

Entender os registros de atualização do ISE SXP junto com os registros de depuração do Catalyst

Contents

[Introdução](#)

[Informações de Apoio](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configuração](#)

[Diagrama de Rede](#)

[Fluxo de tráfico](#)

[Configurar o switch](#)

[Configurar o ISE](#)

[Etapa 1. Habilitar serviço SXP no ISE](#)

[Etapa 2. Adicionar dispositivos SXP](#)

[Etapa 3. Configurações do SXP](#)

[Verificar](#)

[Etapa 1. Conexão SXP no Switch](#)

[Etapa 2. verificação de ISE SXP](#)

[Etapa 3. Contabilidade RADIUS](#)

[Etapa 4. Mapeamentos ISE SXP](#)

[Etapa 5. Mapeamentos SXP no Switch](#)

[Troubleshooting](#)

[Relatório do ISE](#)

[Depurações no ISE](#)

[Depurações no Switch](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar e entender a conexão do Security Group Exchange Protocol (SXP) entre o ISE e o Switch Catalyst 9300.

Informações de Apoio

O SXP é o protocolo de intercâmbio SGT (marcação de grupo de segurança) usado pelo TrustSec para propagar IP para mapeamentos SGT para dispositivos TrustSec.

O SXP foi desenvolvido para permitir que as redes que incluem dispositivos de terceiros ou

dispositivos Cisco legados que não suportam marcação em linha SGT tenham recursos TrustSec.

O SXP é um protocolo de peering; um dispositivo pode atuar como Locutor e o outro como Ouvinte.

O alto-falante SXP é responsável por enviar as vinculações IP-SGT e o ouvinte é responsável por coletar essas vinculações.

A conexão SXP usa a porta TCP 64999 como o protocolo de transporte subjacente e MD5 para integridade/autenticidade da mensagem.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento da configuração do protocolo SXP e do Identity Services Engine (ISE).

Componentes Utilizados

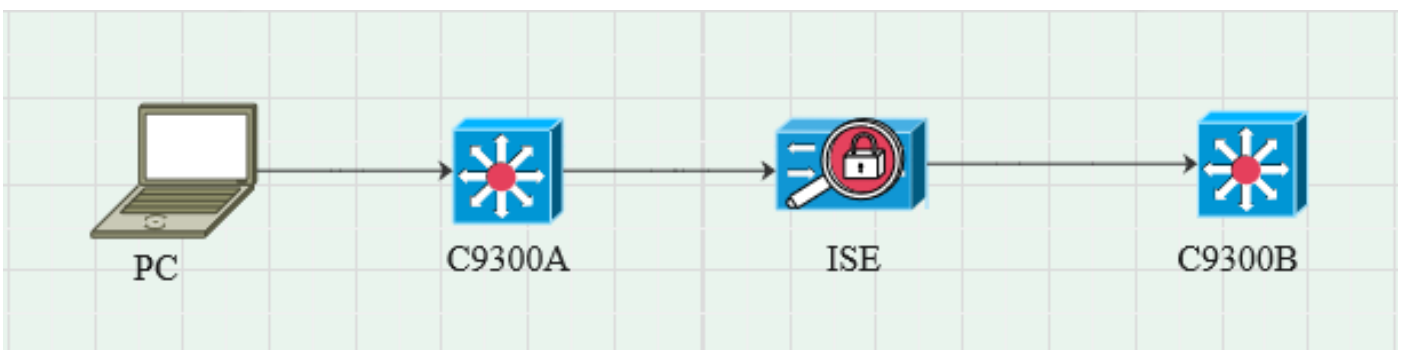
As informações neste documento são baseadas nestas versões de software e hardware:

- Switch Cisco Catalyst 9300 com software Cisco IOS® XE 17.6.5 e posterior
Cisco ISE, versão 3.1 e posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuração

Diagrama de Rede



Fluxo de tráfego

O PC autentica com C9300A e o ISE atribui dinamicamente SGT através de conjuntos de

políticas.

Quando a autenticação tiver sido aprovada, as associações serão criadas com um IP igual ao atributo RADIUS do endereço IP com quadro e SGT, conforme configurado na política.

As vinculações se propagam em "Todas as vinculações do SXP" no domínio padrão.

O C9300B recebe as informações de mapeamento do SXP do ISE através do protocolo SXP.

