# **Understand ISE SXP Update Logs along with Catalyst Debug Logs**

### Contents

**Introduction Background Information Prerequisites** Requirements Components Used **Configuration** Network Diagram **Traffic Flow Configure Switch** Configure ISE Step 1. Enable SXP service on ISE Step 2. Add SXP devices Step 3. SXP Settings **Verify** Step 1. SXP connection on Switch Step 2. ISE SXP verification Step 3. Radius Accounting Step 4. ISE SXP Mappings Step 5. SXP Mappings on Switch Troubleshoot ISE Report Debugs on ISE Debugs on Switch **Related Information** 

# Introduction

This document describes how to configure and understand the Security Group Exchange Protocol (SXP) connection between ISE and Catalyst 9300 Switch.

# **Background Information**

SXP is the SGT (Security Group Tag) Exchange Protocol used by TrustSec to propagate IP to SGT mappings to TrustSec Devices.

SXP was developed to allow networks including third-party devices or legacy Cisco devices that do not support SGT inline tagging to have TrustSec capabilities.

SXP is a peering protocol; one device can act as a Speaker and the other as a Listener.

The SXP speaker is responsible for sending the IP-SGT bindings and the listener is responsible for collecting these bindings.

The SXP connection uses TCP port 64999 as the underlying transport protocol and MD5 for message integrity/authenticity.

# Prerequisites

### Requirements

Cisco recommends that you have knowledge of the SXP Protocol and Identity Services Engine (ISE) configuration.

#### **Components Used**

The information in this document is based on these software and hardware versions:

• Cisco Catalyst 9300 switch with software Cisco IOS® XE 17.6.5 and later Cisco ISE, Release 3.1 and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

### Configuration

#### **Network Diagram**



### **Traffic Flow**

PC authenticates with C9300A and ISE dynamically assigns SGT through Policy sets. When the authentication has passed, bindings are created with an IP equal to the Framed-IP address RADIUS attribute and SGT as configured in the policy. The bindings propogate in "All SXP bindings" under the default domain. C9300B receives the SXP mapping information from ISE through SXP protocol.

### **Configure Switch**

Configure the switch as an SXP listener to get the IP-SGT mappings from 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

### **Configure ISE**

### Step 1. Enable SXP service on ISE

Navigate to Administration > System > Deployment > Edit the node and under Policy Service select Enable SXP Service.

≡ Cisco I	SE					Adm	inistration System		
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
			Ad	Iministration					
				Monitoring					
			<b></b> •	Policy Service	ssion Service	8 0			
			M	Enable Profiling Service	:e 🕕				
				Enable Threat Centric	NAC Service 🕕				
				✓ Enable SXI	PService 🕕				
				Use Interface	GigabitEth	ernet 0	~		
				Enable Device Admin	Service 🕕				
				Enable Passive Identi	ty Service 🕕				
				pxGrid 🕕					
				Enable pxGrid Cloud	0				

### Step 2. Add SXP devices

In order to configure SXP listener and speaker for the corresponding switches, navigate to **Workcenters** > **Trustsec** > **SXP** > **SXP** Devices.

Add the switch with peer role as Listener and assign to default domain.

≡ Cisco	ISE							Work Centers - TrustSec
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings
SXP Devices		Input fields marked	l with an asterisk (	(*) are req	uired.			
All SXP Mappings		Nате с9300В						
		IP Address * 10.127.213.27						
		Peer Role *						
		Connected PSNs * pk3-1a ×						
		SXP Domains * default ×						
		Status * Enabled						
		Password Type * CUSTOM						
		Password						
		Version * V4						
		Advanced Setting	JS					
				Sav	e			

### **Step 3. SXP Settings**

Ensure **Add radius mappings into SXP IP SGT mapping table** is checked, so that ISE learns dynamic IP-SGT mappings through Radius Authentications.

