

# ISE 3.2でのパッシブIDセッションの認可フローの設定

## 内容

[概要](#)

[背景説明](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、セッションにSGTを割り当てるためにパッシブIDイベントの認可ルールを設定する方法について説明します。

## 背景説明

パッシブIDサービス ( パッシブID ) は、ユーザを直接認証するのではなく、Active Directory(AD)などの外部の認証サーバ ( プロバイダーと呼ばれます ) からユーザアイデンティティとIPアドレスを収集し、その情報をサブスクライバと共有します。

ISE 3.2では、Active Directoryグループメンバーシップに基づいてセキュリティグループタグ (SGT) をユーザに割り当てるように許可ポリシーを設定できる新機能が導入されています。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco ISE 3.X
- 任意のプロバイダーとのパッシブID統合
- Active Directory(AD)の管理
- セグメンテーション(Trustsec)
- PxGrid(Platform Exchange Grid)

### 使用するコンポーネント

- Identity Service Engine(ISE)ソフトウェアバージョン3.2
- Microsoft Active Directory
- Syslog

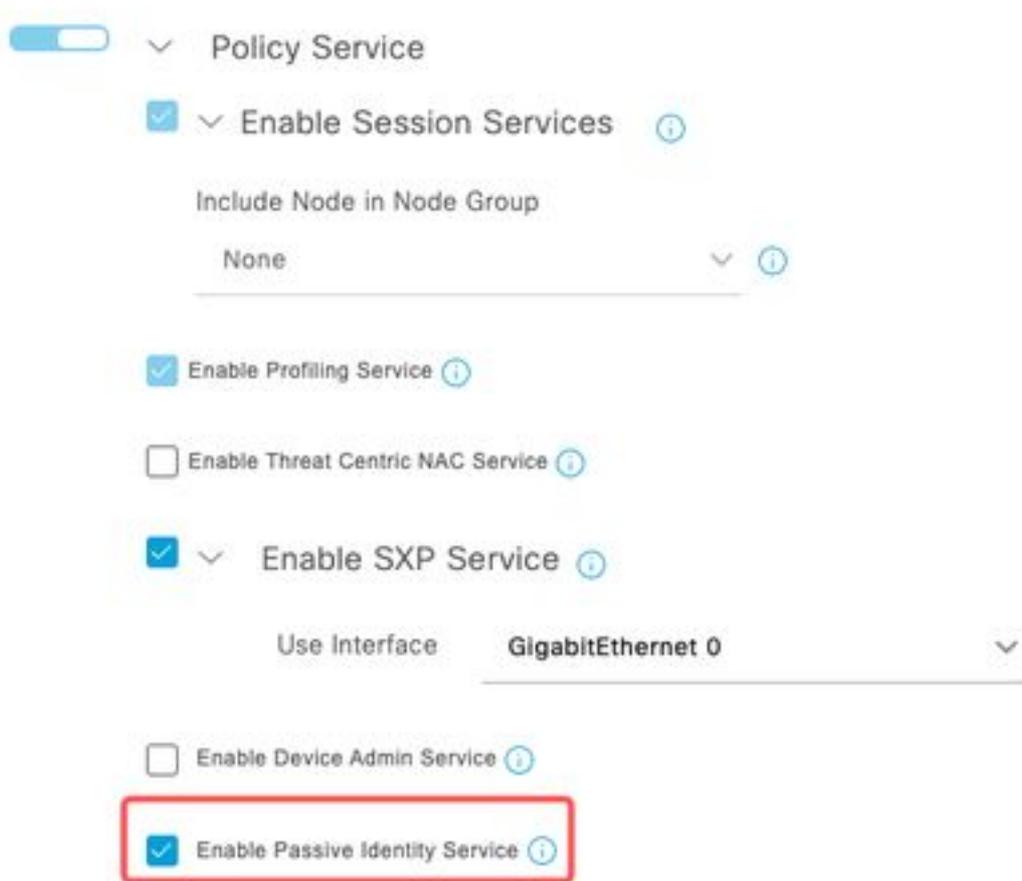
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## コンフィギュレーション

ステップ 1：ISEサービスを有効にします。

1. ISEで、[Administration] > [Deployment] に移動し、ISEノードを選択して、[Edit] をクリックし、[Policy Service] を有効にして、[Enable Passive Identity Service] を選択します。オプションで、パッシブIDセッションをそれぞれ介して公開する必要がある場合は、SXPとPxGridを有効にできます。[Save] をクリックします。

**警告：** APIプロバイダーによって認証されるPassiveIDログインユーザのSGTの詳細は、SXPに公開できません。ただし、これらのユーザのSGTの詳細は、pxGridおよびpxGrid Cloudを通じて公開できます。



有効なサービス

ステップ 2：Active Directoryを設定します。

1. [Administration] > [Identity Management] > [External Identity Sources] に移動し、[Active directory] を選択して、[Add] ボタンをクリックします。
2. [Join Point Name] と [Active Directory Domain] を入力します。[Submit] をクリックします。

