

Configuratie van autorisatiestroom voor passieve ID-sessies in ISE 3.2

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u autorisatieregels kunt configureren voor passieve ID-gebeurtenissen om SGT's aan de sessies toe te wijzen.

Achtergrondinformatie

De passieve identiteitsdiensten (Passieve ID) verifiëren gebruikers niet direct, maar verzamelen gebruikersidentiteiten en IP-adressen van externe verificatieservers zoals Active Directory (AD), bekend als providers, en delen die informatie vervolgens met abonnees.

ISE 3.2 introduceert een nieuwe functie waarmee u een autorisatiebeleid kunt configureren om een Security Group Tag (SGT) toe te wijzen aan een gebruiker die is gebaseerd op het groepslidmaatschap van Active Directory.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ISE-lijnkaart 3.x
- Passieve ID-integratie met elke provider
- Active Directory (AD)-beheer
- Segmentatie (Trustsec)
- PxGrid (Platform Exchange Grid)

Gebruikte componenten

- Software voor Identity Service Engine (ISE), versie 3.2
- Microsoft Active Directory

- Syslogs

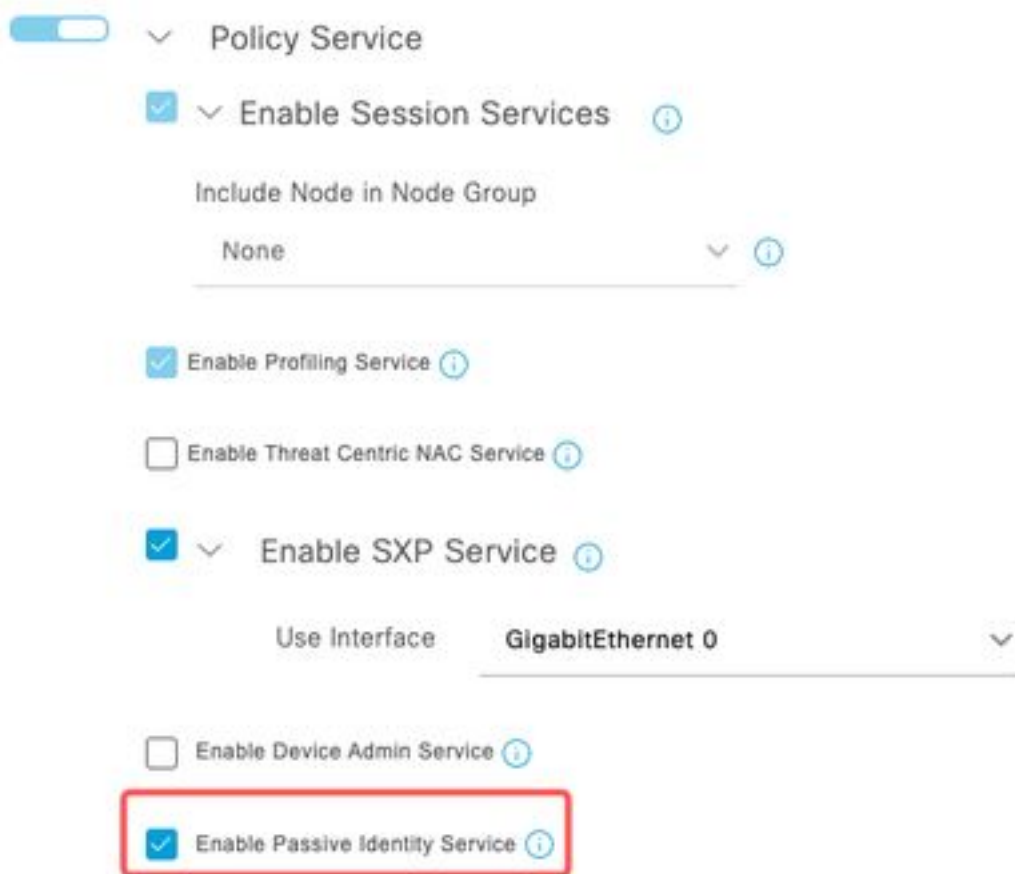
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratie

Stap 1. Schakel ISE-services in.

1. Ga op ISE naar Beheer > **Implementatie**, kies het ISE-knooppunt en klik op **Bewerken**, schakel **de beleidsservice** in en kies **Passieve identiteitservice inschakelen**. Optioneel kunt u SXP en PxGrid inschakelen als de passieve id-sessies door elke sessie moeten worden gepubliceerd. Klik op Save (Opslaan).

