

Begrijp de logboeken van de Update van ISE SXP samen met Catalyst Debug Logs

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratie](#)

[Netwerkdigram](#)

[Traffic Flow](#)

[Switch configureren](#)

[ISE configureren](#)

[Stap 1. SXP-service inschakelen op ISE](#)

[Stap 2. SXP-apparaten toevoegen](#)

[Stap 3. SXP-instellingen](#)

[Verifiëren](#)

[Stap 1. SXP-verbinding op Switch](#)

[Stap 2. ISE-SXP-verificatie](#)

[Stap 3. Radius-accounting](#)

[Stap 4. ISE-SXP-toewijzingen](#)

[Stap 5. SXP-toewijzingen op Switch](#)

[Problemen oplossen](#)

[ISE-rapport](#)

[Debugs op ISE](#)

[Debugs op Switch](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe de verbinding tussen ISE en Catalyst 9300 Switch van Security Group Exchange Protocol (SXP) moet worden geconfigureerd en begrepen.

Achtergrondinformatie

SXP is het SGT (Security Group Tag) Exchange Protocol dat door TrustSec wordt gebruikt om IP naar SGT-toewijzingen naar TrustSec-apparaten te verspreiden.

SXP is ontwikkeld om netwerken, waaronder apparaten van derden of oudere Cisco-apparaten die

geen SGT-inline codering ondersteunen, de mogelijkheid te geven om TrustSec-functies te hebben.

SXP is een peering protocol; het ene apparaat kan optreden als Luidspreker en het andere als Luisteraar.

De SXP-luidspreker is verantwoordelijk voor het verzenden van de IP-SGT-banden en de luisteraar is verantwoordelijk voor het verzamelen van deze banden.

De SXP-verbinding gebruikt TCP-64999 als het onderliggende transportprotocol en MD5 voor berichtintegriteit/authenticiteit.

Voorwaarden

Vereisten

Cisco raadt u aan bekend te zijn met de configuratie van SXP Protocol and Identity Services Engine (ISE).

Gebruikte componenten

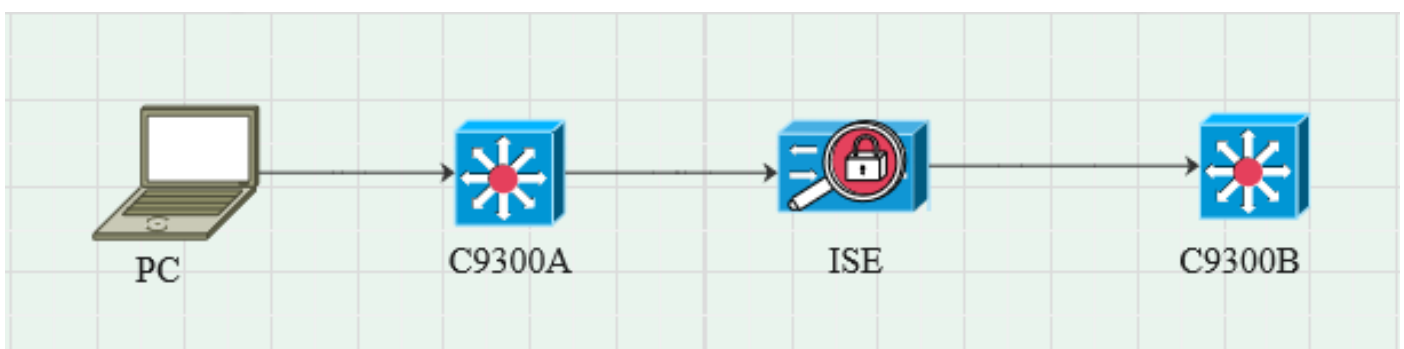
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst 9300 switch met software, Cisco IOS® XE 17.6.5 en hoger
Cisco ISE, release 3.1 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratie

Netwerkdigram



Traffic Flow

PC authenticceert met C9300A en ISE wijst dynamisch SGT toe via beleidssets.

Wanneer de verificatie is doorgegeven, worden bindingen gemaakt met een IP die gelijk is aan het RADIUS-kenmerk van framed-IP-adressen en SGT zoals in het beleid is geconfigureerd.

De bindingen propogeren in "Alle SXP bindingen" onder het standaarddomein.

C9300B ontvangt de SXP-mapping-informatie van ISE via SXP-protocol.

