

Catalyst 디버그 로그와 함께 ISE SXP 업데이트 로그 이해

목차

[소개](#)

[배경 정보](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[설정](#)

[네트워크 다이어그램](#)

[트래픽 흐름](#)

[스위치 구성](#)

[ISE 구성](#)

[1단계. ISE에서 SXP 서비스 활성화](#)

[2단계. SXP 디바이스 추가](#)

[3단계. SXP 설정](#)

[다음을 확인합니다.](#)

[1단계. 스위치의 SXP 연결](#)

[2단계. ISE SXP 확인](#)

[3단계. Radius 계정 관리](#)

[4단계. ISE SXP 매핑](#)

[5단계. 스위치의 SXP 매핑](#)

[문제 해결](#)

[ISE 보고서](#)

[ISE에서 디버깅](#)

[스위치의 디버그](#)

[관련 정보](#)

소개

이 문서에서는 ISE와 Catalyst 9300 스위치 간의 SXP(Security Group Exchange Protocol) 연결을 구성하고 이해하는 방법에 대해 설명합니다.

배경 정보

SXP는 TrustSec에서 TrustSec 디바이스에 IP-SGT 매핑을 전파하는 데 사용하는 SGT(Security Group Tag) 교환 프로토콜입니다.

SXP는 SGT 인라인 태깅을 지원하지 않는 타사 디바이스 또는 레거시 Cisco 디바이스를 비롯한 네

트위크에서 TrustSec 기능을 사용할 수 있도록 개발되었습니다.

SXP는 피어링 프로토콜입니다. 한 디바이스는 스피커로 작동하고 다른 디바이스는 리스너로 작동할 수 있습니다.

SXP 스피커는 IP-SGT 바인딩을 전송하고 리스너는 이러한 바인딩을 수집하는 역할을 담당합니다.

SXP 연결에서는 TCP 포트 64999을 기본 전송 프로토콜로 사용하고 메시지 무결성/신뢰성을 위해 MD5를 사용합니다.

사전 요구 사항

요구 사항

Cisco에서는 SXP 프로토콜 및 ISE(Identity Services Engine) 컨피그레이션에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

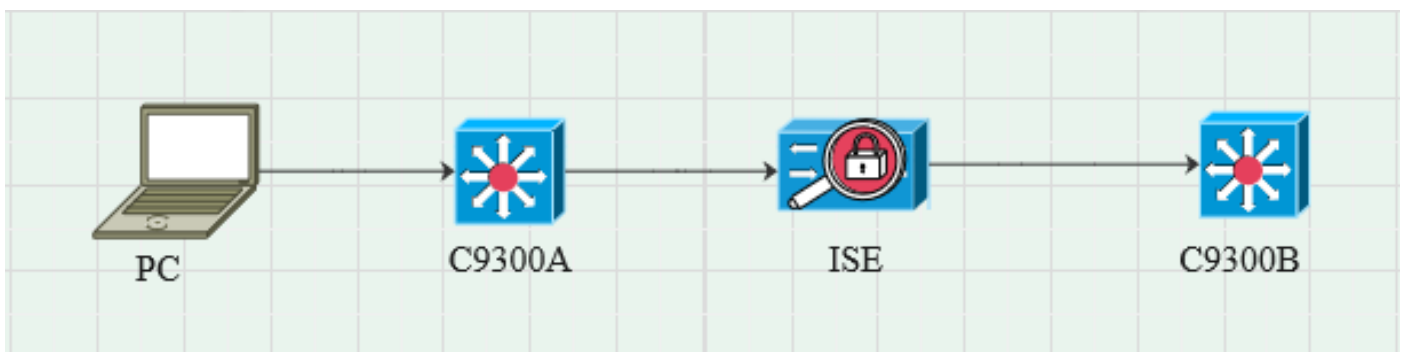
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Catalyst 9300 스위치(소프트웨어 Cisco IOS® XE 17.6.5 이상)
Cisco ISE, 릴리스 3.1 이상

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.

설정

네트워크 다이어그램



트래픽 흐름

PC는 C9300A로 인증하고 ISE는 정책 집합을 통해 SGT를 동적으로 할당합니다.

인증이 통과되면 정책에서 구성된 대로 Framed-IP 주소 RADIUS 특성과 SGT와 동일한 IP를 사용하여 바인딩이 생성됩니다.

바인딩은 기본 도메인 아래의 "모든 SXP 바인딩"에 전파됩니다.
C9300B는 SXP 프로토콜을 통해 ISE로부터 SXP 매핑 정보를 수신합니다.