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

---

**External Identity Sources**

<      

>  Certificate Authentication F

 Active Directory

**Connection**

\* Join Point Name  

\* Active Directory Domain  

*Active Directoryの追加*

3. ISEをADに参加させるポップアップが表示されます。[Yes] をクリックします。[Username] と [Password] を入力します。[OK] をクリックします。



## Information

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

*ISEへの参加を継続する*

## 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 

*Active Directoryへの参加*

4. ADグループを取得します。[Groups] に移動し、[Add] をクリックしてから[Retrieve Groups] をクリックし、目的のグループをすべて選択して[OK] をクリックします。

## 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グループの取得

Connection Allowed Domains PassivID **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

取得されたグループ

5.認可フローを有効にします。[Advance Settings] に移動し、[PassiveID Settings] セクションで [Authorization Flow] チェックボックスをオンにします。[Save] をクリックします。

## 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 ⓘ

許可フローの有効化

ステップ 3 : Syslogプロバイダーを設定します。

1. [Work Centers] > [PassiveID] > [Providers] に移動し、[Syslog Providers] を選択し、[Add] をクリックして情報を入力します。[Save] をクリックします。

**注意 :** この場合、ISEはASAでの正常なVPN接続からsyslogメッセージを受信しますが、このドキュメントではその設定について説明しません。

## Syslog Providers

Name\*  
ASA

Description

Status\*  
Enabled

Host FQDN\*  
asa-rudelave.aaamexrub.com

Connection Type\*  
UDP - Port 40514

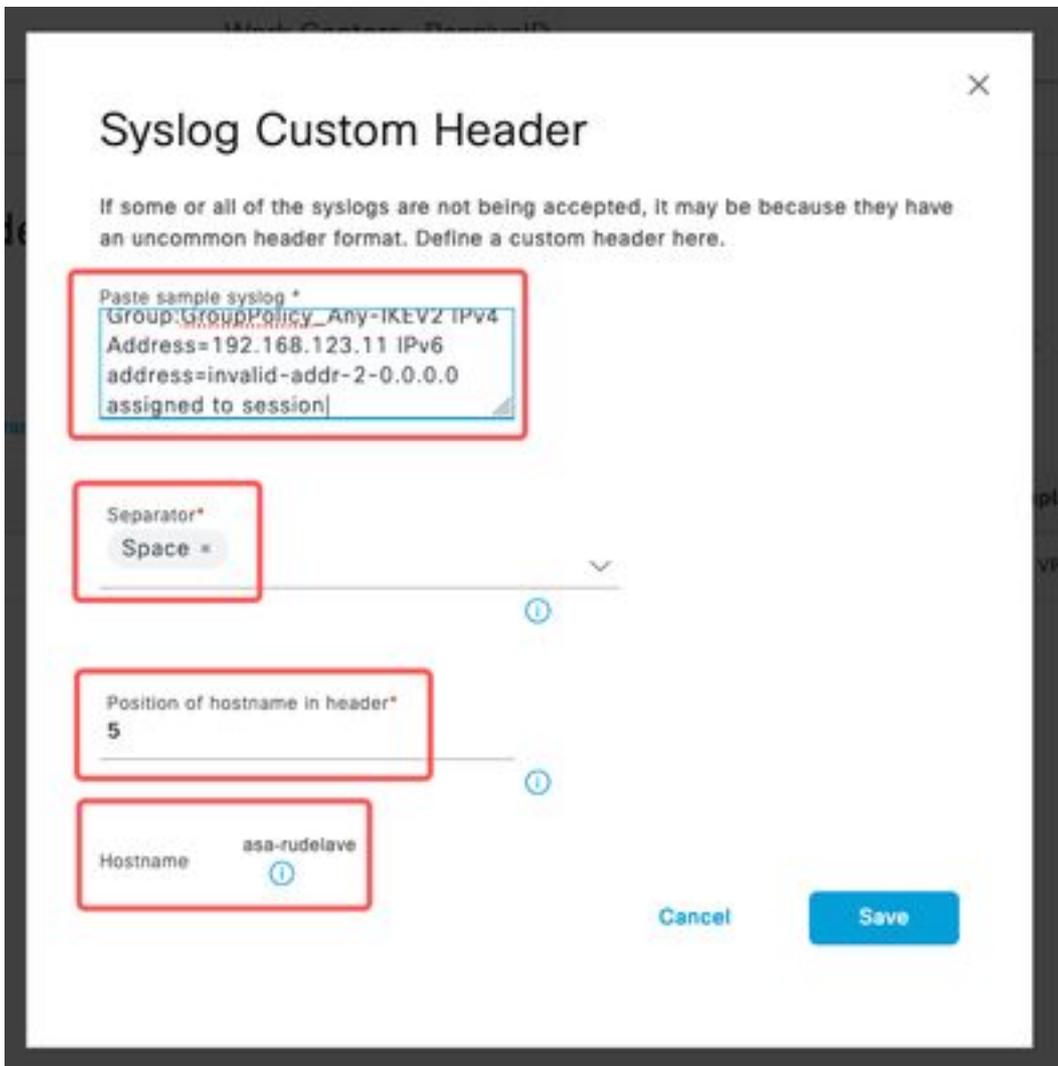
Template\* ASA VPN [View](#) [New](#)

