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

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

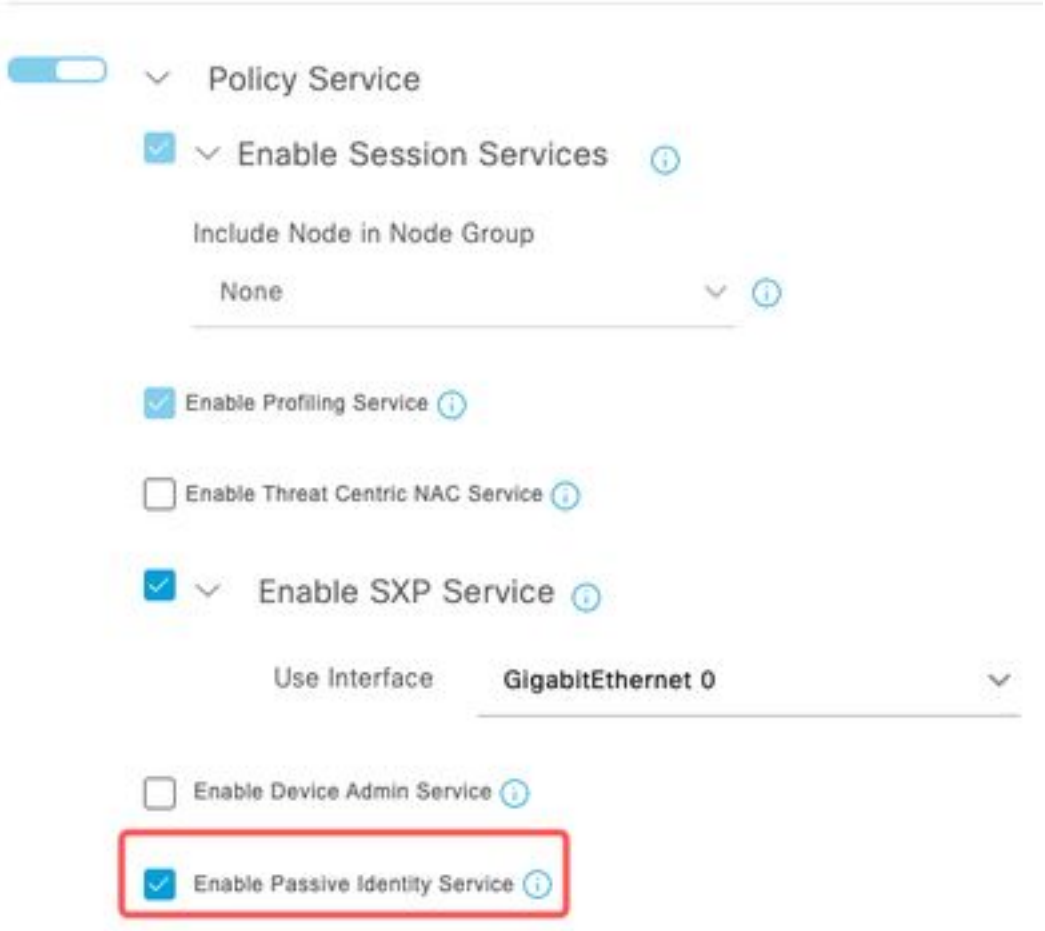
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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。

