

# Configuratie van ISE 3.2 voor het toewijzen van Security Group Tags voor passieve ID-sessies

## Inhoud

- [Inleiding](#)
- [Voorwaarden](#)
- [Vereisten](#)
- [Gebruikte componenten](#)
- [Achtergrondinformatie](#)
- [Configureren](#)
- [Stroomdiagram](#)
- [Configuraties](#)
- [Verifiëren](#)
- [ISE-verificatie](#)
- [Verificatie van PXGrid-abonnee](#)
- [Verificatie van TrustSec SXP-peer](#)
- [Problemen oplossen](#)
- [Debugs inschakelen op ISE](#)
- [Logs-fragmenten](#)

## Inleiding

Dit document beschrijft hoe u Security Group Tags (SGT™s) kunt configureren en toewijzen aan passieve ID-sessies via autorisatiebeleid in ISE 3.2.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ISE-lijnkaart 3.2
- Passieve ID, TrustSec en PxGrid

### Gebruikte componenten

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

- Cisco ISE-lijnkaart 3.2
- VCC 7.0.1
- WS-C3850-24P switch met 16.12.1

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.

## Achtergrondinformatie

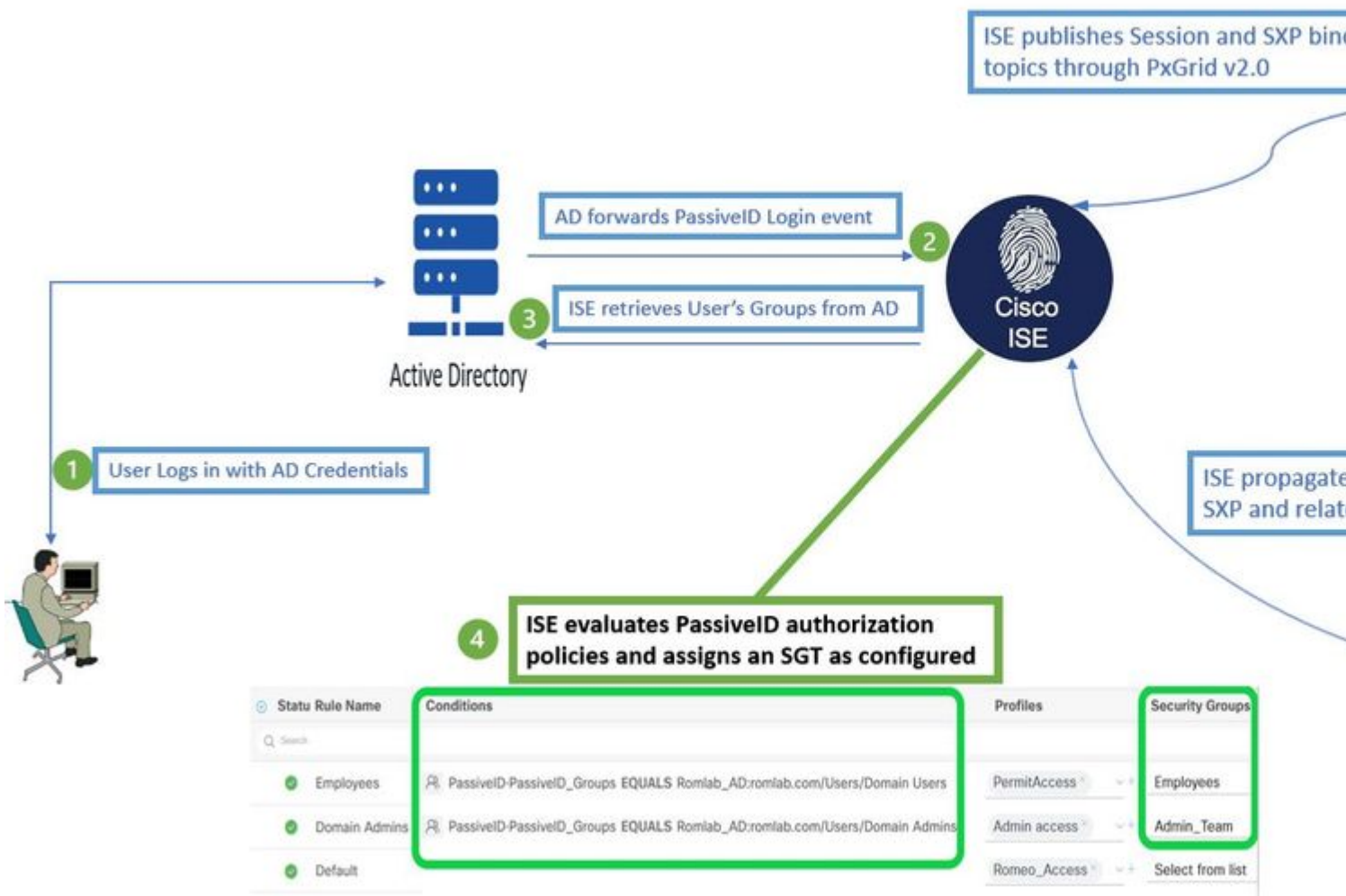
Cisco Identity Services Engine (ISE) 3.2 is de minimumversie die deze mogelijkheid ondersteunt. Dit document is niet van toepassing op de configuratie van PassiveID, PxGrid en SXP. Zie de [Admin Guide voor](#) meer informatie.