Switch configureren

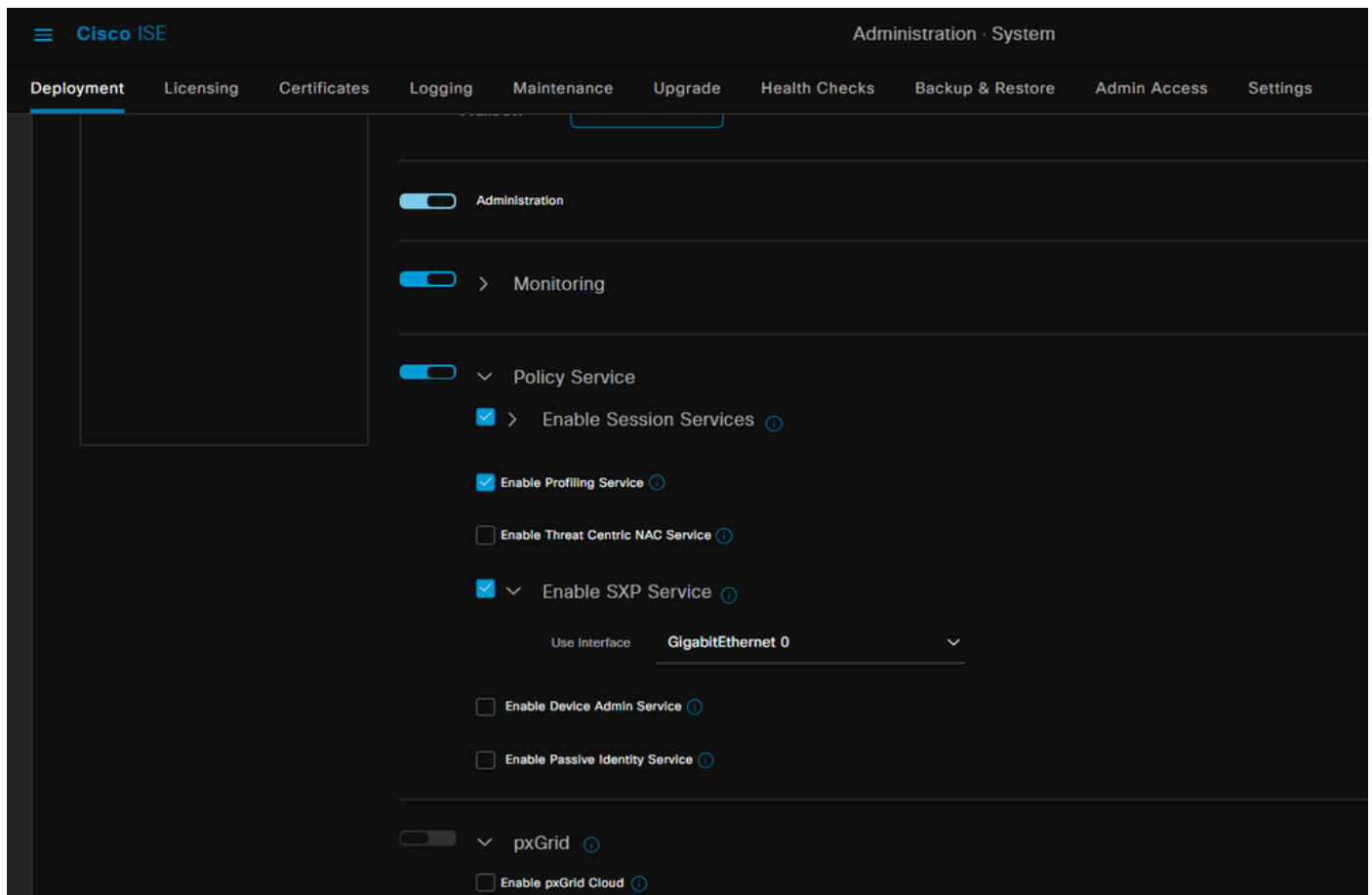
Configureer de switch als een SXP-luisteraar om de IP-SGT-toewijzingen van ISE te verkrijgen.

```
cts sxp inschakelen
cts sxp standaardwachtwoord cisco
cts sxp standaard source-ip 10.127.213.27
cts sxp verbinding peer 10.127.197.53 wachtwoord standaard modus peer speaker hold-time 0 0
vrf Mgmt-vrf
```

ISE configureren

Stap 1. SXP-service inschakelen op ISE

Navigeren naar Beheer > Systeem > Implementatie > Bewerken van de knooppunt en onder Beleidsservice selecteert u SXP-service inschakelen.

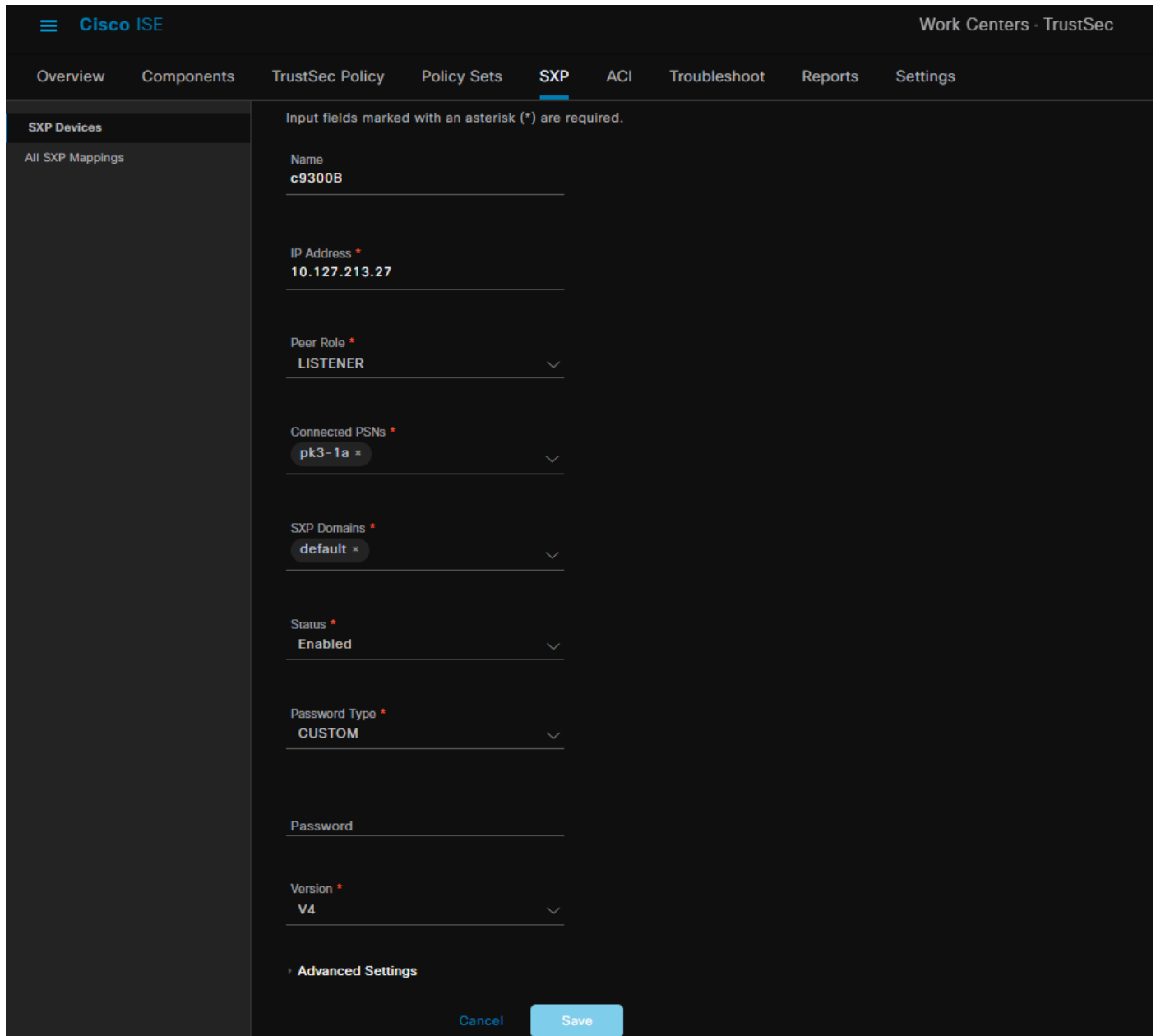


The screenshot displays the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE' and 'Administration · System'. Below this, a menu bar lists various system management options: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The main content area shows the configuration for the SXP service. A sidebar on the left contains a search bar and a list of system services, each with a toggle switch: Administration (on), Monitoring (on), Policy Service (on), and pxGrid (off). Under the Policy Service section, several sub-services are listed with checkboxes: 'Enable Session Services' (checked), 'Enable Profiling Service' (checked), 'Enable Threat Centric NAC Service' (unchecked), and 'Enable SXP Service' (checked). The 'Enable SXP Service' option is expanded, showing a 'Use Interface' dropdown menu currently set to 'GigabitEthernet 0'. Other sub-services like 'Enable Device Admin Service' and 'Enable Passive Identity Service' are unchecked. At the bottom, the 'pxGrid' section is partially visible, showing 'Enable pxGrid Cloud' as unchecked.

Stap 2. SXP-apparaten toevoegen

Om SXP-luisteraar en -luidspreker voor de bijbehorende switches te configureren, navigeer u naar Workcenters > Trustsec > SXP > SXP-apparaten.

Voeg de switch toe met peer rol als Luisteraar en wijs aan standaarddomein toe.



