Configurer ISE pour attribuer des balises de groupe de sécurité Trustsec aux sessions PassiveID

Table des matières

Introduction

Ce document décrit comment configurer et attribuer des balises de groupe de sécurité (SGT) aux sessions d'ID passif via des stratégies d'autorisation dans ISE 3.2.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ISE 3.2
- ID passif, TrustSec et PxGrid

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE 3.2
- FMC 7.0.1
- WS-C3850-24P qui exécute 16.12.1

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Cisco Identity Services Engine (ISE) 3.2 est la version minimale qui prend en charge cette fonctionnalité. Ce document ne couvre pas la configuration PassiveID, PxGrid et SXP. Pour obtenir des informations connexes, consultez le Guide d'administration.

Dans ISE 3.1 ou les versions antérieures, une balise de groupe de sécurité (SGT) ne peut être attribuée qu'à une session Radius ou à une authentification active telle que 802.1x et MAB. Avec ISE 3.2, nous pouvons configurer des stratégies d'autorisation pour les sessions PassiveID de telle sorte que lorsque Identity Services Engine (ISE) reçoit des événements de connexion utilisateur d'un fournisseur tel que WMI ou Agent AD DC (Active Directory Domain Controllers), il attribue une balise SGT (Security Group Tag) à la session PassiveID en fonction de l'appartenance au groupe Active Directory (AD) de l'utilisateur. Le mappage IP-SGT et les détails du groupe AD pour l'ID passif peuvent être publiés dans le domaine TrustSec via le protocole SXP (SGT Exchange Protocol) et/ou vers les abonnés Platform Exchange Grid (pxGrid) tels que Cisco Firepower Management Center (FMC) et Cisco Secure Network Analytics (Stealthwatch).

