

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

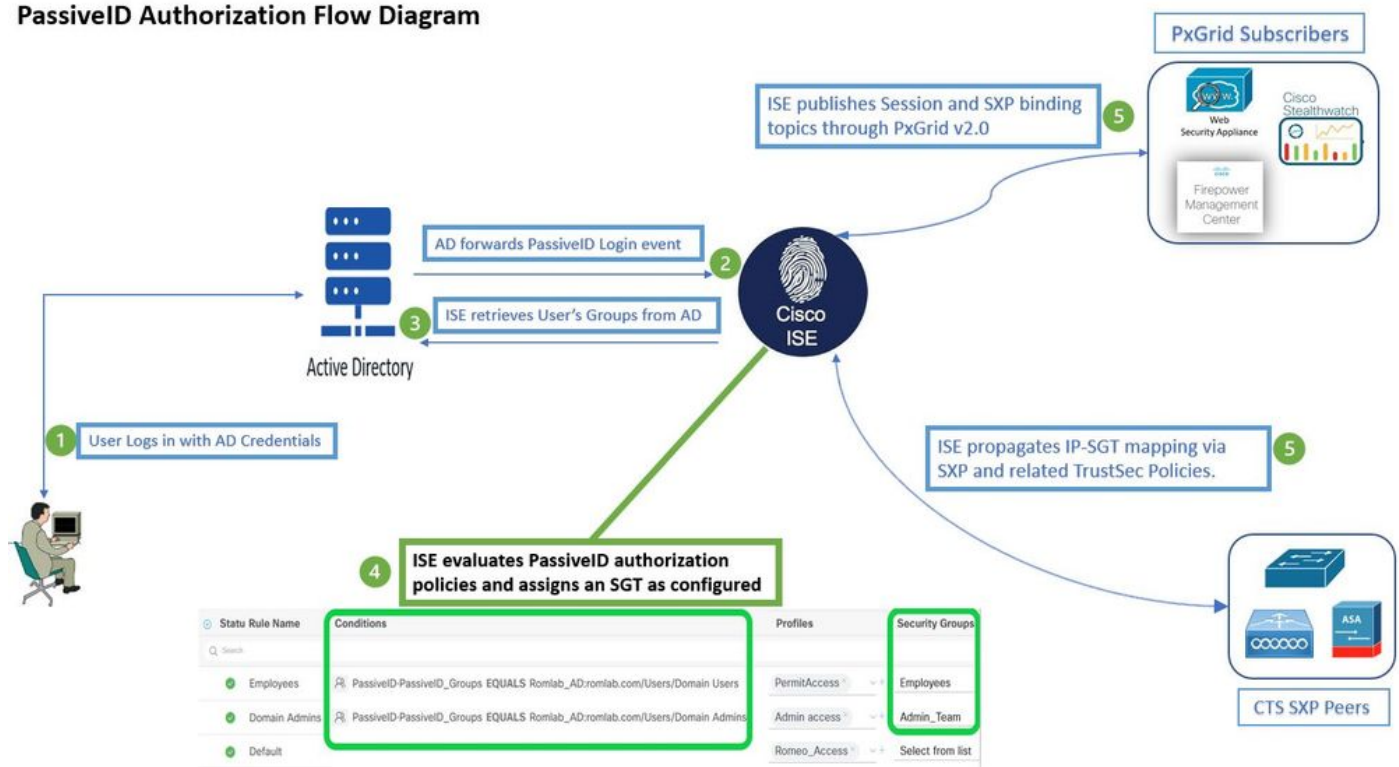
Cisco Identity Services Engine (ISE) 3.2 is de minimumversie die deze mogelijkheid ondersteunt. Dit document is niet van toepassing op de configuratie van PassiveID, PxGrid en SXP. Zie de [Admin Guide voor](#) meer informatie.