스위치 구성

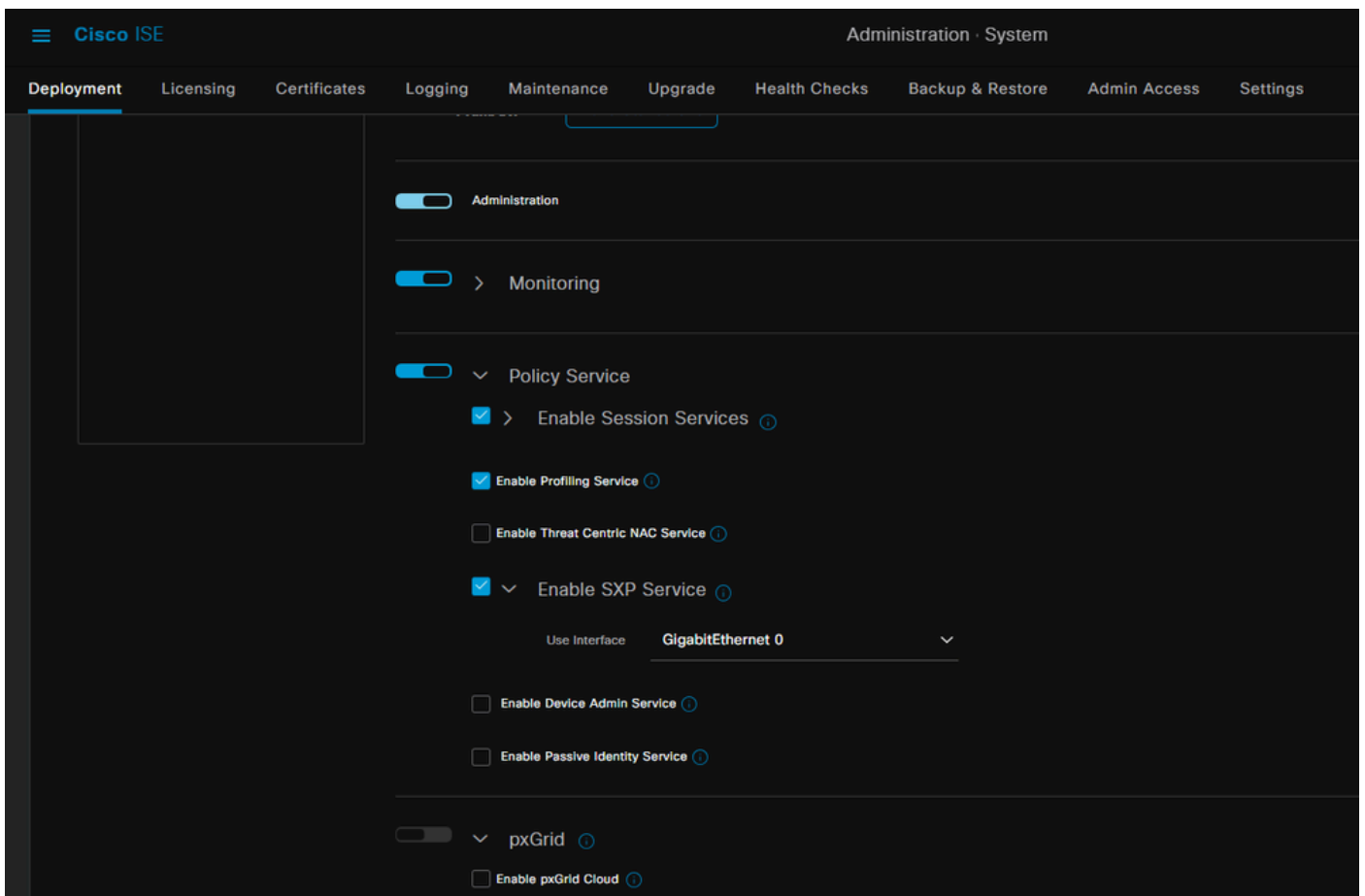
ISE에서 IP에 SGT 매핑을 가져오려면 스위치를 SXP 리스너로 구성합니다.

```
cts sxp 사용
cts sxp 기본 비밀번호 cisco
cts sxp default source-ip 10.127.213.27
cts sxp 연결 피어 10.127.197.53 비밀번호 기본 모드 피어 스피커 보류 시간 0 0 vrf Mgmt-vrf
```

ISE 구성

1단계. ISE에서 SXP 서비스 활성화

Administration(관리) > System(시스템) > Deployment(구축) > Edit the node(노드 편집)로 이동하고 Policy Service(정책 서비스)에서 Enable SXP Service(SXP 서비스 활성화)를 선택합니다.