In ISE 3.1 of oudere versies kan alleen een Security Group Tag (SGT) worden toegewezen aan een RADIUS-sessie of actieve verificatie zoals 802.1x en MAB. Met ISE 3.2 kunnen we het autorisatiebeleid voor PassiveID-sessies zodanig configureren dat wanneer Identity Services Engine (ISE) inloggebeurtenissen van gebruikers ontvangt van een provider zoals Active Directory Domain Controllers (AD DC) WMI of AD Agent, het een Security Group Tag (SGT) toewijst aan de PassiveID-sessie op basis van het lidmaatschap van de gebruikers Active Directory (AD)-groep. De IP-SGT-mapping en AD-groepsdetails voor de PassiveID kunnen worden gepubliceerd op het TrustSec-domein via SGT Exchange Protocol (SXP) en/of op de Platform Exchange Grid-abonnees (pxGrid) zoals Cisco Firepower Management Center (FMC) en Cisco Secure Network Analytics (Stealthwatch).

## **Configureren**

### **Stroomdiagram**

# PassiveID Authorization Flow Diagram



Stroomdiagram

## Configuraties

Schakel de autorisatiestroom in:

Naar navigeren **Active Directory** > **Advanced Settings** > **PassiveID Settings** en controleer de **Authorization Flow** selectievakje om het autorisatiebeleid te configureren voor gebruikers van PassiveID-aanmelding. Deze optie is standaard uitgeschakeld.

### PassiveID Settings

The PassiveID settings that are configured in this section are applied to all the join points in Cisco ISE.

History interval\*

Domain Controller event inactivity time\*  
(monitored by Agent)

Latency interval of events from agent\*

---

: om deze functie te laten werken, moet u ervoor zorgen dat u PassiveID-, PxGrid- en SXP-services uitvoert in uw implementatie. U kunt dit controleren onder **Administration > System > Deployment** .

---

Configuratie beleidsset:

1. Maak een aparte beleidsset voor passieve id (aanbevolen).
2. Voor Voorwaarden, gebruik de eigenschap **PassiveID·PassiveID\_Provider** en selecteer het type provider.

Policy Sets Reset

Status	Policy Set Name	Description	Conditions	Allowed Protocols / S
✓	PassiveID_Sessions		PassiveID-PassiveID_Provider EQUALS Agent	Default Network Ac
✓	Default	Default policy set		Default Network Ac

*Beleidssets*

3. Configureer de autorisatieregels voor de beleidsset die in stap 1 is gemaakt.

- Maak een voorwaarde voor elke regel en gebruik het PassiveID woordenboek op basis van AD-groepen, gebruikersnamen of Beide.
- Wijs een Security Group Tag toe aan elke regel en sla de configuraties op.

PassiveID\_Sessions PassiveID-PassiveID\_Provider EQUALS Agent

> Authentication Policy (1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

▼ Authorization Policy (3)

Status	Rule Name	Conditions	Profiles	Security Gro
✓	Employees	PassiveID-PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Users	PermitAccess x	Employ
✓	Domain Admins	PassiveID-PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Admins	Admin access x	Admin_
✓	Default		DenyAccess x	Select t

*Vergunningsbeleid*

**Opmerking:** het authenticatiebeleid is irrelevant omdat het niet wordt gebruikt in deze stroom.

**Opmerking:** u kunt `PassiveID_Username`, `PassiveID_Groups`, of `PassiveID_Provider` eigenschappen om de autorisatieregels te creëren.

4. Navigeer naar **Work Centers > TrustSec > Settings > SXP Settings** toelaten **Publish SXP bindings on pxGrid** en

om PassiveID-toewijzingen te delen met PxGrid-abonnees en deze op te nemen in de SXP-toewijzingstabel op ISE.

**Cisco ISE**

Overview Components TrustSec Policy Policy Sets SXP ACI Troubleshoot

General TrustSec Settings  
TrustSec Matrix Settings  
Work Process Settings  
**SXP Settings**  
ACI Settings

**SXP Settings**

Publish SXP bindings on pxGrid  Add Radius and PassiveID mappings into SXP IP S...