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

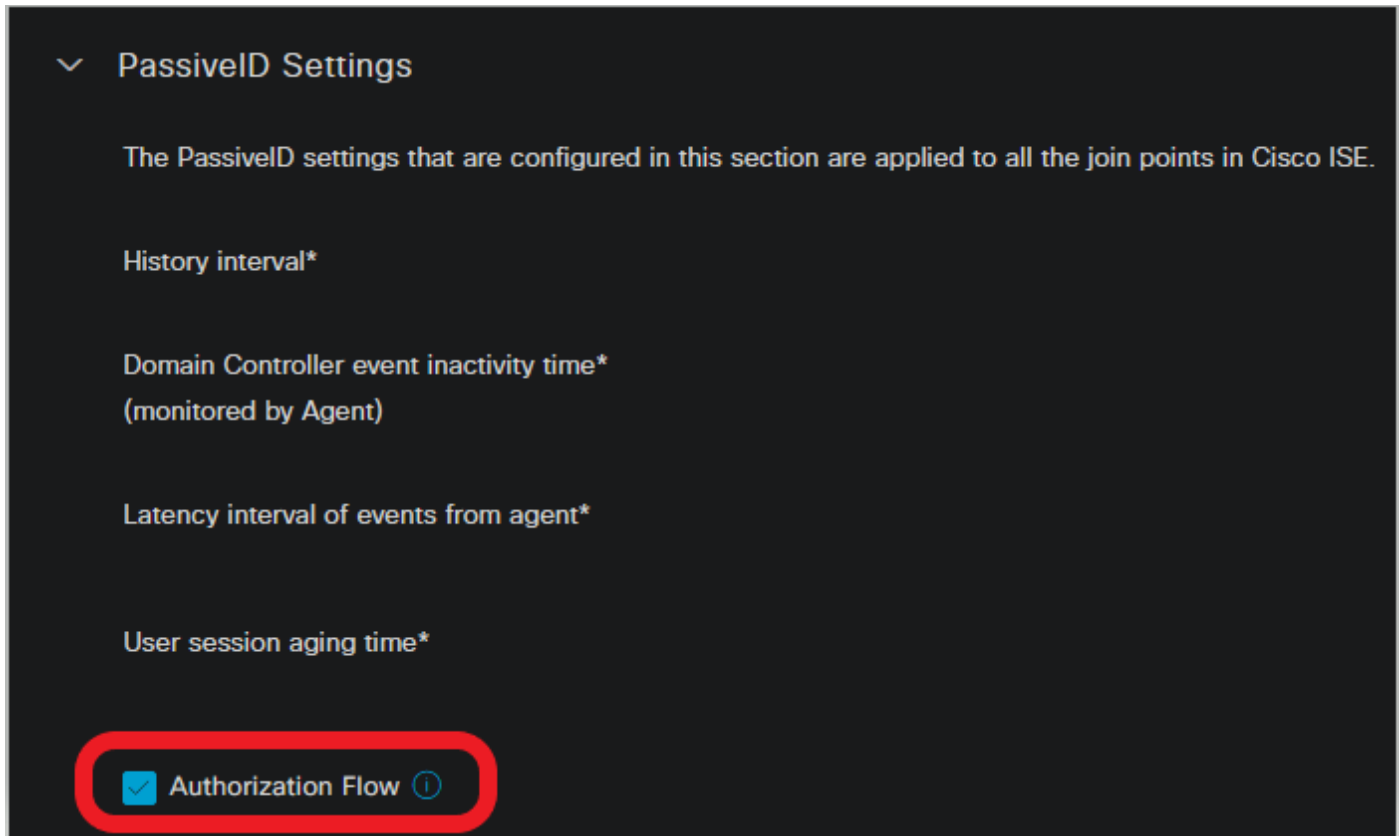


Configuraties

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.

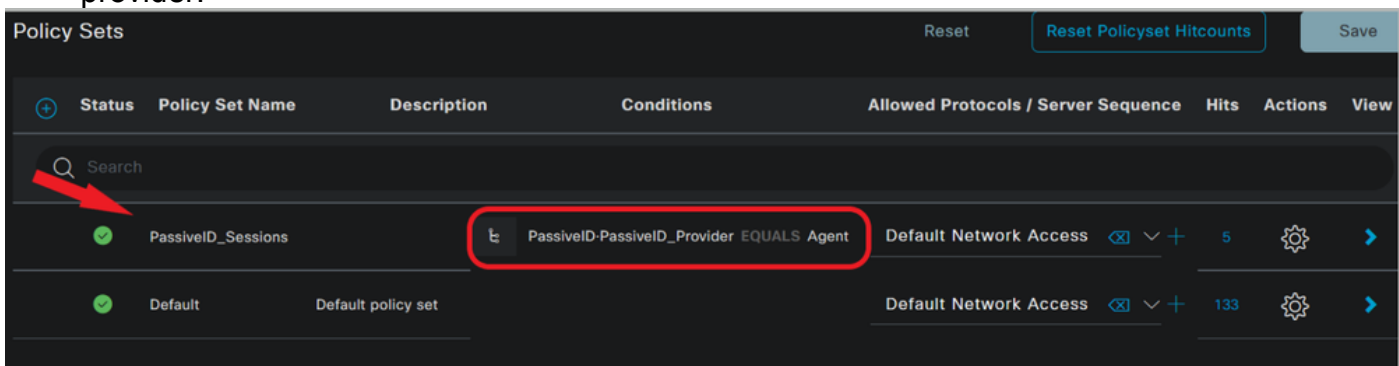


De autorisatiestroom inschakelen

Opmerking: 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.



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.

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Employees	PassiveID:PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Users	PermitAccess x	Employees	3	ⓘ ⌵ + ⚙
✓	Domain Admins	PassiveID:PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Admins	Admin access x	Admin_Team	2	ⓘ ⌵ + ⚙
✓	Default		DenyAccess x	Select from list	0	ⓘ ⌵ + ⚙

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 Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table om PassiveID-toewijzingen te delen met PxGrid-abonnees en deze op te nemen in de SXP-toewijzingstabel op ISE.

Cisco ISE Work Centers - TrustSec

Overview Components TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports **Settings**

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 SGT mapping table

Global Password

Global Password
●●●●●●●●●●

This global password will be overridden by the device specific password

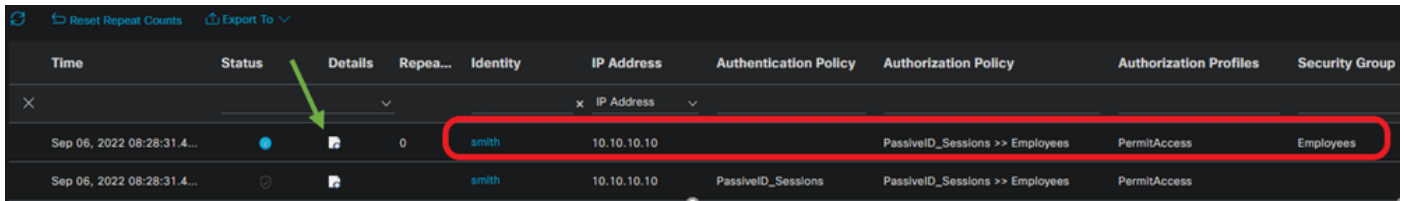
SXP-instellingen

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	Authorization Profiles	Security Group
Sep 06, 2022 08:28:31.4...			0	smith	10.10.10.10	PassiveID_Sessions >> Employees	PermitAccess	Employees	Employees
Sep 06, 2022 08:28:31.4...				smith	10.10.10.10	PassiveID_Sessions	PassiveID_Sessions >> Employees	PermitAccess	

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.

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.