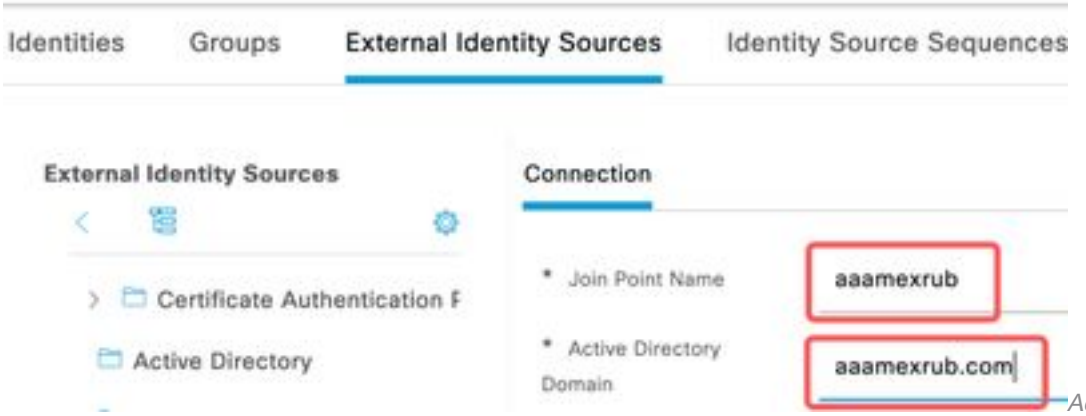
   警告： APIプロバイダーによって認証されるPassiveIDログインユーザのSGTの詳細は、SXPに公開できません。ただし、これらのユーザのSGTの詳細は、pxGridおよびpxGrid Cloudを通じて公開できます。



有効なサービス

ステップ 2：Active Directoryを設定します。

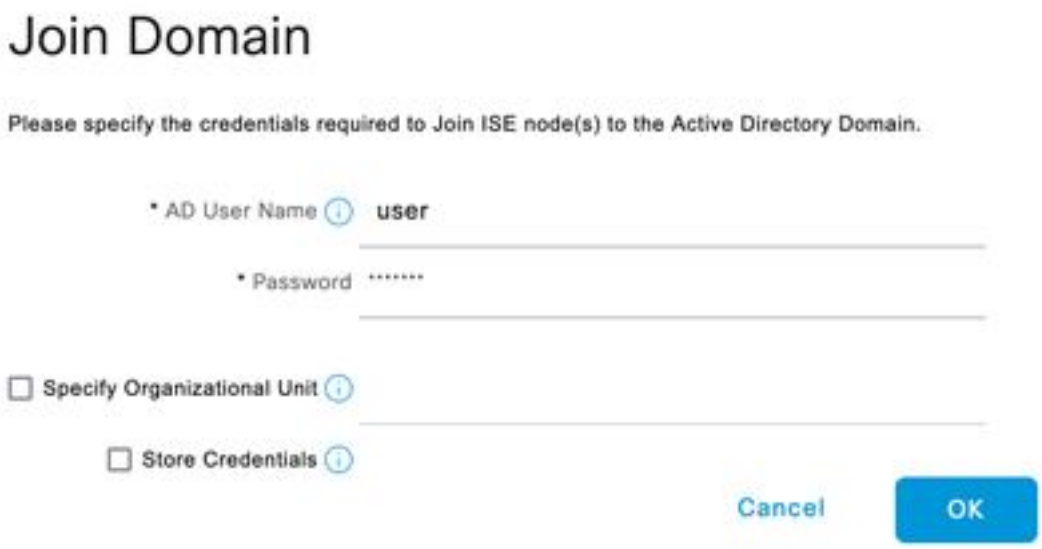
1. [Administration] > [Identity Management] > [External Identity Sources] に移動し、[Active directory] を選択して、[Add] ボタンをクリックします。
2. [Join Point Name] と[Active Directory Domain] を入力します。[Submit] をクリックします。