Configurer

Diagramme De Flux

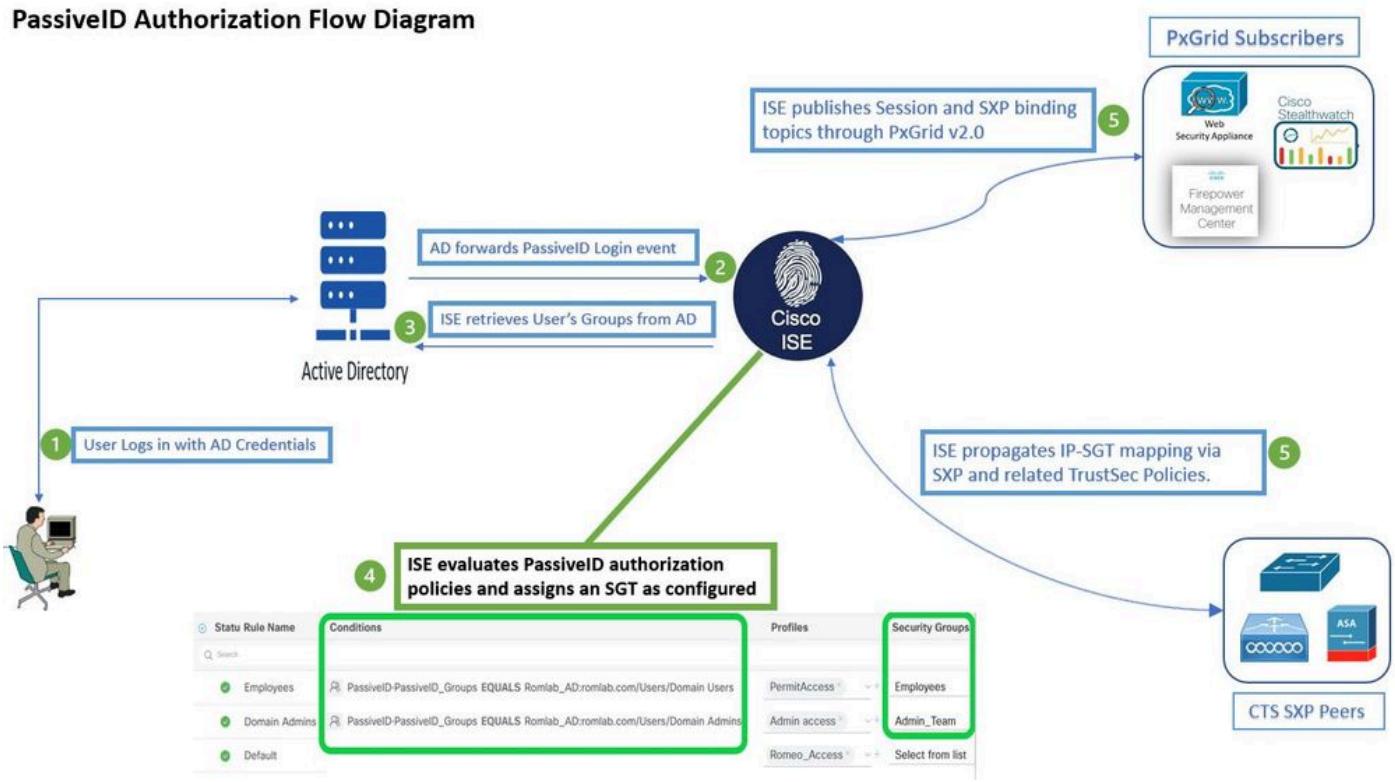
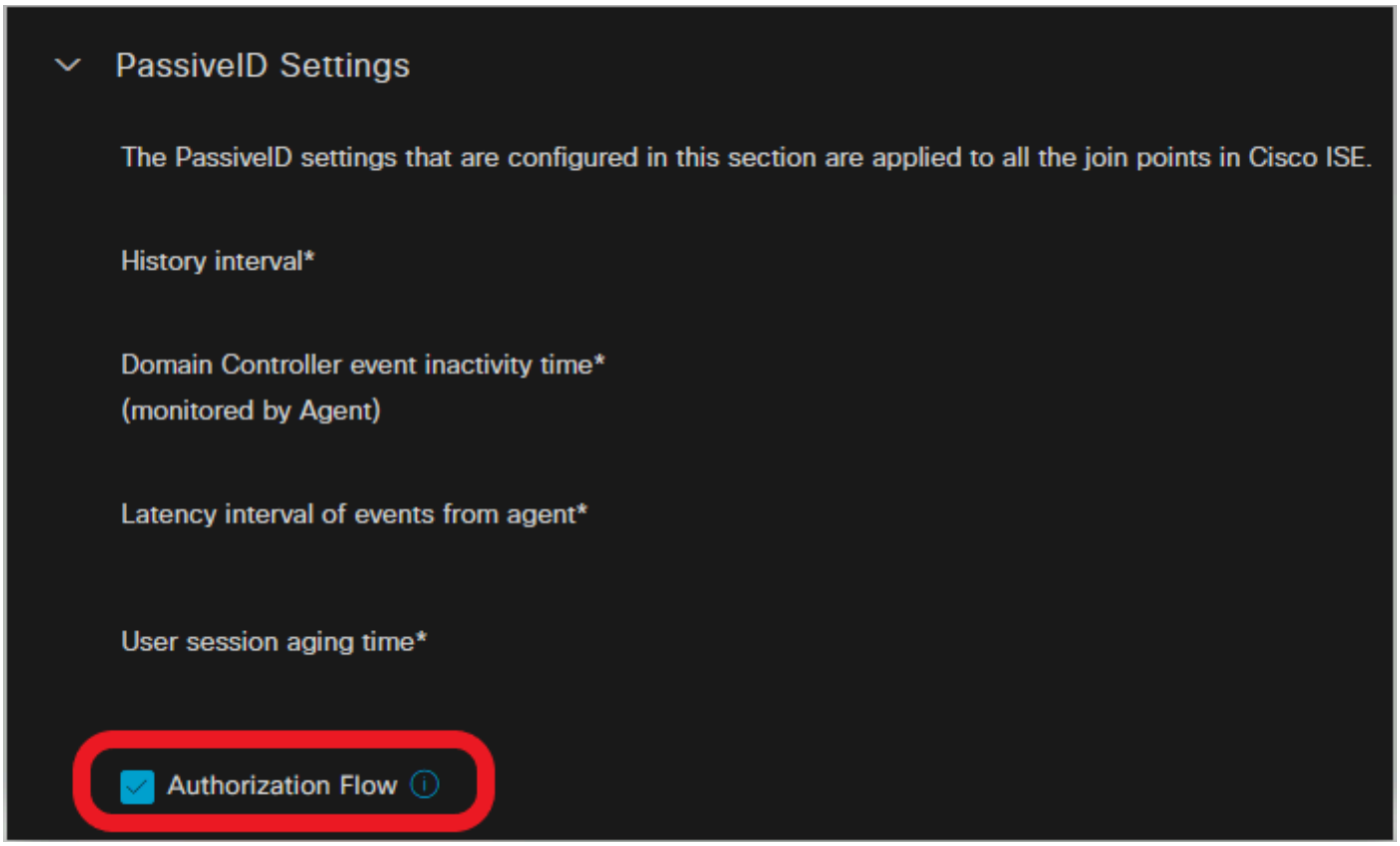


Diagramme De Flux

Configurations

Activez le flux d'autorisation :

Naviguez jusqu'à **Active Directory** > **Advanced Settings > PassiveID Settings** et cochez la **Authorization Flow** case afin de configurer les stratégies d'autorisation pour les utilisateurs de connexion PassiveID. Cette option est désactivée par défaut.

