

TrustSec تاي ناكما اهل نوكي نأب بيقرلل رطسلا يف تامالع عضو معدت ال يتلا

امن ي ب توص ربكم ك ةزهجال دحا لمعي نأ نكمي شيح، مزح يف عي مجتلل لوكوتورب وه SXP نإ
يف غصمك رخال لمعي

هذه عي مجت نع الوؤسم عم تسملا نوكي و IP-SGT طباور لاسرا نع لوؤسم SXP توص ربكم
طباورلا

ةلاصا/ةالسل MD5 و ياساسالا لقنلا لوكوتوربك TCP 64999 ذفم SXP لاصتا مدختسي
لائسارلا

ةياساسالا تابلطتملا

تابلطتملا

Identity Services Engine (ISE) و لوكوتورب SXP ل نم ةفرعم تنأ يقلتني نأ ي صوي Cisco
لي كشت

ةمدختسملا تانوكملا

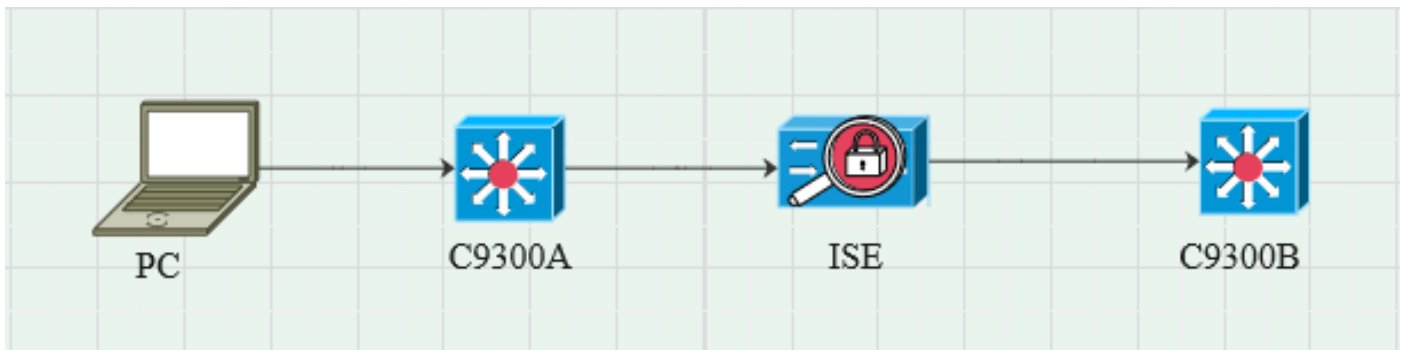
ةيلال ةيداملا تانوكملا و جماربلا تارادصا يلا دن تسملا اذه يف ةدراولا تامولعمل دن تست

- ثدخال تارادصا او Cisco IOS® XE 17.6.5 جمارب Cisco Catalyst 9300 switch ل وجملا
ثدخال تارادصا او 3.1 رادصا، Cisco ISE

ةصاخ ةيلمعم ةئي ي يف ةدوجوملا ةزهجال نم دن تسملا اذه يف ةدراولا تامولعمل ءاشنإ مت
تناك اذا. (يضا رتفا) حوسمم نيوكتب دن تسملا اذه يف ةمدختسملا ةزهجال عي مج تادب
رمأ يال لم تحمل ري ثاتلل كم هف نم دكأتف، لي غشتلا دي ق ك تكبش

نيوكتلا

ةكبش ل لطيطختلا مسرلا



رورملا ةكرح قفدت

لالخ نم يكي مانيد لكشب بيقرلل ISE رايعم ني عي و C9300a زارطلا عم رتوي بكمكلا قداصي
تاسايسلا تاعومجم

ناونعل RADIUS ةمس يواسي IP مادختساب طباورلا عاشنإ متي ،ةقداصملا ريرمت دنع ةسايسلا ي ف هنيوكت مت امك بيقرلا او Framed-IP .
يضايرتفالا لاجملا نمض "SXP طباور ةفاك" ي ف طبورلا ةدعاق .
SXP لوكوتورب لال خ نم ISE نم SXP نينيغت تامولعم C9300B يقرلتي .