Active Directoryの追加

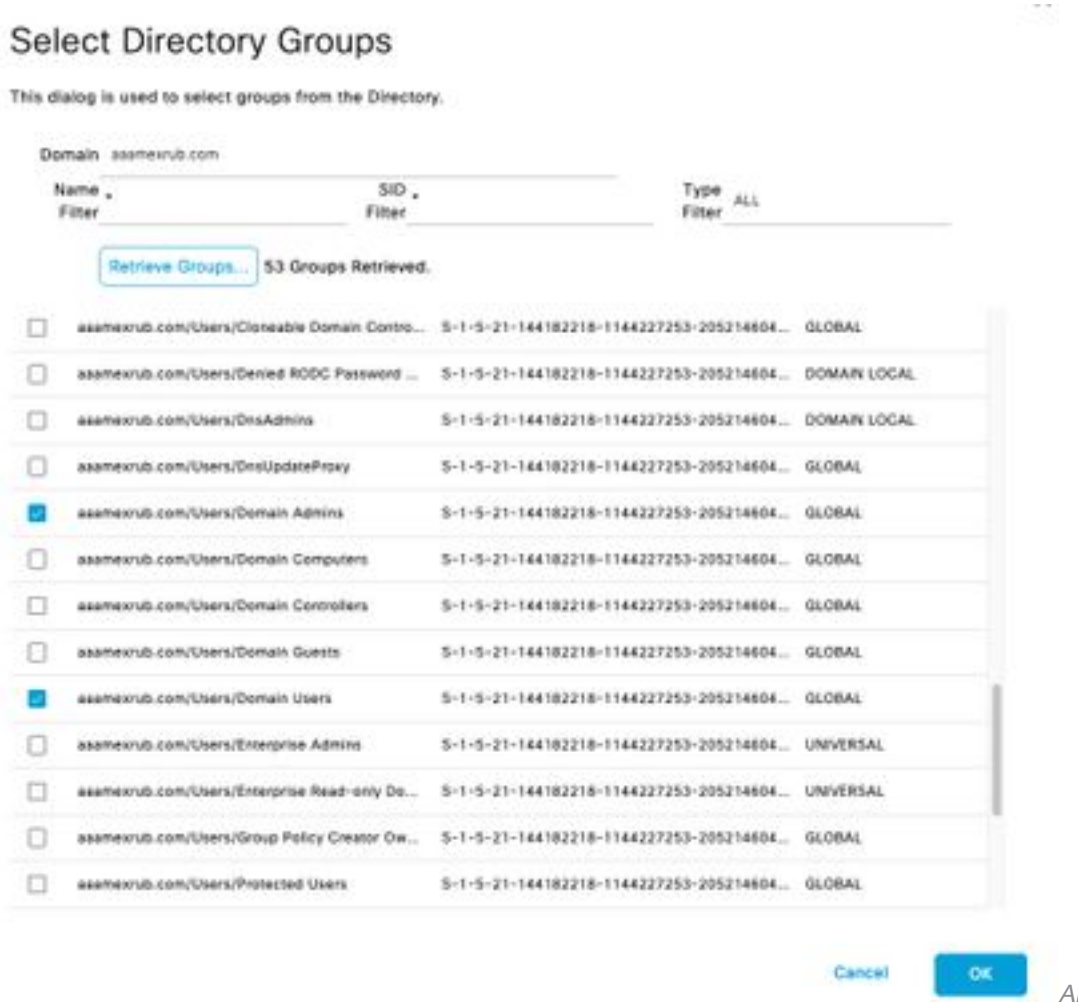
3. ISEをADに参加させるポップアップが表示されます。[Yes] をクリックします。**[Username] と [Password]** を入力します。[OK] をクリックします。