Waarschuwing: SGT-gegevens van de PassiveID-gebruikers die door de API-provider zijn geverifieerd, kunnen niet in SXP worden gepubliceerd. De SGT-gegevens van deze gebruikers kunnen echter worden gepubliceerd via pxGrid en pxGrid Cloud.



Ingeschakeld voor services

Stap 2. Configureer de actieve map.

1. Ga naar Beheer > **Identiteitsbeheer** > **Externe Identiteitsbronnen** en kies **Actieve map** en klik vervolgens op de knop **Toevoegen**.
2. Voer de **Join Point Name** en **Active Directory Domain** in. Klik op **Verzenden**.

Identities Groups **External Identity Sources** Identity Source Sequences

External Identity Sources

<

> Certificate Authentication F

Active Directory

Connection

* Join Point Name

* Active Directory Domain

Actieve map toevoegen

3. Er verschijnt een pop-up om ISE aan te sluiten op de AD. Klik op **Ja**. Voer de **gebruikersnaam** en het **wachtwoord in**. Klik op OK.

Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No

Doorgaan met aanmelden bij

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name

* Password

Specify Organizational Unit

Store Credentials

ISE map *Aanmelden bij actieve*

4. AD-groepen ophalen. Navigeer naar **Groepen**, klik op **Toevoegen**, klik vervolgens op **Groepen ophalen** en kies alle geïnteresseerde groepen en klik op **OK**.

Select Directory Groups

This dialog is used to select groups from the Directory.

Domain: aaamexrub.com

Name Filter: _____ SID Filter: _____ Type Filter: All

Retrieve Groups... 53 Groups Retrieved.

<input type="checkbox"/>	aaamexrub.com/Users/Cloneable Domain Contro...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Denied RODC Password ...	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
<input type="checkbox"/>	aaamexrub.com/Users/DnsAdmins	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
<input type="checkbox"/>	aaamexrub.com/Users/DnsUpdateProxy	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input checked="" type="checkbox"/>	aaamexrub.com/Users/Domain Admins	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Computers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Controllers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Guests	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input checked="" type="checkbox"/>	aaamexrub.com/Users/Domain Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Enterprise Admins	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
<input type="checkbox"/>	aaamexrub.com/Users/Enterprise Read-only De...	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
<input type="checkbox"/>	aaamexrub.com/Users/Group Policy Creator Ow...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Protected Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL

Cancel OK

AD-groepen ophalen

Connection Allowed Domains Passiveld Groups

Edit + Add Delete Group Update SID Values

<input type="checkbox"/>	Name	S
<input type="checkbox"/>	aaamexrub.com/Users/Domain Admins	S
<input type="checkbox"/>	aaamexrub.com/Users/Domain Users	S
<input type="checkbox"/>	aaamexrub.com/Users/sponsors	S

Opgevraagde groepen

5. Schakel de autorisatiestroom in. Navigeer naar **Geavanceerde instellingen** en controleer in het gedeelte **Passiveld-instellingen** het selectievakje **Autorisation Flow**. Klik op Save (Opslaan).

PassiveID Settings

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

History interval*	10
Domain Controller event inactivity time* (monitored by Agent)	0
Latency interval of events from agent*	0
User session aging time*	24

Authorization Flow ⓘ

inschakelen

Autorisatiedoorloop

Stap 3. Configureer de Syslog-provider.

1. Navigeer naar de werkcentra > **PassiveID** > **Providers**, kies **Syslog Providers**, klik op **Toevoegen** en vul de informatie in. Klik op Opslaan

Waarschuwing: in dit geval ontvangt ISE het syslogbericht van een succesvolle VPN-verbinding in een ASA, maar deze configuratie wordt in dit document niet beschreven.

