > **Add(추가)**

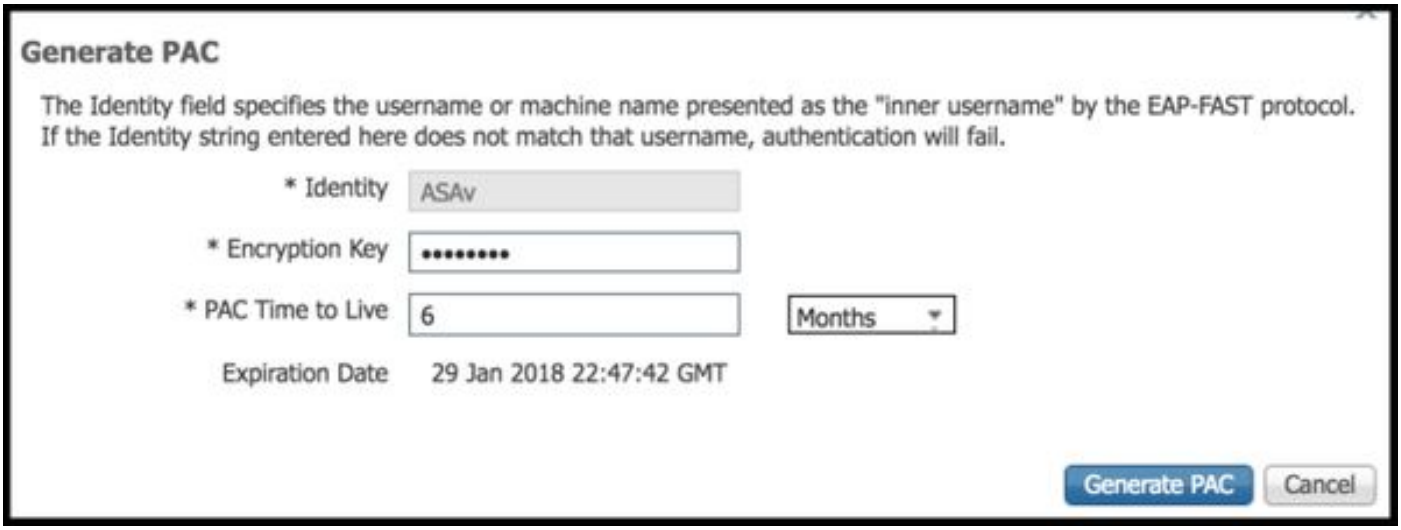


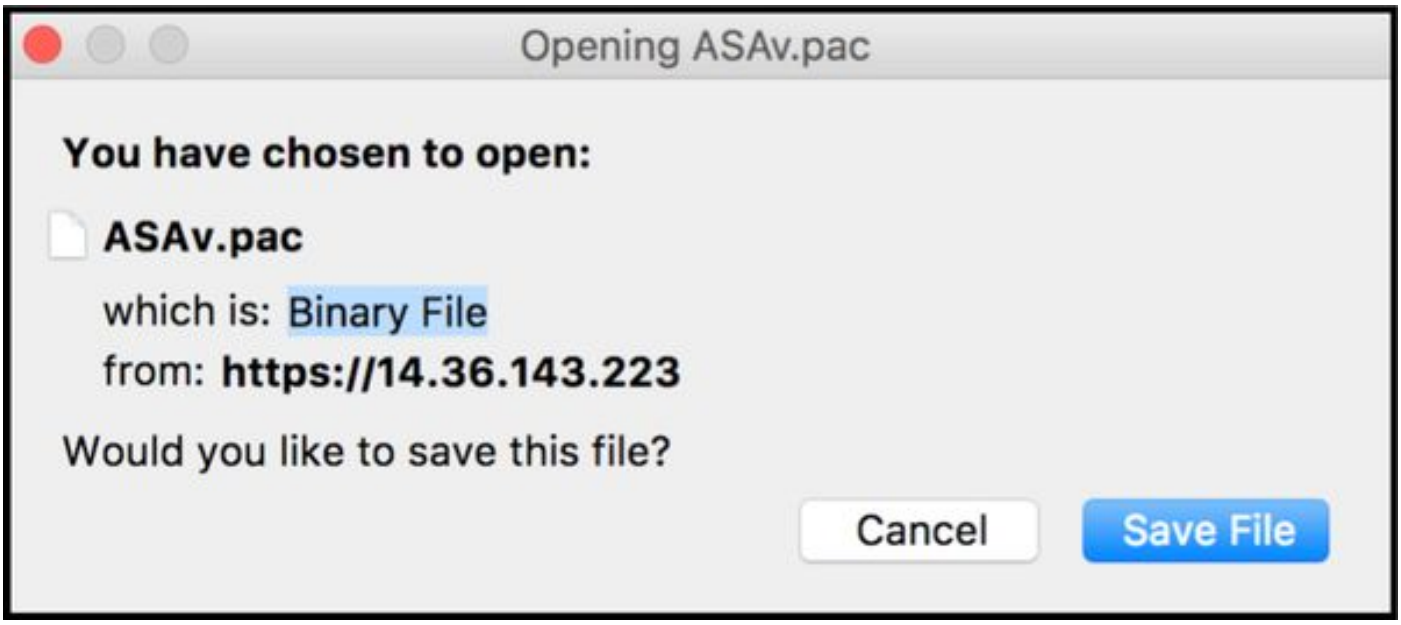




OOB(Out of Band) PAC(Protected Access Credential) 생성 및 다운로드



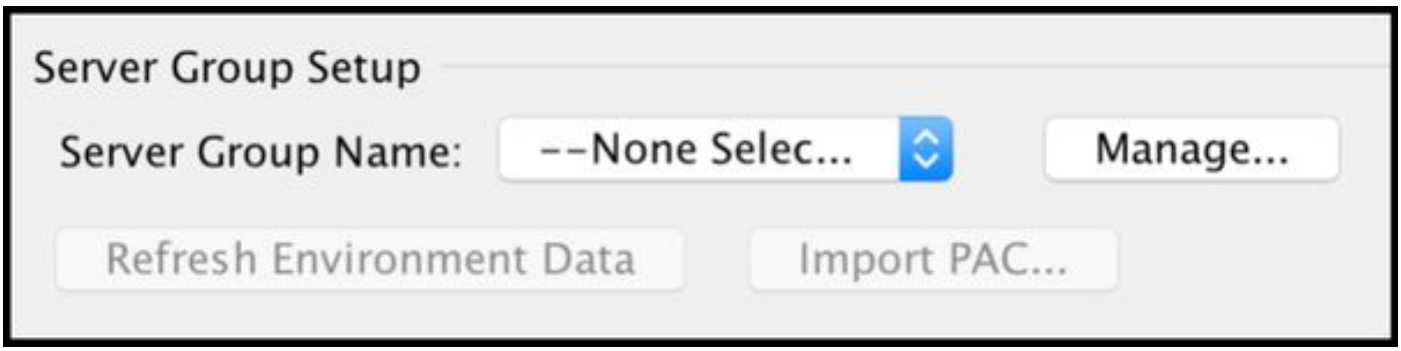