ISEへの参加を継続する

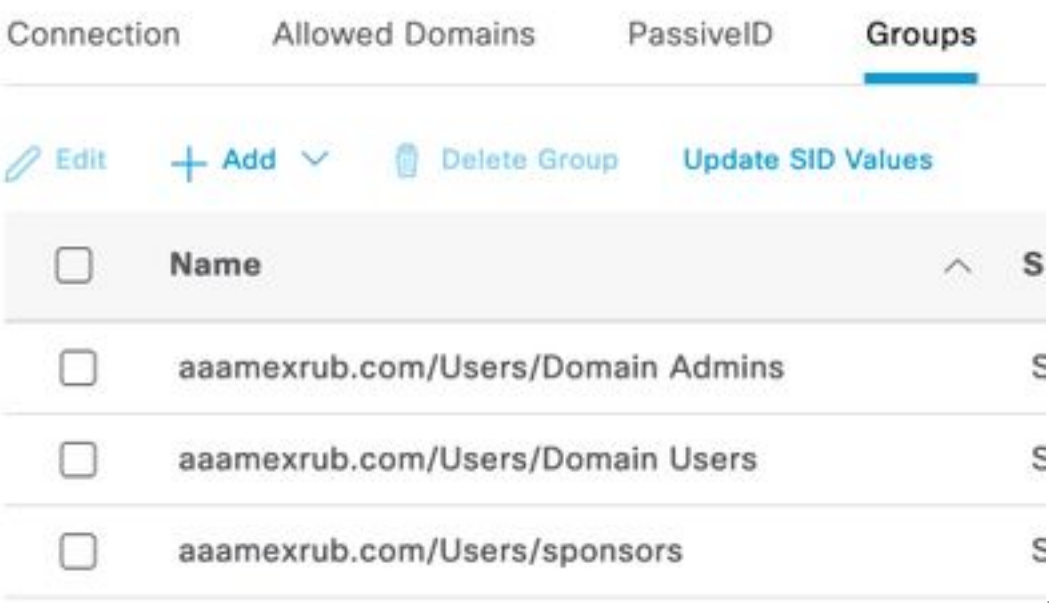


Active Directoryへの参加

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。

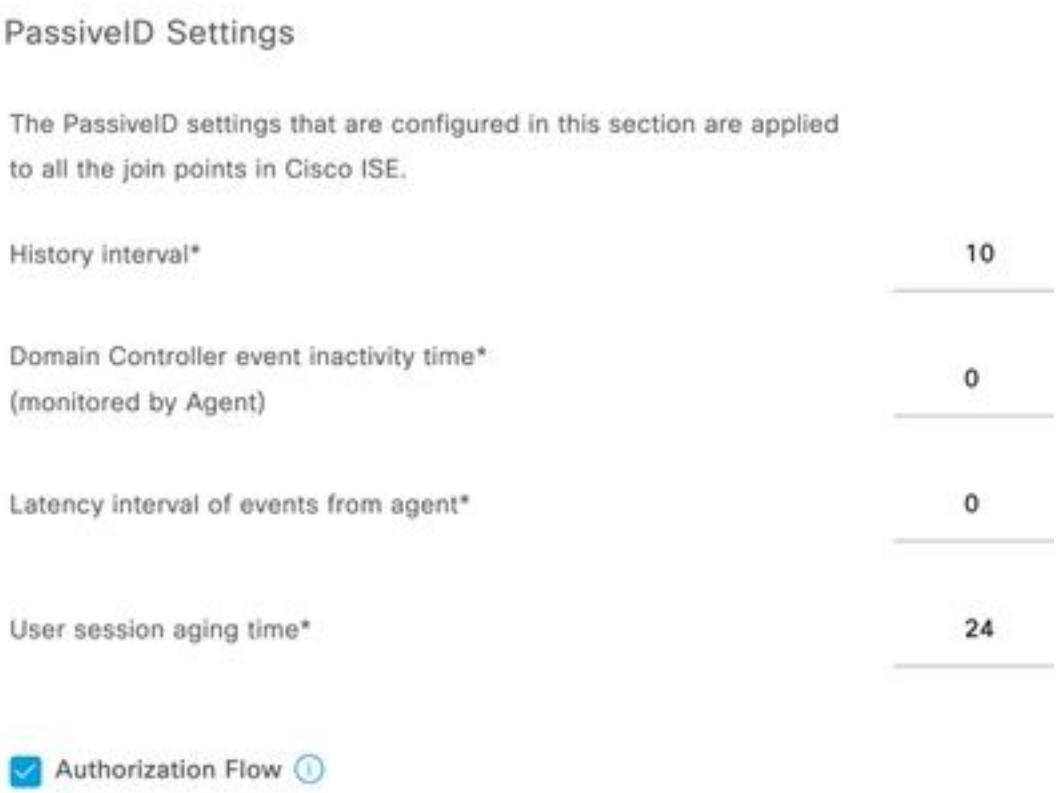