لوحملا نيوكت

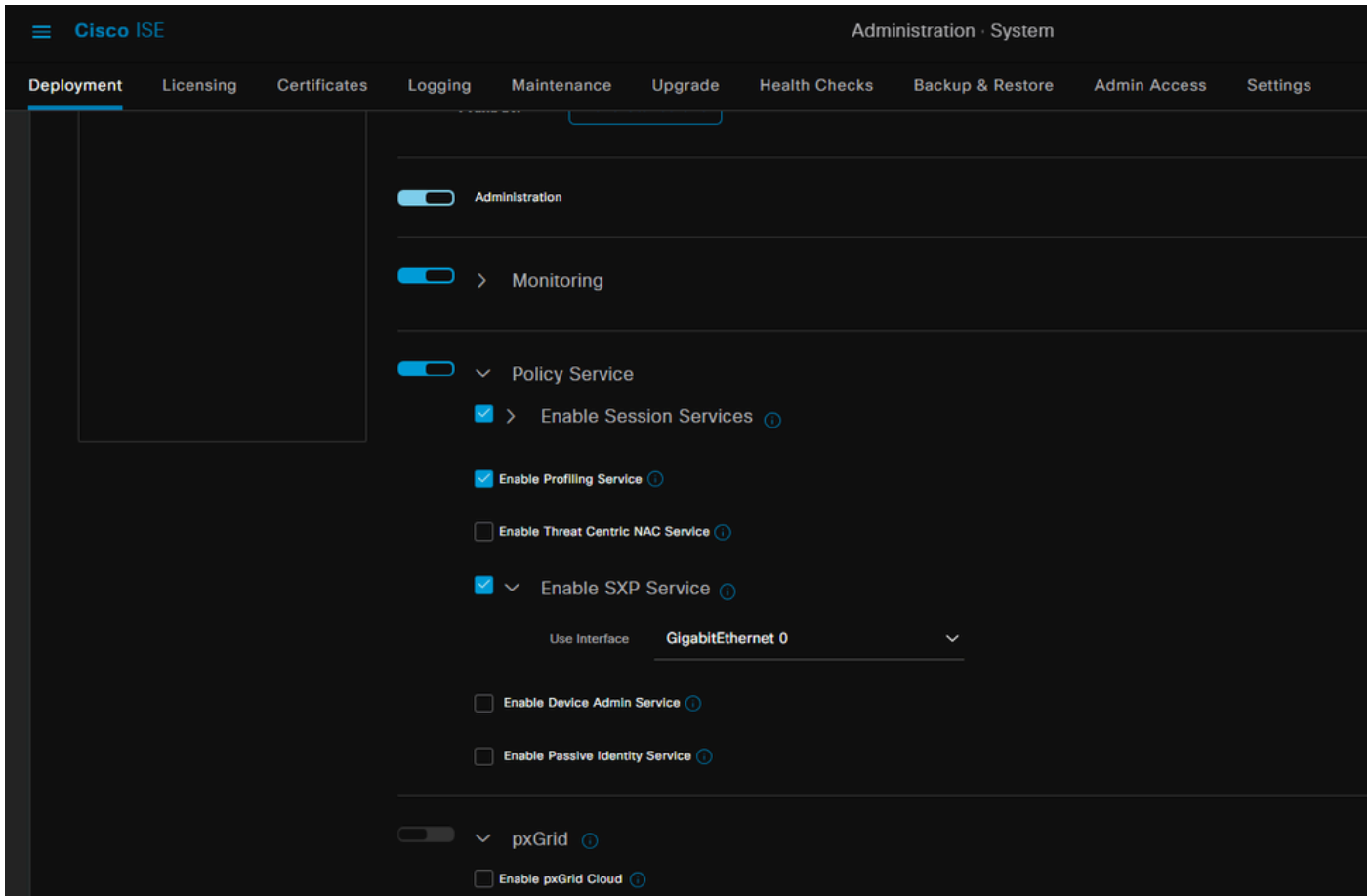
ISE نم IP-SGT تانيغت يلع لوصحلل SXP عمتمسمك لوحملا نيوكتب مق

```
CTS sxp نيكمت  
Cisco نم cts sxp ةيضايرتفالا رورملا ةملاك  
cts sxp default source-ip 10.127.213.27  
ريظنلا توص ربكمل يضايرتفالا عضولا رورم ةملاك 10.127.197.53 CTS sxp لاصتا ريظن  
vrf Mgmt-vrf 0 راطتال اتقو
```