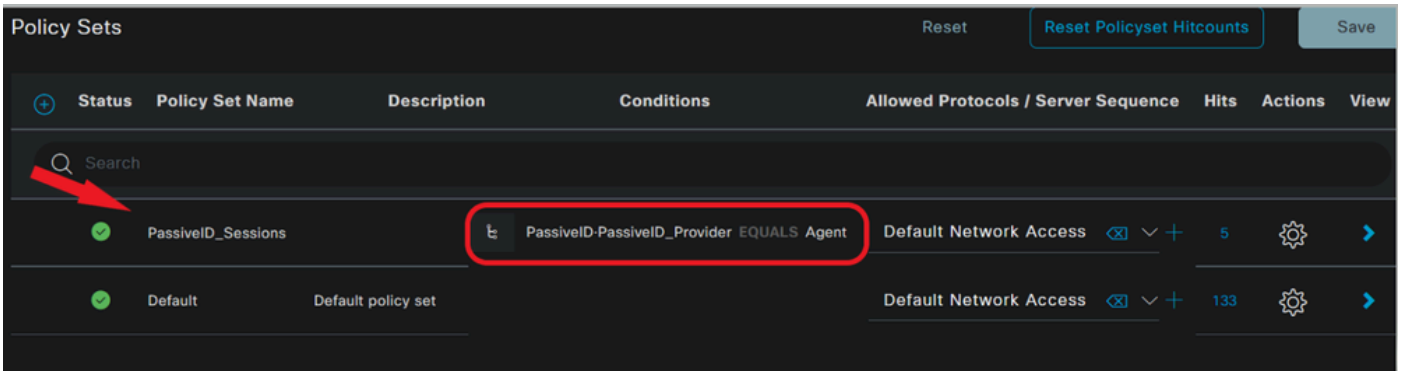


Activer le flux d'autorisation

Remarque : Pour que cette fonctionnalité fonctionne, assurez-vous d'exécuter les services PassiveID, PxGrid et SXP dans votre déploiement. Vous pouvez le vérifier sous **Administration** > **System** > **Deployment**.

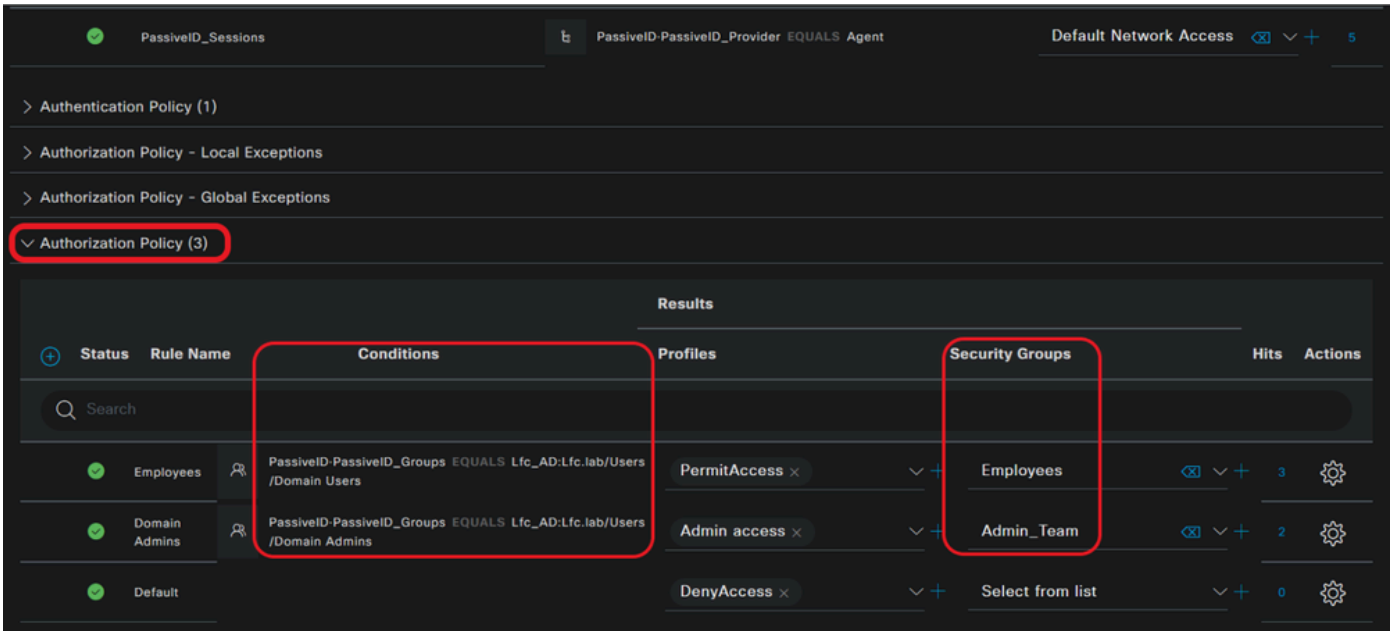
Configuration du jeu de stratégies :

1. Créez un ensemble de stratégies distinct pour PassiveID (recommandé).
2. Pour Conditions, utilisez l'attribut **PassiveID·PassiveID_Provider** et sélectionnez votre type de fournisseur.



3. Configurez les règles d'autorisation pour l'ensemble de stratégies créé à l'étape 1.

- Créez une condition pour chaque règle et utilisez le dictionnaire PassiveID basé sur les groupes Active Directory, les noms d'utilisateur ou les deux.
- Attribuez une balise de groupe de sécurité pour chaque règle et enregistrez les configurations.