ADグループの取得



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。

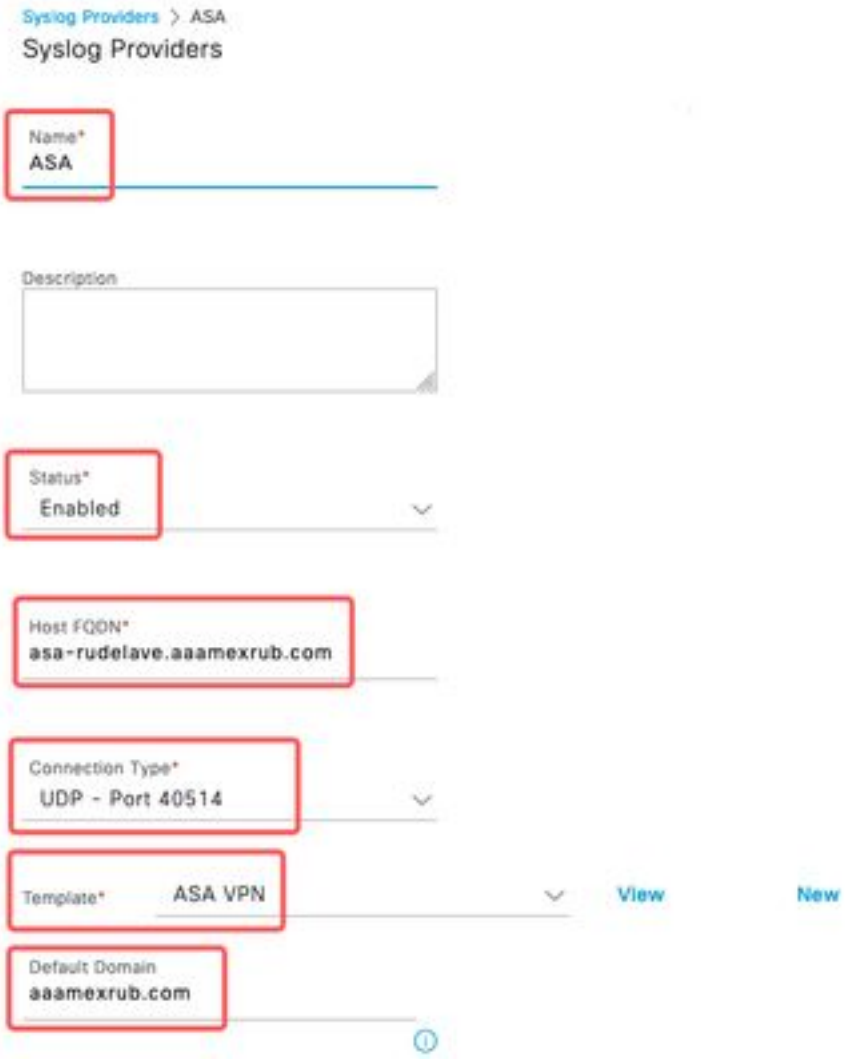


許可フローの有効化

ステップ 3：Syslogプロバイダーを設定します。