Default Domain  
aaamexrub.com

[?](#)

Syslogプロバイダーの設定

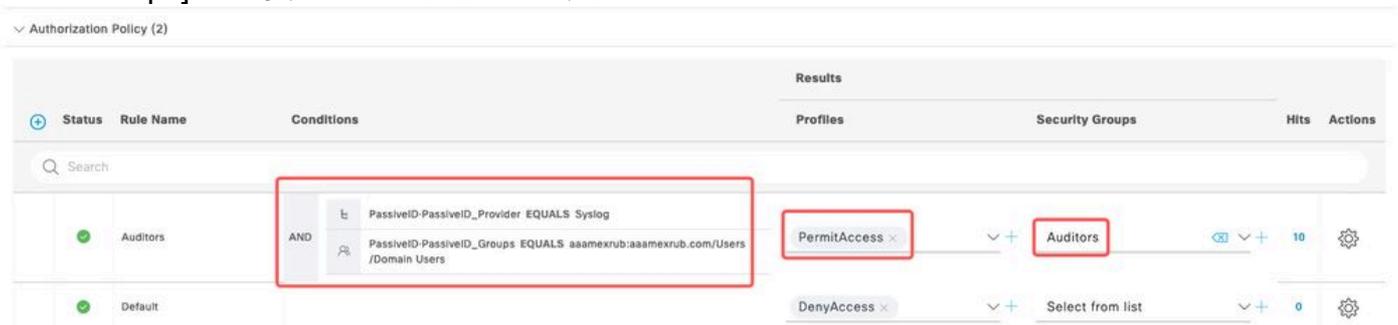
2. [Custom Header] をクリックします。サンプルsyslogを貼り付け、セパレータまたはタブを使用してデバイスのホスト名を検索します。正しい場合は、ホスト名が表示されます。  
[Save] をクリックします。



カスタムヘッダーの設定

#### ステップ 4 : 許可ルール ( Authorization Rule ) の設定

1. [Policy] > [Policy Sets] に移動します。この場合は、デフォルトポリシーを使用します。[Default] ポリシーをクリックします。[Authorization Policy] で、新しいルールを追加します。PassiveIDポリシーでは、ISEにすべてのプロバイダーがあります。これをPassiveIDグループと組み合わせることができます。[Profile]として[Permit Access] を選択し、[Security Groups] で必要なSGTを選択します。



許可ルール ( Authorization Rule ) の設定

## 確認

ISEがSyslogを受信したら、Radiusライブログを確認して認可フローを確認できます。[Operations] > [Radius] > [Live logs] に移動します。

ログで、認証イベントを確認できます。これには、ユーザ名、許可ポリシー、およびセキュリティグループタグが関連付けられています。

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ライブログ

詳細を確認するには、[Detail Report] をクリックします。ここでは、SGTを割り当てるポリシーを評価するAuthorize-Onlyフローを確認できます。

#### 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ライブログレポート

## トラブルシュート

この場合、passiveIDセッションと認証フローの2つのフローを使用します。デバッグを有効にするには、[Operations] > [Troubleshoot] > [Debug Wizard] > [Debug Log Configuration] に移動し、ISEノードを選択します。

PassiveIDに対して、次のコンポーネントをDEBUGレベルに有効にします。

- PassiveID

パッシブIDプロバイダーに基づいてログをチェックし、このシナリオをチェックするファイルを調べるには、他のプロバイダーのfile passiveid-syslog.logを確認する必要があります。

- passiveid-agent.log

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

認可フローで、次のコンポーネントをDEBUGレベルに有効にします。

- ポリシーエンジン
- prrt-JNI

例：

The screenshot shows the 'Debug Wizard' interface for a Node.js application. The main heading is 'Debug Level Configuration'. Below the heading, there are 'Edit' and 'Reset to Default' buttons. A table lists the configured components, their log levels, descriptions, and log file names. The log level for all components is set to 'DEBUG'. The log file names 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

デバッグ有効

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。