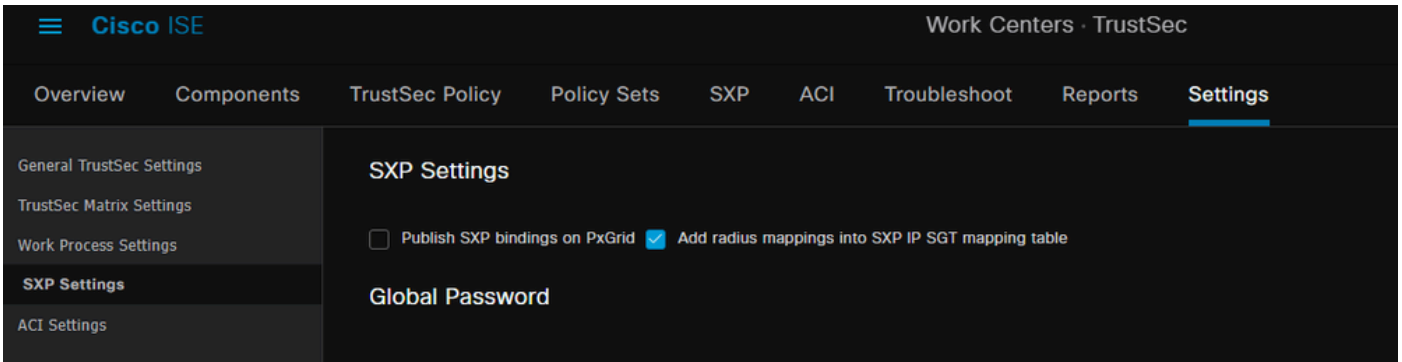
ISE نيوكت

ISE يلع SXP ةمدخ نيكمت 1. ةوطخلا

SXP ةمدخ نيكمت ةسايسلا ةمدخ تحت دحو ،ةدقعالا ريرحت > رشن > ماظن > ةرادا يلا لقتنا



SXP ةزهجأ ةفاضلا 2. ةوطخلا



ةحصلا نم ققحتلا

لوحمل اىل ع SXP لاصتا 1. ةوطخل

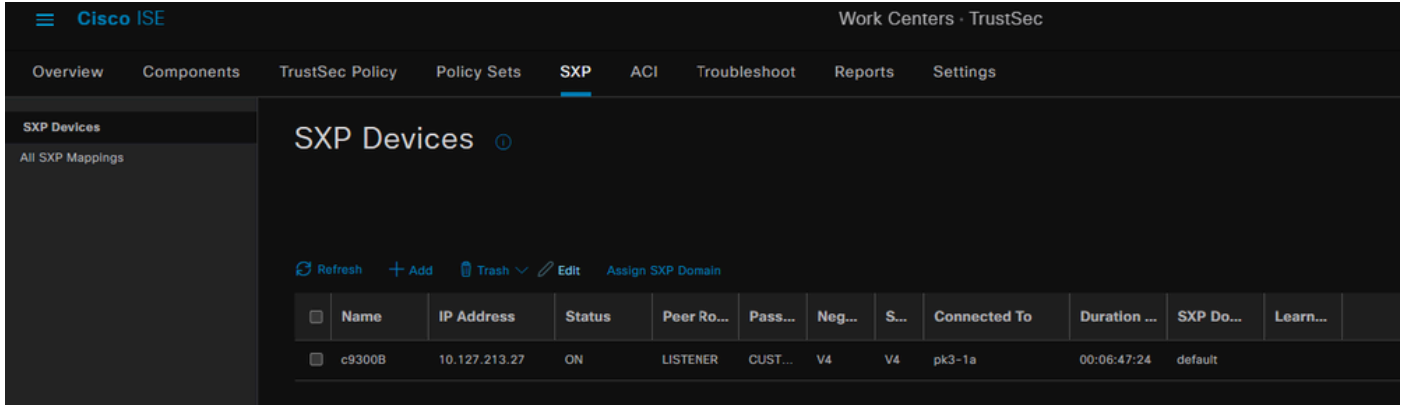
```
C9300B#show cts sxp connections vrf mgmt-vrf
SXP: نمم
م و ع دم ر ا د ص ا ا ا ع ا : 4
ة و م ج م : ة ا ض ا ر ت ف ا ل ا ر س ل ا ة م ل ك
ا ه ن ي ي ع ت م ت ي م ل : ة ا ض ا ر ت ف ا ل ا ح ي ت ا ف م ل ا ة ل س ل س
ق ي ب ط ت ل ل ل ب ا ق ر ي غ : ي ا ض ا ر ت ف ا ل ا ح ي ت ا ف م ل ا ة ل س ل س م س ا
IP: 10.127.213.27 ل ي ا ض ا ر ت ف ا ل ا ر د ص م ل ا
ة ي ن ا ث : 120 ل ا ص ت ا ل ا ة ل و ا ح م ة د ا ع ا ل ة ح و ت ف م ل ا ة ر ت ف ا ل
ة ي ن ا ث : 120 : ة ي و س ت ل ا ة ر ت ف
ل ي غ ش ت ل ا د ي ق ر ي غ ت ق و م ل ا ح ت ف ة ل و ا ح م ة د ا ع ا
ه ن ي ي ع ت م ت ي م ل : ر ي د ص ت ل ل ر ي ط ن ل ل س ل س ت ز ا ي ت ج ا د ح
ه ن ي ي ع ت م ت ي م ل : د ا ر ي ت س ا ل ل ر ي ط ن ل ل س ل س ت ز ا ي ت ج ا د ح
—
ر ي ط ن ل ل ت ن ر ت ن ا ل ل و ك و ت و ر ب : 10.127.197.53
IP: 10.127.213.27 ر د ص م ل ا
ل ي غ ش ت : ط و ر خ م ل ا ة ل ا ح
: 4 ر ا د ص ا ل ا ط و ر خ م
ة ي ع ر ف - IPv4-IPv6 ة ك ب ش : ل ا ص ت ا ل ا ة ي ن ا ك م ا
ة ي ن ا ث : 120 C O N N : ي ف ر ا ط ت ن ا ل ا ت ق و
SXP ع م ت س م : ي ل ح م ل ا ع ض و ل ا
: 1 ل ا ص ت ا ل ا م ق ر
: 1 F D : ع م T C P ق ف ا و ت
ة ي ا ض ا ر ت ف ا ل ا SXP ر و ر م ة م ل ك : T C P ق ف ا و ت ر و ر م ة م ل ك
ل ي غ ش ت ل ا د ي ق ز ا ج ت ح ا ل ا ت ق و م
: 0:00:23:36 (dd:hr:mm:sec) ة ل ا ح ل ل ر ي ي غ ت ر خ ا ذ ن م ة د م ل ا

SXP = 1 ت ا ل ا ص ت ا ل ا ن u m ي ل ا م ج ا

0x7F128DF555E0 VRF:Mgmt-vrf, fd: 1, Peer IP: 10.127.197.53
cdcbp:0x7F128DF555E0 MGMT-VRF <10.127.197.53 و 10.127.213.27> tableid:0x1
```

