

# Comprensione dei log di aggiornamento di ISE SXP e dei log di debug di Catalyst

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Flusso traffico](#)

[Configura switch](#)

[Configurare ISE](#)

[Passaggio 1. Abilitare il servizio SXP su ISE](#)

[Passaggio 2. Aggiungere dispositivi SXP](#)

[Passaggio 3. Impostazioni SXP](#)

[Verifica](#)

[Passaggio 1. Connessione SXP su switch](#)

[Passaggio 2. Verifica di ISE SXP](#)

[Passaggio 3. Accounting Radius](#)

[Passaggio 4. Mapping ISE SXP](#)

[Passaggio 5. Mapping SXP sullo switch](#)

[Risoluzione dei problemi](#)

[Report ISE](#)

[Debug su ISE](#)

[Debug sullo switch](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come configurare e comprendere il protocollo SXP (Security Group Exchange Protocol) tra ISE e Catalyst 9300 Switch.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza del protocollo SXP e della configurazione di Identity Services Engine (ISE).

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Cisco Catalyst 9300 con software Cisco IOS® XE 17.6.5 e versioni successive  
Cisco ISE versione 3.1 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

SXP è il protocollo SGT (Security Group Tag) Exchange utilizzato da TrustSec per propagare i mapping IP-SGT ai dispositivi TrustSec.

SXP è stato sviluppato per consentire alle reti, inclusi i dispositivi di terze parti o i dispositivi Cisco legacy che non supportano il tagging in linea SGT, di avere funzionalità TrustSec.

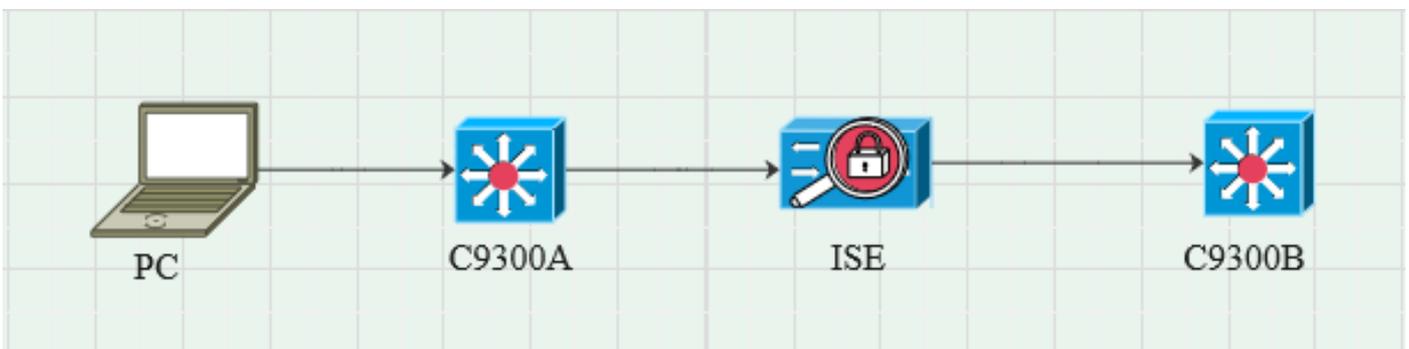
SXP è un protocollo peer; un dispositivo può fungere da altoparlante e l'altro da listener.

Il diffusore SXP è responsabile dell'invio dei binding IP-SGT e il listener è responsabile della raccolta di tali binding.

La connessione SXP utilizza la porta TCP 64999 come protocollo di trasporto sottostante e MD5 per l'integrità/autenticità dei messaggi.

## Configurazione

### Esempio di rete



### Flusso traffico

PC esegue l'autenticazione con C9300A e ISE assegna dinamicamente SGT tramite set di criteri. Una volta superata l'autenticazione, i binding vengono creati con un indirizzo IP uguale all'attributo

RADIUS dell'indirizzo IP con frame e a SGT come configurato nel criterio.

Le associazioni vengono propagate in tutte le associazioni SXP nel dominio predefinito.

C9300B riceve le informazioni di mappatura SXP da ISE attraverso il protocollo SXP.