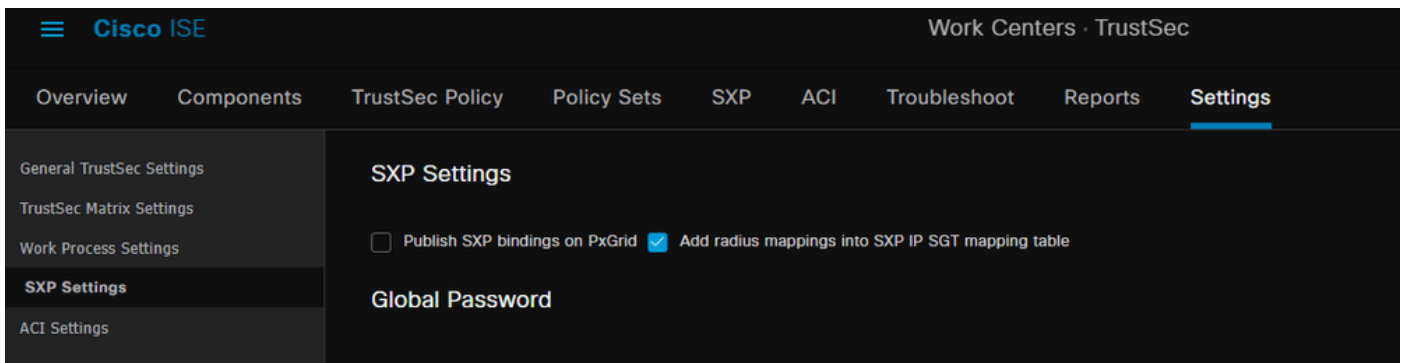
The screenshot shows the Cisco ISE configuration interface for SXP devices. The breadcrumb trail is Work Centers > TrustSec > SXP. The left sidebar shows 'SXP Devices' and 'All SXP Mappings'. The main content area displays the configuration for a device named 'c9300B'. The configuration fields are as follows:

- 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, there is an 'Advanced Settings' section and two buttons: 'Cancel' and 'Save'.

Stap 3. SXP-instellingen

Zorg ervoor dat de optie Radius-toewijzingen toevoegen aan de SXP IP SGT-toewijzingstabel is ingeschakeld, zodat ISE dynamische IP-SGT-toewijzingen leert via Radius-verificaties.



Verifiëren

Stap 1. SXP-verbinding op Switch

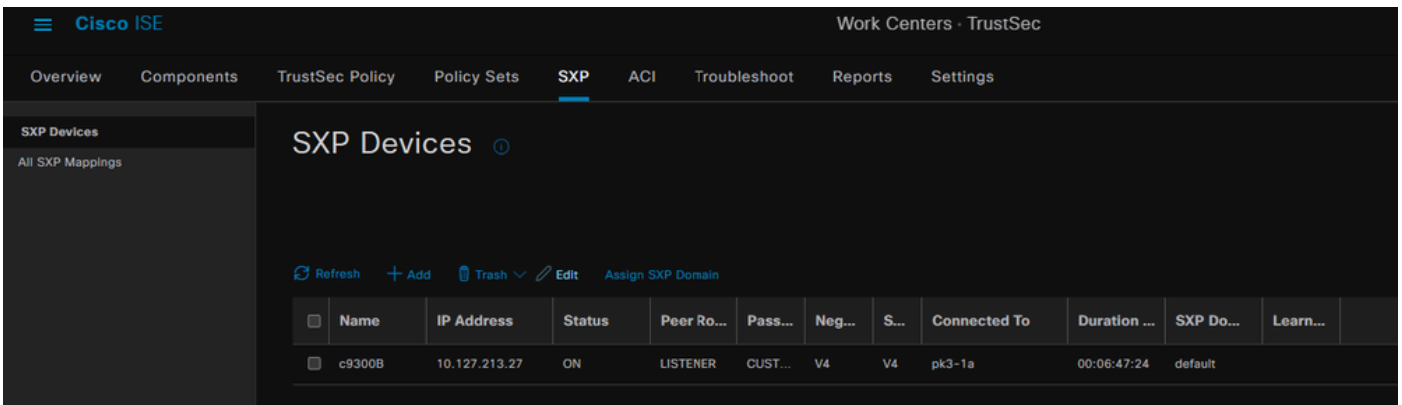
```
C9300B#show cts sxp verbindingen vrf Mgmt-vrf
SXP: ingeschakeld
Hoogste ondersteunde versie: 4
Standaardwachtwoord: instellen
Standaard sleutelketen: niet instellen
Standaard sleutelketennaam: niet van toepassing
Standaard IP-bron: 10.127.213.27
Openstaande periode verbinding opnieuw proberen: 120 seconden
Reconcile-periode: 120 seconden
Open timer opnieuw proberen is niet actief
Peer-sequentie verplaatsen-limiet voor export: niet instellen
Peer-sequentie verplaatsen-limiet voor import: niet instellen
-----
IP-peer : 10.127.197.53
Bron IP: 10.127.213.27
Conn status : Aan
Conversie : 4
Conn-mogelijkheid: IPv4-IPv6-Subnet
Conn houdtijd: 120 seconden
Lokale modus : SXP-luisteraar
Verbinding met #: 1
TCP/Conn Fd: 1
TCP verbinding wachtwoord: standaard SXP wachtwoord
Hold timer is actief
Duur sinds laatste statuswijziging: 0:00:23:36 (dd:uur:mm:sec)

Totaal aantal SXP-verbindingen = 1

0x7F128DF55E0 VRF:Mgmt-vrf, fd: 1, peer ip: 10.127.197.53
cdbp:0x7F128DF55E0 Mgmt-vrf <10.127.197.53, 10.127.213.27>, tabel:0x1
```

Stap 2. ISE-SXP-verificatie

Controleer of de SXP-status is ingeschakeld voor de Switch onder Workcenters > Trustsec > SXP > SXP-apparaten.

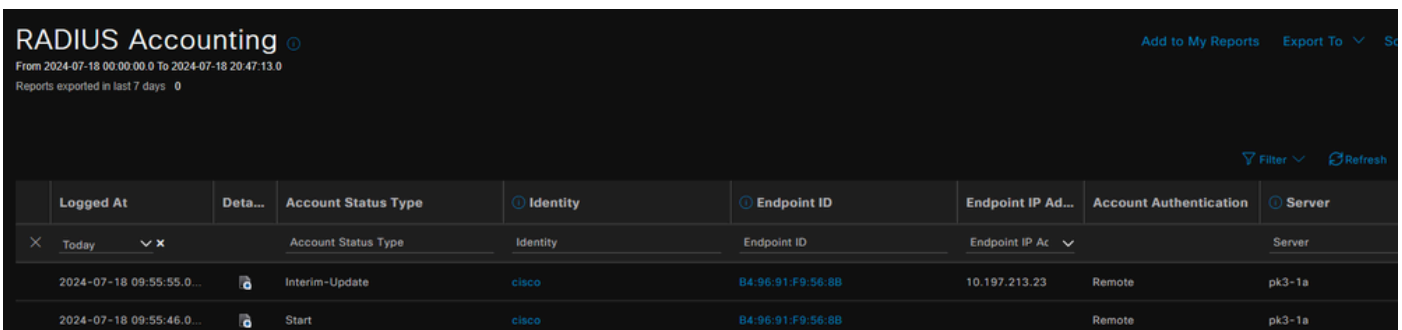


The screenshot shows the Cisco ISE interface for SXP Devices. The navigation menu includes Overview, Components, TrustSec Policy, Policy Sets, SXP (selected), ACI, Troubleshoot, Reports, and Settings. The main content area is titled 'SXP Devices' and contains a table with the following data:

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	

Stap 3. Radius-accounting

Zorg ervoor dat ISE na succesvolle verificatie het RADIUS-kenmerk framed-IP-adres van het RADIUS-accounting-pakket heeft ontvangen.

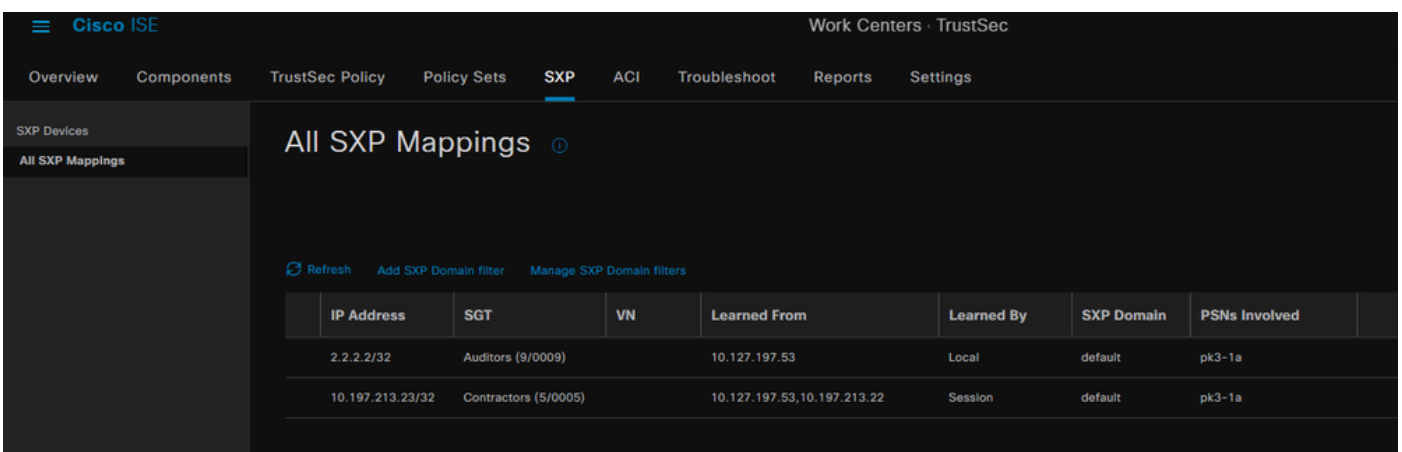


The screenshot shows the Cisco ISE RADIUS Accounting page. The navigation menu includes Overview, Components, TrustSec Policy, Policy Sets, SXP, ACI, Troubleshoot, Reports, and Settings. The main content area is titled 'RADIUS Accounting' and contains a table with the following data:

Logged At	Deta...	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

Stap 4. ISE-SXP-toewijzingen

Navigeer naar Workcenters > Trustsec > SXP > Alle SXP-toewijzingen om de dynamisch aangeleerde IP-SGT-toewijzingen van Radius-sessies te bekijken.