≡ Cisco	E Cisco ISE Work Centers - TrustSec										
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings			
General TrustSec S TrustSec Matrix Se	Settings ettings	SXP Settings									
Work Process Setti	ings	Publish SXP bindi	ings on PxGrid 🔽 🕯	dd radius m	appings into	SXP IP SGT mapping ta	able				
SXP Settings		Global Password									
ACI Settings											

# Verify

#### Step 1. SXP connection on Switch

C9300B#show cts sxp connections vrf Mgmt-vrf SXP : Enabled Highest Version Supported: 4 Default Password : Set Default Key-Chain: Not Set Default Key-Chain Name: Not Applicable Default Source IP: 10.127.213.27 Connection retry open period: 120 secs Reconcile period: 120 secs Retry open timer is not running Peer-Sequence traverse limit for export: Not Set Peer-Sequence traverse limit for import: Not Set \_\_\_\_\_ Peer IP : 10.127.197.53 Source IP: 10.127.213.27 Conn status : On Conn version : 4 Conn capability : IPv4-IPv6-Subnet Conn hold time : 120 seconds Local mode : SXP Listener Connection inst# : 1 TCP conn fd : 1 TCP conn password: default SXP password Hold timer is running Duration since last state change: 0:00:23:36 (dd:hr:mm:sec) Total num of SXP Connections = 10x7F128DF555E0 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

### Step 2. ISE SXP verification

Verfiy the SXP status is **ON** for the Switch under **Workcenters** > **Trustsec** > **SXP** > **SXP Devices**.

<b>≡ Cisco</b> ISE			Worl	Work Centers · TrustSec								
Overview Components	TrustSec Policy	Policy Sets	SXP AC	l Troub	leshoot	Repo	rts	Settings				
SXP Devices	SXP Devices											
All SXP Mappings												
			Edit Assign									
	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		

#### **Step 3. Radius Accounting**

Ensure ISE received the Framed-IP address RADIUS attribute from Radius Accounting Packet following successful authentication.

RA From 2 Report	DIUS Accou 024-07-18 00:00 00 0 To 2024-07- s exported in last 7 days 0	nting 18 20:47:13.	© ,				Add to My Reports	: Export To ∨ So Filter ∨ ØRefresh
	Logged At	Deta	Account Status Type	Identity	Endpoint ID	Endpoint IP Ad	Account Authentication	O Server
×	Today 🗸 🗙		Account Status Type	Identity	Endpoint ID	Endpoint IP Ac 🗸		Server
	2024-07-18 09:55:55.0	6	Interim-Update			10.197.213.23	Remote	pk3-1a
	2024-07-18 09:55:46.0	ò	Start				Remote	pk3-1a

#### **Step 4. ISE SXP Mappings**

Navigate to **Workcenters** > **Trustsec** > **SXP** > **All SXP Mappings** to view the dynamically learned IP-SGT mappings from Radius session.

≡ Cisco	o ISE					Work Centers	TrustSec			
Overview	Components	TrustSec Policy	Policy Sets SX	P ACI	Troubleshoot	Reports Se	ettings			
SXP Devices All SXP Mapping	5	All SXP M	lappings (	)						
		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 (5/00	005)	10.127.197.53,1	0.197.213.22	Session	default	pk3-1a	

#### Learned By

Local - Statically assigned IP-SGT bindings on ISE. Session - Dynamically learned IP-SGT bindings from Radius session.



**Note**: The ISE has the capability to receive IP-SGT bindings from another device. These bindings could be displayed as **Learned by SXP** under All SXP Mappings.

### Step 5. SXP Mappings on Switch

The switch learned IP-SGT mappings from ISE through SXP protocol.

C9300B**#show cts sxp sgt-map vrf Mgmt-vrf brief** SXP Node ID(generated):0x03030303(3.3.3.3) IP-SGT Mappings as follows: IPv4,SGT: <2.2.2.2, 9> **IPv4,SGT: <10.197.213.23 , 5>** Total number of IP-SGT Mappings: 2 conn in the sxp\_bnd\_exp\_conn\_list (total:0): C9300B**#** C9300B**#show cts role-based sgt-map vrf Mgmt-vrf all** Active IPv4-SGT Bindings Information

IP Address SGT Source
2.2.2.2 9 SXP 10.197.213.23 5 SXP
IP-SGT Active Bindings Summary
Total number of SXP bindings = 2 Total number of active bindings = 2

# Troubleshoot

This section provides information you can use to troubleshoot your configuration.