2. ISE SXP نم ققحتللا ةوطخل

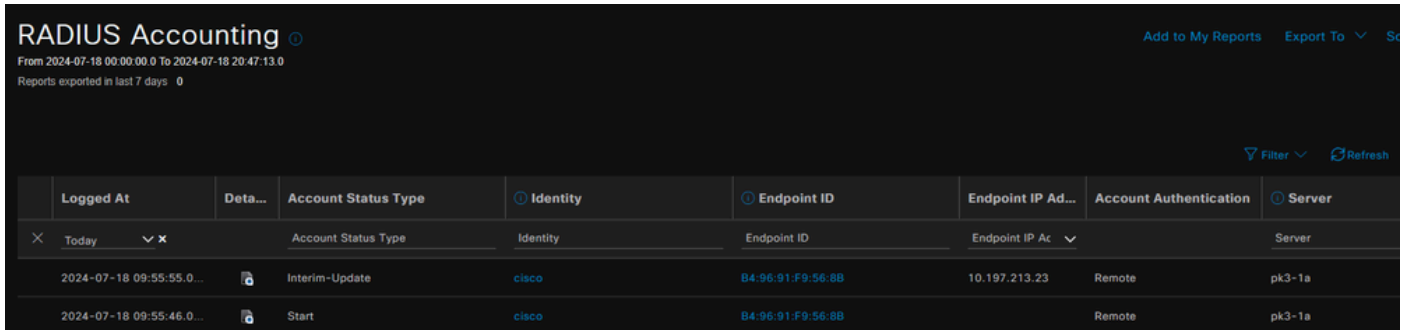
SXP ةزهجأ > TrustSec > SXP > لمعلل زكارم نمض لوجم لل ليغشتلا ديقي SXP ةلح عبطلاب



The screenshot shows the Cisco ISE Work Centers interface for TrustSec. The 'SXP' tab is selected, and the 'SXP Devices' page is displayed. The page includes a navigation bar with 'Overview', 'Components', 'TrustSec Policy', 'Policy Sets', 'SXP', 'ACI', 'Troubleshoot', 'Reports', and 'Settings'. The main content area shows a table of SXP Devices with columns for Name, IP Address, Status, Peer Role, Pass..., Neg..., S..., Connected To, Duration, SXP Domain, and Learn... A single device is listed with Name 'e9300B', IP Address '10.127.213.27', Status 'ON', Peer Role 'LISTENER', Pass... 'CUST...', Neg... 'V4', S... 'V4', Connected To 'pk3-1a', Duration '00:06:47:24', and SXP Domain 'default'.