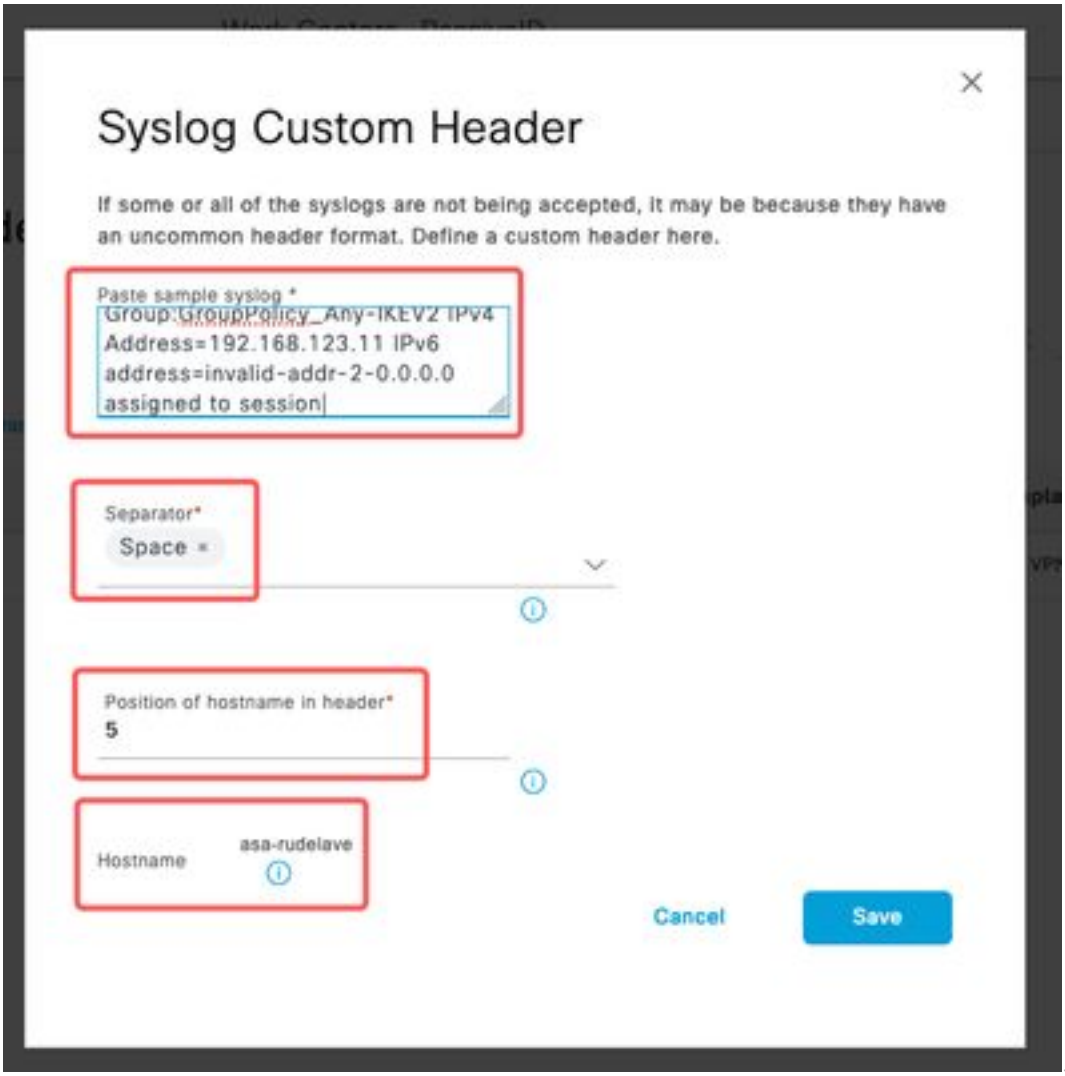
1. [Work Centers] > [PassiveID] > [Providers] に移動し、[Syslog Providers] を選択し、[Add] をクリックして情報を入力します。[Save] をクリックします。