### **ISE Report**

ISE also allows to generate SXP binding and connection reports, as shown in this image.

■ Cisco ISE							Work Cent	ers · Trusts	Sec			A Eva	Nation Mode 24 Days Q 🕜 🞜 🖗
Overview Compone	ents	TrustS	ec Policy	Policy Se	ets SXP	ACI Tro	ubleshoot	Reports	Settings				
Export Summary		SX	P Bind	dina o									
My Reports		Frem 2024-07-18 00 000 00 10 2024-07-18 20-53-57.0 Reports exported in last 7 days 0											
Reports													
TrustSec Reports													
RBACL Drop Summary			Logged At		IP Address	TAG	SXP Node	lp	VPN	SRC	Is Active	Operation	Binding Source Type
SXP Binding													
			Today	××	IP Address	TAG	SXP Node I		VPN	SRC	Is Active	Operation	Binding Source Type
			2024-07-18						default				LOCAL
									default			ADD	SESSION
ACI with Data Plane/Hard TrustSec Deployment Veril			2024-07-18					53	default		false	DELETE	LOCAL

### **Debugs on ISE**

Collect the ISE support bundle with these atributes to be set at the debug level:

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

When a user is authenticated from ISE server, ISE assigns an SGT in the access accept response packet. Once the user gets the IP address, the switch sends the Framed IP address in the Radius Accounting Packet.

#### show logging application localStore/iseLocalStore.log:

2024-07-18 09:55:55.051 +05:30 0000017592 **3002 NOTICE Radius-Accounting**: RADIUS Accounting watchdog update, 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: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=method=dot1x, cisco-av-pair=cts:security-group-tag=0005-00, AcsSessionID=pk3-1a/510648097/28,

SelectedAccessService=Default Network Access, 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, Network Device Profile=Cisco, 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 -::::logging the session values received from PrrtCpmBridge : Operation type ==>ADD, sessionId ==> 16D5C50A00000017C425E3C6, sessionState ==> ACCEPTED, inputIp ==> 10.197.213.23, inputSgTag ==> 0005-00, nasIp ==> 10.197.213.22null, vn ==> null

The SXP node stores the IP + SGT mapping in its H2DB table and later PAN node gathers this IP SGT mapping and reflects in All SXP mappings in ISE GUI (Workcenters ->Trustsec -> SXP->All SXP Mappings).

#### 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 Add Session Bindings batch-size: 1 2024-07-18 10:01:01,317 DEBUG [SxpNotificationSerializer-Thread] cpm.sxp.engine.services.NotificationSerializerImpl:202 - processing task Task [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'] Adding new binding: MasterBindingIdentity

cisco.cpm.sxp.engine.SxpEngine:1543 - [VPN: 'default'] Adding new binding: 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 - Adding 1 binding(s) 2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread] cisco.cpm.sxp.engine.MasterDbListener:251 - Submitting task to H2 Handler for adding bindings, bindings count: 1 2024-07-18 10:01:01,344 DEBUG [H2\_HANDLER] cisco.cpm.sxp.engine.MasterDbListener:256 -MasterDbListener Processing onAdded - bindingsCount: 1

The SXP node updates the Peer Switch with the latest IP-SGT bindings.

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 to [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 SUCCESSFUL to [ISE:10.127.197.53][10.127.197.53:64999/10.127.213.27:31025][O|Sv4]

#### **Debugs on Switch**

Enable these debugs on the switch to troubleshoot SXP connections and updates.

debug cts sxp conn

debug cts sxp error

debug cts sxp mdb

debug cts sxp message

Swicth received the SGT-IP mappings from the SXP Speaker "ISE".

Check Show logging to view these logs:

Jul 18 04:23:04.324: CTS-SXP-MSG:sxp\_recv\_update\_v4 <1> peer ip: 10.127.197.53 Jul 18 04:23:04.324: CTS-SXP-MDB:IMU Add binding:- <conn\_index = 1> from 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 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 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 Done

### **Related Information**

ISE 3.1 Admin Guide Segmentation

Catalyst Configuration Guide Trustsec Overview