2단계. SXP 디바이스 추가

해당 스위치에 대해 SXP 수신기 및 스피커를 구성하려면 Workcenters(작업 센터) > Trustsec >

SXP > SXP Devices(SXP 디바이스)로 이동합니다.

피어 역할이 있는 스위치를 리스너로 추가하고 기본 도메인에 할당합니다.

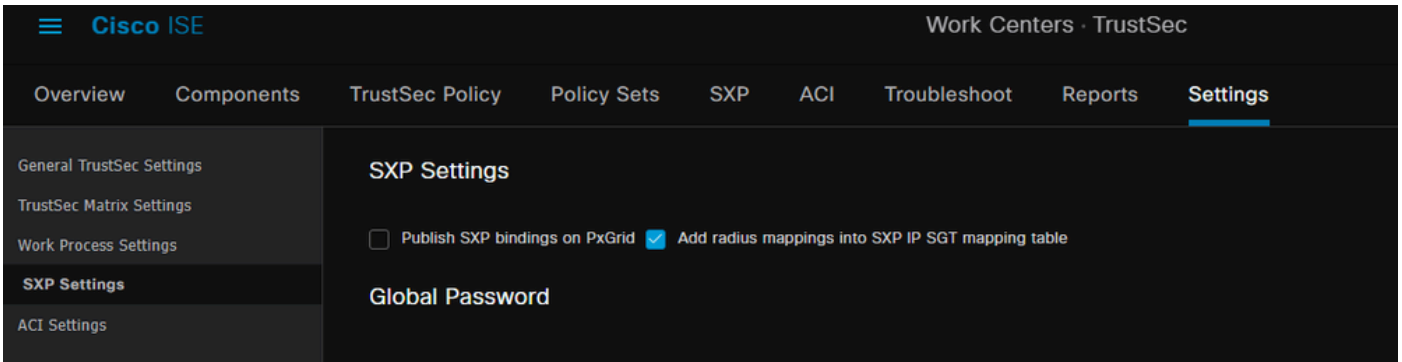
The screenshot displays the Cisco ISE configuration interface for an SXP device. The main content area is titled 'SXP Devices' and contains a form for configuring a device named 'c9300B'. The form includes the following fields and values:

- Name: c9300B
- IP Address *: 10.127.213.27
- Peer Role *: LISTENER
- Connected PSNs *: pk3-1a
- SXP Domains *: default
- Status *: Enabled
- Password Type *: CUSTOM
- Password: (empty)
- Version *: V4

At the bottom of the form, there is an 'Advanced Settings' section. The page also features a navigation menu with options: Overview, Components, TrustSec Policy, Policy Sets, SXP, ACI, Troubleshoot, Reports, and Settings. The top right corner indicates the current work center is 'TrustSec'.

3단계. SXP 설정

Add radius mappings into SXP IP SGT mapping table(SXP IP SGT 매핑 테이블에 RADIUS 매핑 추가)이 선택되어 있는지 확인하여 ISE가 Radius 인증을 통해 동적 IP에 SGT 매핑을 학습하도록 합니다.



다음을 확인합니다.

