

Configurar o ISE 3.2 para atribuir tags de grupos de segurança para sessões PassiveID

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de fluxo](#)

[Configurações](#)

[Verificar](#)

[Verificação do ISE](#)

[Verificação de assinante do PxGrid](#)

[Verificação de mesmo nível TrustSec SXP](#)

[Troubleshooting](#)

[Habilitar depurações no ISE](#)

[Registra trechos](#)

Introdução

Este documento descreve como configurar e atribuir tags de grupos de segurança (SGTs) a sessões de ID passiva por meio de políticas de autorização no ISE 3.2.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ISE 3.2
- ID Passivo, TrustSec e PxGrid

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE 3.2
- FMC 7.0.1
- WS-C3850-24P que executa 16.12.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco Identity Services Engine (ISE) 3.2 é a versão mínima que suporta esse recurso. Este documento não aborda a configuração PassivelD, PxGrid e SXP. Para obter informações relacionadas, consulte o [Guia do administrador](#).

No ISE 3.1 ou em versões mais antigas, uma Security Group Tag (SGT) só pode ser atribuída à sessão Radius ou à autenticação ativa, como 802.1x e MAB. Com o ISE 3.2, podemos configurar políticas de autorização para Sessões PassivelD, de forma que, quando o Identity Services Engine (ISE) receber eventos de logon de usuário de um provedor, como o Active Directory Domain Controllers (AD DC) WMI ou o AD Agent, ele atribua uma Marca de Grupo de Segurança (SGT) à Sessão PassivelD com base na associação de grupo do Active Directory (AD) do usuário. O mapeamento IP-SGT e os detalhes do grupo AD do PassivelD podem ser publicados no domínio do TrustSec por meio do SGT Exchange Protocol (SXP) e/ou para assinantes do Platform Exchange Grid (pxGrid), como o Cisco Firepower Management Center (FMC) e o Cisco Secure Network Analytics (Stealthwatch).