## Configura switch

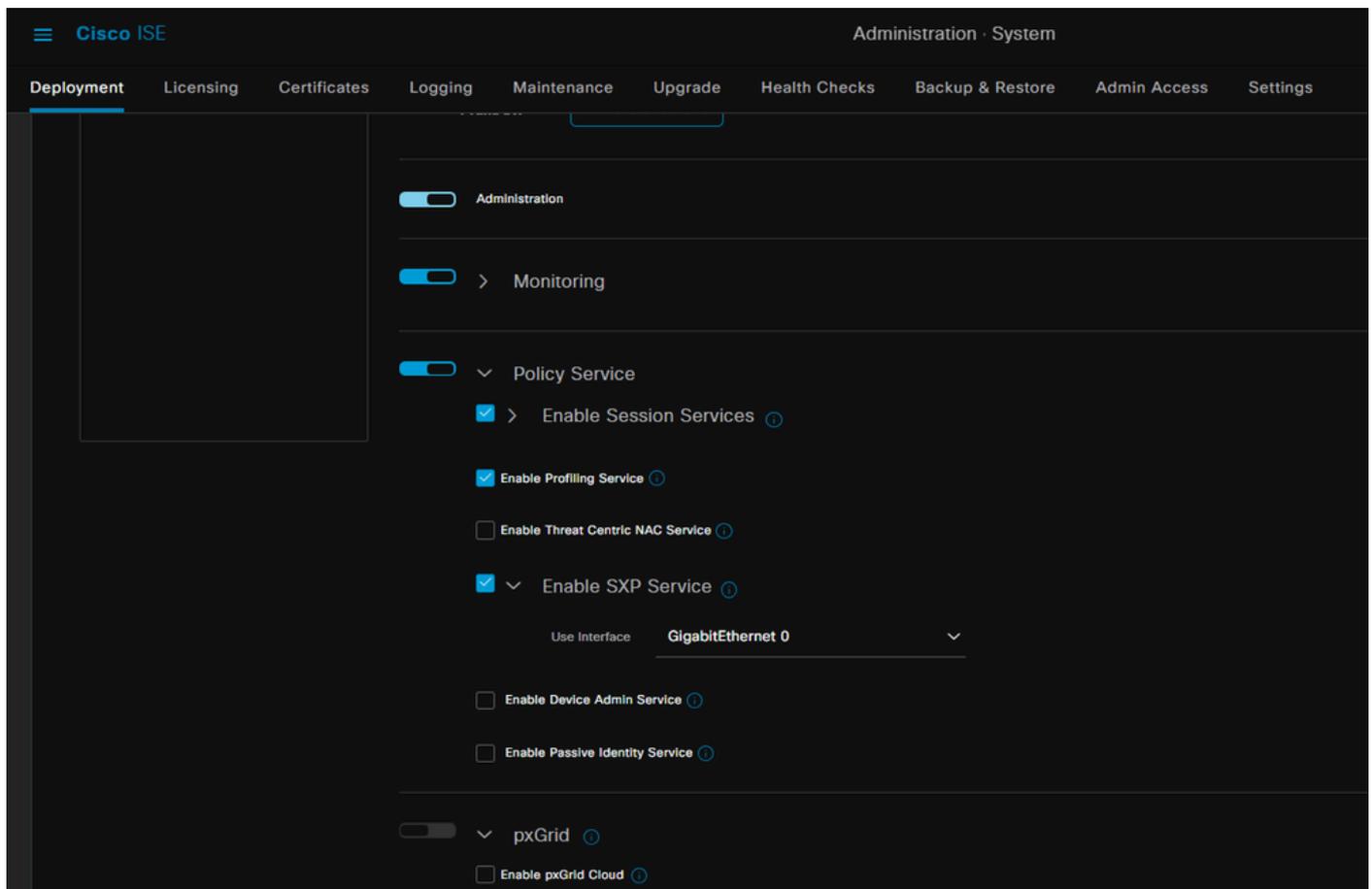
Configurare lo switch come listener SXP per ottenere le mappature IP-SGT da ISE.

```
cts sxp enable
cts sxp password predefinita cisco
cts sxp default source-ip 10.127.213.27
cts sxp connection peer 10.127.197.53 password default mode peer speaker hold-time 0 vrf
Mgmt-vrf
```

## Configurare ISE

### Passaggio 1. Abilitare il servizio SXP su ISE

Selezionare Amministrazione > Sistema > Distribuzione > Modifica il nodo e in Policy Service selezionare Abilita servizio SXP.



