

# PassiveIDセッションにセキュリティグループタグを割り当てるためのISE 3.2の設定

## 内容

---

### [概要](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [背景説明](#)

### [設定](#)

#### [フロー図](#)

#### [コンフィギュレーション](#)

### [確認](#)

#### [ISEの検証](#)

#### [PxGridサブスクリバの検証](#)

#### [TrustSec SXPピアの検証](#)

### [トラブルシューティング](#)

#### [ISEでのデバッグの有効化](#)

#### [ログのスニペット](#)

---

## 概要

このドキュメントでは、ISE 3.2の認可ポリシーを介してパッシブIDセッションにセキュリティグループタグ(SGT)を設定し、割り当てる方法について説明します。

## 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 3.2
- パッシブID、TrustSec、およびPxGrid

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE 3.2
- FMC 7.0.1
- 16.12.1が稼働するWS-C3850-24P

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、クリアな（デフォルト）設定で作業を開始しています。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。

## 背景説明

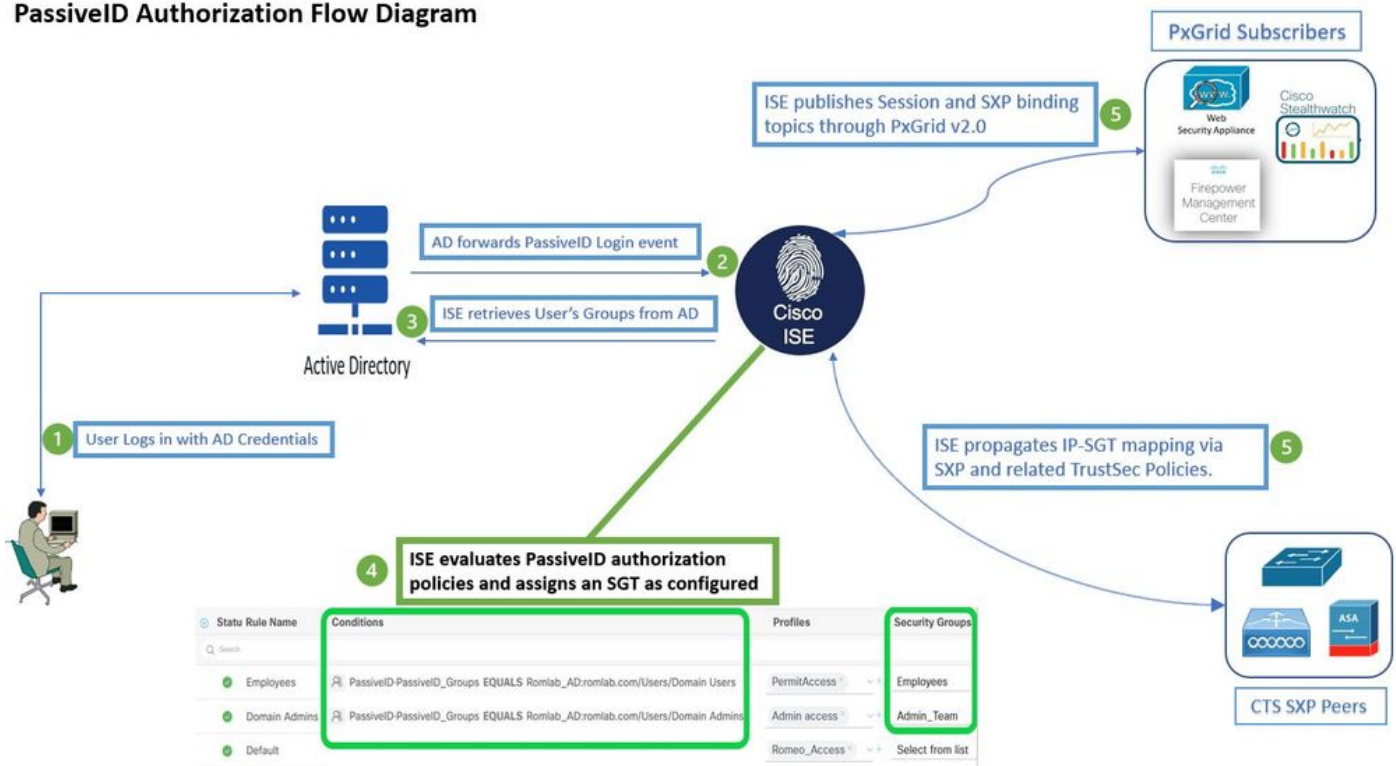
Cisco Identity Services Engine(ISE)3.2はこの機能をサポートする最小バージョンです。このドキュメントでは、PassiveID、PxGrid、およびSXPの設定については説明しません。関連情報については、『[管理者ガイド](#)』を参照してください。