Configurar

Diagrama de fluxo

PassiveID Authorization Flow Diagram

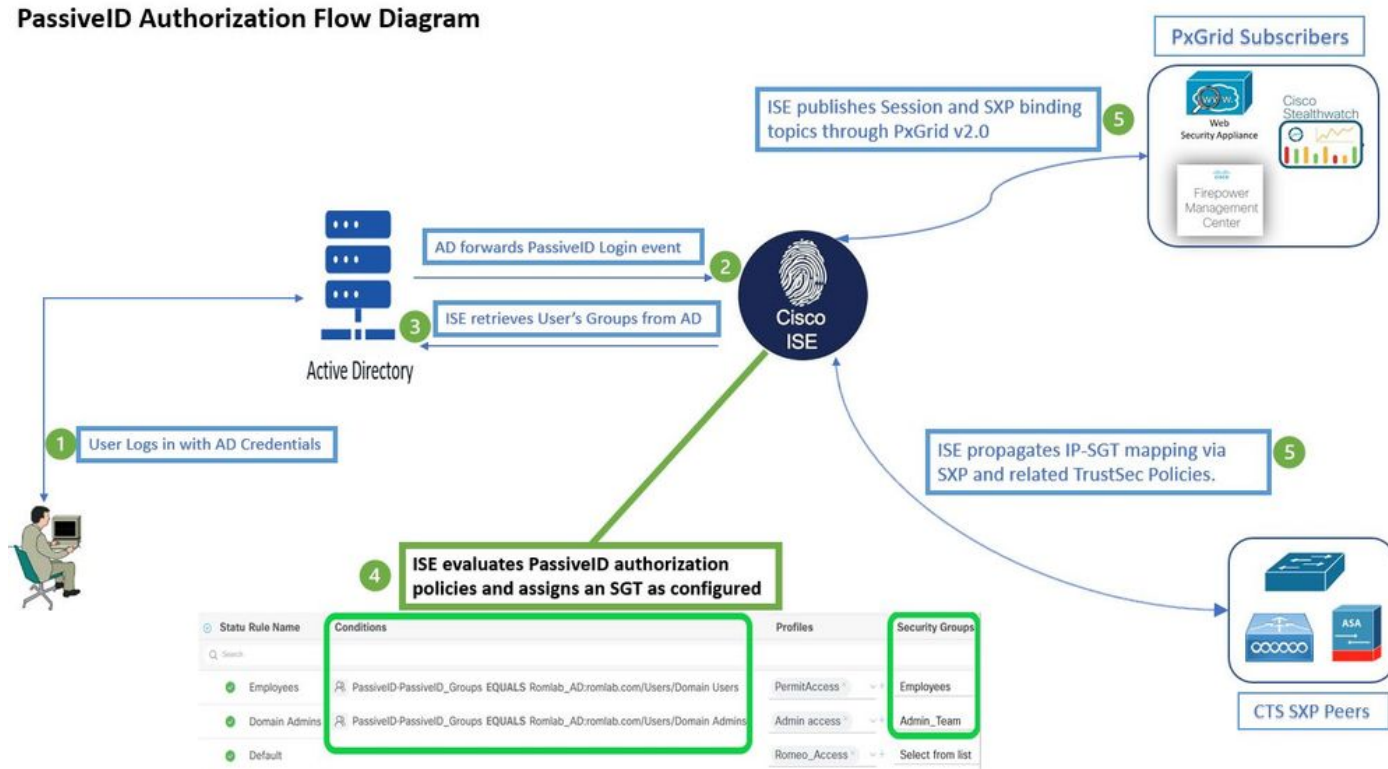
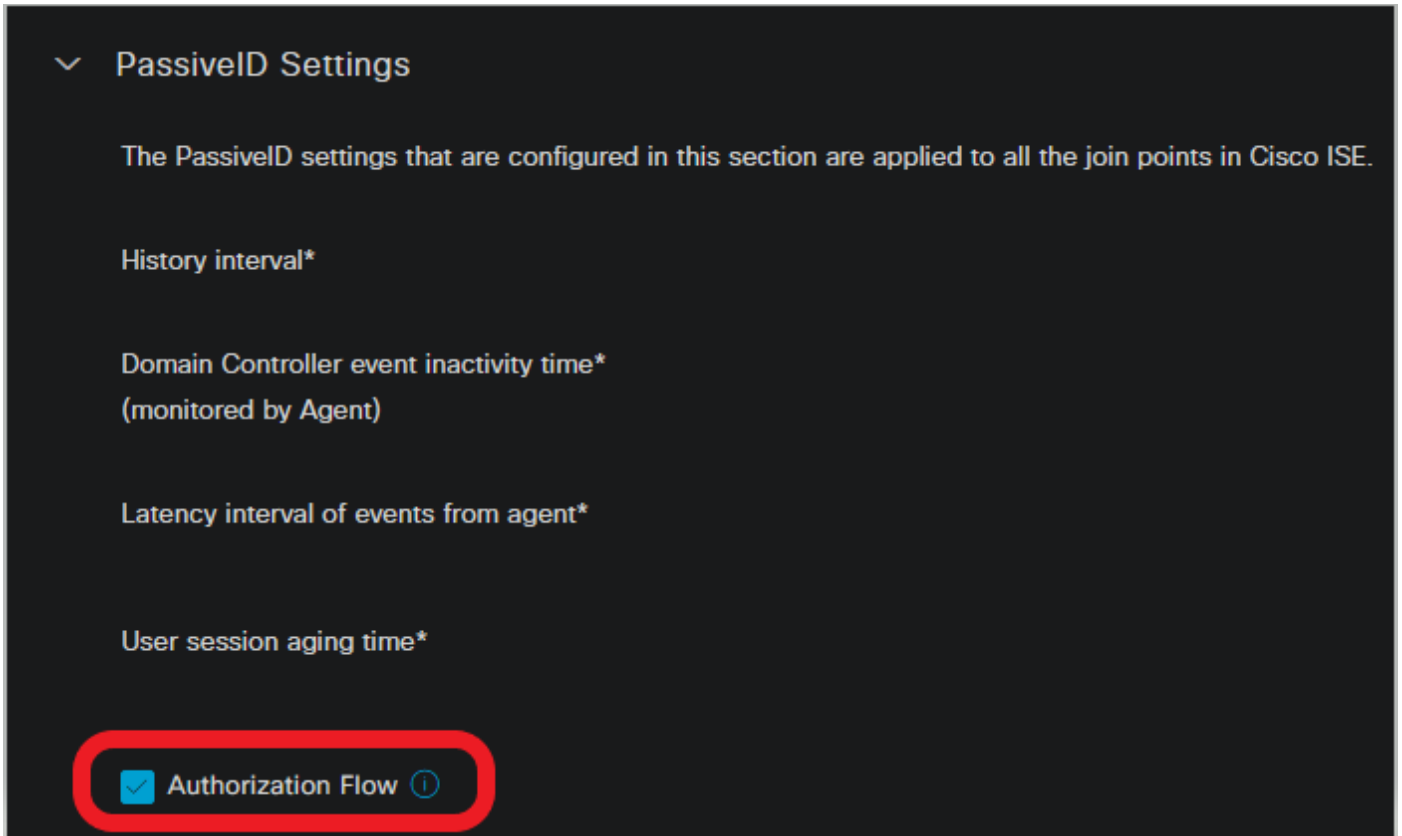