3. RADIUS ةبساخم ةوطخل

دعب RADIUS ةبساخم ةمزح نم Framed-IP ناو نعل RADIUS ةمس ملتسا ISE أن نم دكأت ةحجانلا ةقداصملا

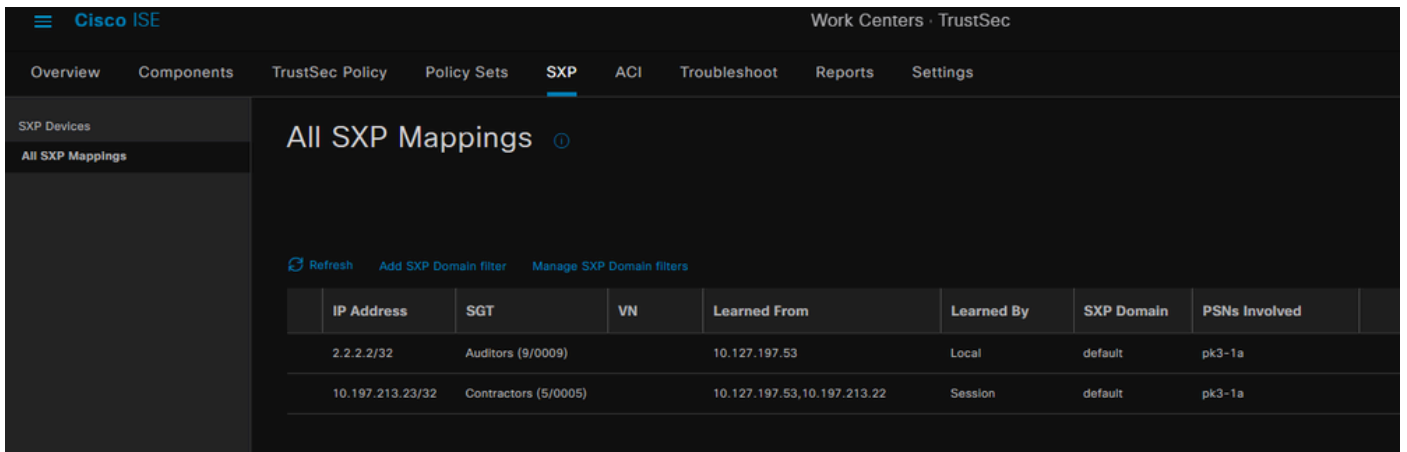


The screenshot shows the Cisco ISE Work Centers interface for TrustSec, displaying the 'RADIUS Accounting' report. The report is for the period from 2024-07-18 00:00:00.0 to 2024-07-18 20:47:13.0. The report is filtered by 'Today' and shows two entries. The columns are Logged At, Detail, Account Status Type, Identity, Endpoint ID, Endpoint IP Address, Account Authentication, and Server.