ISE 3.1以前のバージョンでは、セキュリティグループタグ(SGT)はRADIUSセッションまたは802.1xやMABなどのアクティブ認証にのみ割り当てることができます。ISE 3.2では、Identity Services Engine(ISE)がActive Directoryドメインコントローラ(AD DC) WMIやADエージェントなどのプロバイダーからユーザログインイベントを受信したときに、ユーザのActive Directory(AD)グループメンバーシップに基づいてPassiveIDセッションにセキュリティグループタグ(SGT)を割り当てるように、PassiveIDセッションの認証ポリシーを設定できます。PassiveIDのIP-SGTマッピングとADグループの詳細は、SGT Exchange Protocol(SXP)を介してTrustSecドメインにパブリッシュするか、Cisco Platform Management Center(FMC)やCisco Secure Network Analytics(Stealthwatch)などのFirepowerエクスチェンジグリッド(pxGrid)サブスクリバにパブリッシュすることができます。

## 設定

### フロー図

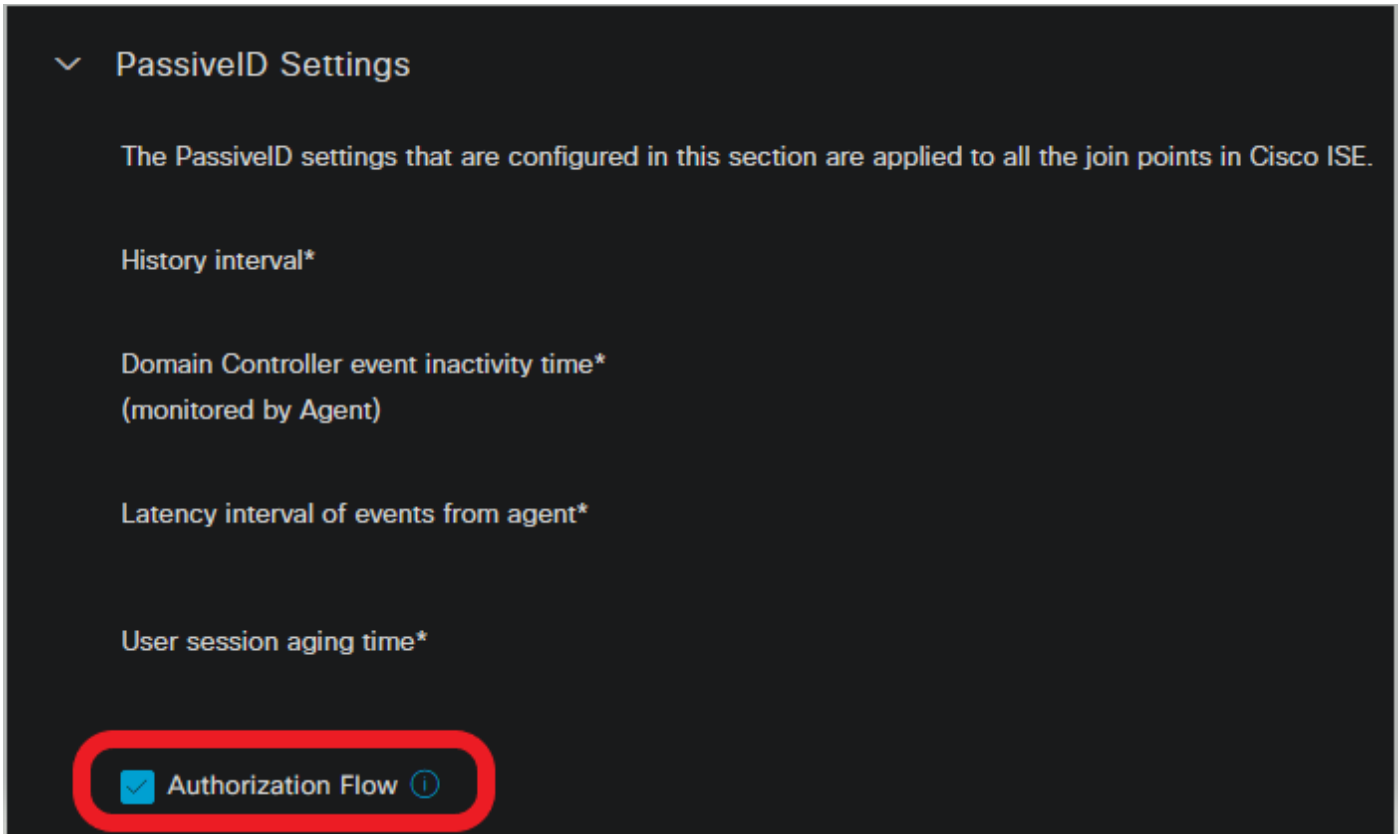
PassiveID Authorization Flow Diagram




## コンフィギュレーション

許可フローを有効にします。

移動先 [Active Directory > Advanced Settings > PassiveID Settings](#) をクリックして、[Authorization Flow](#) チェックボックスをオンにして、PassiveIDログインユーザの認可ポリシーを設定します。このオプションはデフォルトで無効になっています。



認証フローを有効にする

 注：この機能を使用するには、PassiveID、PxGrid、およびSXPサービスを必ず導入で実行してください。これは、次のURLで確認できます [Administration > System > Deployment](#) .

ポリシーセットの設定：

1. PassiveID用に別のポリシーセットを作成します（推奨）。
2. Conditionsには、属性を使用します `PassiveID:PassiveID_Provider` プロバイダーの種類を選択します。

| Status | Policy Set Name    | Description        | Conditions                                | Allowed Protocols / Server Sequence | Hits | Actions | View |
|--------|--------------------|--------------------|---|-------------------------------------|------|---------|------|
| ✓      | PassiveID_Sessions |                    | PassiveID-PassiveID_Provider EQUALS Agent | Default Network Access              | 5    | ⚙️      | ➔    |
| ✓      | Default            | Default policy set |   | Default Network Access              | 133  | ⚙️      | ➔    |

## ポリシーセット

3. 手順1で作成したポリシーセットの認可ルールを設定します。

- 各ルールの条件を作成し、ADグループ、ユーザ名、または両方に基づいてPassiveIDディクショナリを使用します。
- 各ルールにセキュリティグループタグを割り当て、設定を保存します。

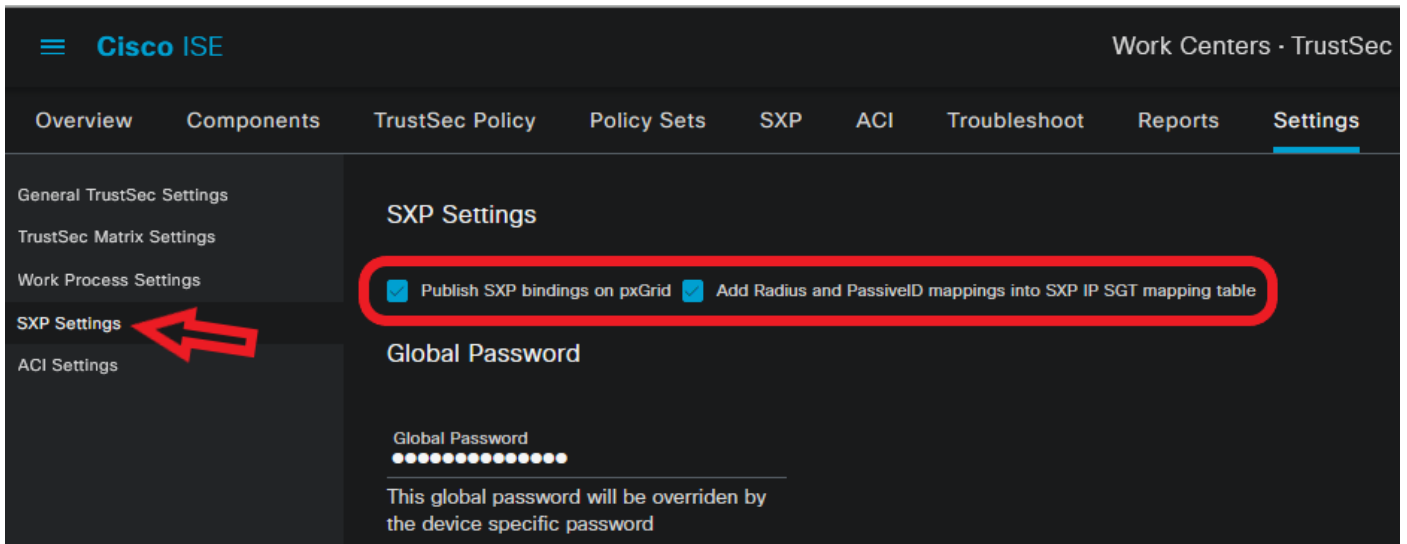
| Status | Rule Name     | Conditions  | Profiles     | Security Groups  | Hits | Actions |
|--------|---------------|---|--------------|------------------|------|---------|
| ✓      | Employees     | PassiveID-PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Users  | PermitAccess | Employees   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

## 認可ポリシー

注：このフローでは使用されないため、認証ポリシーは無関係です。

注：以下を使用できます。 PassiveID\_Username, PassiveID\_Groups, または PassiveID\_Provider 許可ルールを作成するための属性です。

4.次に移動します。 Work Centers > TrustSec > Settings > SXP Settings を有効にする Publish SXP bindings on pxGrid と Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table PassiveIDマッピングをPxGridサブスクライバと共有し、ISEのSXPマッピングテーブルに含めます。



SXPの設定

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

## ISEの検証

Active Directoryドメインコントローラ(AD DC)WMIまたはADエージェントなどのプロバイダーからISEにユーザログインイベントが送信されたら、ライブログの確認に進みます。移動先 **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    | PassiveID_Sessions >> Employees | PermitAccess           | Employees      |
| Sep 06, 2022 08:28:31.4... | ○      |         |          | smith    | 10.10.10.10 | PassiveID_Sessions    | PassiveID_Sessions >> Employees | PermitAccess           |                |

Radiusライブログ

「詳細」列の拡大鏡アイコンをクリックして、ユーザーの詳細レポートを表示します。この例では、次に示すようにsmith (ドメイン・ユーザー) です。

## 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 |
| Authorization Result  | PermitAccess                    |

## Authentication Details

|                       |                               |
|-----------------------|-------------------------------|
| Source Timestamp      | 2022-09-06 20:28:31.393       |
| Received Timestamp    | 2022-09-06 20:28:31.393       |
| Policy Server         | ise-3-2                       |
| Event                 | 5236 Authorize-Only succeeded |
| Username              | smith                         |
| Endpoint Id           | 10.10.10.10                   |
| Calling Station Id    | 10.10.10.10                   |
| IPv4 Address          | 10.10.10.10                   |
| Authorization Profile | PermitAccess                  |


## Other Attributes

|                             |  |
|-----------------------------|--|
| ConfigVersionId             | 108  |
| AuthorizationPolicyMatched_ | Employees  |
| ISEPolicySetName            | PassiveID_Sessions                                   |
| AD-User-Resolved-Identities | smith@Lfc.lab  |
| AD-User-Resolved-DNs        | CN=smith,CN=Users,DC=Lfc,DC=lab                      |
| AD-User-DNS-Domain          | Lfc.lab  |
| AD-Groups-Names             | Lfc.lab/Builtin/Administrators                       |
| AD-Groups-Names             | Lfc.lab/Builtin/Remote Desktop Users                 |
| AD-Groups-Names             | Lfc.lab/Builtin/Remote Management Users              |
| AD-Groups-Names             | Lfc.lab/Builtin/Users                                |
| AD-Groups-Names             | Lfc.lab/Users/Denied RODC Password Replication Group |
| AD-Groups-Names             | Lfc.lab/Users/Domain Test                            |
| AD-Groups-Names             | Lfc.lab/Users/NAD Admins                             |
| AD-Groups-Names             | Lfc.lab/Users/Domain Users                           |
| AD-User-NetBios-Name        | Lfc  |
| AD-User-SamAccount-Name     | smith  |
| AD-User-Qualified-Name      | smith@Lfc.lab  |
| AuthorizationSGTName        | Employees  |
| ProviderIpAddress           | 10.10.10.132   |
| SessionId                   | cf0d2acd-0d3d-413b-b2fb-6860df3f0d84                 |
| provider                    | Agent  |
| UseCase                     | PassiveIDAuthZOnly                                   |

## 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 - All_AD_Join_Points |
| 22037 | Authentication Passed  |
| 90506 | Running Authorize Only Flow for Passive ID - Provider Agent                  |
| 15049 | Evaluating Policy Group  |
| 15008 | Evaluating Service Selection Policy  |
| 15036 | Evaluating Authorization Policy  |
| 90500 | New Identity Mapping   |
| 5236  | Authorize-Only succeeded   |

|        |        |      |                  |
|--------|--------|------|------------------|
| パッシブID | 受動静脈ID | トレース | passiveid-*.log  |
| pxGrid | pxgrid | トレース | pxgridサーバ.log    |
| SXP    | sxp    | デバッグ | sxp.log (ダウンロード) |

 注：トラブルシューティングが終了したら、デバッグをリセットして関連ノードを選択し、Reset to Defaultを参照。

## ログのスニペット

1. ISEがプロバイダーからログインイベントを受信します。

Passiveid-\*.logファイル：

```

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Received login event.
Identity Mapping.probe = Agent , dc-host = /10.10.10.132 , Identity Mapping.server = ise-3-2 , event-operation-
type = ADD ,

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

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Building login event to be
published to session directory.
2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- retrieving user's additional
information from Active Directory.

2022-09-06 20:28:31,326 DEBUG [Grizzly-worker(26)][[]] com.cisco.idc.agent-probe- Forwarded login event to
session directory. Identity Mapping.id-src-first-port = -1 , Identity Mapping.dc-domainname = Lfc.lab , Identity
Mapping.id-src-port-start = -1 , Identity Mapping.probe = Agent , Identity Mapping.id-src-port-end = -1 , Identity
Mapping.event-user-name = smith , Identity Mapping.dc-host = /10.10.10.132 , Identity Mapping.agentId = ,
Identity Mapping.server = ise-3-2 , Identity Mapping.event-ip-address = 10.10.10.10 ,

```

Passiveid-\*.logファイル

2. ISEは設定された許可ポリシーに従ってSGTを割り当て、PassiveIDユーザのIP-SGTマッピングをPxGridサブスクリバおよびSXPピアに公開します。

sxp.logファイル：

```
2022-09-06 20:28:31,587 DEBUG [sxp-service-http-96443] cisco.ise.sxp.rest.SxpGlueRestAPI:27 - Adding session 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.SxpGlueRestAPI:23 - session binding created for ip address : 10.10.10.10/32
```

```
2022-09-06 20:28:31,613 DEBUG [SxpNotification] cisco.cpm.sxp.engine.SxpEngine:23 - Adding 1 session bindings
```

```
2022-09-06 20:28:31,613 DEBUG [SxpNotificationSerializer-Thread] cisco.cpm.sxp.engine.SxpEngine:42 - Adding session binding RestSxpLocalBinding(tag=4, groupName=null, ipAddress=10.10.10.10/32, nasIp=10.10.10.132, sessionId=cf0d2acd-0d3d-413b-b2fb-6860df3f0d84, peerSequence=null, sxpBindingOpType=ADD, sessionExpiryTimelnMillis=-1, apic=false, routable=true, vns=[DEFAULT_VN]) to VPNs [default]
```

sxp.log ファイル

pxgrid-server.log ファイル :

```
2022-09-06 20:28:31,693 TRACE [Grizzly(1)][] cpm.pxgrid.ws.client.WsEndpoint -::: Send. session=[id=b0df936b-bfab-435f-80e6-aa836aa3b24c,client=~ise-fanout-ise-3-2,server=wss://ise-3-2.Lfc.lab:8910/pxgrid/ise/pubsub] frame=[command=SEND,headers=[content-length=1859, destination=/topic/distributed, from=~ise-fanout-ise-3-2, via=~ise-fanout-ise-3-2],content-len=1859] content=MESSAGE content-length:1/30
```

```
destination:/topic/com.cisco.ise.session
```

```
message-id:616
```

```
subscription:2
```

```
via::~ise-fanout-ise-3-2
```

```
{"sessions":[{"timestamp":"2022:09:06T20:28:31.41105:00","state":"AUTHENTICATED","userName":"smith","callingStationId":"10.10.10.10","auditSessionId":"ddda40ec-e557-4457-81db-a36af7b7d4ec","ipAddresses":["10.10.10.10"],"nasIpAddress":"10.10.10.132","ctsSecurityGroup":"Employees","adNormalizedUser":"smith","adUserDomainName":"Lfc.lab","adUserNetBiosName":"Lfc","adUserResolvedIdentities":"smith@Lfc.lab","selectedAuthzProfiles":["PermitAccess"]},"sequence":13}
```

```
2022-09-06 20:28:31,673 TRACE [Grizzly(1)][] cpm.pxgrid.ws.client.WsEndpoint -::: Send. session=[id=b0df936b-bfab-435f-80e6-aa836aa3b24c,client=~ise-fanout-ise-3-2,server=wss://ise-3-2.Lfc.lab:8910/pxgrid/ise/pubsub] frame=[command=SEND,headers=[content-length=308, destination=/topic/distributed, from=~ise-fanout-ise-3-2, via::~ise-fanout-ise-3-2],content-len=308] content=MESSAGE content-length:176
```

```
destination:/topic/com.cisco.ise.sxp.binding
```

```
message-id:612
```

```
subscription:2
```

```
via::~ise-fanout-ise-3-2
```

```
{"operation":"CREATE","binding":{"ipPrefix":"10.10.10.10/32","tag":4,"source":"10.10.10.132","peerSequence":["10.10.10.135","10.10.10.132"],"vpn":"default"},"sequence":17}
```

pxgrid-server.log ファイル



## 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。