Diagrama de fluxo


Configurações

Habilitar o fluxo de autorização:

Navegue até [Active Directory > Advanced Settings > PassiveID Settings](#) e verifique a [Authorization Flow](#) para configurar políticas de autorização para usuários de login PassiveID. Essa opção está desativada por padrão.



Habilitar o fluxo de autorização

 Observação: para que esse recurso funcione, certifique-se de executar os serviços PassiveID, PxGrid e SXP em sua implantação. Você pode verificar isso em [Administration > System > Deployment](#).

Configuração do conjunto de políticas:

1. Criar um conjunto de políticas separado para PassiveID (recomendado).
2. Para Condições, use o atributo `PassiveID:PassiveID_Provider` e selecione o tipo de provedor.

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		


Conjuntos de políticas

3. Configure as regras de Autorização para o Conjunto de Políticas criado na Etapa 1.

- Crie uma condição para cada regra e use o dicionário PassiveID com base em grupos do AD, Nomes de usuário ou Ambos.
- Atribua uma Tag de grupo de segurança para cada regra e salve as configurações.

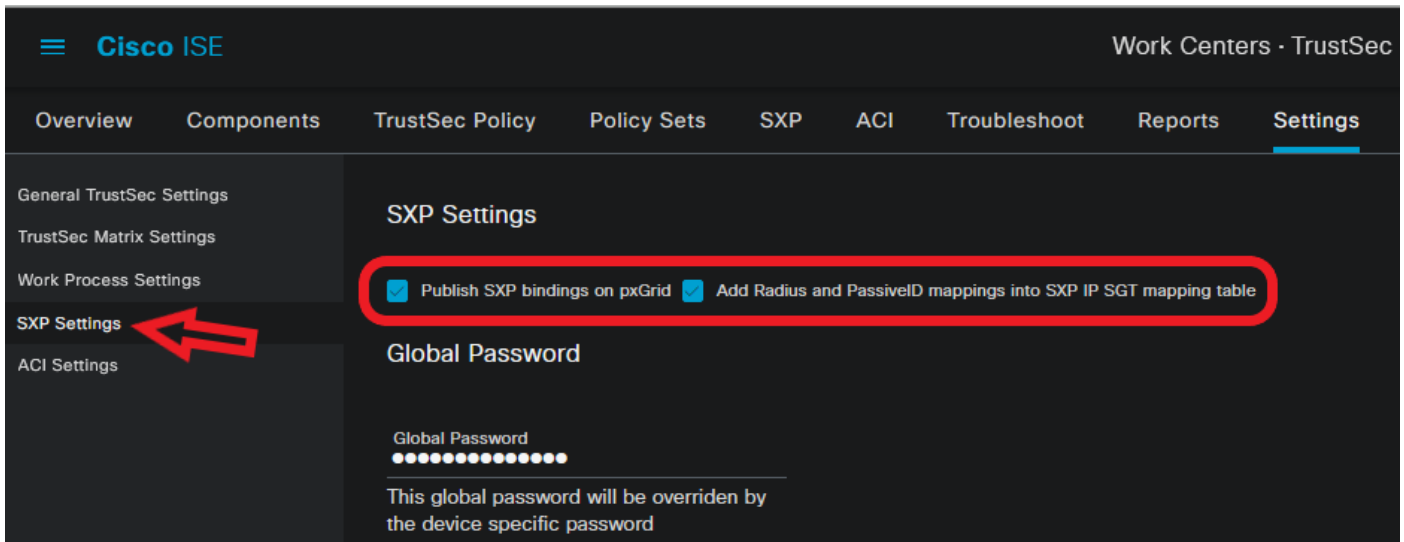
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Employees	PassiveID-PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Users	PermitAccess	Employees	3	
✓	Domain Admins	PassiveID-PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Admins	Admin access	Admin_Team	2	
✓	Default		DenyAccess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

Política de Autorização

 Observação: a política de autenticação é irrelevante, pois não é usada nesse fluxo.