1단계. 스위치의 SXP 연결

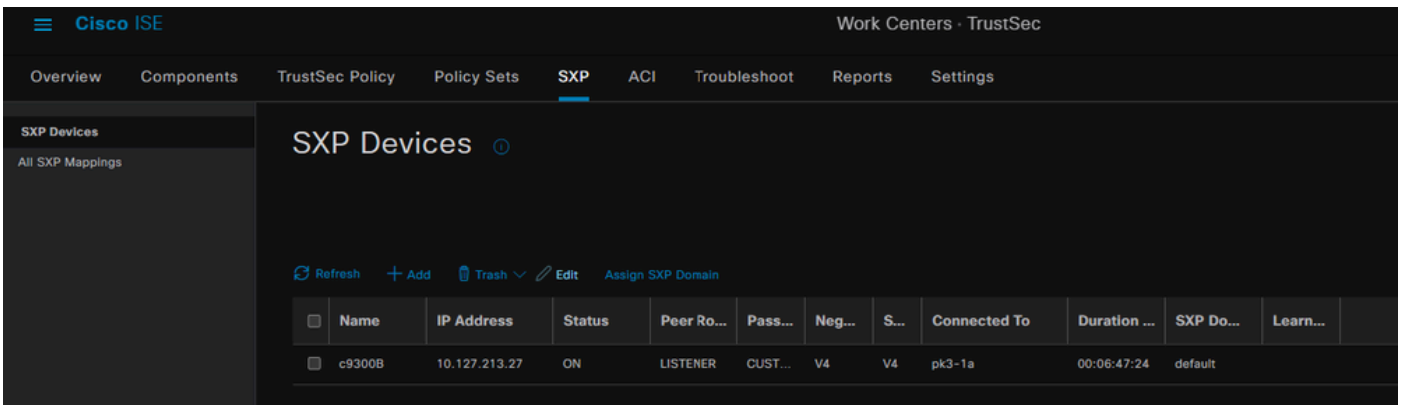
```
C9300B#show cts sxp connections vrf Mgmt-vrf
SXP: 활성화됨
지원되는 최고 버전: 4
기본 비밀번호: 설정
기본 키 체인: 설정되지 않음
기본 키 체인 이름: 해당 없음
기본 소스 IP: 10.127.213.27
연결 다시 시도 열기 기간: 120초
조정 기간: 120초
열기 재시도 타이머가 실행되고 있지 않습니다.
내보내기에 대한 피어 시퀀스 통과 제한: 설정되지 않음
가져오기에 대한 피어 시퀀스 통과 제한: 설정되지 않음
-----
피어 IP: 10.127.197.53
소스 IP: 10.127.213.27
연결 상태: 켜짐
Conn 버전: 4
Conn 기능: IPv4-IPv6-서브넷
Conn 보류 시간: 120초
로컬 모드: SXP 수신기
연결 inst#: 1
TCP conn fd: 1
TCP 연결 비밀번호: 기본 SXP 비밀번호
보류 타이머가 실행 중입니다.
마지막 상태 변경 이후의 기간: 0:00:23:36(dd:hr:mm:초)

총 SXP 연결 수 = 1

0x7F128DF555E0 VRF:Mgmt-vrf, fd: 1, 피어 ip: 10.127.197.53
cdbp:0x7F128DF555E0 Mgmt-vrf <10.127.197.53, 10.127.213.27> tableid:0x1
```

2단계. ISE SXP 확인

Workcenters(작업 센터) > Trustsec > SXP > SXP Devices(SXP 디바이스) 아래에서 스위치에 대한 SXP 상태가 ON(켜짐)인지 확인합니다.

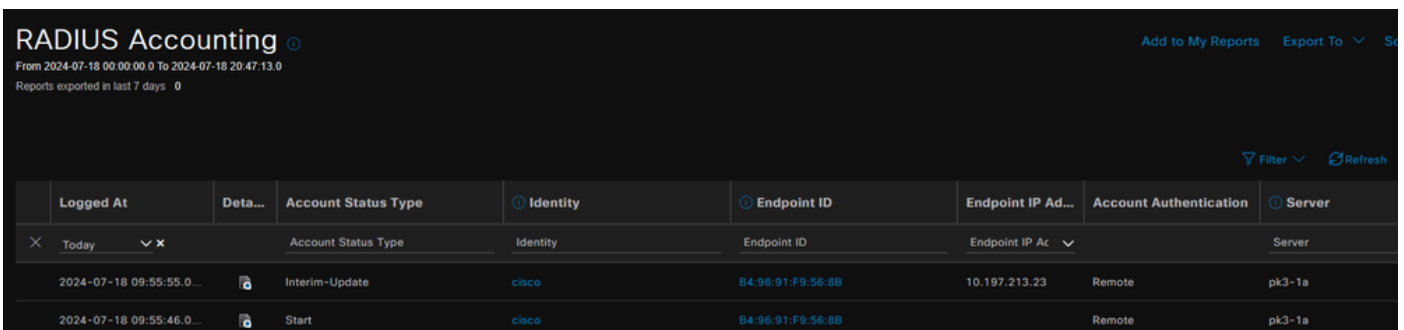


The screenshot shows the Cisco ISE interface for SXP Devices. The navigation menu includes Overview, Components, TrustSec Policy, Policy Sets, SXP (selected), ACI, Troubleshoot, Reports, and Settings. The main content area is titled 'SXP Devices' and contains a table with the following data:

Name	IP Address	Status	Peer Ro...	Pass...	Neg...	S...	Connected To	Duration ...	SXP Do...	Learn...
c9300B	10.127.213.27	ON	LISTENER	CUST...	V4	V4	pk3-1a	00:06:47:24	default	

3단계. Radius 계정 관리

성공적인 인증 후 ISE가 Radius 계정 관리 패킷에서 프레이밍 IP 주소 RADIUS 특성을 받았는지 확인합니다.

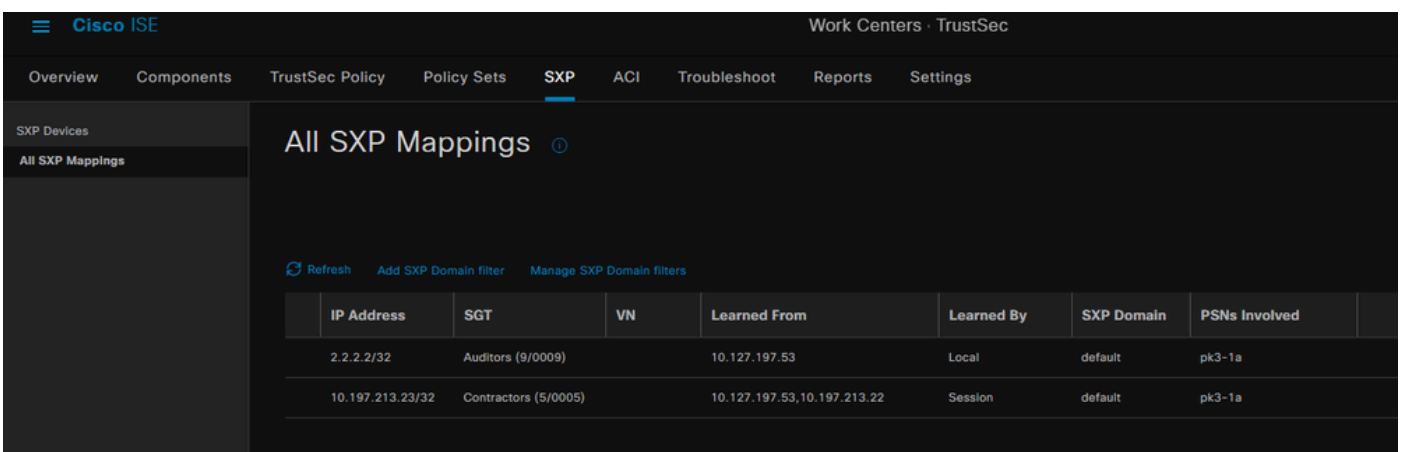


The screenshot shows the Cisco ISE interface for RADIUS Accounting. The page title is 'RADIUS Accounting' and it displays a table of accounting records. The table has the following data:

Logged At	Account Status Type	Identity	Endpoint ID	Endpoint IP Ad...	Account Authentication	Server
2024-07-18 09:55:55.0...	Interim-Update	cisco	B4-96:91:F9-56:8B	10.197.213.23	Remote	pk3-1a
2024-07-18 09:55:46.0...	Start	cisco	B4-96:91:F9-56:8B		Remote	pk3-1a

4단계. ISE SXP 매핑

Workcenters(작업 센터) > Trustsec > SXP > All SXP Mappings(모든 SXP 매핑)로 이동하여 Radius 세션에서 동적으로 학습된 IP에 SGT 매핑을 확인합니다.



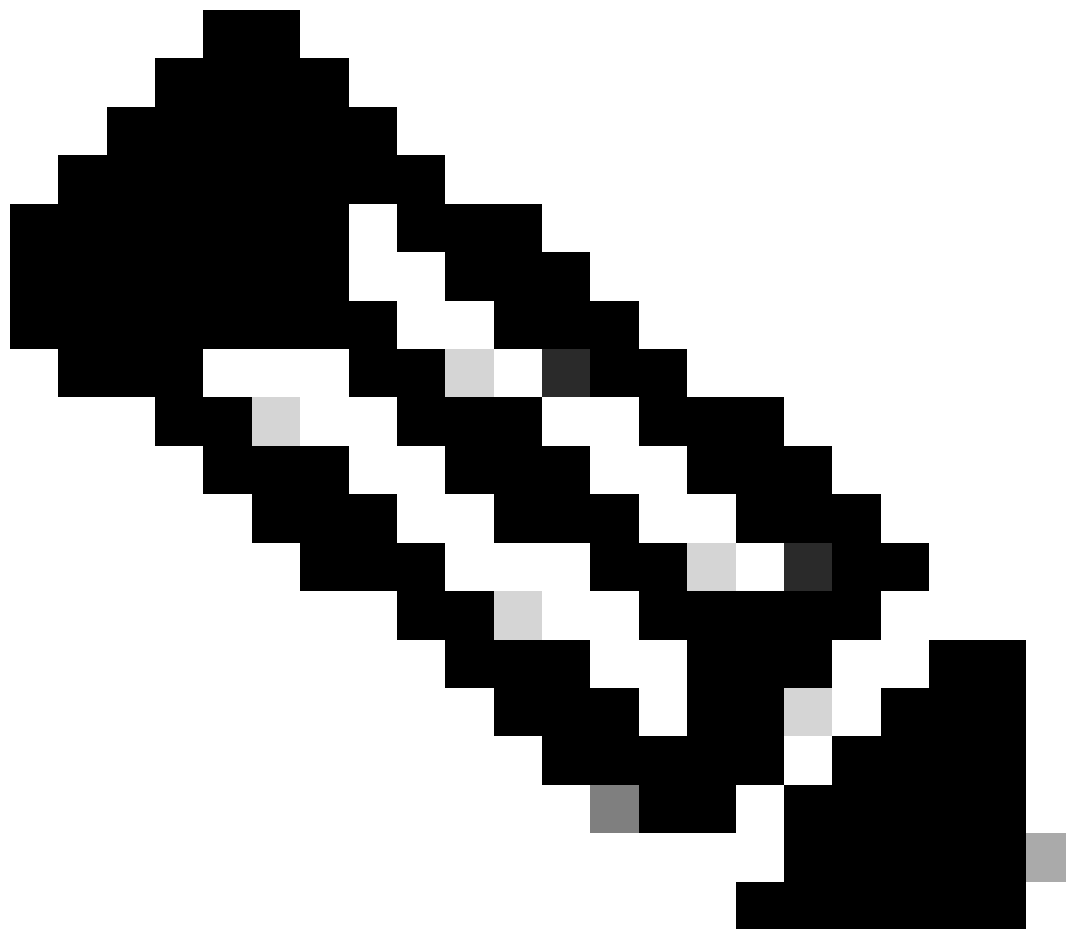
The screenshot shows the Cisco ISE interface for All SXP Mappings. The navigation menu includes Overview, Components, TrustSec Policy, Policy Sets, SXP (selected), ACI, Troubleshoot, Reports, and Settings. The main content area is titled 'All SXP Mappings' and contains a table with the following data:

IP Address	SGT	VN	Learned From	Learned By	SXP Domain	PSNs Involved
2.2.2.2/32	Auditors (9/0009)		10.127.197.53	Local	default	pk3-1a
10.197.213.23/32	Contractors (5/0005)		10.127.197.53,10.197.213.22	Session	default	pk3-1a

학습자

Local - ISE에서 정적으로 할당된 IP-SGT 바인딩입니다.

Session - Radius 세션에서 동적으로 학습된 IP-SGT 바인딩입니다.



참고: ISE에는 다른 디바이스에서 IP-SGT 바인딩을 수신하는 기능이 있습니다. 이러한 바인딩은 모든 SXP 매핑 아래에서 SXP가 학습한 것으로 표시될 수 있습니다.

5단계. 스위치의 SXP 매핑

스위치는 SXP 프로토콜을 통해 ISE에서 IP에 SGT 매핑을 학습했습니다.

```
C9300B#show cts sxp sgt-map vrf Mgmt-vrf brief
SXP 노드 ID(생성됨):0x03030303(3.3.3.3)
다음과 같은 IP-SGT 매핑:
IPv4, SGT: <2.2.2.2 , 9>
IPv4, SGT: <10.197.213.23 , 5>
총 IP-SGT 매핑 수: 2
```

```
sxp_bnd_exp_conn_list의 conn(total:0):  
C9300B#
```

```
C9300B#show cts role-based sgt-map vrf Mgmt-vrf all  
활성 IPv4-SGT 바인딩 정보
```

```
IP 주소 SGT 소스
```

```
=====
```

```
2.2.2.2 9 SXP  
10.197.213.23 5 SXP
```

```
IP-SGT 활성 바인딩 요약
```

```
=====
```

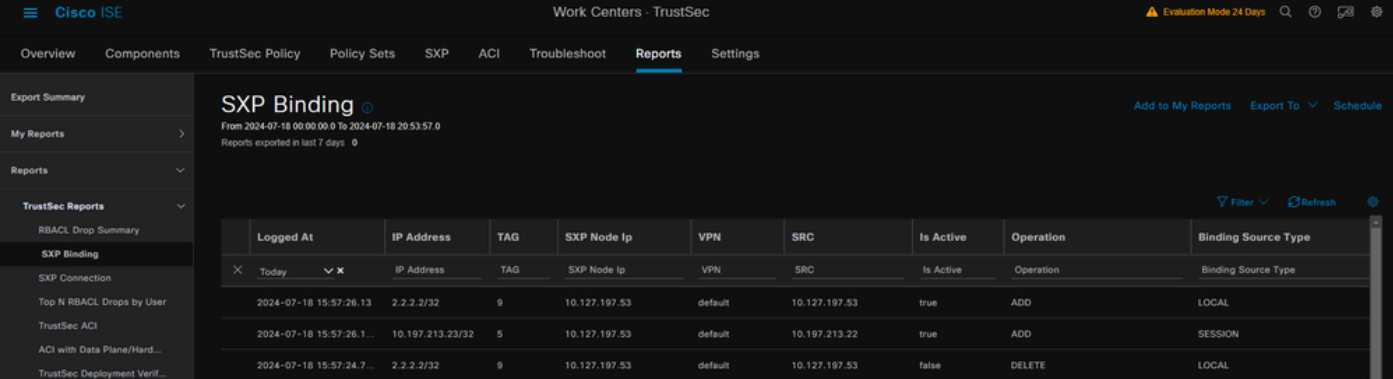
```
총 SXP 바인딩 수 = 2  
총 활성 바인딩 수 = 2
```