### Passaggio 2. Aggiungere dispositivi SXP

Per configurare il listener e l'altoparlante SXP per gli switch corrispondenti, selezionare Workcenter > Trustsec > SXP > Dispositivi SXP. Aggiungere lo switch con ruolo di peer come listener e assegnarlo al dominio predefinito.

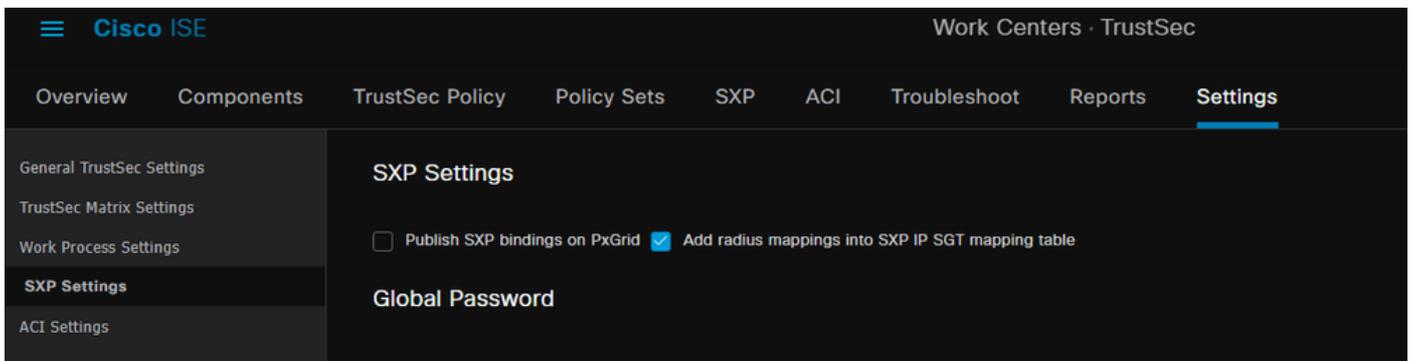
The screenshot shows the Cisco ISE configuration interface for SXP devices. The breadcrumb trail is Work Centers > TrustSec > SXP. The left sidebar shows 'SXP Devices' and 'All SXP Mappings'. The main content area displays the configuration for a device named 'c9300B'. The configuration includes the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

- 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 field)
- Version \*: V4

At the bottom, there is an 'Advanced Settings' section and 'Cancel' and 'Save' buttons.

### Passaggio 3. Impostazioni SXP

Verificare che l'opzione Add radius mappings into SXP IP SGT mapping table sia selezionata, in modo che ISE apprenda le mappature IP-SGT dinamiche tramite le autenticazioni Radius.