Configurar o switch

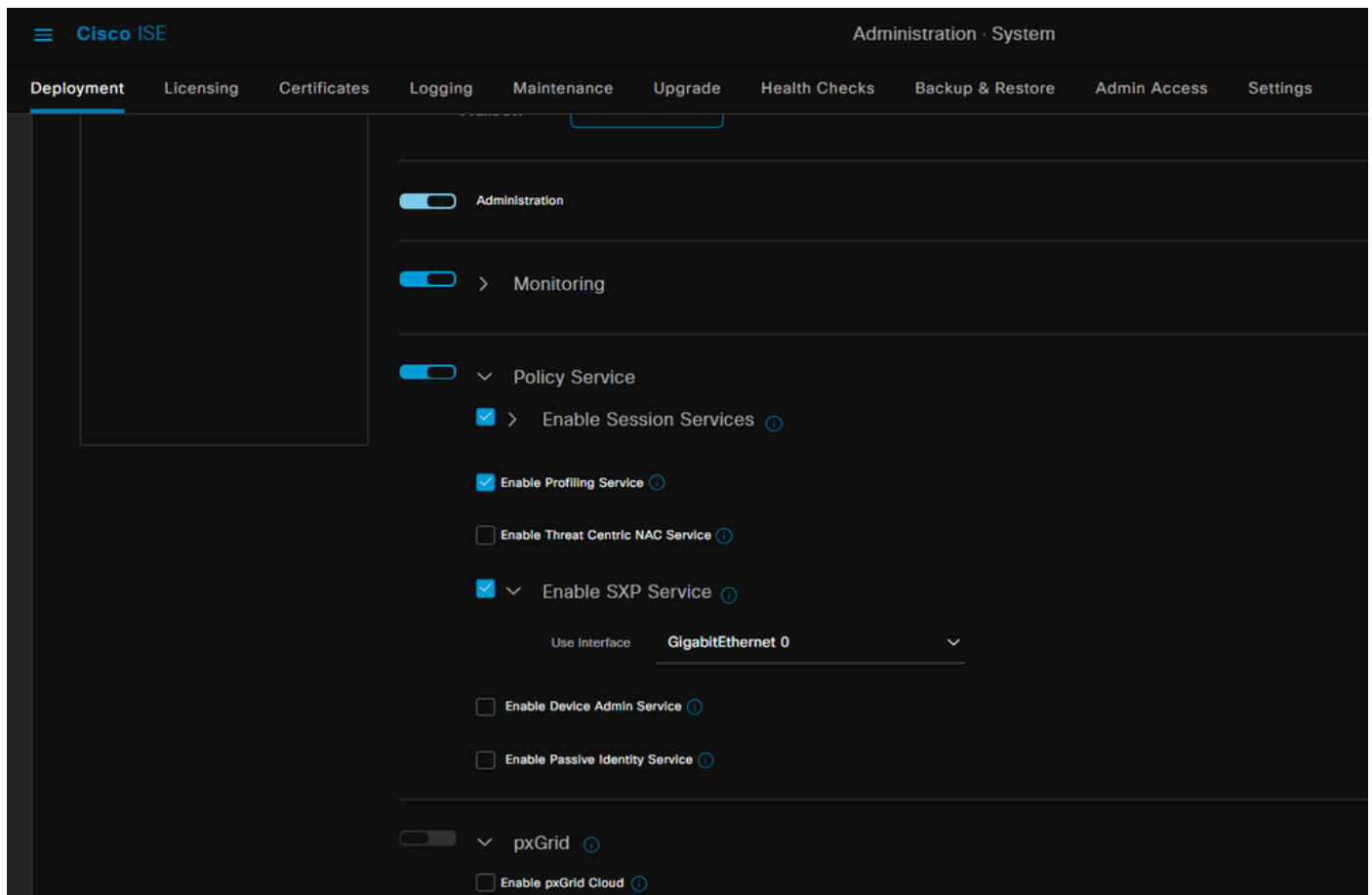
Configure o switch como um ouvinte SXP para obter os mapeamentos IP-SGT do ISE.

```
cts sxp enable
cts sxp default password 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 0 vrf
Mgmt-vrf
```

Configurar o ISE

Etapa 1. Habilitar serviço SXP no ISE

Navegue para Administração > Sistema > Implantação > Editar o nó e, em Serviço de política, selecione Habilitar serviço SXP.