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

ISE 보고서

ISE에서는 이 이미지에 표시된 대로 SXP 바인딩 및 연결 보고서를 생성할 수도 있습니다.



The screenshot shows the Cisco ISE interface with the 'Reports' tab selected. The main content area displays the 'SXP Binding' report for the period from 2024-07-18 00:00:00.0 to 2024-07-18 20:53:57.0. The report is presented as a table with the following columns: Logged At, IP Address, TAG, SXP Node Ip, VPN, SRC, Is Active, Operation, and Binding Source Type. The table contains three rows of data.

Logged At	IP Address	TAG	SXP Node Ip	VPN	SRC	Is Active	Operation	Binding Source Type
2024-07-18 15:57:26.13	2.2.2.2/32	9	10.127.197.53	default	10.127.197.53	true	ADD	LOCAL
2024-07-18 15:57:26.1...	10.197.213.23/32	5	10.127.197.53	default	10.197.213.22	true	ADD	SESSION
2024-07-18 15:57:24.7...	2.2.2.2/32	9	10.127.197.53	default	10.127.197.53	false	DELETE	LOCAL

ISE에서 디버깅

다음 속성을 사용하여 디버그 레벨에서 설정할 ISE 지원 번들을 수집합니다.

- sxp
- sgtbinding
- nsf
- nsf 세션
- 트러스트섹(trustsec)

사용자가 ISE 서버에서 인증되면 ISE는 액세스 수락 응답 패킷에 SGT를 할당합니다. 사용자가 IP 주소를 가져오면 스위치는 Radius 어카운팅 패킷에서 프레임 IP 주소를 전송합니다.

show logging application localStore/iseLocalStore.log:

```
2024-07-18 09:55:55.051 +05:30 0000017592 3002 NOTICE Radius-Accounting: RADIUS Accounting watchdog 업데이트, ConfigVersionId=129, Device IP Address=10.197.213.22, UserName=cisco, NetworkDeviceName=pk, User-Name=cisco, NAS-IP-Address=10.197.23.2, NAS-Port=50124 Framed-IP-Address=10.197.213.23, Class=CACS:16D5C50A00000017C425E3C6:pk3-1a/510648097/25, Called-Station-ID=C4-B2-39-ED-AB-18, Calling-Station-ID=B4-96-91-F9-56-8B, Acct-Status-Type=Interim-Update, Acct-Delay-Time=0, Acct-Input-Octets=413, acct-Output-Octets=0, Acct-Session-Id=00000007, Acct-Authentic=Remote, Acct-Input-Packets=4, Acct-Output-Packets=0, Event-Timestamp=1721277745, NAS-Port-Type=Ethernet, NAS-Port-Id=TenGigabitEthernet1/0/24, cisco-av-pair=audit-session-id=16D5C50A00000017C425E3C6, cisco-av-pair=dot1x, cisco-av-pair=cts:security-group-tag=000, Acs SessionID=3 -1a/510648097/28, SelectedAccessService=기본 네트워크 액세스, RequestLatency=6, Step=11004, Step=11017, Step=15049, Step=15008, Step=22085, Step=11005, NetworkDeviceGroups=IPSEC#Is IPSEC Device#No, NetworkDeviceGroups=Location#All Locations, NetworkDeviceGroups=Device Type#All Device Types, CPMSessionID=16D5C50A00000017C425E3C6, TotalAuthenLatency=6, ClientLatency=0, 네트워크 장치 프로파일=Cisco , Location=Location#모든 위치, Device Type=Device Type#모든 디바이스 유형, IPSEC=IPSEC#Is IPSEC Device#No,
```

show logging application ise-psc.log:

```
2024-07-18 09:55:55,054 디버그 [SxpSessionNotifierThread][]  
ise.sxp.sessionbinding.util.SxpBindingUtil -::-  
prrtCpmBridge에서 받은 세션 값 로깅:  
작업 유형 ==>ADD, sessionId ==> 16D5C50A00000017C425E3C6, sessionState ==>  
ACCEPTED, inputIp ==> 10.197.213.23, inputSgTag ==> 0005-00, nasIp ==> 10.197.213.22null,  
vn ==> null
```