## Verifica

### Passaggio 1. Connessione SXP su switch

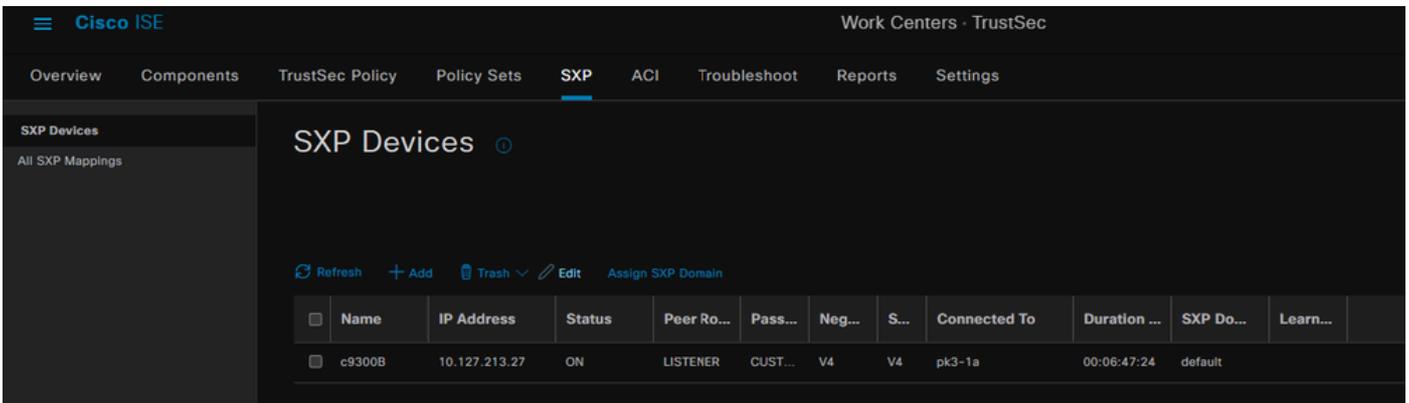
```
C9300B#show cts connessioni sxp vrf Mgmt-vrf
SXP Attivato
Versione più recente supportata: 4
Password predefinita: Imposta
Catena di chiavi predefinita: Non impostato
Nome catena di chiavi predefinita: Non applicabile
IP di origine predefinito: 10.127.213.27
Periodo di apertura tentativi di connessione: 120 sec
Periodo di riconciliazione: 120 sec
Il timer di riavvio non è in esecuzione
Limite di attraversamento sequenza peer per esportazione: Non impostato
Limite di attraversamento sequenza peer per importazione: Non impostato
—
IP peer: 10.127.197.53
IP di origine: 10.127.213.27
Stato connessione: On
Conversione: 4
Funzionalità Conn: Subnet IPv4-IPv6
Tempo di attesa continua: 120 secondi
Modalità locale: Listener SXP
N. inizializzazione connessione: 1
TCP conn fd: 1
Password conn TCP: password SXP predefinita
Timer di attesa in esecuzione
Durata dall'ultima modifica dello stato: 0:00:23:36 (gg:hr:mm:sec)

Numero totale di connessioni SXP = 1

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

## Passaggio 2. Verifica di ISE SXP

Verificare che lo stato SXP sia ON per lo switch in Workcenter > Trustsec > SXP > Dispositivi SXP.

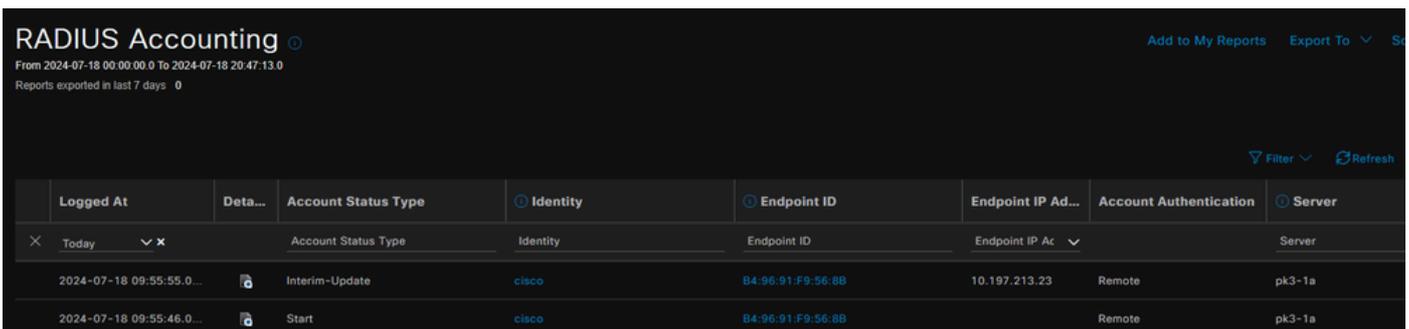


The screenshot shows the Cisco ISE interface for SXP Devices. The navigation menu includes Overview, Components, TrustSec Policy, Policy Sets, SXP, ACI, Troubleshoot, Reports, and Settings. The SXP Devices page displays a table with the following data:

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	

## Passaggio 3. Accounting Radius

Verificare che ISE abbia ricevuto l'attributo RADIUS dell'indirizzo IP con frame dal pacchetto di accounting Radius dopo l'autenticazione.

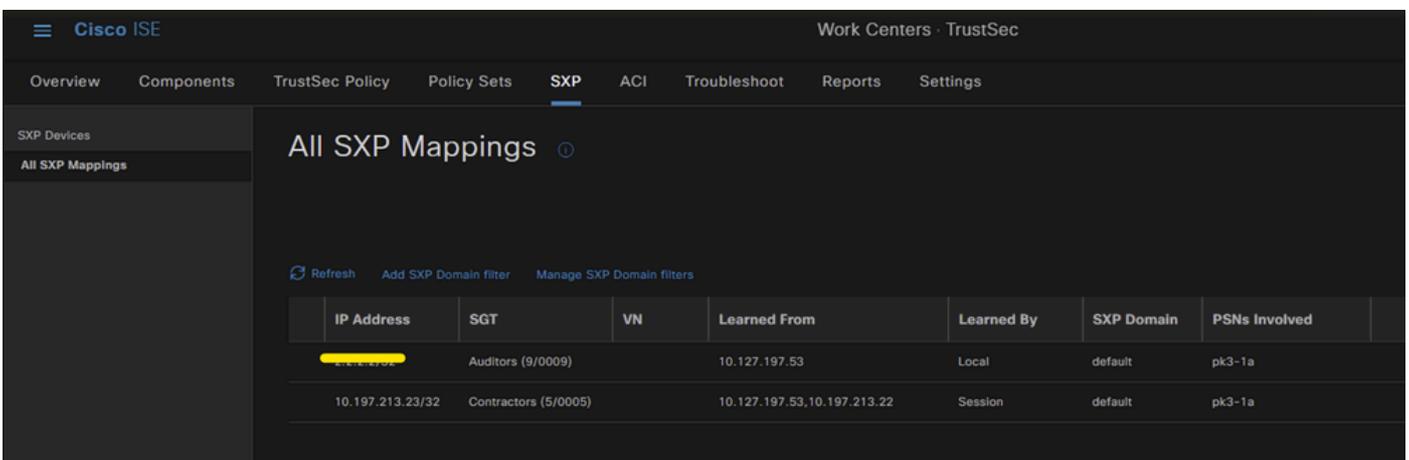


The screenshot shows the RADIUS Accounting page in Cisco ISE. The page displays a table with the following data:

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

## Passaggio 4. Mapping ISE SXP

Passare a Workcenter > Trustsec > SXP > Tutti i mapping SXP per visualizzare i mapping IP-SGT appresi in modo dinamico dalla sessione Radius.



The screenshot shows the All SXP Mappings page in Cisco ISE. The page displays a table with the following data:

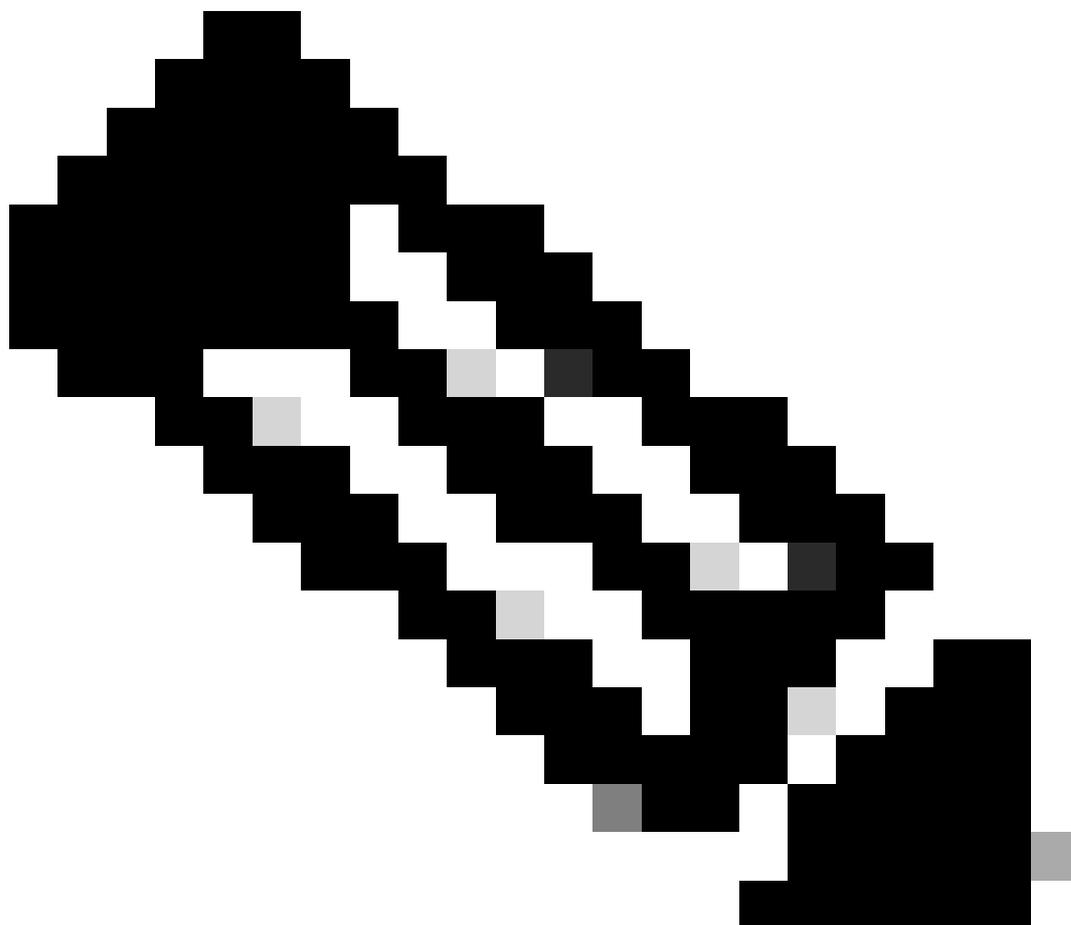
IP Address	SGT	VN	Learned From	Learned By	SXP Domain	PSNs Involved
10.127.197.53	Auditors (9/0009)		10.127.197.53	Local	default	pk3-1a
10.197.213.23/32	Contractors (5/0005)		10.127.197.53,10.197.213.22	Session	default	pk3-1a

Autore

Locale: binding IP-SGT assegnati in modo statico su ISE.

Sessione: associazioni IP-SGT apprese in modo dinamico dalla sessione Radius.

---



Nota: ISE ha la capacità di ricevere i binding IP-SGT da un altro dispositivo. Queste associazioni possono essere visualizzate come Apprese da SXP in Tutti i mapping SXP.

---

## Passaggio 5. Mapping SXP sullo switch

Lo switch ha appreso le mappature IP-SGT da ISE al protocollo SXP.