   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

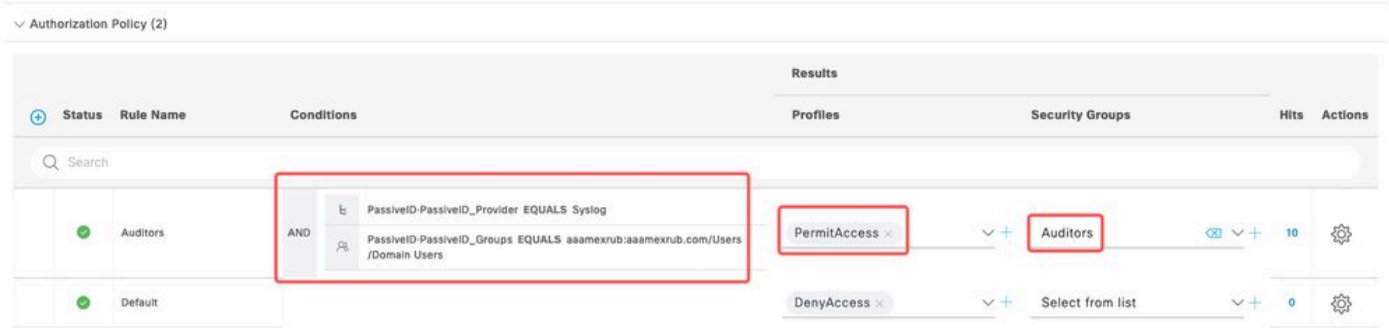
2. [Custom Header] をクリックします。サンプルsyslogを貼り付け、セパレータまたはタブを使用してデバイスのホスト名を検索します。正しい場合は、ホスト名が表示されます。[Save] をクリックします。