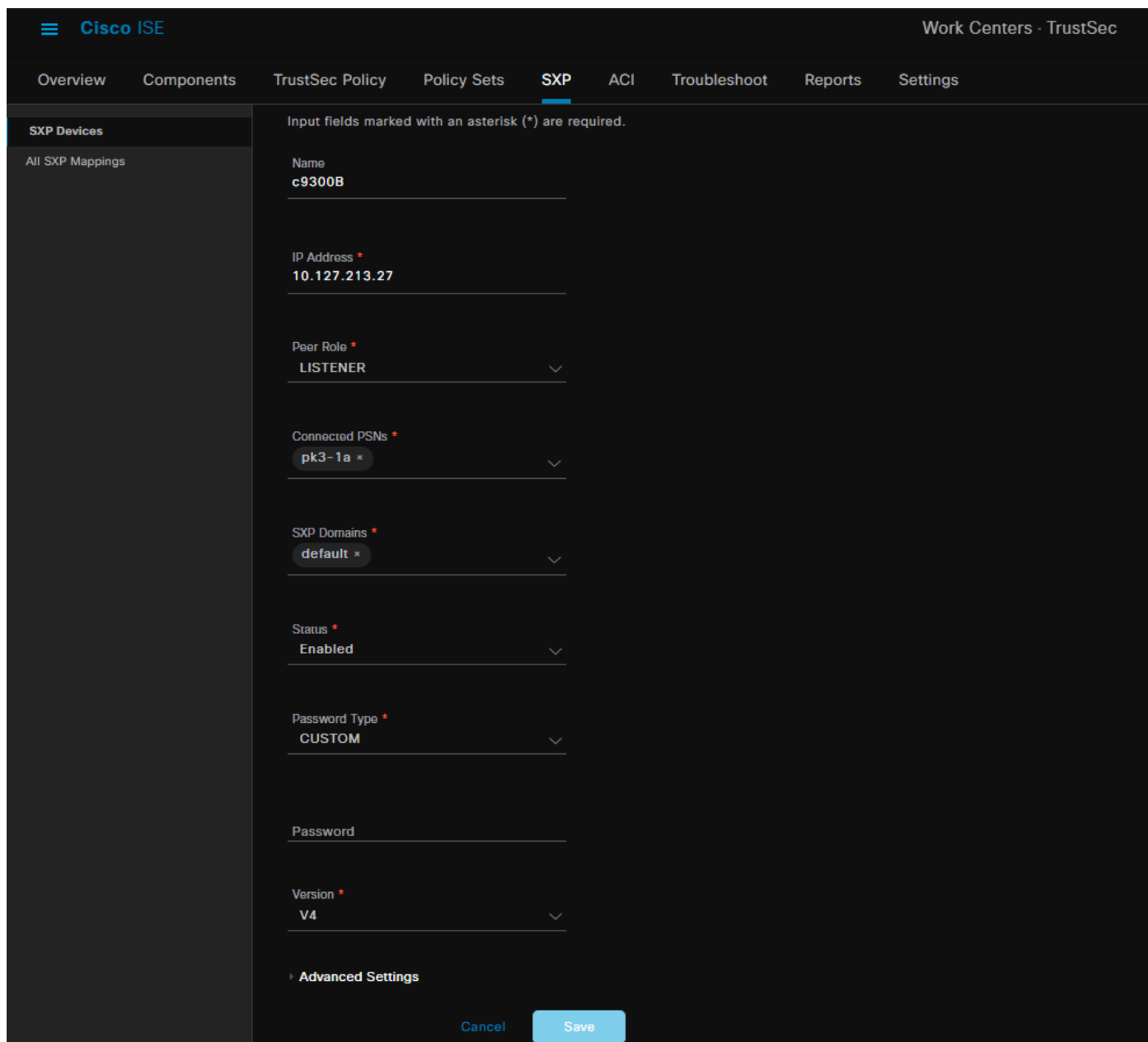
The screenshot shows the Cisco ISE Administration console interface. The top navigation bar includes "Administration · System" and various menu items: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The "Deployment" menu is selected. The main content area displays a list of services with their status (enabled/disabled) and checkboxes for enabling specific services. The "Enable SXP Service" checkbox is checked, and the "Use Interface" dropdown is set to "GigabitEthernet 0".

Service	Enabled	Configuration
Administration	Yes	
Monitoring	Yes	
Policy Service	Yes	
Enable Session Services	Yes	
Enable Profiling Service	Yes	
Enable Threat Centric NAC Service	No	
Enable SXP Service	Yes	Use Interface: GigabitEthernet 0
Enable Device Admin Service	No	
Enable Passive Identity Service	No	
pxGrid	No	
Enable pxGrid Cloud	No	

Etapa 2. Adicionar dispositivos SXP

Para configurar o ouvinte e o alto-falante SXP para os switches correspondentes, navegue para Workcenters > Trustsec > SXP > Dispositivos SXP.

Adicione o switch com a função de peer como Listener e atribua ao domínio padrão.