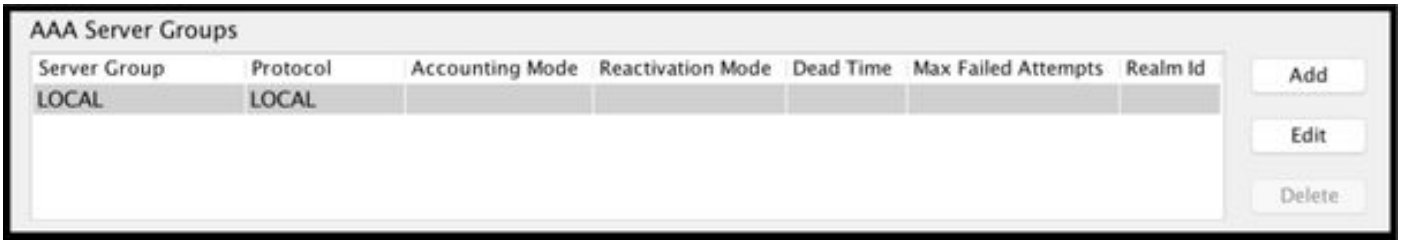
ASDM AAA 서버 컨피그레이션

AAA 서버 그룹 생성

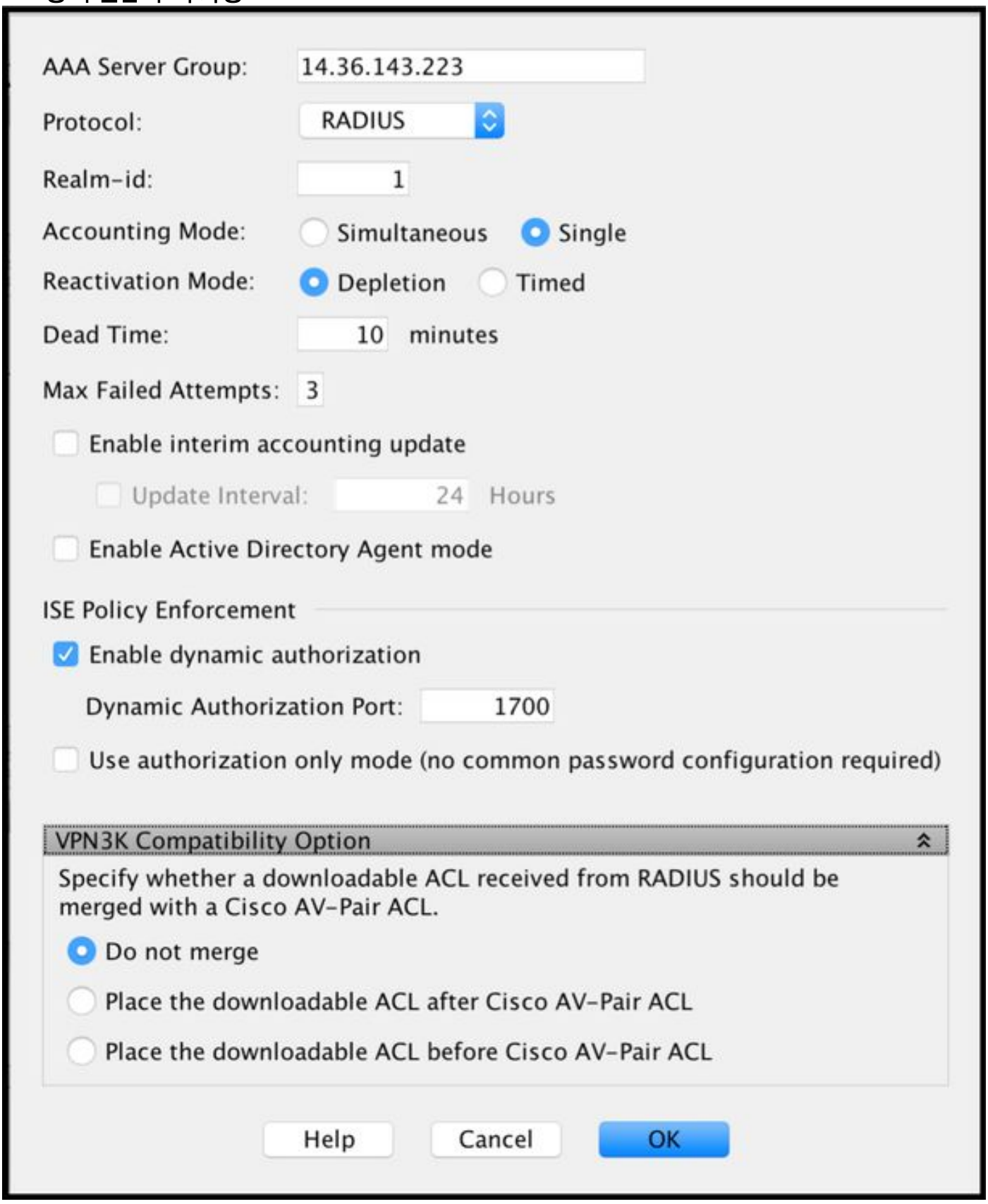
Configuration(컨피그레이션) > Firewall(방화벽) > Identity by TrustSec(TrustSec별 ID) > Server Group Setup(서버 그룹 설정) > **Manage(관리)...**