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

4. ISE SXP تانييغت ةوطخل

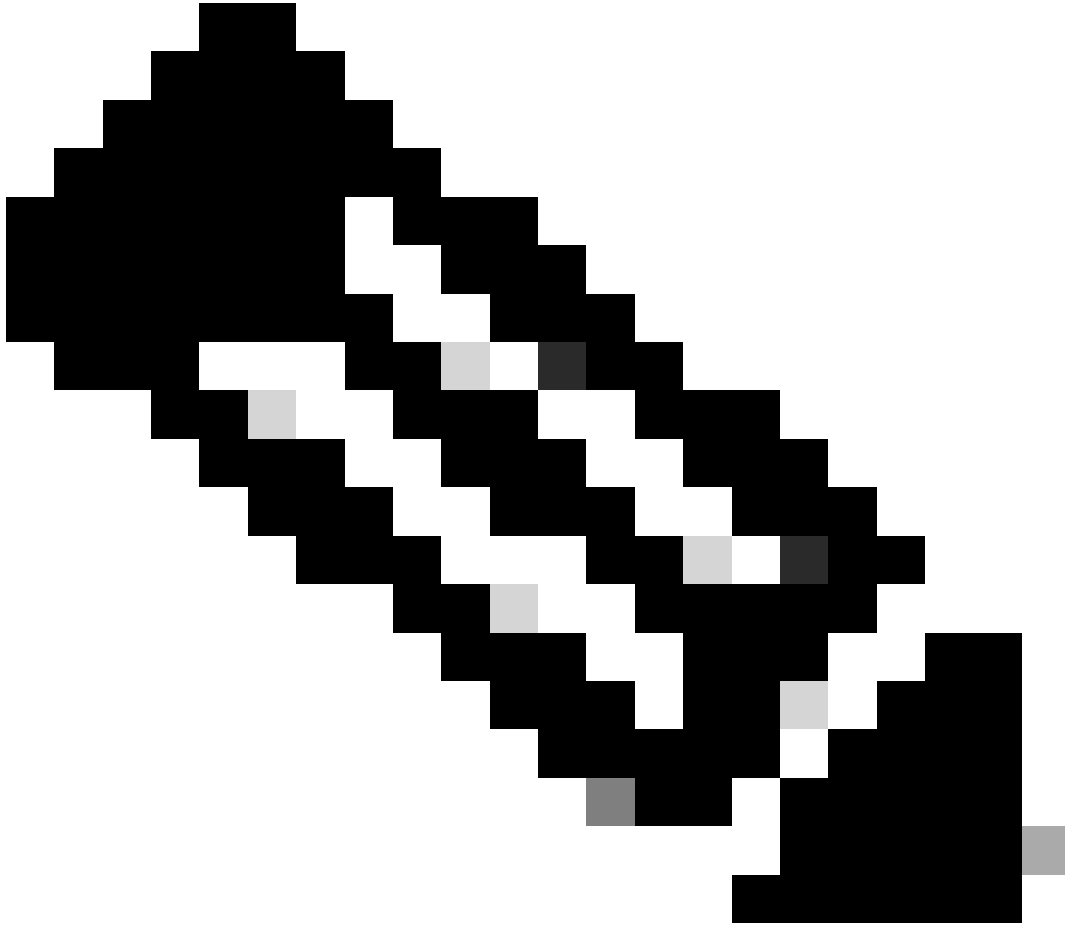
IP-SGT تانييغت ضرعل SXP تانييغت عيجم > TrustSec > SXP > لمعلل زكارم ىلا لقتنا RADIUS لمعل ةسلج نم ايكيمانيد اهيلع فرعتلا مت يتلا



The screenshot shows the Cisco ISE Work Centers interface for TrustSec, displaying the 'All SXP Mappings' page. The page includes a navigation bar with 'Overview', 'Components', 'TrustSec Policy', 'Policy Sets', 'SXP', 'ACI', 'Troubleshoot', 'Reports', and 'Settings'. The main content area shows a table of SXP Mappings with columns for IP Address, SGT, VN, Learned From, Learned By, SXP Domain, and PSNs Involved. Two mappings are listed: one for IP Address '2.2.2.2/32' with SGT 'Auditors (9/0009)' and VN '10.127.197.53', and another for IP Address '10.197.213.23/32' with SGT 'Contractors (5/0005)' and VN '10.127.197.53, 10.197.213.22'.

لبق نم ملعتلا مت ISE. ىلع تباث لكشب ةنيعم IP-Sgt يبقرب طباور - يلحم

RADIUS. ةسلج نم ايكيمانيده ايلع فرعلا متي ال IP-SGT طب اور - لمعلا ةسلج



هذه ضرع نكمي. رخآ زاغ نم IP-Sgt طب اور يقلت ىلع ةردق لاب ISE عتمتي: ةطخال م
SXP تانيي عت عيمج نمض SXP لبق نم ايلع فرعلا مت امك طب اورلا

لوحملا ىلع SXP تانيي عت 5. ةوطخال

SXP لوكوتورب لالخ نم ISE نم IP-SGT تانيي عت ىلع لوحملا فرعت

```
C9300B#show cts sxp sgt-map vrf mgmt-vrf
SXP ةدقع فرع م (هؤاشنإ م):0x030303(3.3.3.3)
ىلي امك (IP) تنرتنإلا لوكوتورب بيقرن نيي عت تاي لمع:
<2.2.2، 9> بيقرلا، IPv4 لوكوتورب
<5 و 10.197.213.23> بيقرلا، IPv4 لوكوتورب
IP-SGT: 2 تانيي عت ددع يلامجإ
sxp_bnd_exp_conn_list (total:0): في عبات
```

C9300B#

C9300B#show cts map vrf mgmt-vrf all
بيقرلا عم (IP) تترت نإلا لوكوت ورب نم ع بارلا رادصلإا ربع طشنلا طبرلا تامولعم

IP ناو نع بيقر ردصم

2.2.2.2 9 SXP

10,197,213,23 5 SXP

IP بيقرلة طشنلا طباورلا صلخم

SXP = 2 طباور ددع يلامجإ

= 2 طشنلا طباورلل يلامجإا ددعلا

اهحالصا واطخال فاشكتسا

اهحالصا ونيوكتلا ااطخا فاشكتسال اهمادختسا كنكمي تامولعم مسقلا اذ رفوي

ISE ريرقت

ةروصللا هذه يف حضورم وه امك ،لاصتالا ريرقتو SXP طبر عاشنإ اضيأ ISE حمسي

The screenshot shows the Cisco ISE Reports page for TrustSec. The main report is titled "SXP Binding" and covers the period from 2024-07-18 00:00:00 to 2024-07-18 20:53:57. The report is filtered by "Today" and shows 3 entries. The table below is a representation of the data shown in the screenshot.