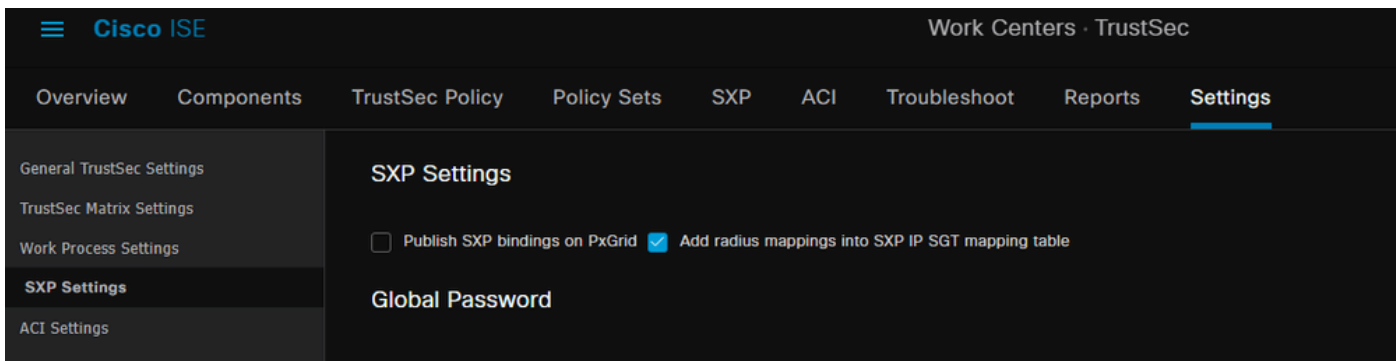
The screenshot shows the Cisco ISE configuration interface for SXP devices. The breadcrumb navigation is Work Centers > TrustSec > SXP. The left sidebar shows 'SXP Devices' and 'All SXP Mappings'. The main configuration area is titled 'SXP Devices' and contains the following fields:

- 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 two buttons: 'Cancel' and 'Save'.

Etapa 3. Configurações do SXP

Certifique-se de que Add radius mappings into SXP IP SGT mapping table esteja marcado, para que o ISE aprenda os mapeamentos IP-SGT dinâmicos por meio de Autenticações Radius.