Syslog Providers

Name*
ASA

Description


Status*
Enabled

Host FQDN*
asa-rudelave.aaamexrub.com

Connection Type*
UDP - Port 40514

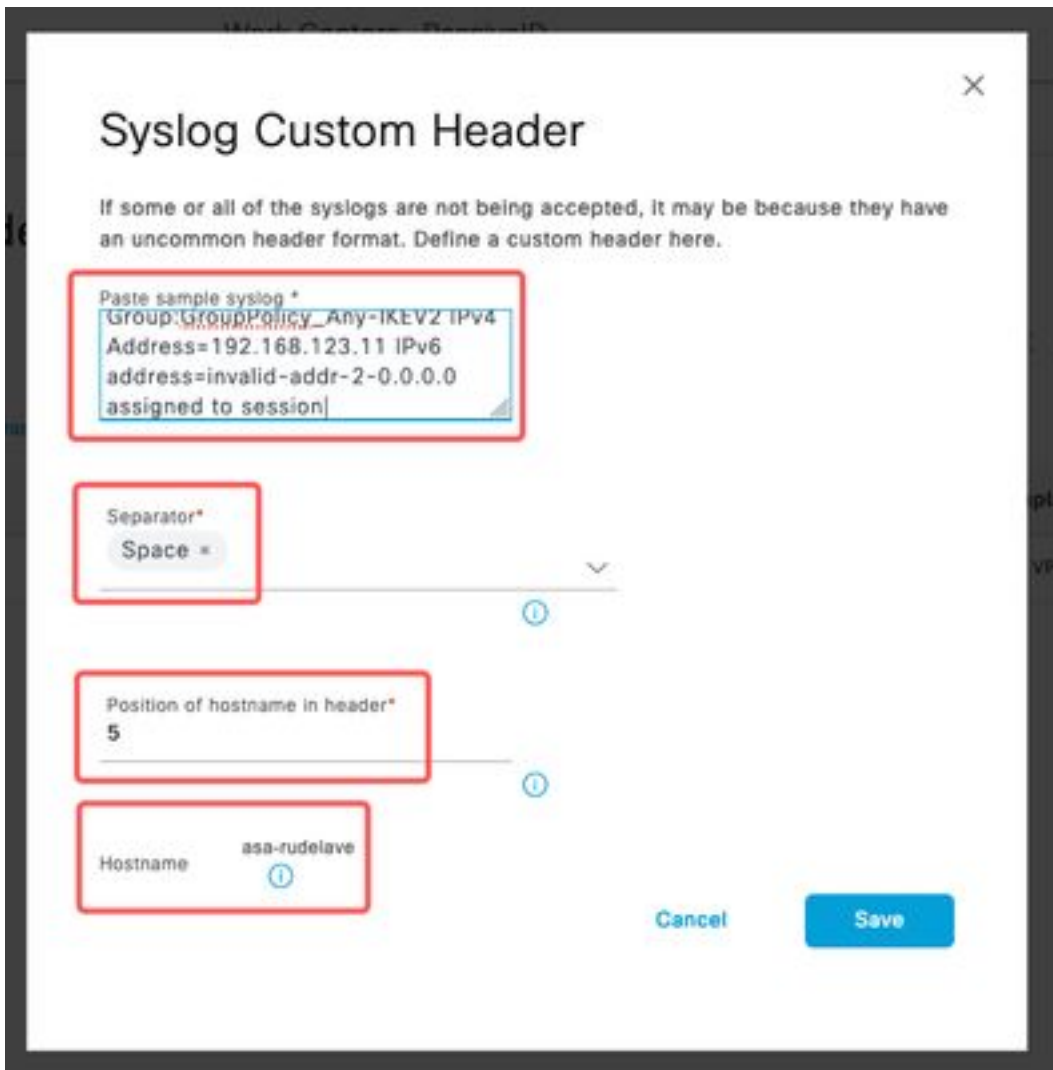
Template* ASA VPN [View](#) [New](#)

Default Domain
aaamexrub.com



Syslog-provider configureren

2. Klik op **Aangepaste header**. Plakt het voorbeeldsysteem en gebruik een Separator of Tab om het apparaat hostname te vinden. Als het juist is, wordt Hostname weergegeven. Klik op Opslaan