 Observação: você pode usar `PassiveID_Username`, `PassiveID_Groups`, Or `PassiveID_Provider` atributos para criar as regras de autorização.

4. Navegue até **Work Centers > TrustSec > Settings > SXP Settings** para permitir **Publish SXP bindings on pxGrid** e **Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table** para compartilhar mapeamentos PassiveID com assinantes PxGrid e incluí-los na tabela de mapeamentos SXP no ISE.



Configurações do SXP

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verificação do ISE

Depois que os eventos de login do usuário tiverem sido enviados ao ISE por um provedor, como o WMI ou o Agente AD DC (Controladores de Domínio do Active Directory), continue para verificar os logs ao vivo. Navegue até **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	

LiveLogs do Radius

Clique no ícone de lupa na coluna Detalhes para exibir um relatório detalhado de um usuário, neste exemplo, smith (Usuários do domínio), como mostrado aqui.

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

 : eventos PassiveID de um provedor de API não podem ser publicados em pares SXP. No entanto, os detalhes de SGT desses usuários podem ser publicados por meio do pxGrid.

Verificação de assinante do PxGrid

Este snippet CLI verifica se o FMC aprendeu os mapeamentos IP-SGT para as sessões PassiveID mencionadas anteriormente do ISE.

```
admin@fmc:~$ sudo su
root@fmc:/Volume/home/admin# uip_reader -f sxp_log_entries.1 -b

current set of sxp bindings
ipPrefix 10.10.10.10, tag 4
*****
ipPrefix 10.10.10.20, tag 16
*****
ipPrefix 10.10.10.104, tag 2
*****
root@fmc:/Volume/home/admin#
```

Verificação de FMC CLI

Verificação de mesmo nível TrustSec SXP

O switch aprendeu os mapeamentos de IP-SGT para sessões PassiveID do ISE, como visto neste trecho da CLI.

sw-3850#sho cts sxp connections brief

SXP: Enabled
Default Source IP: 10.10.10.104

Peer_IP	Source_IP	Conn Status	Duration
10.10.10.135	10.10.10.104	On(Speaker)::On(Listener)	0:01:29:19

sw-3850#sho cts role-based sgt-map all ipv4 details


Active IPv4-SGT Bindings Information

IP Address	Security Group	Source
10.10.10.104	2:TrustSec Devices	INTERNAL
10.10.10.10	4:Employees	SXP
10.10.10.20	16:Admin_Team	SXP

IP-SGT Active Bindings Summary

=====
Total number of SXP bindings = 2
Total number of INTERNAL bindings = 1
Total number of active bindings = 3

Verificação CLI do switch

 Observação: a configuração do switch para AAA e TrustSec está fora do escopo deste documento. Verifique o [Cisco TrustSec Guide](#) para obter as configurações relacionadas.

Troubleshooting


Esta seção disponibiliza informações para a solução de problemas de configuração.

Habilitar depurações no ISE

Navegue até **Administration > System > Logging > Debug Log Configuration** para definir os próximos componentes para o nível especificado.

Nó	Nome do componente	Nível de log	Nome do arquivo de log
----	--------------------	--------------	------------------------

IDpassiva	passiveid	Rastrear	passiveid-*.log
PxGrid	pxgrid	Rastrear	pxgrid-server.log
SXP	sxp	Debug	sxp.log

 Observação: ao concluir a solução de problemas, lembre-se de redefinir as depurações, selecionar o nó relacionado e clicar em **Reset to Default**.

Registra trechos

1. O ISE recebe eventos de login do provedor:

Arquivo Passiveid-*.log:

```
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 ,
```

Arquivo Passiveid-*.log

2. O ISE atribui SGT de acordo com a política de autorização configurada e publica o mapeamento IP-SGT para usuários PassiveID para assinantes PxGrid e pares SXP:

arquivo sxp.log:

```
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]
```

arquivo sxp.log

arquivo pxgrid-server.log:

```
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}
```

arquivo pxgrid-server.log

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.