SXP 노드는 H2DB 테이블에 IP + SGT 매핑을 저장하며 이후 PAN 노드는 이 IP SGT 매핑을 수집하고 ISE GUI의 모든 SXP 매핑에 반영합니다(Workcenters ->Trustsec ->SXP->All SXP Mappings).

show logging application sxp_appserver/sxp.log:

```
2024-07-18 10:01:01,312 정보 [sxp-service-http-96441] cisco.ise.sxp.rest.SxpGlueRestAPI:147 -  
SXP-PEERF 세션 바인딩 추가 배치 크기: 1  
2024-07-18 10:01:01,317 DEBUG [SxpNotificationSerializer-Thread]  
cpm.sxp.engine.services.NotificationSerializerImpl:202 - 처리 작업 [add=true,  
notification=RestSxpLocalBinding(tag=5, groupName=null, ipAddress=10.197.213.23/32,  
nasIp=10.197.213.22, sessionId=16D5C50A00000017C425E3C6, peerSequence=null,  
sxpBindingOpOp type=null, sessionExpiryTimeInMillis=0, apic=false, routable=true, vns=[])]
```

```
2024-07-18 10:01:01,344 디버그 [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.SxpEngine:1543 - [VPN: 'default'] 새 바인딩 추가: MasterBindingIdentity
[ip=10.197.213.23/32, peerSequence=10.127.197.53,10.197.213.22, tag=5, isLocal=true,
sessionId=16D5C50A00000017C42 E3C6, vn=DEFAULT_VN]
2024-07-18 10:01:01,344 디버그 [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.SxpEngine:1581 - 바인딩 1개 추가
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.MasterDbListener:251 - H2 처리기에 바인딩 추가를 위한 작업 제출, 바인딩
수: 1
2024-07-18 10:01:01,344 디버그 [H2_HANDLER] cisco.cpm.sxp.engine.MasterDbListener:256 -
MasterDbListener Processing onAdded - bindingsCount: 1
```

SXP 노드는 최신 IP-SGT 바인딩으로 피어 스위치를 업데이트합니다.

```
2024-07-18 10:01:01,346 디버그 [pool-7-thread-4]
opendaylight.sxp.core.service.UpdateExportTask:93 -
SXP_PERF:SEND_UPDATE_BUFFER_SIZE=32
2024-07-18 10:01:01,346 디버그 [pool-7-thread-4]
opendaylight.sxp.core.service.UpdateExportTask:116 -
[[SE:10.127.197.53][10.127.197.53:64999/10.127.213.27:31025]][O|Sv4](으)로 SENT_UPDATE
2024-07-18 10:01:01,346 DEBUG [pool-7-thread-4]
opendaylight.sxp.core.service.UpdateExportTask:137 - SENT_UPDATE SUCCESSFUL to
[[SE:10.127.197.53][10.127.197.53:64999/10.127.213.27:31025]][O|Sv4]
```

스위치의 디버그

SXP 연결 및 업데이트 문제를 해결하려면 스위치에서 이러한 디버그를 활성화합니다.

cts sxp conn 디버그

cts sxp 디버그 오류

cts sxp mdb 디버그

cts sxp 메시지 디버그

Switch가 SXP Speaker "ISE"에서 SGT-IP 매핑을 수신했습니다.

다음 로그를 보려면 Show logging을 선택합니다.

```
7월 18일 04:23:04.324: CTS-SXP-MSG:sxp_rcv_update_v4 <1> 피어 ip: 10.127.197.53
7월 18일 04:23:04.324: CTS-SXP-MDB:IMU 피어 10.127.197.53에서 바인딩 추가:- <conn_index
= 1>
7월 18일 04:23:04.324: CTS-SXP-MDB:mdb_send_msg <IMU_ADD_IPSGT_DEVID>
```

```
7월 18일 04:23:04.324: CTS-SXP-INTNL:mdb_send_msg_process_add_ipsgt_devid Start
Jul 18 04:23:04.324: CTS-SXP-MDB:sxp_mdb_inform_rbm tableid:0x1 sense:1 sgt:5
peer:10.127.197.53
7월 18일 04:23:04.324: CTS-SXP-MDB:SXP MDB: 항목 추가 ip 10.197.213.23 sgt 0x0005
7월 18일 04:23:04.324: CTS-SXP-INTNL:mdb_send_msg_process_add_ipsgt_devid 완료
```

관련 정보

[ISE 3.1 관리 가이드 세그멘테이션](#)

[Catalyst 컨피그레이션 가이드 Trustsec 개요](#)

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.