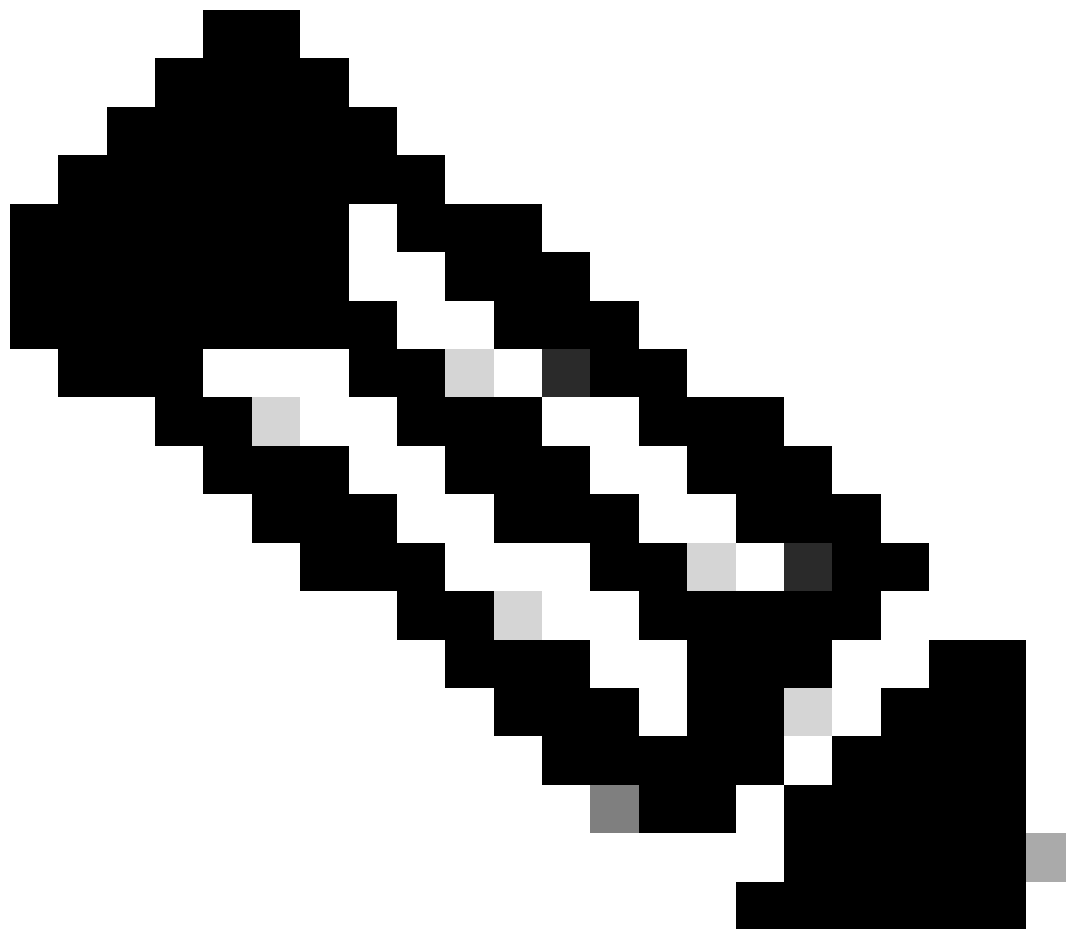
The screenshot shows the Cisco ISE interface for All SXP Mappings. The navigation menu includes Overview, Components, TrustSec Policy, Policy Sets, SXP (selected), ACI, Troubleshoot, Reports, and Settings. The main content area is titled 'All SXP Mappings' and contains a table with the following data:

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

Geleerd door

Lokaal - Statisch toegewezen IP-SGT-bindingen op ISE.

Sessie - Dynamisch aangeleerde IP-SGT-banden van Radius-sessie.



Opmerking: de ISE heeft de mogelijkheid om IP-SGT-bindingen van een ander apparaat te ontvangen. Deze banden kunnen worden weergegeven zoals geleerd door SXP onder Alle SXP-toewijzingen.

Stap 5. SXP-toewijzingen op Switch

De switch heeft IP-SGT-toewijzingen geleerd van ISE via SXP-protocol.

```
C9300B#show cts sxp sgt-map vrf Mgmt-vrf kort
SXP-knooppunt-ID (gegenereerd):0x03030303(3.3.3.3)
IP-SGT-toewijzingen als volgt:
IPv4,SGT: <2.2.2.2, 9>
IPv4.SGT: <10.197.213.23, 5>
```

Totaal aantal IP-SGT-toewijzingen: 2
conn in de sxp_bnd_exp_conn_list (totaal:0):
C9300B#

C9300B#show cts op rollen gebaseerd Sgt-map vrf Mgmt-vrf alles
Informatie over actieve IPv4-SGT-banden