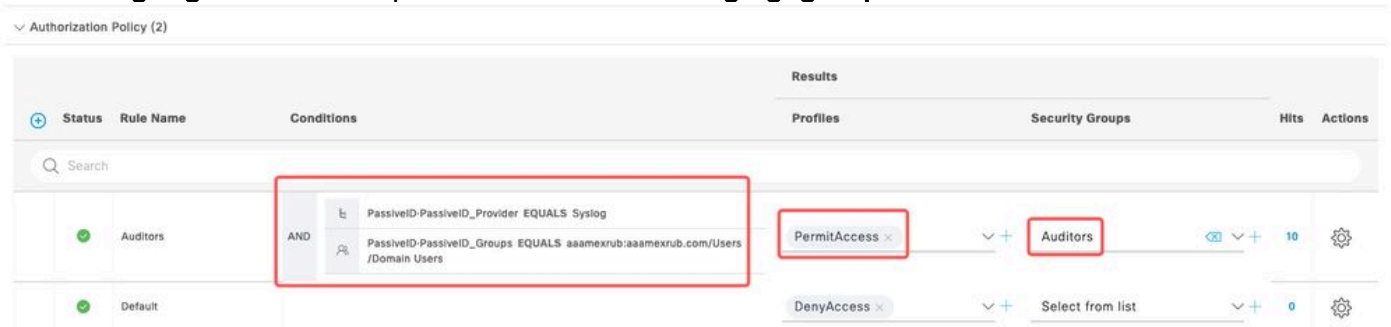


Aangepaste header

configureren

Stap 4. Autorisatieregels configureren

1. Ga naar **Beleid > Beleidssets**. In dit geval wordt het Standaardbeleid gebruikt. Klik op het **Standaardbeleid**. Voeg in het **autorisatiebeleid** een nieuwe regel toe. In het PassiveID-beleid beschikt ISE over alle aanbieders. Je kan deze combineren met een PassiveID groep. Kies **Toegang toestaan** als profiel en kies in **beveiligingsgroepen** de behoefte aan SGT.



Autorisatieregels configureren

Verifiëren

Zodra ISE de Syslog ontvangt, kunt u de Radius Live Logs controleren om Autorisation Flow te zien. Navigeer naar **Operations > Radius > Live logs**.

In de logboeken kunt u de gebeurtenis van de Vergunning zien. Deze bevat de gebruikersnaam, het autorisatiebeleid en de beveiligingsgroep die aan de gebruikersnaam zijn gekoppeld.

Reset Repeat Counts Export To

Time	Status	Details	Repea...	Identity	Endpoint ID	Authenticatio...	Authorization Policy	Authorization ...	Security ...	IP Address
Jan 31, ...			0	test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess	Auditors	192.168.123.10
Jan 31, ...				test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess		192.168.123.10

Radius live log

Klik op het **Detailrapport** om meer details te controleren. Hier kunt u de stroom autoriseren-alleen zien die het beleid evalueert om de SGT toe te wijzen.

Overview

Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Endpoint Profile	
Authentication Policy	PassiveID provider
Authorization Policy	PassiveID provider >> Auditors
Authorization Result	PermitAccess

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 - test@aaamexrub.com
- 24313 Search for matching accounts at join point - aaamexrub.com
- 24319 Single matching account found in forest - aaamexrub.com
- 24323 Identity resolution detected single matching account
- 24355 LDAP fetch succeeded - aaamexrub.com
- 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 Syslog
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15036 Evaluating Authorization Policy
- 90500 New Identity Mapping
- 5236 Authorize-Only succeeded

Authentication Details

Source Timestamp	2023-01-31 16:15:04.507
Received Timestamp	2023-01-31 16:15:04.507
Policy Server	asc-ise32-726
Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Calling Station Id	192.168.123.10
IPv4 Address	192.168.123.10
Authorization Profile	PermitAccess

Radius Live log-rapport

Problemen oplossen

In dit geval worden twee stromen gebruikt: de passieve ID-sessies en de autorisatiestroom. Om de debugs in te schakelen, navigeer naar **Operations > Probleemoplossing > Debug Wizard > Debug Log Configuration**, kies vervolgens het ISE-knooppunt.

Voor PassiveID, laat de volgende componenten toe om niveau te **ZUIVEREN**:

- Passieve id

Om de logbestanden te controleren, op basis van de Passieve ID-provider, het bestand om te controleren op dit scenario, moet u het **bestand** passiveid-syslog.log bekijken, voor de andere providers:

- passiveid-agent.log
- passiveid-api.log
- gepassiveerd-endpoint.log
- passiveid-span.log
- passiveid-wmilog

Schakel de volgende componenten in voor het **debug**-niveau voor de autorisatiestroom:

- beleidsinstrument
- prt-JNI

Voorbeeld:

The screenshot shows the 'Debug Wizard' interface for a node named 'asc-ise32-726.aaamexrub.com'. The main section is titled 'Debug Level Configuration'. Below the title, there are 'Edit' and 'Reset to Default' buttons. A table lists the configuration for three components, all set to the 'debug' level. The log file names for each component are highlighted with red boxes.

Component Name	Log Level	Description	Log file Name
<input type="radio"/> PassiveID	DEBUG	PassiveID events and messages	passiveid-wmi.log
<input type="radio"/> policy-engine	DEBUG	Policy Engine 2.0 related messages	ise-psc.log
<input type="radio"/> prrt-JNI	DEBUG	prrt policy decision request processing layer related ...	prrt-management.log

Debugs ingeschakeld

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.