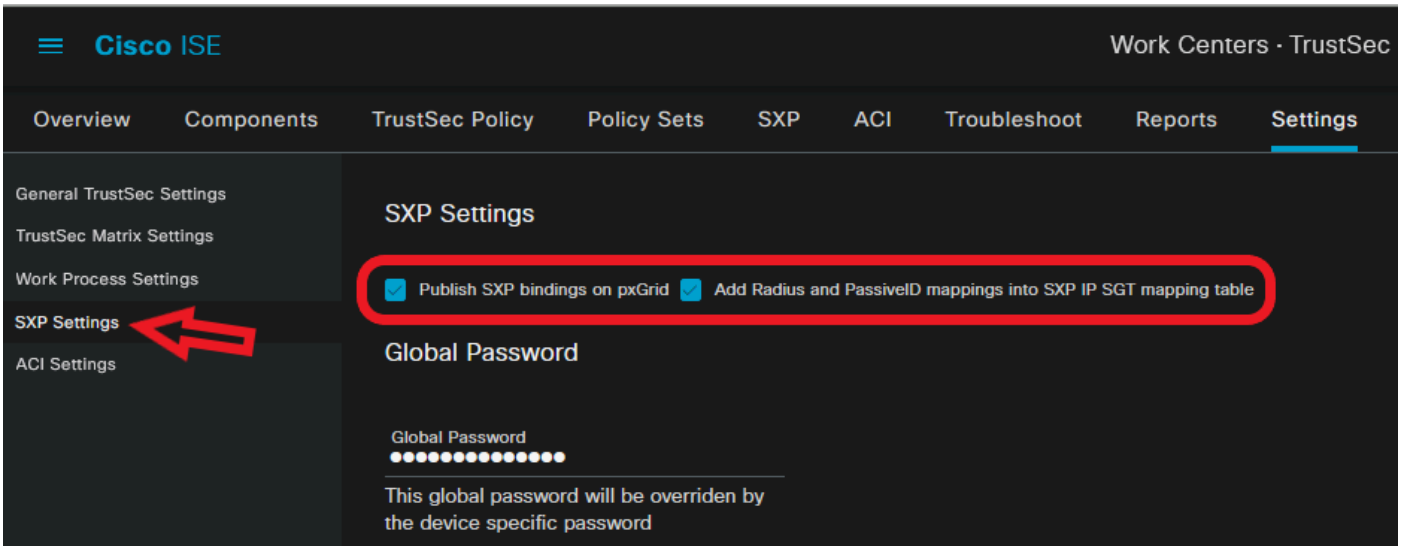


Politique d'autorisation

Remarque : La stratégie d'authentification n'est pas pertinente car elle n'est pas utilisée dans ce flux.

Remarque : Vous pouvez utiliser PassiveID_Username, PassiveID_Groups,ou des PassiveID_Provider attributs pour créer les règles d'autorisation.

4. Accédez à **Work Centers > TrustSec > Settings > SXP Settings** pour activer **Publish SXP bindings on pxGrid** et partager les mappings PassiveID avec les abonnés PxGrid, **Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table** puis incluez-les dans la table des mappings SXP sur ISE.



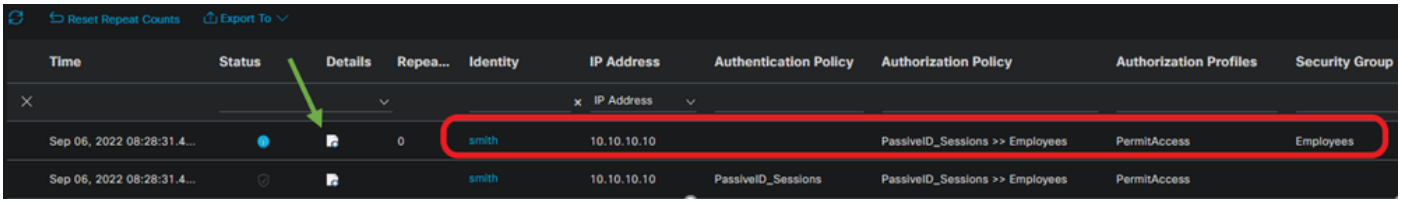
Paramètres SXP

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vérification ISE

Une fois que les événements de connexion de l'utilisateur ont été envoyés à ISE par un fournisseur tel que WMI ou Agent AD DC (Active Directory Domain Controllers), vérifiez les journaux actifs. Naviguez jusqu'à **Operations** > **Radius** > **Live Logs**.



Journaux dynamiques Radius

Cliquez sur l'icône loupe dans la colonne Détails pour afficher un rapport détaillé pour un utilisateur, dans cet exemple smith (Utilisateurs de domaine) comme illustré ici.