IP-adresswitchbron

```
=====
9 SXP-module
10 197 213 23 5 SXP
```

Samenvatting van IP-SGT actieve banden

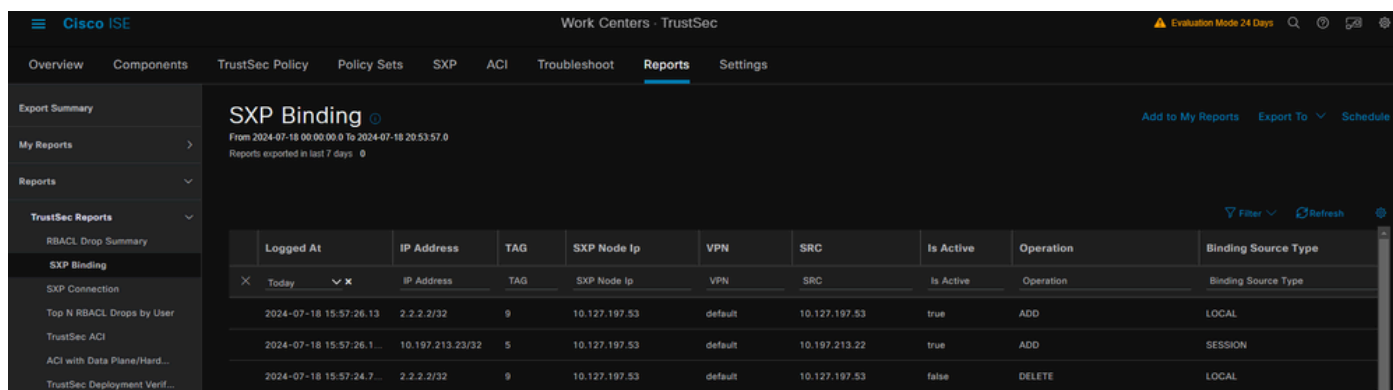
```
=====
Totaal aantal SXP-banden = 2
Totaal aantal actieve bindingen = 2
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

ISE-rapport

Met ISE kunnen ook SXP-band- en verbinding rapporten worden gegenereerd, zoals in deze afbeelding wordt getoond.



The screenshot shows the Cisco ISE interface with the 'Reports' tab selected. The main content area displays an '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 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

Debugs op ISE

Verzamel de ISE-ondersteuningsbundel met deze kenmerken die op debugniveau moeten worden ingesteld:

- sxp
- sgtbinding
- nsf
- NSF-sessie
- trustsec

Wanneer een gebruiker is geverifieerd vanaf een ISE-server, wijst ISE een SGT toe in het access acceptance response-pakket. Zodra de gebruiker het IP-adres heeft, verstuurt de switch het framed IP-adres in het Radius Accounting Packet.

toon registrerentoe passing localStore/iseLocalStore.log:

```
2024-07-18 09:55:55.051 +05:30 000017592 3002 OPMERKING RADIUS-accounting: RADIUS-accounting waakhond update, ConfigVersieID=129, Apparaat IP-adres=10.197.213.22, Gebruikersnaam=cisco, NetworkDeviceName=pk, Gebruiker-IP-naam=cisco E-mailadres=10.197.213.22, NAS-poort=50124, framed-IP-adres=10.197.213.23, Class=CACS:16D5C50A00000017C425E3C6:pk3-1a/510648097/25, Calling-Station-ID=C4-B2-39-ED-AB-18, Calling-Station-ID=B4-96-F-F 56-8B, Act-Status-Type=Interim-Update, Act-Delay-Time=0, Act-Input-Octets=413, Act-Output-Octets=0, Act-Session-ID=00000007, Act-Authentic=Remote, Act-Input-Packets=4, Act-Output-Packets=0, Event-Time=1721277745, NAS-Port-Type=Ethernet, NAS-Port-ID=TenGigabit Ethernet1/0/24, cisco-av-pair=audit-sessie-id=16D50A00000017C425E3C6, cisco-av-pair=method=dot1x, cisco-av-pair=cts:security-group-tag=005-00, acsSessionID=pk3-1a/510648097/28, SelectedAccessService=Default Network Access=Network, RequestLatency=6, Step=11004,=11017, Step=15049, Step=15008, Step=22085, Step=11005, Step=00000017, Step=, Step=, NetworkDeviceGroups=IPSEC#is Alle locaties, NetworkDeviceGroups=Device Type#Alle apparaattypes, CPMSessionID=16D5C50A C425E3C6, TotalAutoLatency=6, ClientLatency=0, Network Device Profile=Cisco, Location=Location#Alle locaties, Apparaatype#Alle apparaattypes, IPSEC=IPSEC#is IPSEC Device#No,
```

toon registrerentoe passing ise-psc.log:

```
2024-07-18 09:55:55,054 DEBUG [SXPSessionNotifierThread][  
ise.sxp.sessionbinding.util.sxpBindingUtil -::  
het registreren van de sessiewaarden die van PortCpmBridge worden ontvangen:  
Bediening type ==>ADD, sessieID ==> 16D5C50A00000017C425E3C6, sessieStatus ==>  
GEACCEPTEERD, inputIP ==> 10.197.213.23, inputSGTag ==> 0005-00, nasIP ==>  
10.197.213.22null, van == null>
```

Het SXP-knooppunt slaat de IP + SGT-toewijzing op in de H2DB-tabel en later het PAN-knooppunt verzamelt deze IP SGT-toewijzing en wordt weergegeven in alle SXP-toewijzingen in ISE GUI (Workcenters ->Trustsec -> SXP->Alle SXP-toewijzingen).

toon registrerentoe passing sxp_appserver/sxp.log:

```
2024-07-18 10:01:01,312 INFO [sxp-service-http-96441] cisco.ise.sxp.rest.sxpGlueRestAPI:147 -  
SXP-PEERF  
2024-07-18 10:01:01,317 DEBUG [SXPNotificationSerializer-Thread]
```

```
cpm.sxp.engine.services.NotificationSerializerImpl:202 - verwerkingstaak [add=true, notification=RestSxpLocalBinding(tag=5, groupName=null, ipAddress=10.197.213.23/32, nasIP=10.197.21, sessieID=1 6D5C50A00000017C425E3C6, peerSequence=null, sxpBindingOpType=null, sessieExpiryTimeInMillis=0, apic=false, routable=true, vns=[])]
```

```
2024-07-18 10:01:01,344 DEBUG [SXPNotificationSerializer-Thread]
```

```
cisco.cpm.sxp.engine.sxpEngine:1543 - [VPN: 'standaard'] Nieuwe binding toevoegen:
```

```
MasterBindingIdentity [ip=10.197.213.23/32, peerSequence=10.127.197.53,10.197.217 3.22, tag=5, isLocal=true, sessieID=16D5C50A00000017C425E3C6, vn=DEFAULT_VN]
```

```
2024-07-18 10:01:01,344 DEBUG [SXPNotificationSerializer-Thread]
```

```
cisco.cpm.sxp.engine.sxpEngine:1581 - Toevoeging 1 band(en)
```

```
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
```

```
cisco.cpm.sxp.engine.MasterDbListener:251 - Indienen taak aan H2 Handler voor het toevoegen van bindingen, bindingen tellen: 1
```

```
2024-07-18 10:01:01,344 DEBUG [H2_HANDLER] cisco.cpm.sxp.engine.MasterDbListener:256 - MasterDbListener Verwerking opToegevoegd - bindingenTel: 1
```

Het SXP-knooppunt werkt de peer-Switch bij met de nieuwste IP-SGT-banden.

```
2024-07-18 10:01:01,346 DEBUG [pool-7-thread-4]
```

```
opendaylight.sxp.core.service.UpdateExportTask:93 - SXP_PERF:SEND_UPDATE_BUFFER_SIZE=32
```

```
2024-07-18 10:01:01,346 DEBUG [pool-7-thread-4]
```

```
opendaylight.sxp.core.service.UpdateExportTask:116 - SEND_UPDATE naar [ISE:10.127.197.53][10.127.197.53:64999/10.127.213.27:31025][O|Sv4]
```

```
2024-07-18 10:01:01,346 DEBUG [pool-7-thread-4]
```

```
opendaylight.sxp.core.service.UpdateExportTask:137 - SEND_UPDATE Succesvol naar [ISE:10.127.197.53][10.127.197.53:64999/10.127.213.27:31025][O|Sv4]
```

Debugs op Switch

Schakel deze debugs in de switch in om SXP-verbindingen en -updates probleemoplossing te bieden.

```
debug cts sxp conn
```

```
debug cts sxp fout
```

```
debug cts sxp mdb
```

```
debug cts sxp bericht
```

Switch heeft de SGT-IP-toewijzingen ontvangen van de SXP Speaker "ISE".

Logboekregistratie tonen controleren om deze logbestanden te bekijken:

```
Juli 18 04:23:04.324: CTS-SXP-MSG:sxp_rcv_update_v4 <1> peer ip: 10.127.197.53
jul 18 04:23:04.324: CTS-SXP-MDB:IMU Toevoegen aan band:- <conn_index = 1> van peer
10.127.197.53
Juli 18:04:23:04.324: CTS-SXP-MDB:mdb_send_msg <IMU_ADD_IPSGT_DEVID>
jul 18 04:23:04.324: CTS-SXP-INTNL:mdb_send_msg mdb_process_add_ipsgt_devid Start
jul 18 04:23:04.324: CTS-SXP-MDB:sxp_mdb_information_rbm tableid:0x1 sense:1 sgt:5
peer:10.127.197.53
Jul 18 04:23:04.324: CTS-SXP-MDB:SXP MDB: Entry added ip 10.197.213.23 sgt 0x0005
Jul 18 04:23:04.324: CTS-SXP-INTNL:mdb_send_msg mdb_process_add_ipsgt_devid Gereed
```

Gerelateerde informatie

[ISE 3.1 segmentering van beheerdershandleiding](#)

[Catalyst Configuration Guide Trustsec - Overzicht](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.