```
C9300B#show cts sxp sgt-map vrf Mgmt-vrf brief
Mapping IP-SGT come segue:
IPv4, SGT: <10.197.213.23 , 5>
Numero totale di mapping IP-SGT: 2
conn in sxp_bnd_exp_conn_list (totale:0):
C9300B#
```

C9300B#show cts mappa dei segmenti basata sul ruolo vrf Mgmt-vrf all  
Informazioni sui binding IPv4-SGT attivi

Origine SGT indirizzo IP

=====  
10.197.213.23.5 SXP

Riepilogo binding attivi IP-SGT

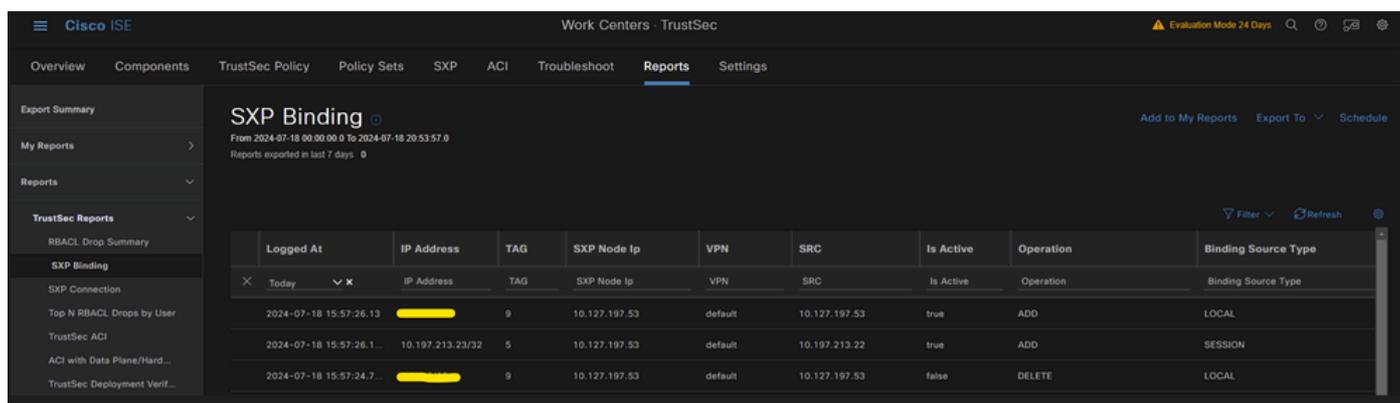
=====  
Numero totale di binding SXP = 2  
Numero totale di binding attivi = 2

## Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

### Report ISE

ISE consente anche di generare rapporti di collegamento e connessione SXP, come mostrato in questa immagine.



The screenshot shows the Cisco ISE interface for 'Work Centers - TrustSec' under the 'Reports' tab. The main content is 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 displayed 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	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...	10.197.213.23/32	9	10.127.197.53	default	10.127.197.53	false	DELETE	LOCAL

### Debug su ISE

Raccogliere il bundle di supporto ISE con questi attributi da impostare al livello di debug:

- sxp
- sgtbinding
- nsf
- sessione nsf
- trustsec

Quando un utente viene autenticato dal server ISE, ISE assegna un SGT nel pacchetto di risposta di accettazione dell'accesso. Una volta che l'utente riceve l'indirizzo IP, lo switch invia l'indirizzo IP con frame nel pacchetto di accounting Radius.

show logging application localStore/iseLocalStore.log:

```
2024-07-18 09:55:55.051 +05:30 000017592 3002 AVVISO Radius-Accounting: Aggiornamento watchdog accounting RADIUS, ConfigVersionId=129, Device IP Address=10.197.213.22, UserName=cisco, NetworkDeviceName=pk, User-Name=cisco, NAS-IP-Address=10.197.213.22, NAS-Port=50124, Framed-IP-Address=10.197.213.23, Class=CACS:16D5C50A0000017C425E3C6: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=0000007, Acct-Authentic=Remote, Acct-Input-Packets=4, Acct-Output-Packets=0, Event-Timestamp=1721277745, NAS-Port-Type=Ethernet, NAS-Port-Id=TenGigabit Ethernet1/0/24, cisco-av-pair=audit-session-id=16D5C50A0000017C425E3C6, cisco-av-pair=method=dot1x, cisco-av-pair=cts:security-group-tag=0005-00, AcsSessionID=pk3-1a/510648097/28, SelectedAccessService=Default Network Access, RequestLatency=6, Step=1 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=16D5C50A0000017C425E3C6, TotalAuthenDevice Latency=6, ClientNetwork Location=Location#All Locations, Device Type=Device Type#All Device Types, IPSEC=IPSEC#Is IPSEC Device#No,
```

show logging application ise-psc.log:

```
2024-07-18 09:55:55,054 DEBUG [SxpSessionNotifierThread][]  
ise.sxp.sessionbinding.util.SxpBindingUtil -::  
registrazione dei valori di sessione ricevuti da PortCpmBridge:  
Tipo operazione ==>ADD, sessionId ==> 16D5C50A0000017C425E3C6, sessionState ==>  
ACCETTATO, inputIp ==> 10.197.213.23, inputSgTag ==> 0005-00, nasIp ==>  
10.197.213.22null, vn ==> null
```

Il nodo SXP memorizza il mapping IP + SGT nella tabella H2DB e il nodo PAN successivo raccoglie il mapping IP + SGT e riflette in Workcenter > Trustsec > SXP > Tutti i mapping SXP.

show logging application sxp\_appserver/sxp.log:

```
2024-07-18 10:01:01,312 INFO [sxpservice-http-96441] cisco.ise.sxp.rest.SxpGlueRestAPI:147 -  
SXP-PEERF Aggiungi dimensioni batch associazioni sessioni: 1  
2024-07-18 10:01:01,317 DEBUG [SxpNotificationSerializer-Thread]  
cpm.sxp.engine.services.NotificationSerializerImpl:202 - attività di elaborazione [add=true,  
notification=RestSxpLocalBinding(tag=5, groupName=null, ipAddress=10.197.213.23/32,  
nasIp=10.197.213.22, sessionId=16D5C50A0000017C425E3C6, peerSequence=null,  
sxpBindingOpType=null, sessionExpiryTimeInMillis=0, apic=false, routable=true, vns=[])  
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]  
cisco.cpm.sxp.engine.SxpEngine:1543 - [VPN: 'default'] Aggiunta nuova associazione:  
MasterBindingIdentity [ip=10.197.213.23/32, peerSequence=10.127.197.53,10.197.213.22,
```

```
tag=5, isLocal=true, sessionId=16D5C50A0000017C425E3C6, vn=DEFAULT_VN]
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.SxpEngine:1581 - Aggiunta di 1 binding
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.MasterDbListener:251 - Invio dell'attività al gestore H2 per l'aggiunta di
binding, numero di binding: 1
2024-07-18 10:01:01,344 DEBUG [H2_HANDLER] cisco.cpm.sxp.engine.MasterDbListener:256 -
Elaborazione di MasterDbListener su aggiunta - bindingsCount: 1
```

Il nodo SXP aggiorna lo switch peer con i binding IP-SGT più recenti.

```
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 a
[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 - SENT_UPDATE RIUSCITO a
[ISE:10.127.197.53][10.127.197.53:64999/10.127.213.27:31025][O|Sv4]
```

## Debug sullo switch

Abilitare questi debug sullo switch per la risoluzione dei problemi relativi alle connessioni e agli aggiornamenti SXP.

debug cts sxp conn

errore debug cts sxp

debug cts sxp mdb

messaggio debug cts sxp

Switch ha ricevuto le mappature SGT-IP dall'altoparlante SXP ISE.

Selezionare Mostra log per visualizzare i seguenti log:

```
18 lug 04:23:04,324: CTS-SXP-MSG:sxp_rcv_update_v4 <1> ip peer: 10.127.197.53
18 lug 04:23:04,324: CTS-SXP-MDB:IMU Aggiungi binding:- <conn_index = 1> dal peer
10.127.197.53
18 lug 04:23:04,324: CTS-SXP-MDB:mdb_send_msg <IMU_ADD_IPSGT_DEVID>
18 lug 04:23:04,324: CTS-SXP-INTNL:mdb_send_msg mdb_process_add_ipsgt_device_Start
```

18 lug 04:23:04,324: CTS-SXP-MDB:sxp\_mdb\_inform\_rbm tableid:0x1 sense:1 sgt:5  
peer:10.127.197.53

18 lug 04:23:04,324: CTS-SXP-MDB:SXP MDB: Voce aggiunta ip 10.197.213.23 sgt 0x0005

18 lug 04:23:04,324: CTS-SXP-INTNL:mdb\_send\_msg mdb\_process\_add\_ipsgt\_device Fine

## Informazioni correlate

[Guida dell'amministratore di Cisco Identity Services Engine, versione 3.1](#)

[Guida alla configurazione di Cisco TrustSec, Cisco IOS XE Bengaluru 17.6.x \(switch Catalyst 9300\)](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).