Cisco ISE

Overview

Event	5236 Authorize-Only succeeded
Username	smith
Endpoint Id	10.10.10.10
Endpoint Profile	
Authentication Policy	PassiveID_Sessions
Authorization Policy	PassiveID_Sessions >> Employees
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2022-09-06 20:28:31.393
Received Timestamp	2022-09-06 20:28:31.393
Policy Server	ise-3-2
Event	5236 Authorize-Only succeeded
Username	smith
Endpoint Id	10.10.10.10
Calling Station Id	10.10.10.10
IPv4 Address	10.10.10.10
Authorization Profile	PermitAccess

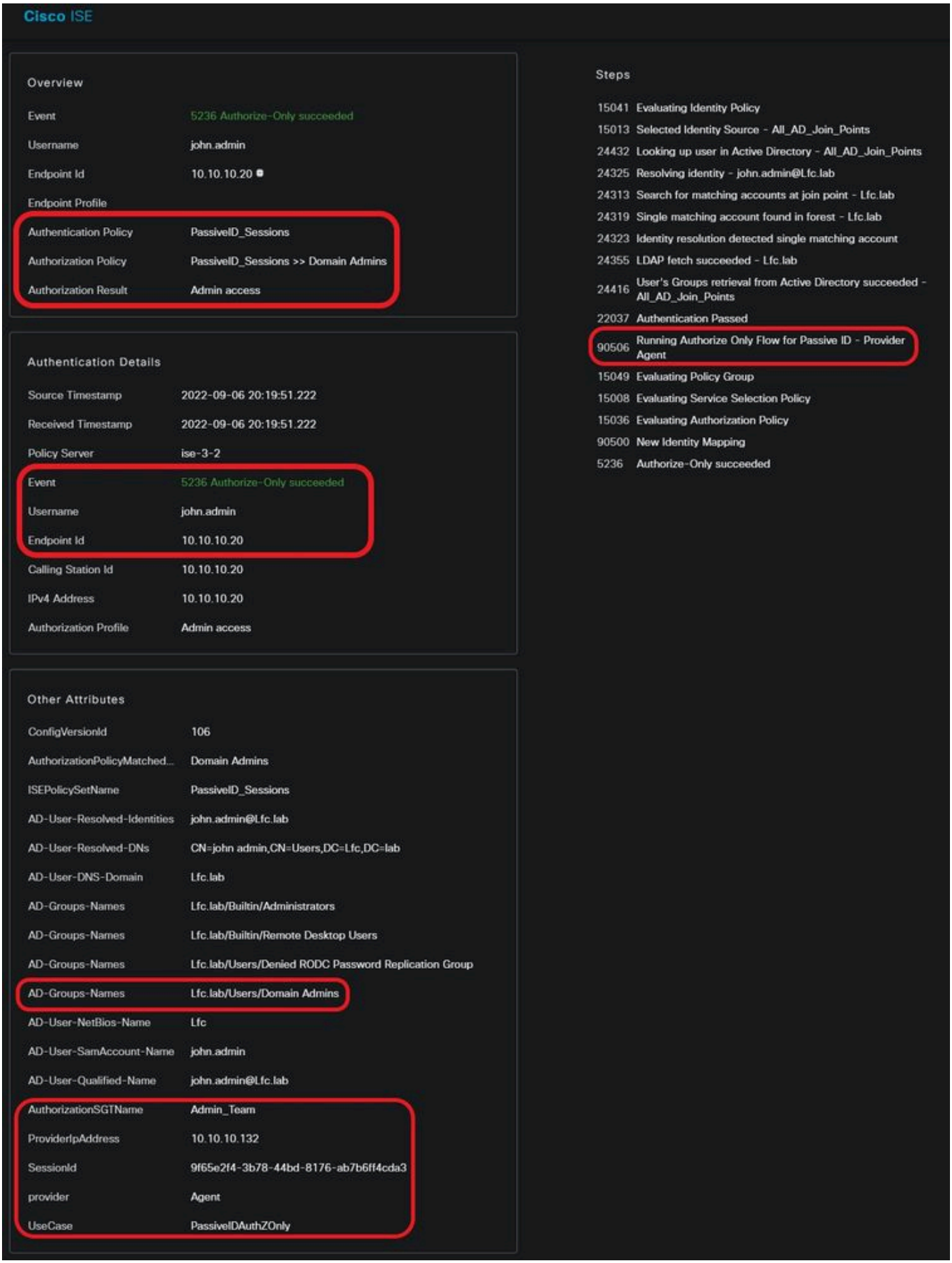
Other Attributes

ConfigVersionId	108
AuthorizationPolicyMatched...	Employees
ISEPolicySetName	PassiveID_Sessions
AD-User-Resolved-Identities	smith@Lfc.lab
AD-User-Resolved-DNs	CN=smith,CN=Users,DC=Lfc,DC=lab
AD-User-DNS-Domain	Lfc.lab
AD-Groups-Names	Lfc.lab/Builtin/Administrators
AD-Groups-Names	Lfc.lab/Builtin/Remote Desktop Users
AD-Groups-Names	Lfc.lab/Builtin/Remote Management Users
AD-Groups-Names	Lfc.lab/Builtin/Users
AD-Groups-Names	Lfc.lab/Users/Denied RODC Password Replication Group
AD-Groups-Names	Lfc.lab/Users/Domain Test
AD-Groups-Names	Lfc.lab/Users/NAD Admins
AD-Groups-Names	Lfc.lab/Users/Domain Users
AD-User-NetBios-Name	Lfc
AD-User-SamAccount-Name	smith
AD-User-Qualified-Name	smith@Lfc.lab
AuthorizationSGTName	Employees
ProviderIpAddress	10.10.10.132
SessionId	cf0d2acd-0d3d-413b-b2fb-6860df3f0d84
provider	Agent
UseCase	PassiveIDAuthZOnly

Steps

15041	Evaluating Identity Policy
15013	Selected Identity Source - All_AD_Join_Points
24432	Looking up user in Active Directory - All_AD_Join_Points
24325	Resolving identity - Lfc\smith
24313	Search for matching accounts at join point - Lfc.lab
24315	Single matching account found in domain - Lfc.lab
24323	Identity resolution detected single matching account
24355	LDAP fetch succeeded - Lfc.lab
24416	User's Groups retrieval from Active Directory succeeded - All_AD_Join_Points
22037	Authentication Passed
90506	Running Authorize Only Flow for Passive ID - Provider Agent
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15036	Evaluating Authorization Policy
90500	New Identity Mapping
5236	Authorize-Only succeeded

Rapport détaillé pour un autre utilisateur (administrateurs de domaine). Comme indiqué ici, un SGT différent est attribué selon la stratégie d'autorisation configurée.



Vérifiez la table de mappage SGT/IP dans ISE. Naviguez jusqu'à **Work Centers > TrustSec > All SXP**

Mappings.

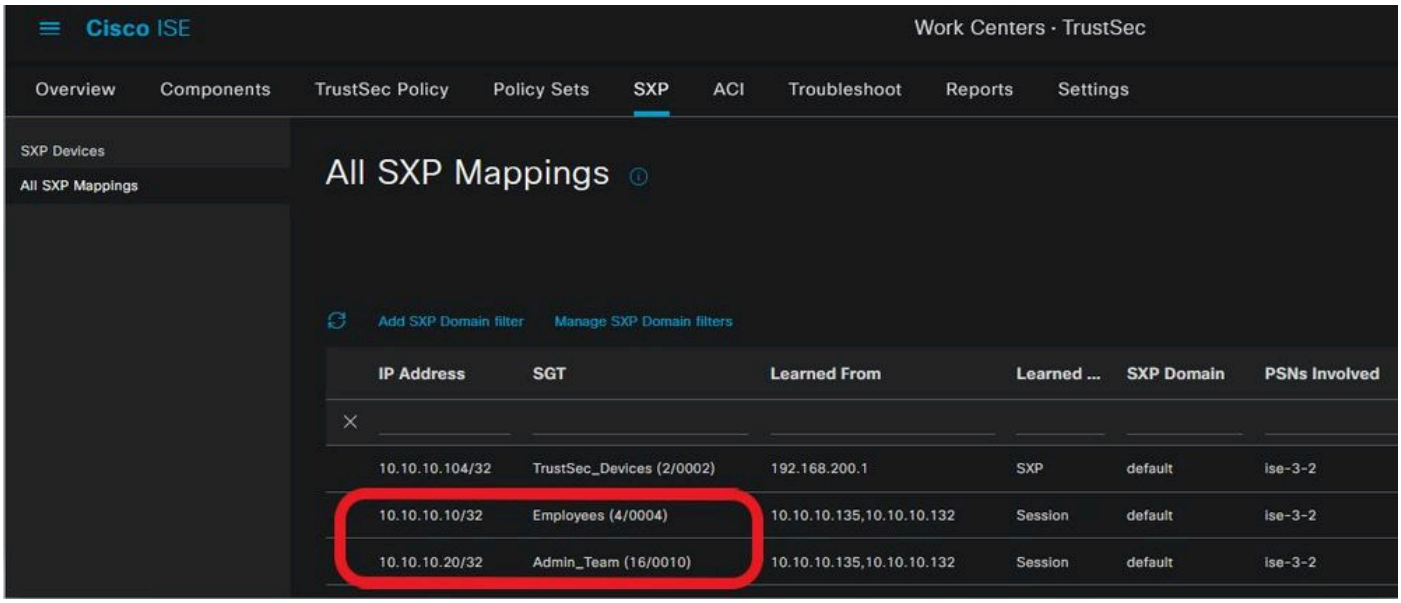
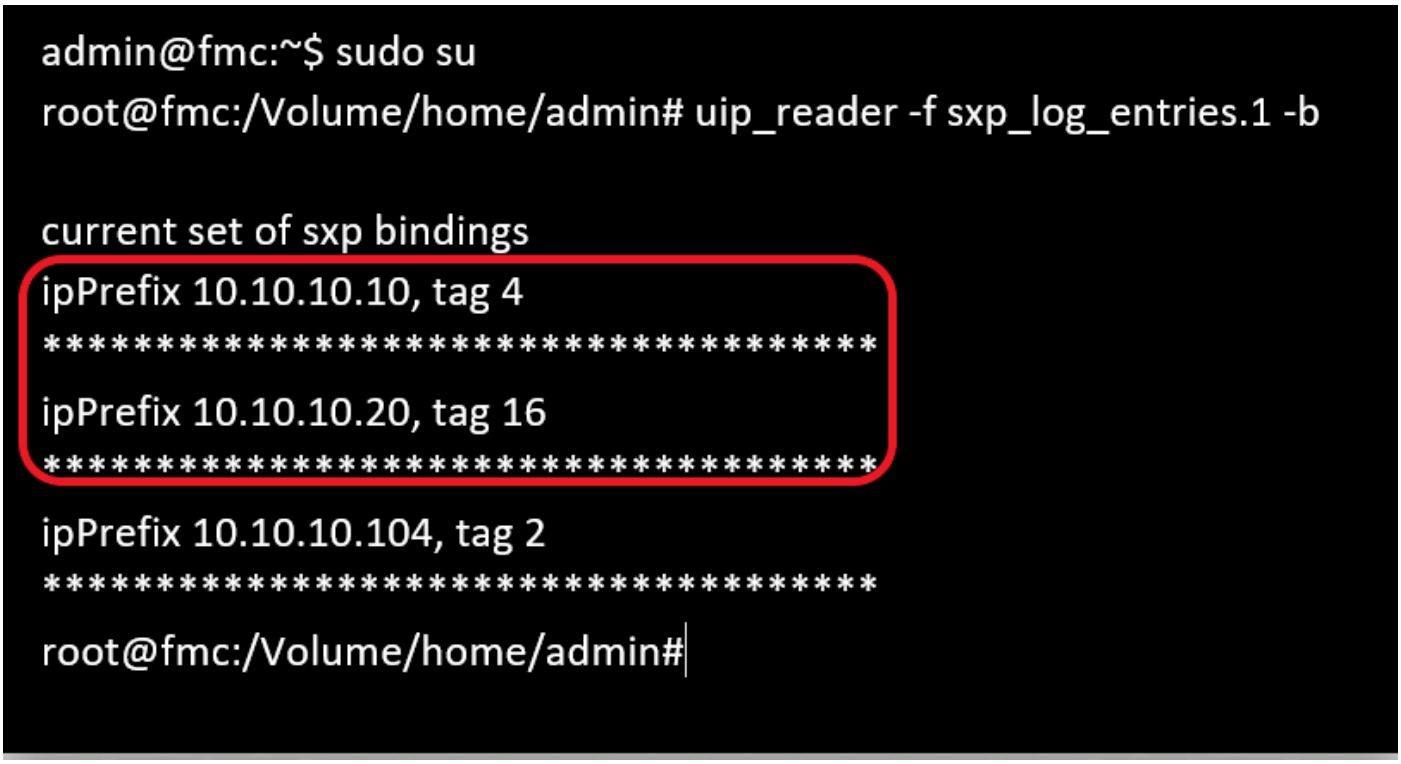


Table de mappages SXP

Remarque : Les événements PassiveID d'un fournisseur d'API ne peuvent pas être publiés sur des homologues SXP. Cependant, les détails SGT de ces utilisateurs peuvent être publiés via pxGrid.

Vérification des abonnés PxGrid

Cet extrait de CLI vérifie que le FMC a appris les mappages IP-SGT pour les sessions PassiveID mentionnées précédemment à partir d'ISE.



Vérification CLI FMC

Vérification des homologues TrustSec SXP

Le commutateur a appris les mappages IP-SGT pour les sessions PassiveID à partir d'ISE, comme le montre cet extrait de l'interface de ligne de commande.

```
sw-3850#sho cts sxp connections brief
 SXP: Enabled
Default Source IP: 10.10.10.104
------------------------------------------------------------------------------------------
   Peer_IP            Source_IP            Conn Status                 Duration
------------------------------------------------------------------------------------------
10.10.10.135       10.10.10.104    On(Speaker)::On(Listener)     0:01:29:19

sw-3850#sho cts role-based sgt-map all ipv4 details

Active IPv4-SGT Bindings Information
IP Address       Security Group                Source
10.10.10.104     2:TrustSec  Devices           INTERNAL
10.10.10.10      4:Employees                   SXP
10.10.10.20      16:Admin_Team                 SXP

IP-SGT Active Bindings Summary
============================================
Total number of SXP      bindings = 2
Total number of INTERNAL bindings = 1
Total number of active   bindings = 3
```

Vérification CLI du commutateur

Remarque : La configuration du commutateur pour AAA et TrustSec sort du cadre de ce document. Consultez le Guide Cisco TrustSec pour connaître les configurations associées.

Dépannage

Cette section fournit des informations que vous pouvez utiliser afin de dépanner ce flux.

Activer les débogages sur ISE

Accédez à **Administration** > **System** > **Logging** > **Debug Log Configuration** pour définir les composants suivants sur

le niveau spécifié.

Noeud	Nom du composant	Niveau de consignation	Nom du fichier journal
ID passif	passif	Suivre	passiveid-*.log
PxGrid	grille pxgrid	Suivre	pxgrid-server.log
SXP	sxp	Déboguer	sxp.log

Remarque : après le dépannage, réinitialisez les paramètres de débogage en sélectionnant le noeud approprié et en cliquant sur Reset to Default.