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

ISE يلع ااطخال حيصت

ااطخال حيصت يوتسم يلع اهنبيعت متيس يتلا ةزهجالا هذه عم ISE معد ةمزح عمجت

- sxp
- sgtbinding
- فإسإ
- ةسلج-NSF
- ةقتلا

ةمزح يف ي مقر دعاسم نيبيعتب ISE موقوي ،ISE مداخ نم مدختسمل ةقداصم متت امدنع IP ناو نع لوصللا لسري ،IP ناو نع يلع مدختسمل لوصح درجمب .لوصللا لوبق ةباجتسا ISE ةب ساجم ةمزح يف رطؤملا RADIUS.

show logging application localStore/iseLocalStore.log:

```
2024-07-18 09:55.051 +05:30 000017592 راعش Radius-Accounting: تاباسح ةبقارم شي دحت
RADIUS. ConfigVersionId=129، ناونع IP زاه ل ل IP=10.197.213.22، UserName=Cisco،
NetworkDeviceName=pk، User-Name=Cisco، NAS-IP ناونع=10.197.213.22، NAS-Port=50124،
Framed-IP-address=10.197.213.23، فة=CACS:16d5C50a000017c425e3c6:pk3-
1a/510648097/25، station id=c4-b2-39-ed-ab-18، call-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=000007، acct-authentic=remote، acct-input-packet=4،-output-packet=0، event-
timestamp=172127745، NAS-Port-type=Ethernet، NAS-Port-ID=TenGigabitEthernet1/0/24، cisco-
av-pair=audit-session-id=16D5C50A000017C425E3C6، cisco-av-pair=method=dot1x، cisco-av-
pair=cts:security-group=0 005-00، AcsSessionID=pk3-1a/510648097/28،
SelectAccessService=Default Network Access، RequestLatency=6، Step=11004، Step=11017،
step=15049، step=15008، step=22085، step=11005، networkDevice Groups=IPSec#IPISsec
device#no، NetworkDeviceGroups=location#all sites، NetworkDeviceGroups=Device Type#All
Device Types، CPMSessionID=16D5C50A000017C425E3C6، TotalAuthenLatency=6،
ClientLatency=0، ة=Cisco، ة#All Sites، ةون
ل زاه=Device#All Device Types، IPSEC=IPSEC sec#is زاه IPsec#no،
```

show logging application ise-psc.log:

```
2024-07-18 09:55:55.054 [SxpSessionNotifierThread]]
ise.sxp.sessionBinding.util.SxpBindingUtil -:::-
PrirtCpmBridge :
نم ةملت سمل ة س ل ل ميق ل ل س ت
ل و ب ق م ==> ADD، sessionId ==> 16D5C50A000017C425E3C6، sessionState ==>
inputIp ==> 10.197.213.23، inputSgTag ==> 0005-00، nasIp => 10.197.213.22null، vn = = = null>
```

IP SGT ني ني عت عي مجت ب ث د ح أ ل PAN ة د ق و ة ا ب ص ا خ ل H2DB ل و د ج ي ف IP + SGT ني ني عت ني ز خ ت ب SXP ة د ق ع م و ق ت
- ل م ل ز ك ا ر م) ل ي غ ش ت ل ل م ا ط ن ل (GUI) ة ي م و س ر ل ل م د خ ت س م ل ة ه ج ا و ي ف SXP ت ا ن ي ي ع ت ع ي م ج ي ف ك ل ذ س ك و ا ذ ه
>TrustSec -> SXP->ح م ع ي ع ت ع ي م ج ي ف SXP).