AAA Server Groups(AAA 서버 그룹) > **Add(추가)**

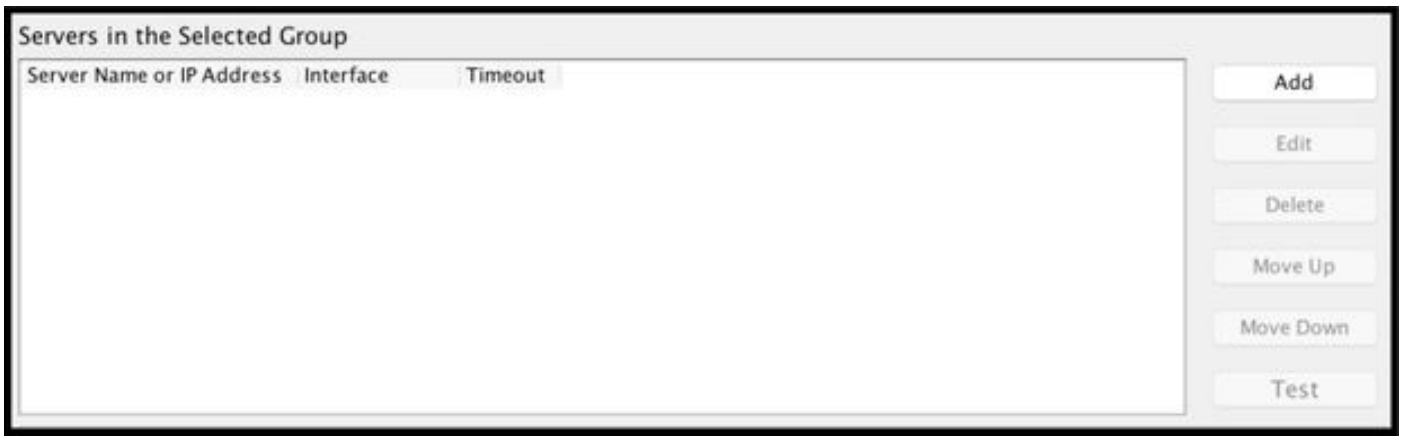


- AAA 서버 그룹:**<그룹 이름>**
- **동적 권한 부여 사용**

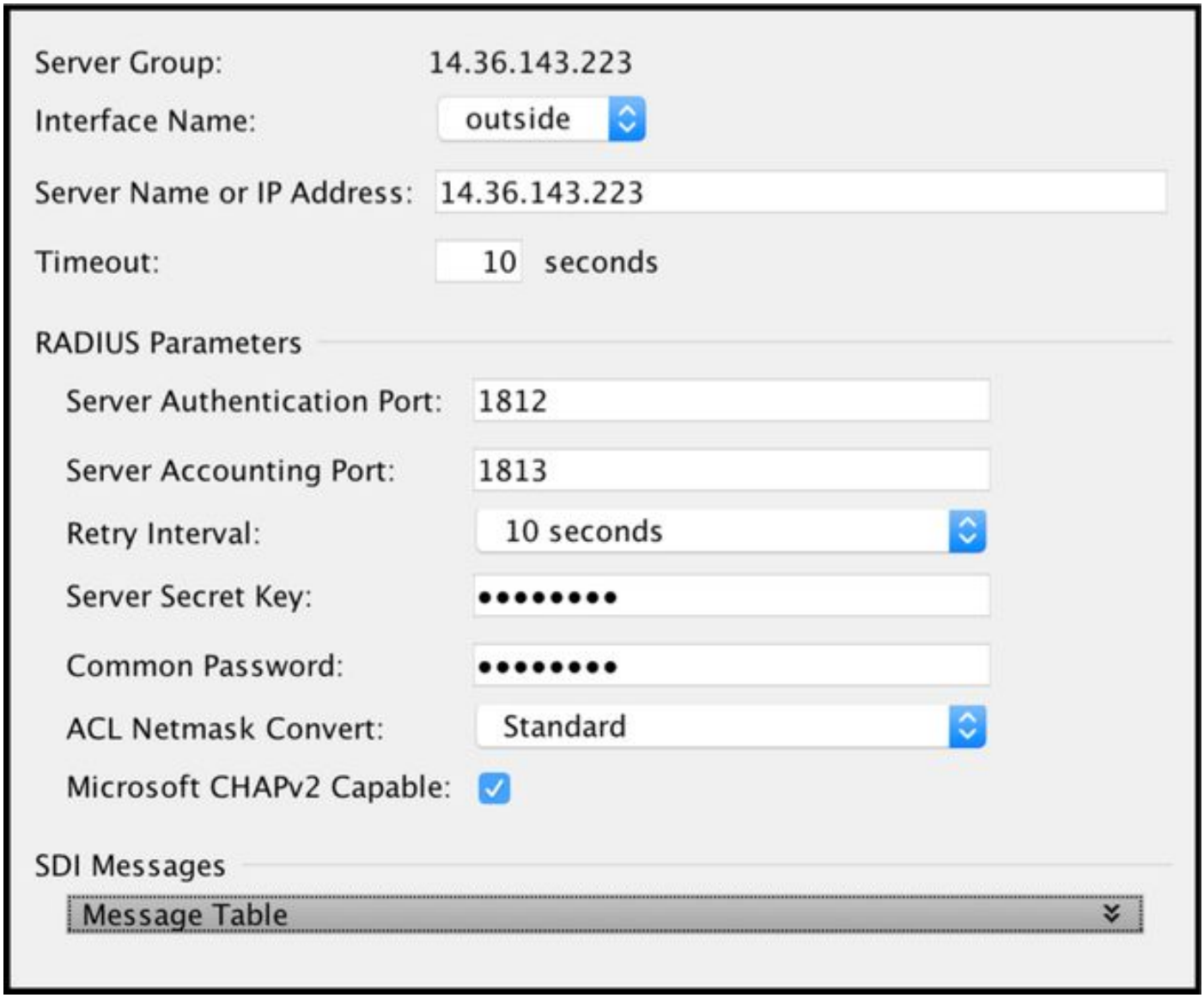


서버 그룹에 서버 추가

선택한 그룹의 서버 > **추가**

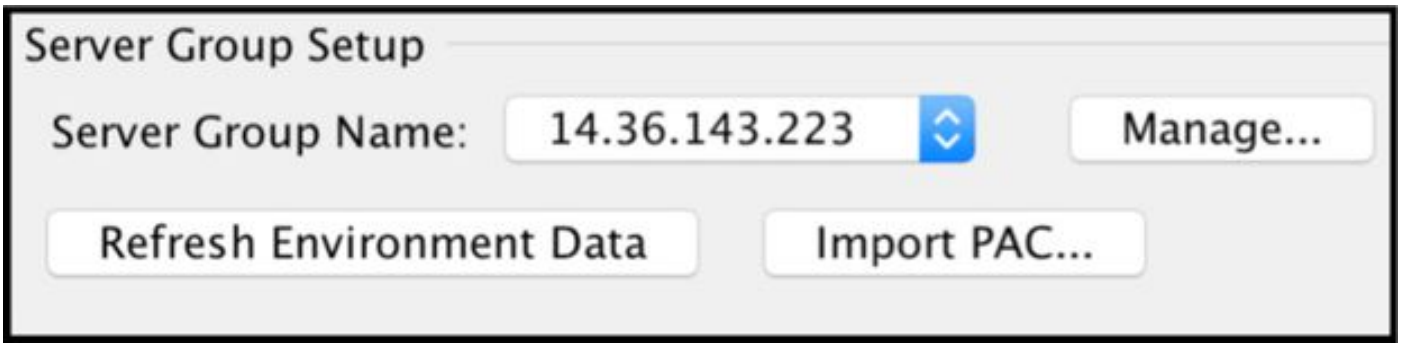


- 서버 이름 또는 IP 주소:**<ISE IP 주소>**
- 서버 인증 포트:1812
- 서버 계정 포트:1813
- 서버 암호 키:**Cisco0123**
- 일반 암호:**Cisco0123**

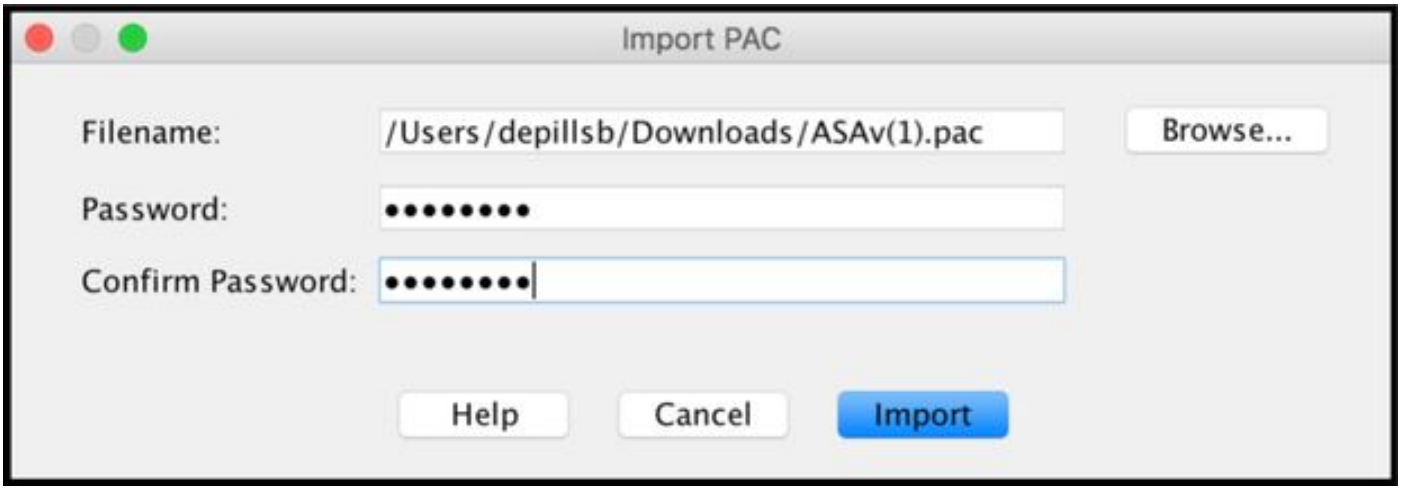


ISE에서 다운로드한 PAC 가져오기

Configuration(컨피그레이션) > Firewall(방화벽) > Identity by TrustSec(TrustSec별 ID) > Server Group Setup(서버 그룹 설정) > **Import PAC(PAC 가져오기)...**



- 암호:**Cisco0123**



환경 데이터 새로 고침

Configuration(컨피그레이션) > Firewall(방화벽) > Identity by TrustSec(TrustSec별 ID) > Server

Group Setup(서버 그룹 설정) > **Refresh Environment Data(환경 데이터 새로 고침)**

확인

ISE 라이브 로그

작업 > RADIUS > **라이브 로그**

Authentication Details

Source Timestamp	2017-07-30 00:05:53.432
Received Timestamp	2017-07-30 00:05:53.433
Policy Server	ISE23
Event	5233 TrustSec Data Download Succeeded
Username	#CTSREQUEST#
Network Device	ASAv
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	14.36.143.30
NAS Port Type	Virtual
Security Group	TrustSec_Devices
Response Time	33 milliseconds

CiscoAVPair	cts-environment-data=ASAv, cts-environment-version=1, cts-device-capability=env-data-fragment, cts-pac-opaque=****, coa-push=true

Result

State	ReauthSession:0e248fdff2l7TiOfK10NeCx1yRhjPAO8_ssZ9U9VVy/o3dfT_tk
Class	CACS:0e248fdff2l7TiOfK10NeCx1yRhjPAO8_ssZ9U9VVy/o3dfT_tk:ISE23/290687604/9
cisco-av-pair	cts:server-list=CTSServerList1-0001
cisco-av-pair	cts:security-group-tag=0002-02
cisco-av-pair	cts:environment-data-expiry=86400
cisco-av-pair	cts:security-group-table=0001-18

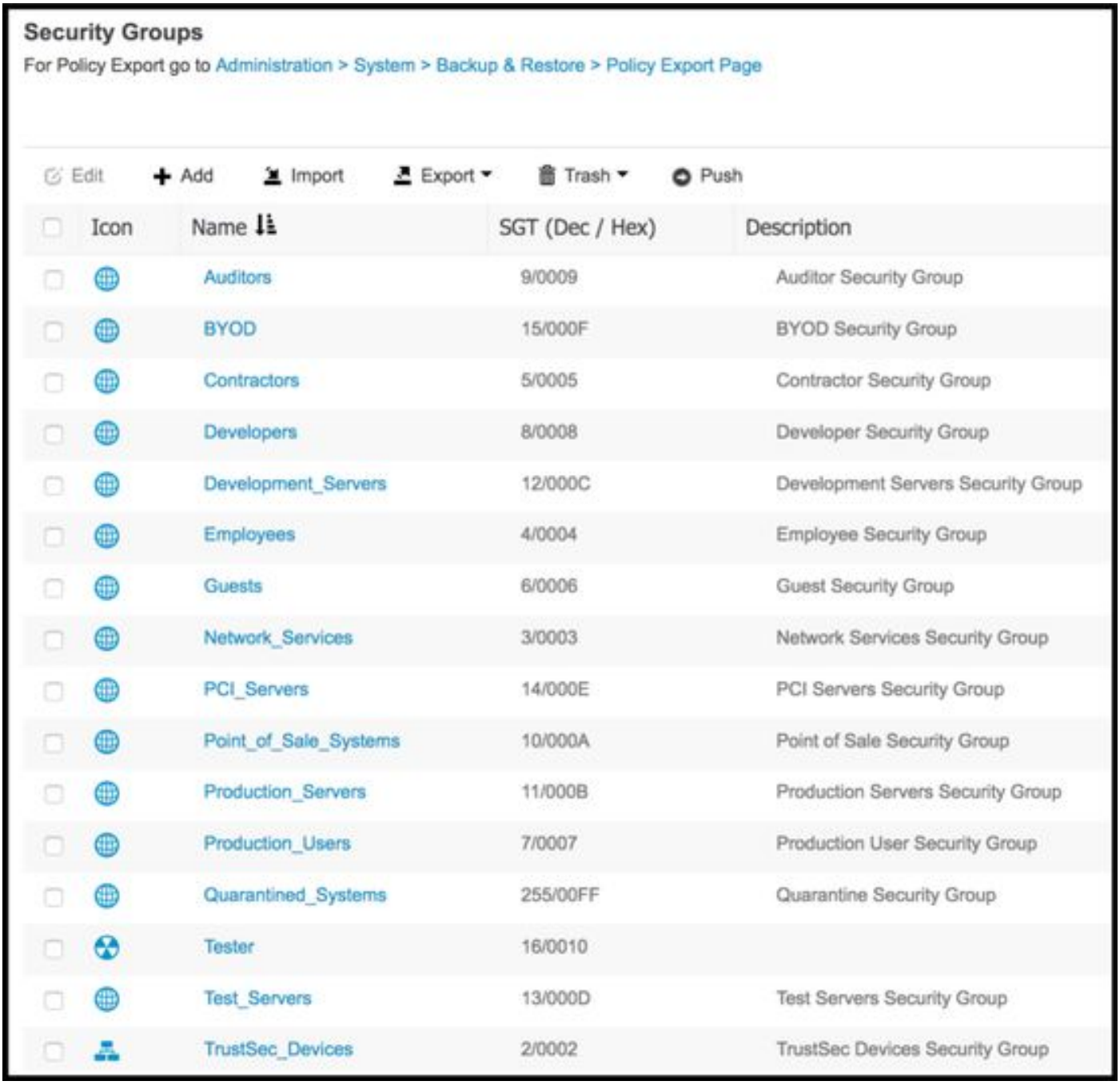
CiscoAVPair	cts-security-group-table=0001, cts-pac-opaque=****, coa-push=true

Result

State	ReauthSession:0e248fdfc4PVaU72zvhHwsT3F4qpdgq4rMsifPkqEcQiG4O_YZw
Class	CACS:0e248fdfc4PVaU72zvhHwsT3F4qpdgq4rMsifPkqEcQiG4O_YZw:ISE23/290687604/10
cisco-av-pair	cts:security-group-table=0001-18
cisco-av-pair	cts:security-group-info=0-0-00-Unknown
cisco-av-pair	cts:security-group-info=ffff-1-00-ANY
cisco-av-pair	cts:security-group-info=9-0-00-Auditors
cisco-av-pair	cts:security-group-info=f-0-00-BYOD
cisco-av-pair	cts:security-group-info=5-0-00-Contractors
cisco-av-pair	cts:security-group-info=8-0-00-Developers
cisco-av-pair	cts:security-group-info=c-0-00-Development_Servers
cisco-av-pair	cts:security-group-info=4-0-00-Employees
cisco-av-pair	cts:security-group-info=6-2-00-Guests
cisco-av-pair	cts:security-group-info=3-0-00-Network_Services
cisco-av-pair	cts:security-group-info=e-0-00-PCI_Servers
cisco-av-pair	cts:security-group-info=a-0-00-Point_of_Sale_Systems
cisco-av-pair	cts:security-group-info=b-0-00-Production_Servers
cisco-av-pair	cts:security-group-info=7-0-00-Production_Users
cisco-av-pair	cts:security-group-info=ff-0-00-Quarantined_Systems
cisco-av-pair	cts:security-group-info=d-0-00-Test_Servers
cisco-av-pair	cts:security-group-info=2-2-00-TrustSec_Devices
cisco-av-pair	cts:security-group-info=10-0-00-Tester

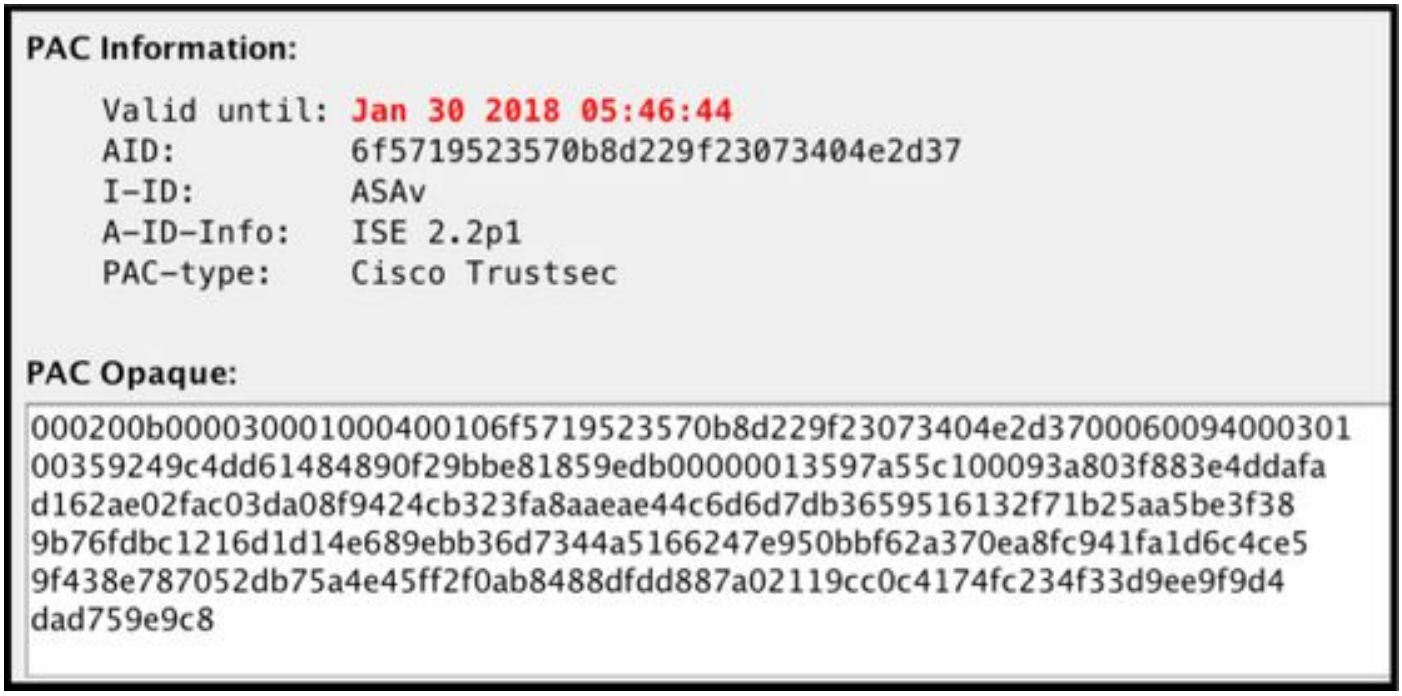
ISE 보안 그룹

작업 센터 > TrustSec > 구성 요소 > **보안 그룹**



ASDM PAC

Monitoring > Properties > Identity by TrustSec > **PAC**



ASDM 환경 데이터 및 보안 그룹

Monitoring > Properties > Identity by TrustSec > **Environment Data**

Environment Data:

```
Status:                     Active
Last download attempt:      Successful
Environment Data Lifetime: 86400 secs
Last update time:           21:07:01 UTC Jul 29 2017
Env-data expires in:        0:21:39:07 (dd:hr:mm:sec)
Env-data refreshes in:      0:21:29:07 (dd:hr:mm:sec)
```

Security Group Table:

```
Valid until:                21:07:01 UTC Jul 30 2017
Total entries:              18
```

Name	Tag	Type
ANY	65535	unicast
Auditors	9	unicast
BYOD	15	unicast
Contractors	5	unicast
Developers	8	unicast
Development_Servers	12	unicast
Employees	4	unicast
Guests	6	unicast
Network_Services	3	unicast
PCI_Servers	14	unicast
Point_of_Sale_Systems	10	unicast
Production_Servers	11	unicast
Production_Users	7	unicast
Quarantined_Systems	255	unicast
Test_Servers	13	unicast
Tester	16	unicast
TrustSec_Devices	2	unicast
Unknown	0	unicast

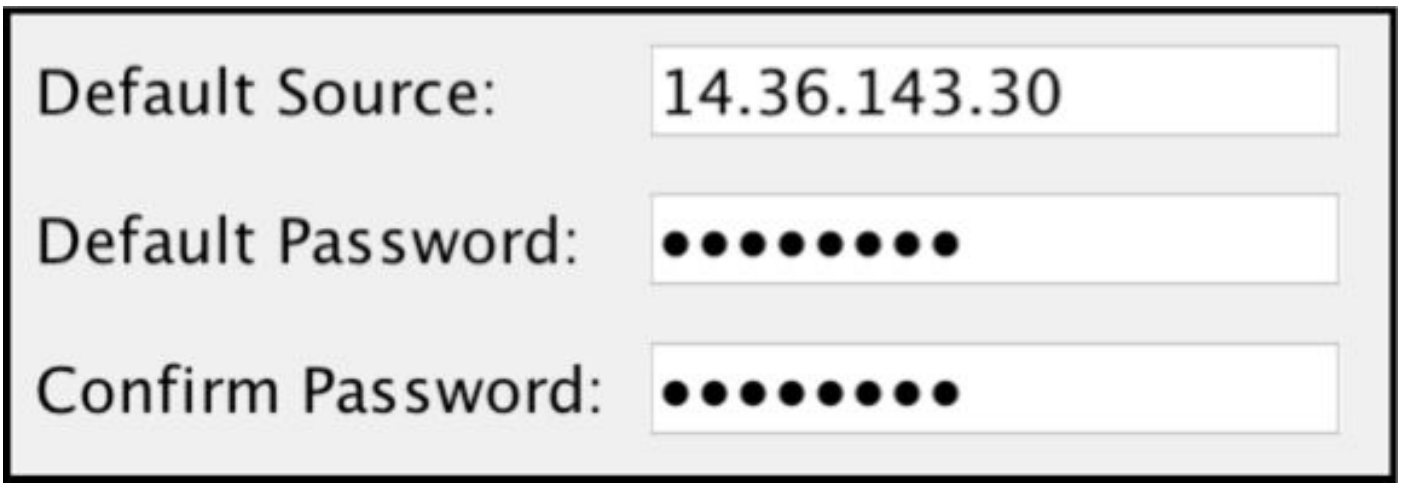
ASDM SXP 컨피그레이션

SXP 사용

Configuration(컨피그레이션) > Firewall(방화벽) > Identity by TrustSec(TrustSec별 ID) > **Enable SGT Exchange Protocol(SXP 활성화)**

기본 SXP 소스 IP 주소 및 기본 SXP 비밀번호 설정

Configuration(컨피그레이션) > Firewall(방화벽) > Identity by TrustSec(TrustSec별 ID) > **Connection Peers(연결 피어)**



SXP 피어 추가

Configuration(컨피그레이션) > Firewall(방화벽) > Identity by TrustSec(TrustSec별 ID) > Connection Peers(연결 피어) > **Add(추가)**

- 피어 IP 주소:**<ISE IP 주소>**

ISE SXP 컨피그레이션

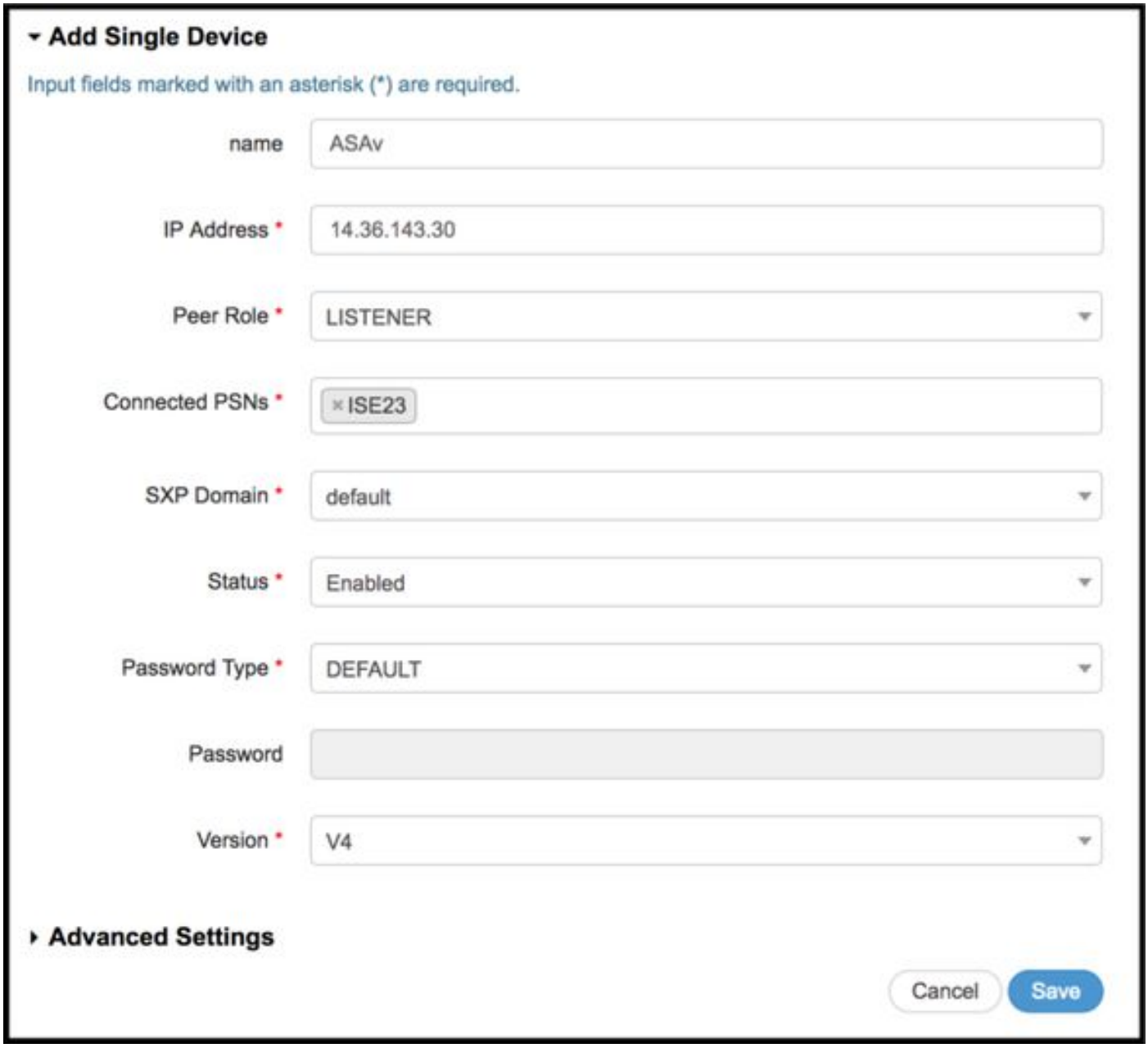
전역 SXP 비밀번호 설정

WorkCenters(작업 센터) > TrustSec > Settings(설정) > **SXP Settings(SXP 설정)**

- 전역 암호:**Cisco0123**

SXP 장치 추가

WorkCenters(작업 센터) > TrustSec > SXP > SXP Devices(SXP 디바이스) > **Add(추가)**



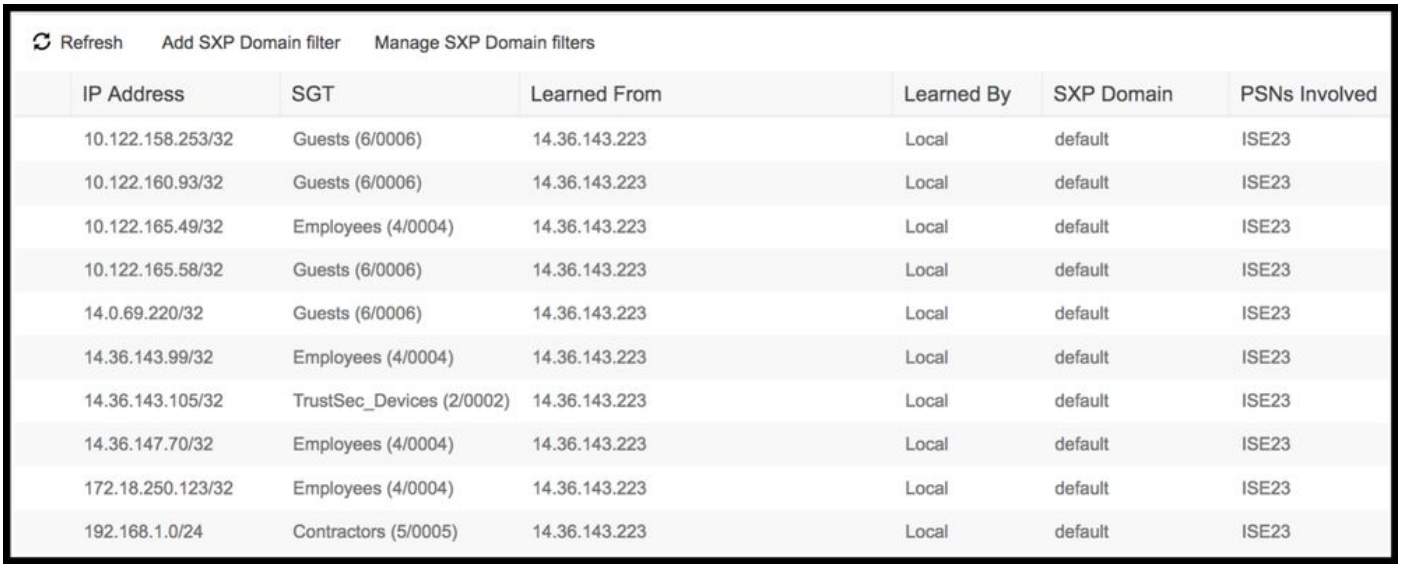
SXP 확인

ISE SXP 확인

WorkCenters(작업 센터) > TrustSec > SXP > **SXP Devices(SXP 디바이스)**

ISE SXP 매핑

WorkCenters(작업 센터) > TrustSec > SXP > **모든 SXP 매핑**

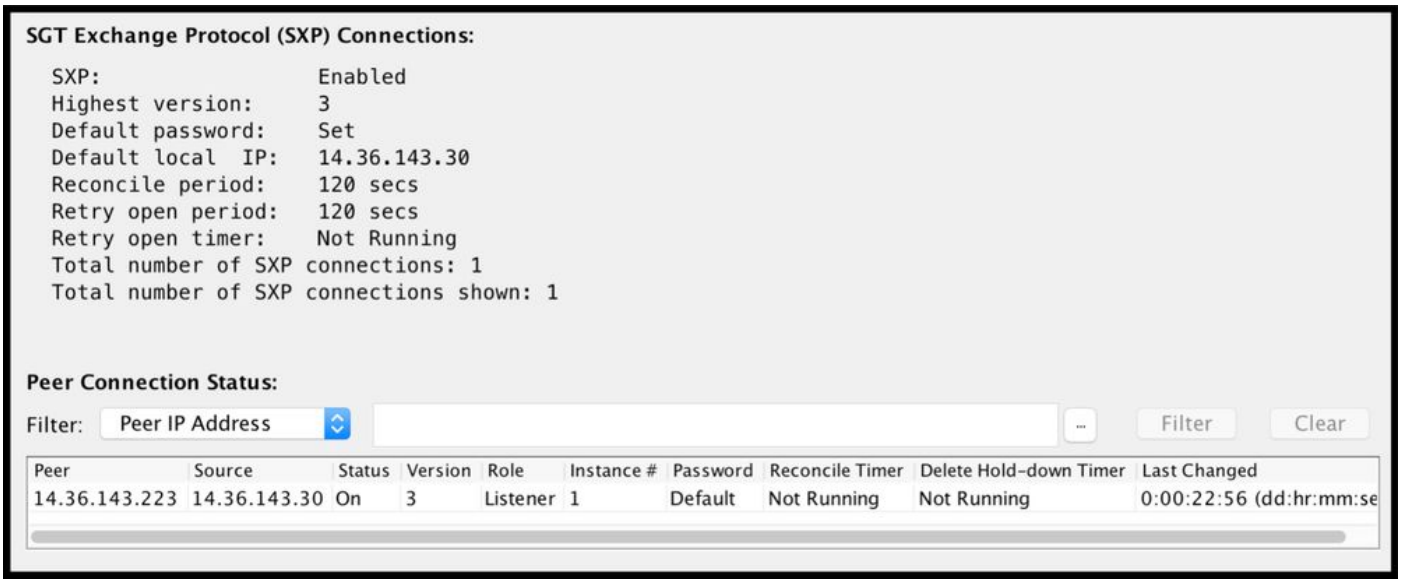


Refresh Add SXP Domain filter Manage SXP Domain filters

IP Address	SGT	Learned From	Learned By	SXP Domain	PSNs Involved
10.122.158.253/32	Guests (6/0006)	14.36.143.223	Local	default	ISE23
10.122.160.93/32	Guests (6/0006)	14.36.143.223	Local	default	ISE23
10.122.165.49/32	Employees (4/0004)	14.36.143.223	Local	default	ISE23
10.122.165.58/32	Guests (6/0006)	14.36.143.223	Local	default	ISE23
14.0.69.220/32	Guests (6/0006)	14.36.143.223	Local	default	ISE23
14.36.143.99/32	Employees (4/0004)	14.36.143.223	Local	default	ISE23
14.36.143.105/32	TrustSec_Devices (2/0002)	14.36.143.223	Local	default	ISE23
14.36.147.70/32	Employees (4/0004)	14.36.143.223	Local	default	ISE23
172.18.250.123/32	Employees (4/0004)	14.36.143.223	Local	default	ISE23
192.168.1.0/24	Contractors (5/0005)	14.36.143.223	Local	default	ISE23

ASDM SXP 확인

Monitoring > Properties > Identity by TrustSec > **SXP Connections**



SGT Exchange Protocol (SXP) Connections:

```
SXP:                  Enabled
Highest version:      3
Default password:     Set
Default local  IP:    14.36.143.30
Reconcile period:     120 secs
Retry open period:    120 secs
Retry open timer:     Not Running
Total number of SXP connections: 1
Total number of SXP connections shown: 1
```

Peer Connection Status:

Filter: Peer IP Address ... Filter Clear

Peer	Source	Status	Version	Role	Instance #	Password	Reconcile Timer	Delete Hold-down Timer	Last Changed
14.36.143.223	14.36.143.30	On	3	Listener	1	Default	Not Running	Not Running	0:00:22:56 (dd:hr:mm:se

ASDM에서 SXP IP와 SGT 간 매핑 학습

Monitoring > Properties > Identity by TrustSec > **IP Mappings**

Security Group IP Mapping Table:

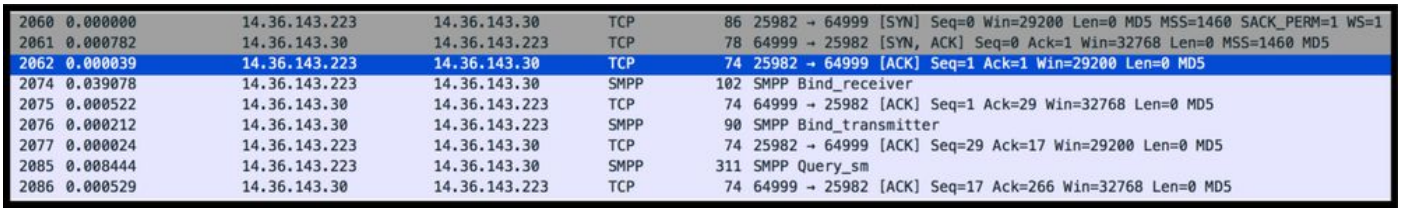
Total number of Security Group IP Mappings: 10

Total number of Security Group IP Mappings shown: 10

Filter: TAG

Tag	Name	IP Address
4	Employees	14.36.143.99
6	Guests	10.122.158.253
6	Guests	10.122.160.93
4	Employees	14.36.147.70
2	TrustSec_Devices	14.36.143.105
4	Employees	172.18.250.123
4	Employees	10.122.165.49
6	Guests	14.0.69.220
6	Guests	10.122.165.58
5	Contractors	192.168.1.0/24

ISE에서 가져온 패킷 캡처



```
2060 0.000000   14.36.143.223   14.36.143.30    TCP    86 25982 → 64999 [SYN] Seq=0 Win=29200 Len=0 MD5 MSS=1460 SACK_PERM=1 WS=1
2061 0.000782   14.36.143.30    14.36.143.223   TCP    78 64999 → 25982 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 MD5
2062 0.000039   14.36.143.223   14.36.143.30    TCP    74 25982 → 64999 [ACK] Seq=1 Ack=1 Win=29200 Len=0 MD5
2074 0.039078   14.36.143.223   14.36.143.30    SMPP  102 SMPP Bind_receiver
2075 0.000522   14.36.143.30    14.36.143.223   TCP    74 64999 → 25982 [ACK] Seq=1 Ack=29 Win=32768 Len=0 MD5
2076 0.000212   14.36.143.30    14.36.143.223   SMPP   90 SMPP Bind_transmitter
2077 0.000024   14.36.143.223   14.36.143.30    TCP    74 25982 → 64999 [ACK] Seq=29 Ack=17 Win=29200 Len=0 MD5
2085 0.008444   14.36.143.223   14.36.143.30    SMPP  311 SMPP Query_sm
2086 0.000529   14.36.143.30    14.36.143.223   TCP    74 64999 → 25982 [ACK] Seq=17 Ack=266 Win=32768 Len=0 MD5
```