Extraits de journaux

1. ISE reçoit des événements de connexion du fournisseur :

Fichier Passiveid-*.log :

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- **Received login event.** Identity Mapping.probe = Agent , dc-host = /10.10.10.132 , Identity Mapping.server = ise-3-2 , event-operation-type = ADD ,

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- **Validating incoming loging event...**

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Building login event to be published to session directory.
2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- **retrieving user's additional information from Active Directory.**

2022-09-06 20:28:31,326 DEBUG [Grizzly-worker(26)][[]] com.cisco.idc.agent-probe- **Forwarded login event to session directory**. Identity Mapping.id-src-first-port = -1 , Identity Mapping.dc-domainname = Lfc.lab , Identity Mapping.id-src-port-start = -1 , Identity Mapping.probe = Agent , Identity Mapping.id-src-port-end = -1 , **Identity Mapping.event-user-name = smith** , Identity Mapping.dc-host = /10.10.10.132 , Identity Mapping.agentId = , Identity Mapping.server = ise-3-2 , **Identity Mapping.event-ip-address = 10.10.10.10 ,**

Fichier Passiveid-*.log

2. ISE attribue les balises SGT conformément à la stratégie d'autorisation configurée et publie le mappage IP-SGT pour les utilisateurs PassiveID vers les abonnés PxGrid et les homologues SXP :

fichier sxp.log :

```
2022-09-06 20:28:31,587 DEBUG [sxpservice-http-96443] cisco.ise.sxp.rest.SxpGlueRestAPI:27 - Adding session binding tag=4, ip=10.10.10.10, vns=[], vpns=[null] nasIp=10.10.10.132
2022-09-06 20:28:31,587 DEBUG [sxpservice-http-96443] cisco.ise.sxp.rest.SxpGlueRestAPI:23 - session binding created for ip address : 10.10.10.10/32

2022-09-06 20:28:31,613 DEBUG [SxpNotification] cisco.cpm.sxp.engine.SxpEngine:23 - Adding 1 session bindings

2022-09-06 20:28:31,613 DEBUG [SxpNotificationSerializer-Thread] cisco.cpm.sxp.engine.SxpEngine:42 - Adding session binding RestSxpLocalBinding(tag=4, groupName=null, ipAddress=10.10.10.10/32, nasIp=10.10.10.132, sessionId=cf0d2acd-0d3d-413b-b2fb-6860df3f0d84, peerSequence=null, sxpBindingOpType=ADD, sessionExpiryTimeInMillis=-1, apic=false, routable=true, vns=[DEFAULT_VN]) to VPNs [default]
```

fichier sxp.log

fichier pxgrid-server.log :

```
2022-09-06 20:28:31,693 TRACE  [Grizzly(1)][[]] cpm.pxgrid.ws.client.WsEndpoint -::::- Send. session=[id=b0df936b-bfab-435f-80e6-aa836aa3b24c,client=~ise-fanout-ise-3-2,server=wss://ise-3-2.Lfc.lab:8910/pxgrid/ise/pubsub] frame=[command=SEND,headers=[content-length=1859, destination=/topic/distributed, from=~ise-fanout-ise-3-2, via=~ise-fanout-ise-3-2],content-len=1859] content=MESSAGE
content-length:1730
destination:/topic/com.cisco.ise.session
message-id:616
subscription:2
via:~ise-fanout-ise-3-2
{"sessions":[{"timestamp":"2022:09:06T20:28:31.41105:00","state":"AUTHENTICATED","userName":"smith","callingStationId":"10.10.10.10","auditSessionId":"ddda40ec-e557-4457-81db-a36af7b7d4ec",
"ipAddresses":["10.10.10.10"],"nasIpAddress":"10.10.10.132","ctsSecurityGroup":"Employees","adNormalizedUser":"smith",
"adUserDomainName":"Lfc.lab","adUserNetBiosName":"Lfc","adUserResolvedIdentities":"smith@Lfc.lab","selectedAuthzProfiles":["PermitAccess"]}],"sequence":13}

2022-09-06 20:28:31,673 TRACE  [Grizzly(1)][[]] cpm.pxgrid.ws.client.WsEndpoint -::::- Send. session=[id=b0df936b-bfab-435f-80e6-aa836aa3b24c,client=~ise-fanout-ise-3-2,server=wss://ise-3-2.Lfc.lab:8910/pxgrid/ise/pubsub] frame=[command=SEND,headers=[content-length=308, destination=/topic/distributed, from=~ise-fanout-ise-3-2, via=~ise-fanout-ise-3-2],content-len=308] content=MESSAGE
content-length:176
destination:/topic/com.cisco.ise.sxp.binding
message-id:612
subscription:2
via:~ise-fanout-ise-3-2
{"operation":"CREATE","binding":{"ipPrefix":"10.10.10.10/32","tag":4,"source":"10.10.10.132",
"peerSequence":"10.10.10.135,10.10.10.132","vpn":"default"},"sequence":17}
```

fichier pxgrid-server.log

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.