**Global Password**

Global Password  
●●●●●●●●●●

This global password will be overridden by the device specific password

SXP-instellingen

## Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

### ISE-verificatie

Zodra de gebruikersaanmeldingsgebeurtenissen naar ISE zijn verzonden vanuit een provider zoals Active Directory Domain Controllers (AD DC) WMI of AD Agent, gaat u verder met het controleren van de Live Logs. Naar navigeren **Operations > Radius > Live Logs**.

Time	Status	Details	Repea...	Identity	IP Address	Authentication Policy	Authorization Policy
Sep 06, 2022 08:28:31.4...	●		0	smith	10.10.10.10	PassiveID_Sessions >> Emplo...	PassiveID_Sessions >> Emplo...
Sep 06, 2022 08:28:31.4...	⊙			smith	10.10.10.10	PassiveID_Sessions	PassiveID_Sessions >> Emplo...

Radius LiveLogs

Klik op het pictogram vergrootglas in de kolom Details om een gedetailleerd rapport voor een gebruiker, in dit voorbeeld smith (Domeingebruikers) te bekijken zoals hier getoond.

**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

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 -

---

: gebeurtenissen met passieve ID van een API-provider kunnen niet worden gepubliceerd naar SXP-peers. De SGT-gegevens van deze gebruikers kunnen echter via pxGrid worden gepubliceerd.

---

## **Verificatie van PXGrid-abonnee**

In dit CLI-fragment wordt gecontroleerd of het VCC de IP-SGT-toewijzingen voor de eerder genoemde PassiveID-sessies van ISE heeft geleerd.



```

admin@fmc:~$ sudo su
root@fmc:/Volume/home/admin# uip_reader -f sxp_log_entries.1

current set of sxp bindings
ipPrefix 10.10.10.10, tag 4
*****
ipPrefix 10.10.10.20, tag 16
*****
ipPrefix 10.10.10.104, tag 2
*****
root@fmc:/Volume/home/admin#

```

VCC CLI-verificatie

### Verificatie van TrustSec SXP-peer

De switch heeft de IP-SGT-toewijzingen voor PassiveID-sessies van ISE geleerd, zoals in dit CLI-fragment wordt weergegeven.

#### sw-3850#sho cts sxp connections brief

```

SXP: Enabled
Default Source IP: 10.10.10.104

```

Peer_IP	Source_IP	Conn Status	Du
10.10.10.135	10.10.10.104	On(Speaker)::On(Listener)	0:

#### 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

Passieve id	gepassioneerde	Overtrekken	gepassiveerd-*.log
PxGrid	pxgrid	Overtrekken	pxgrid-server.log
SXP	sxp	Debuggen	sxp.log

---

**Opmerking:** wanneer u klaar bent met probleemoplossing, onthoud dan om de debugs opnieuw in te stellen en selecteer de verwante node en klik op **Reset to Default**.

---

## Logs-fragmenten

1. ISE ontvangt inloggebeurtenissen van de provider:

Passiveid-\*.log bestand:

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

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

```
2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Build  
published to session directory.
```

```
2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- retrie  
information from Active Directory.
```

```
2022-09-06 20:28:31,326 DEBUG [Grizzly-worker(26)][[]] com.cisco.idc.agent-probe- Forw  
session directory. Identity Mapping.id-src-first-port = -1 , Identity Mapping.dc-domainnam  
Mapping.id-src-port-start = -1 , Identity Mapping.probe = Agent , Identity Mapping.id-src-p  
Mapping.event-user-name = smith , Identity Mapping.dc-host = /10.10.10.132 , Identity M  
Identity Mapping.server = ise-3-2 , Identity Mapping.event-ip-address = 10.10.10.10 ,
```

*Passiveid-\*.log-bestand*

2. ISE wijst SGT toe volgens het geconfigureerde autorisatiebeleid en publiceert IP-SGT-mapping voor PassiveID-gebruikers aan PxGrid-abonnees en SXP-peers:

sxp.log-bestand:

```
2022-09-06 20:28:31,587 DEBUG [sxp-service-http-96443] cisco.ise.sxp.rest.SxpGlueRe  
binding tag=4, ip=10.10.10.10, vns=[], vpns=[null] nasIp=10.10.10.132
```

```
2022-09-06 20:28:31,587 DEBUG [sxp-service-http-96443] cisco.ise.sxp.rest.SxpGlueRe  
created for ip address : 10.10.10.10/32
```

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

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

*sxp.log-bestand*

pxgrid-server.log bestand:

```
2022-09-06 20:28:31.693 TRACE [Grizzly(1)][[]] cpm.pxgrid.ws.client.WsEndpoint -:::- Send. se
```

## 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.