show logging application sxp_appserver/sxp.log:

```
2024-07-18 10:01:01.312 [sxp-service-http-96441]
cisco.ise.sxp.rest.sxpGlueRestAPI:147 - SXP-PEERF ا ض ا ط ب ر ة ف ا ض ا
2024-07-18 10:01:01.317 [SxpNotificationSerializer-Thread]
cpm.sxp.engine.services.NotificationSerializerImpl:202 - ة م ه م ة ج ل ا ع م [add=true،
ا ع ا ل م =RestSxpLocalBinding(tag=5، groupName=null، ipAddress=10.197.213.23/32،
nasIp=10.197.213.2، sessionId=16D5C 0A000017C425E3C6، peerSequence=null،
sxpBindingOpType=null، sessionExpiryTimeInMillis=0، apic=false، routable=true، vns=[])
2024-07-18 10:01:01.344 [SxpNotificationSerializer-Thread]
```

```
cisco.cpm.sxp.engine.sxpEngine:1543 - [VPN: 'default'] | ديدج طبر ة فاضا | MasterBindingIdentity  
[ip=10.197.213.23/32، peerSequence=10.127.53.10.197.213.2،5 ةم ال ع ، isLocal=true،  
sessionId=16D5C50A000017C425E3C6، vn=DEFAULT_VN]  
2024-07-18 10:01:01،344 | عاطخ أال | حي حصت [SxpNotificationSerializer-Thread]  
Cisco.cpm.sxp.engine.SxpEngine:1581 - | ة فاضا | 1 طبر (طباور)  
2024-07-18 10:01:01،344 | عاطخ أال | حي حصت [SxpNotificationSerializer-Thread]  
cisco.cpm.sxp.engine.MasterDbListener:251 - | ةم هم ل ل اسر | ددع ، طباور ة فاضا | H2 جل اع م  
طباور ل : 1  
2024-07-18 10:01:01،344 | عاطخ أال | حي حصت [H2_HANDLER]  
cisco.cpm.sxp.engine.MasterDbListener:256 - | ة فاضا | دنع MasterDbListener جل اع م -  
طباور Count: 1
```

IP-SGT. طباور ثدح | مادخت ساب ريظن ل ل وحم ثي دحت ب SXP ة دقع موقت

```
2024-07-18 10:01:01،346 | عاطخ أال | حي حصت [pool-7-thread-4]  
opendaylight.sxp.core.service.updateExportTask:93 - sxp_perf:Send_update_buffer_size=32  
2024-07-18 10:01:01،346 | عاطخ أال | حي حصت [pool-7-thread-4]  
openDaylight.sxp.core.service.UpdateExportTask:116 - | جل | Send_Update  
[ISE:10.127.197.53][10.127.197.53:64999/10.127.213.27:31025] [o|SV4]  
2024-07-18 10:01:01،346 | عاطخ أال | حي حصت [pool-7-thread-4]  
openDaylight.sxp.core.service.UpdateExportTask:137 - | جل | حاجن ب Sent_Update  
[ISE:10.127.197.53][10.127.197.53:64999/10.127.213.27:31025][O|SV4]
```

ل وحم ل ل عاطخ أال | حي حصت

اهال صاوت اثي دحت ل ل و SXP تال اصت | عاطخ | فاشكت س ال ل وحم ل ل ع هذه عاطخ أال | حي حصت تاي ل مع ني كم ت ب مق

debug cts sxp conn

debug cts sxp

debug cts sxp mdb

debug cts sxp message

"ISE". SXP توص رب كم نم Sgt-IP تان يي عت Swich ت ق لت

تال ج سل هذه ضرع ل **show logging** نم ق قحت

```
Jul 18 04:23:04.324: CTS-SXP-MSG:sxp_rcv_update_v4 <1> | ناو نع | IP ريظن ل ل 10.127.197.53  
وي ل وي 1804:23:04.324: CTS-SXP-MDB:IMU | ة فاضا | - <conn_index = 1> | ريظن ل ل نم  
10.127.197.53  
وي ل وي 1804:23:04.324: CTS-SXP-MDB:mdb_send_msg <IMU_Add_IPSGT_DEVID>
```

1804:23:04.324: CTS-SXP-INTL:mdb_send_msg mdb_process_add_ipsgt_devid
وي لوي 1804:23:04.324: CTS-SXP-MDB:sxp_mdb_inform_rbm tableid:0x1 sense:1 sgt:5
peer:10.127.197.53
وي لوي 1804:23:04.324: CTS-SXP-MDB:SXP MDB: 0x005 بې ق ر ل ا ip 10.197.213.23 فاضم لاخدا
وي لوي 1804:23:04.324: CTS-SXP-INTNL:mdb_send_msg mdb_process_add_ipsgt_devid م ت

ةلص تاذا تام ولعم

[ISE 3.1 لوؤسم ليلد ةئزجت](#)

[Catalyst TRUSTsec نيوكت ليلد ىلع ةماع قرظن](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل م عد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل ة مچرت ل ض ف ا ن ا ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رف و ت م ط بار ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا