

Configurazione di ISE 3.2 per l'assegnazione dei tag del gruppo di sicurezza per le sessioni PassiveID

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Diagramma di flusso](#)

[Configurazioni](#)

[Verifica](#)

[Verifica ISE](#)

[Verifica Sottoscrittore PxGrid](#)

[Verifica peer TrustSec SXP](#)

[Risoluzione dei problemi](#)

[Abilita debug su ISE](#)

[Registra frammenti](#)

Introduzione

In questo documento viene descritto come configurare e assegnare i tag SGT (Security Group Tags) alle sessioni di ID passivo tramite i criteri di autorizzazione in ISE 3.2.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ISE 3.2
- ID passivo, TrustSec e PxGrid

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE 3.2
- FMC 7.0.1
- WS-C3850-24P con versione 16.12.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco Identity Services Engine (ISE) 3.2 è la versione minima che supporta questa funzionalità. Questo documento non descrive la configurazione di PassiveID, PxGrid e SXP. Per informazioni correlate, consultare la [Guida dell'amministratore](#).

In ISE 3.1 o versioni precedenti, un tag SGT (Security Group Tag) può essere assegnato solo alla sessione Radius o all'autenticazione attiva, come 802.1x e MAB. Con ISE 3.2 è possibile configurare i criteri di autorizzazione per le sessioni di ID passivo in modo che, quando Identity Services Engine (ISE) riceve eventi di accesso utente da un provider quale WMI o agente AD Controller di dominio Active Directory, assegni un tag del gruppo di sicurezza (SGT) alla sessione di ID passivo in base all'appartenenza al gruppo di Active Directory (AD) dell'utente. I dettagli del mapping IP-SGT e del gruppo AD per l'ID passivo possono essere pubblicati nel dominio TrustSec tramite il protocollo SGT Exchange Protocol (SXP) e/o agli abbonati Platform Exchange Grid (pxGrid), ad esempio Cisco Firepower Management Center (FMC) e Cisco Secure Network Analytics (Stealthwatch).

Configurazione

Diagramma di flusso

PassiveID Authorization Flow Diagram

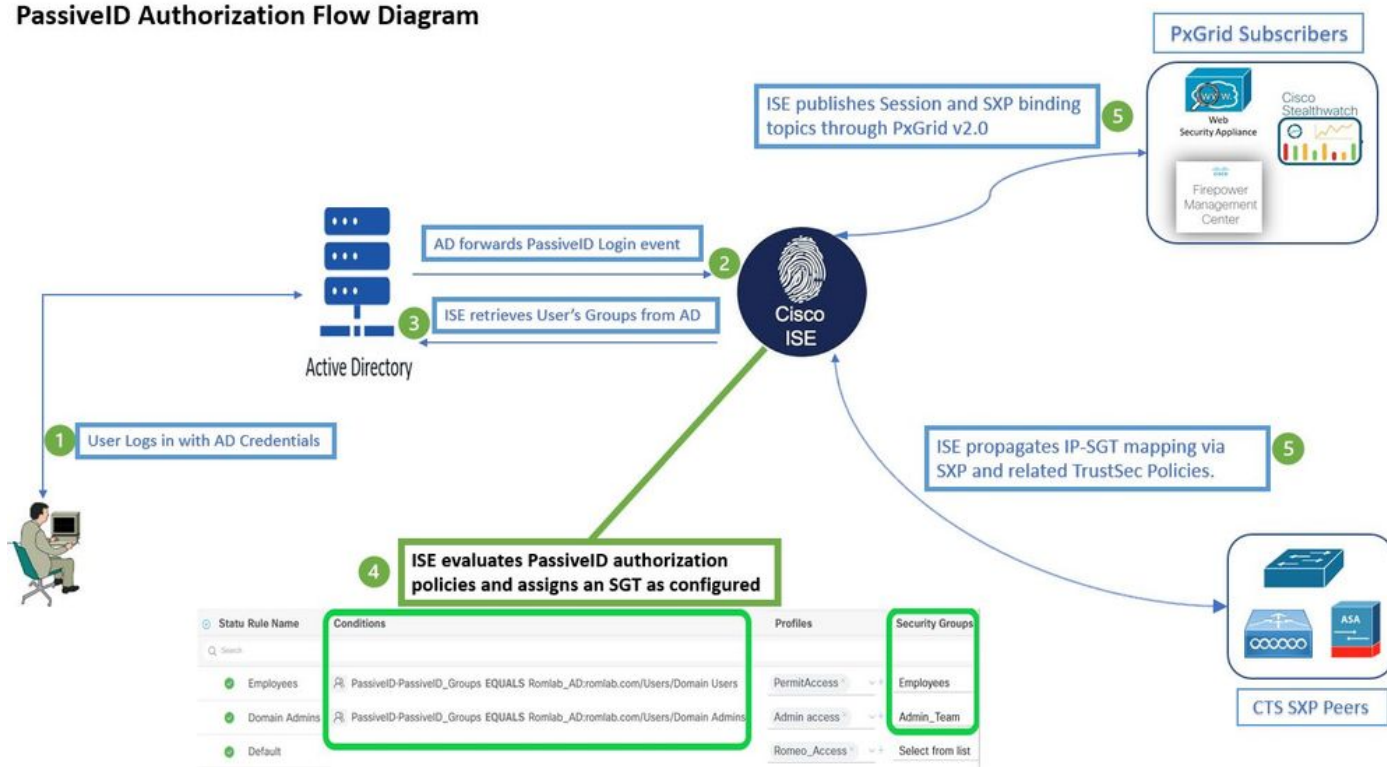


Diagramma di flusso

Configurazioni

Abilitare il flusso di autorizzazione:

Passa a **Active Directory > Advanced Settings > PassiveID Settings** e controllare la **Authorization Flow** per configurare i criteri di autorizzazione per gli utenti di accesso con ID passivo. Questa opzione è disattivata per impostazione predefinita.

PassiveID Settings

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

History interval*


Domain Controller event inactivity time*
(monitored by Agent)

Latency interval of events from agent*

User session aging time*

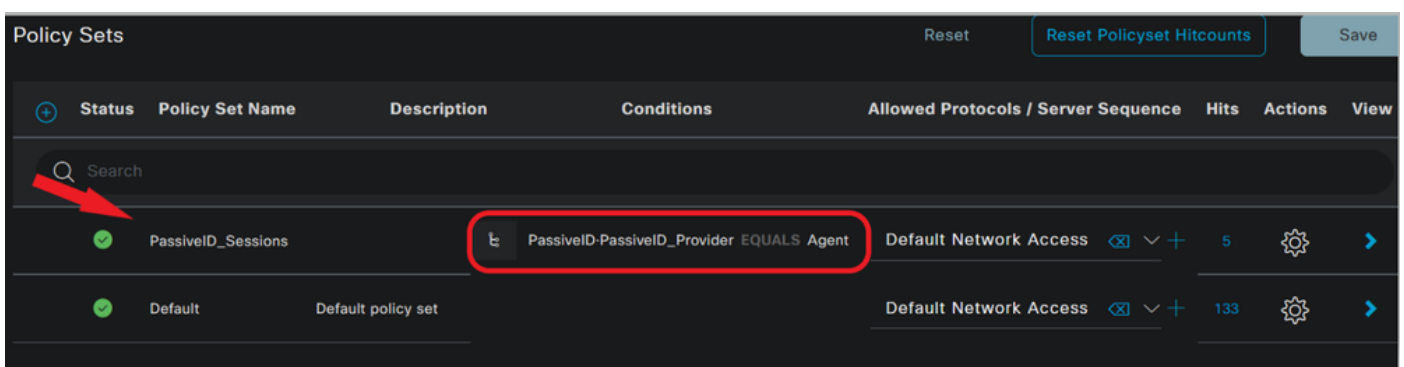
Authorization Flow ⓘ

Abilita il flusso di autorizzazione

 Nota: per il corretto funzionamento di questa funzionalità, assicurarsi di eseguire i servizi PassiveID, PxGrid e SXP nella distribuzione. È possibile verificare questa condizione in **Administration > System > Deployment**.

Configurazione set di criteri:

1. Creare un set di criteri separato per l'ID passivo (scelta consigliata).
2. Per Condizioni, utilizzare l'attributo `PassiveID-PassiveID_Provider` e selezionare il tipo di provider.



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	⚙️	➔

Set di criteri

3. Configurare le regole di autorizzazione per il set di criteri creato nel passaggio 1.
- Creare una condizione per ogni regola e utilizzare il dizionario ID passivo basato su gruppi AD, nomi utente o entrambi.

- Assegnare un tag del gruppo di sicurezza per ogni regola e salvare le configurazioni.

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

Criteri di autorizzazione

Nota: i criteri di autenticazione non sono rilevanti in quanto non vengono utilizzati in questo flusso.

Nota: è possibile utilizzare `PassiveID_Username`, `PassiveID_Groups`, o `PassiveID_Provider` attributi per creare le regole di autorizzazione.

4. Passare a **Work Centers > TrustSec > Settings > SXP Settings** per attivare **Publish SXP bindings on pxGrid** e **Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table** per condividere i mapping PassiveID con gli abbonati PxGrid e includerli nella tabella dei mapping SXP su ISE.

SXP Settings

- Publish SXP bindings on pxGrid
- Add Radius and PassiveID mappings into SXP IP SGT mapping table

Global Password

Global Password
●●●●●●●●●●

This global password will be overridden by the device specific password

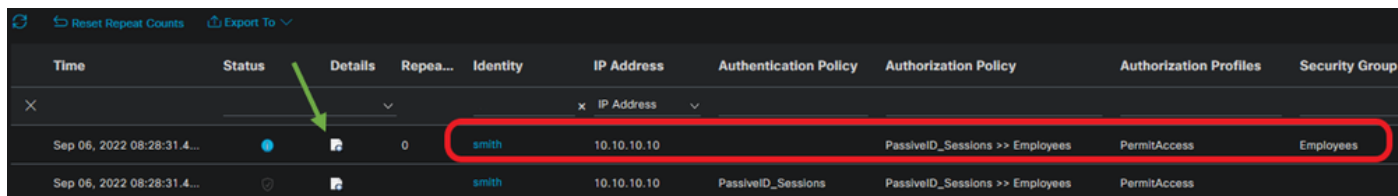
Impostazioni SXP

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Verifica ISE

Dopo aver inviato gli eventi di accesso utente ad ISE da un provider quale WMI o agente AD Controller di dominio Active Directory, procedere alla verifica dei Live Log. Passa a **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	

LiveLog Radius

Fare clic sull'icona della lente di ingrandimento nella colonna Dettagli per visualizzare un report dettagliato per un utente, in questo esempio smith (Domain Users) come illustrato di seguito.

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

 : gli eventi PassiveID di un provider API non possono essere pubblicati nei peer SXP. Tuttavia, i dettagli SGT di questi utenti possono essere pubblicati attraverso pxGrid.

Verifica Sottoscrittore PxGrid

Questo frammento della CLI verifica che la FMC abbia appreso da ISE i mapping IP-SGT per le sessioni PassiveID precedentemente menzionate.

```
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#
```

Verifica CLI FMC

Verifica peer TrustSec SXP

Lo switch ha appreso i mapping IP-SGT per le sessioni PassiveID da ISE, come mostrato in questo estratto della 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

Verifica della CLI dello switch

 Nota: la configurazione dello switch per AAA e TrustSec non rientra nell'ambito di questo documento. Per le configurazioni correlate, consultare la [Cisco TrustSec Guide](#).


Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Abilita debug su ISE

Passa a **Administration > System > Logging > Debug Log Configuration** per impostare i componenti successivi al livello specificato.

Nodo	Nome componente	Livello log	Nome file di log
ID passivo	passiveid	Traccia	passiveid-*.log
PxGrid	pxgrid	Traccia	pxgrid-server.log
SXP	sxp	Debug	log.sxp

 Nota: al termine della risoluzione dei problemi, ripristinare i debug e selezionare il nodo correlato e fare clic su **Reset to Default**.

Registra frammenti

1. ISE riceve eventi di accesso dal fornitore:

File 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 ,

```

File Passiveid-*.log

2. ISE assegna il SGT in base ai criteri di autorizzazione configurati e pubblica il mapping IP-SGT per gli utenti di ID passivi agli abbonati PxGrid e ai peer SXP:

file 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]
```

file sxp.log

file 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}
```

file pxgrid-server.log

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).