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

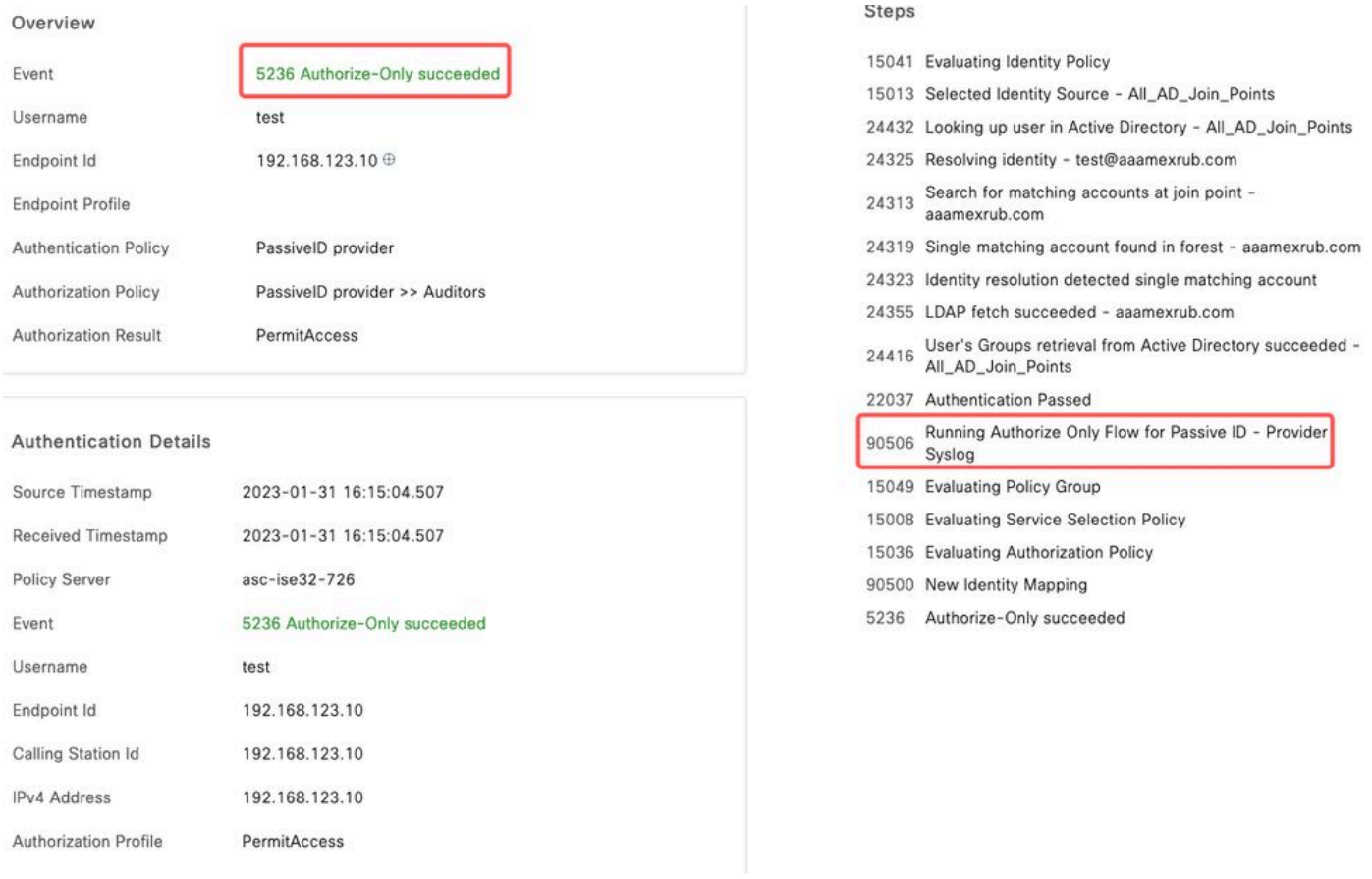
確認

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。

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。



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。

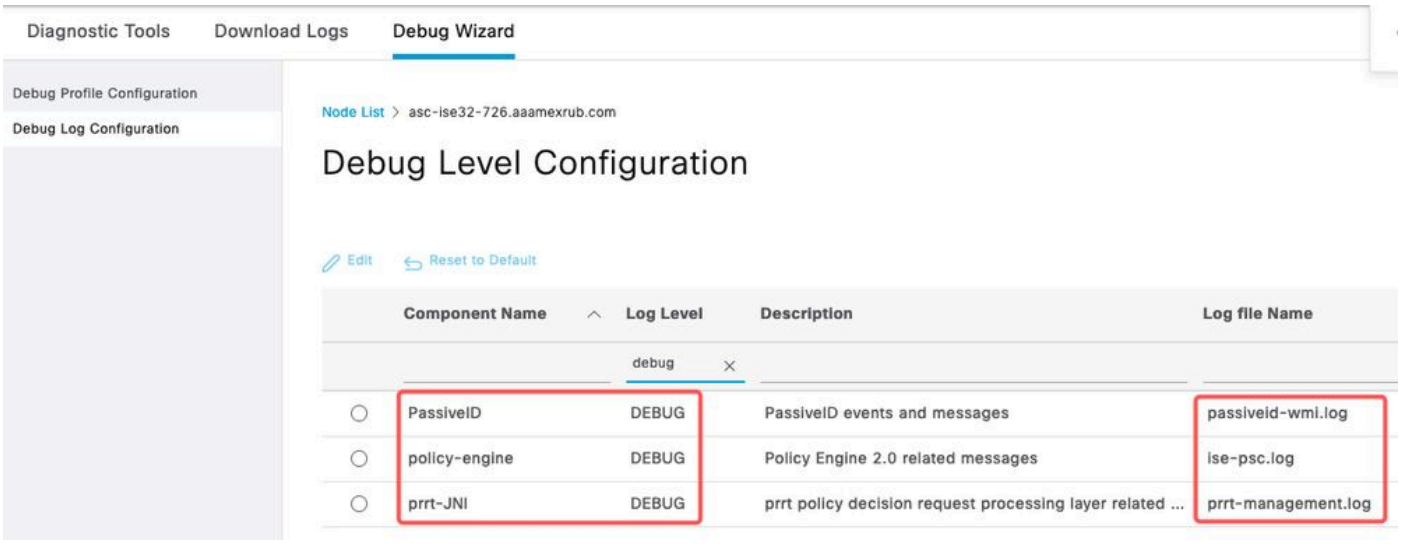
- passiveid-agent.log

- 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：



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。