Verificar

Etapa 1. Conexão SXP no Switch

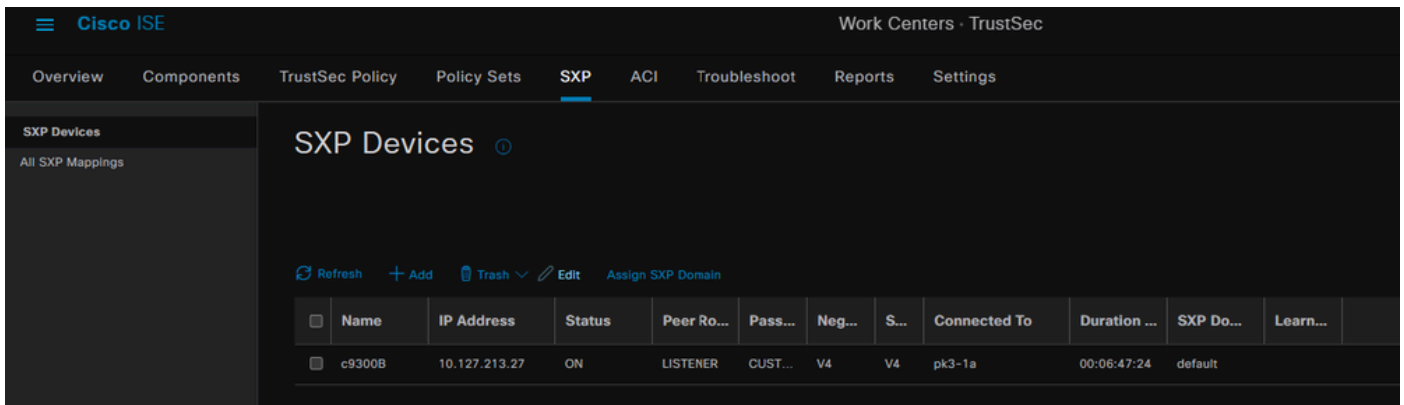
```
C9300B#show cts sxp connections vrf Mgmt-vrf
SXP : Habilitado
Versão mais alta suportada: 4
Senha Padrão : Definir
Cadeia de Chaves Padrão: Não Definida
Nome da Cadeia de Chaves Padrão: Não Aplicável
IP de origem padrão: 10.127.213.27
Período de abertura de novas tentativas de conexão: 120 segundos
Período de reconciliação: 120 segundos
O temporizador de reinício aberto não está em execução
Limite transversal de sequência de mesmo nível para exportação: Não definido
Limite transversal de sequência de mesmo nível para importação: Não definido
-----
IP de mesmo nível: 10.127.197.53
IP de origem: 10.127.213.27
Status da conexão: Ativado
Conn versão : 4
Recurso de conexão: IPv4-IPv6-Subnet
Tempo de espera de conexão: 120 segundos
Modo local : Ouvinte do SXP
Conexão inst# : 1
conn fd de TCP : 1
Senha TCP conn: senha SXP padrão
O temporizador de espera está em execução
Duração desde a última alteração de estado: 0:00:23:36 (dd:hr:mm:sec)

Número total de conexões SXP = 1

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

Etapa 2. verificação de ISE SXP

Verifique se o status do SXP é ON para o Switch em Workcenters > Trustsec > SXP > Dispositivos SXP.

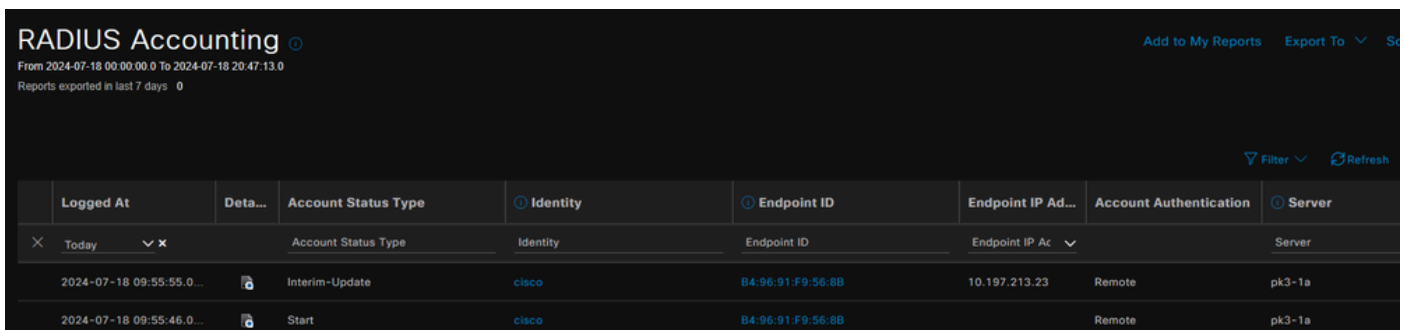


The screenshot shows the Cisco ISE interface for SXP Devices. The navigation menu includes Overview, Components, TrustSec Policy, Policy Sets, SXP (selected), ACI, Troubleshoot, Reports, and Settings. The main content area is titled 'SXP Devices' and contains a table with the following data:

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	

Etapa 3. Contabilidade RADIUS

Verifique se o ISE recebeu o atributo RADIUS do endereço IP com quadros do pacote de contabilização Radius após a autenticação bem-sucedida.

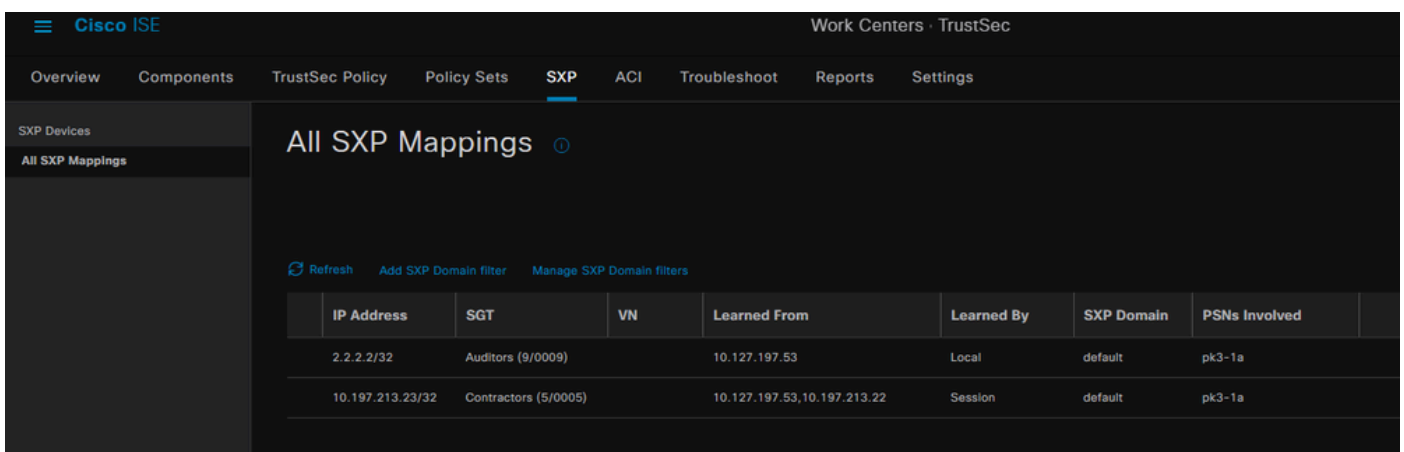


The screenshot shows the Cisco ISE RADIUS Accounting page. The navigation menu includes Overview, Components, TrustSec Policy, Policy Sets, SXP (selected), ACI, Troubleshoot, Reports, and Settings. The main content area is titled 'RADIUS Accounting' and contains a table with the following data:

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

Etapa 4. Mapeamentos ISE SXP

Navegue para Workcenters > Trustsec > SXP > All SXP Mappings para exibir os mapeamentos IP-SGT aprendidos dinamicamente da sessão Radius.



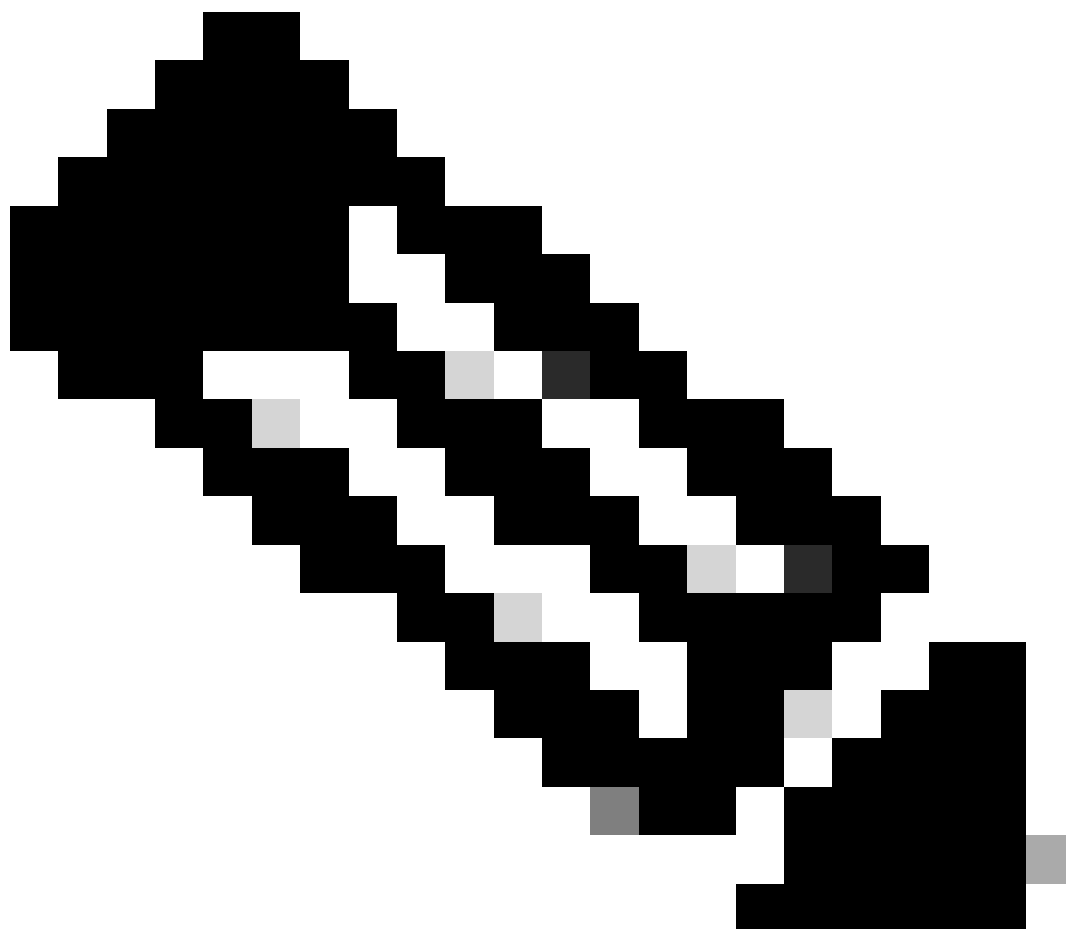
The screenshot shows the Cisco ISE All SXP Mappings page. The navigation menu includes Overview, Components, TrustSec Policy, Policy Sets, SXP (selected), ACI, Troubleshoot, Reports, and Settings. The main content area is titled 'All SXP Mappings' and contains a table with the following data:

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

Aprendido por

Local - Associações IP-SGT atribuídas estaticamente no ISE.

Sessão - Associações IP-SGT aprendidas dinamicamente da sessão Radius.



Observação: o ISE tem a capacidade de receber associações IP-SGT de outro dispositivo. Essas vinculações podem ser exibidas como Aprendidas pelo SXP em Todos os mapeamentos do SXP.

Etapa 5. Mapeamentos SXP no Switch

O switch aprendeu os mapeamentos IP-SGT do ISE através do protocolo SXP.

```
C9300B#show cts sxp sgt-map vrf Mgmt-vrf brief
ID do nó SXP (gerado):0x03030303(3.3.3.3)
Mapeamentos IP-SGT da seguinte maneira:
IPv4,SGT: <2.2.2.2 , 9>
IPv4,SGT: <10.197.213.23 , 5>
```

Número total de mapeamentos IP-SGT: 2
conn na sxp_bnd_exp_conn_list (total:0):
C9300B#

C9300B#show cts role-based sgt-map vrf Mgmt-vrf all
Informações de Associações IPv4-SGT Ativas

Origem SGT do Endereço IP

=====

2.2.2.2.9 SXP
10.197.213.23 5 SXP

Resumo de Associações Ativas IP-SGT

=====

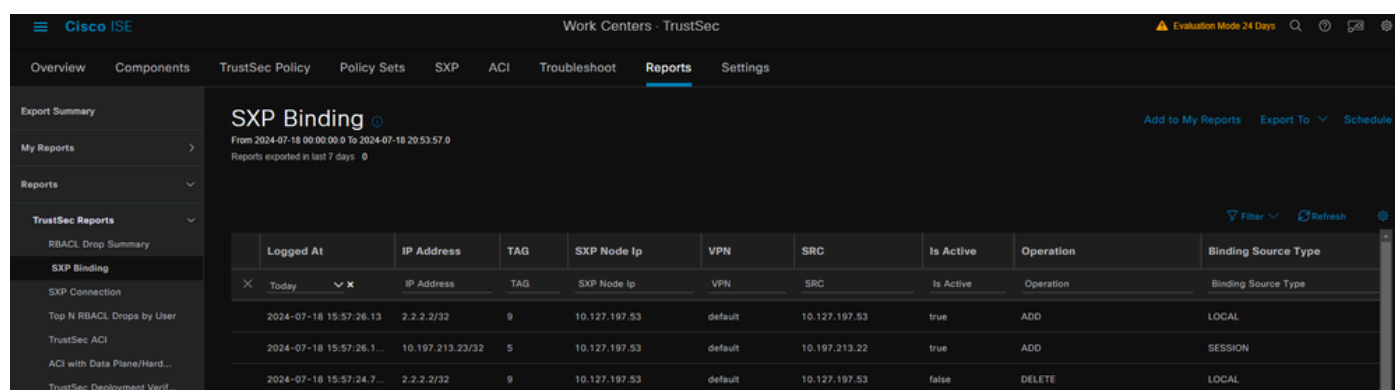
Número total de associações SXP = 2
Número total de associações ativas = 2

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Relatório do ISE

O ISE também permite gerar relatórios de ligação e conexão do SXP, como mostrado nesta imagem.



The screenshot shows the Cisco ISE Reports page for SXP Binding. The report is titled "SXP Binding" and shows data for the period from 2024-07-18 00:00:00.0 to 2024-07-18 20:53:57.0. The report is filtered for "Today" and shows 3 entries.

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

Depurações no ISE

Colete o pacote de suporte do ISE com estes atributos a serem definidos no nível de depuração:

- sxp
- sgtbinding
- nsf
- nsf-session
- trustsec

Quando um usuário é autenticado do servidor ISE, o ISE atribui um SGT no pacote de resposta de aceitação de acesso. Quando o usuário obtém o endereço IP, o switch envia o endereço IP com quadros no pacote de contabilização RADIUS.

show logging application localStore/iseLocalStore.log:

```
2024-07-18 09:55:55.051 +05:30 000017592 3002 AVISO Radius-Accounting: Atualização do watchdog de Contabilidade RADIUS, ConfigVersionId=129, Endereço IP do Dispositivo=10.197.213.22, UserName=cisco, NetworkDeviceName=cisco pk, User-Name=cisco, NAS-IP-Address=10.197.213.22, 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-1 8, 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-Packets d=TenGigabitEthernet1/0/24, cisco-av-pair=audit-session-id=16D5C50A00000017C425E3C6, cisco-av-pair=method=dot1x, cisco-av-pair=cts:security-group-tag=0005-00, AcsSessionID=pk3-1a/510648097/28, SeletedAccessService=Acesso Padrão à Rede, RequestLatency=6, Step=11004, Step=11017 Etapa=15049, Etapa=15008, Etapa=22085, Etapa=11005, NetworkDeviceGroups=IPSEC#Is IPSEC Device#No, NetworkDeviceGroups=Location#Todos os locais, NetworkDeviceGroups=Device Type#Todos os tipos de dispositivo, CPMSessionID=16D5C50A00000017C425E3C6, TotalAuthenLatency=6, ClientLatency=0, Network Device Profile=Cisco, Local=Location#Todos os locais, Tipo de dispositivo=Tipo de dispositivo#Todos os tipos de dispositivo, IPSEC=IPSEC#Is Dispositivo#Não,
```

show logging application ise-psc.log:

```
2024-07-18 09:55:55,054 DEBUG [SxpSessionNotifierThread][]
ise.sxp.sessionbinding.util.SxpBindingUtil -:::-
registrando os valores de sessão recebidos de PrrtCpmBridge:
Tipo de operação ==>ADD, sessionId ==> 16D5C50A00000017C425E3C6, sessionState ==>
ACCEPTED, inputIp ==> 10.197.213.23, inputSgTag ==> 0005-00, nasIp ==> 10.197.213.22null,
vn ==> null
```

O nó SXP armazena o mapeamento IP + SGT em sua tabela H2DB e o nó PAN posterior reúne esse mapeamento IP SGT e reflete em todos os mapeamentos SXP na GUI do ISE (Workcenters ->Trustsec -> SXP->todos os mapeamentos SXP).

show logging application sxp_appserver/sxp.log:

```
2024-07-18 10:01:01,312 INFORMAÇÕES [sxp-service-http-96441]
cisco.ise.sxp.rest.SxpGlueRestAPI:147 - SXP-PEERF Adicionar Ligações de Sessão tamanho de
```

lote: 1

```
2024-07-18 10:01:01,317 DEBUG [SxpNotificationSerializer-Thread]
cpm.sxp.engine.services.NotificationSerializerImpl:202 - tarefa de processamento [add=true,
notification=RestSxpLocalBinding(tag=5, groupName=null, ipAddress=10.197.213.23/32,
nasIp=10.197.213.22, sessionId=16D5C50A00000017C425E3C6, 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'] Adicionando nova associação:
MasterBindingIdentity [ip=10.197.213.23/32, peerSequence=10.127.197.53,10.197.213.22,
tag=5, isLocal=true, sessionId=16D5C50A00000017C425E3C6, vn=DEFAULT_VN]
```

```
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.SxpEngine:1581 - Adicionando 1 associação(ões)
```

```
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.MasterDbListener:251 - Enviando tarefa ao Manipulador H2 para adicionar
associações, contagem de associações: 1
```

```
2024-07-18 10:01:01,344 DEBUG [H2_HANDLER] cisco.cpm.sxp.engine.MasterDbListener:256 -
MasterDbListener Processamento onAdded - bindingsCount: 1
```

O nó SXP atualiza o Peer Switch com as ligações IP-SGT mais recentes.

```
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 - SENT_UPDATE para
[[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 BEM-SUCEDIDO para
[[ISE:10.127.197.53][10.127.197.53:64999/10.127.213.27:31025]][O|Sv4]
```

Depurações no Switch

Ative essas depurações no switch para solucionar problemas de conexões e atualizações do SXP.

```
debug cts sxp conn
```

```
debug cts sxp error
```

```
debug cts sxp mdb
```

```
debug cts sxp message
```

Switch recebeu os mapeamentos SGT-IP do locutor SXP "ISE".

Marque **Show logging** para exibir estes logs:

```
Jul 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 Adicionar vinculação:- <conn_index = 1> do peer
10.127.197.53
Jul 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 Iniciar
Jul 18 04:23:04.324: CTS-SXP-MDB:sxp_mdb_inform_rbm tableid:0x1 sense:1 sgt:5
peer:10.127.197.53
Jul 18 04:23:04.324: CTS-SXP-MDB:SXP MDB: Entrada adicionada ip 10.197.213.23 sgt 0x0005
Jul 18 04:23:04.324: CTS-SXP-INTNL:mdb_send_msg mdb_process_add_ipsgt_devid Concluído
```

Informações Relacionadas

[Segmentação do guia do administrador do ISE 3.1](#)

[Visão geral do Guia de configuração do Catalyst Trustsec](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.