Konfigurieren von ISE 3.2 zum Zuweisen von Sicherheitsgruppen-Tags für PassiveID-Sitzungen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sicherheitsgruppen-Tags (SGTs) konfiguriert und passiven ID-Sitzungen über Autorisierungsrichtlinien in ISE 3.2 zugewiesen werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco ISE 3.2
- Passive ID, TrustSec und PxGrid

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE 3.2
- FMC 7.0.1
- WS-C3850-24P mit 16.12.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

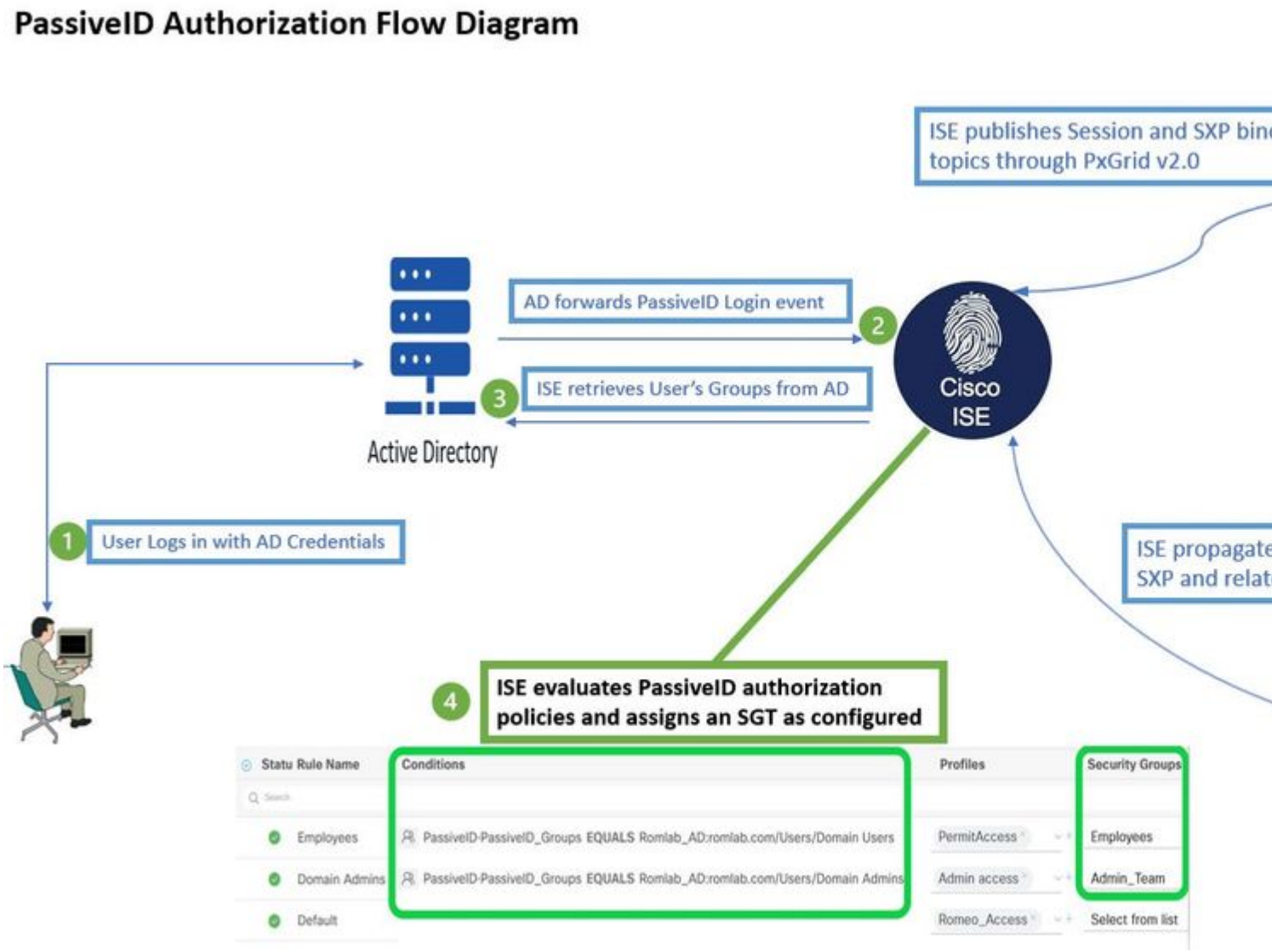
Hintergrundinformationen

Die Cisco Identity Services Engine (ISE) 3.2 ist die Mindestversion, die diese Funktion unterstützt. In diesem Dokument wird nicht auf die Konfiguration von PassiveID, PxGrid und SXP eingegangen. Weitere Informationen finden Sie im Administratorhandbuch.

In ISE 3.1 oder älteren Versionen kann ein Security Group Tag (SGT) nur einer Radius-Sitzung oder einer aktiven Authentifizierung (z. B. 802.1x und MAB) zugewiesen werden. Mit ISE 3.2 können Autorisierungsrichtlinien für PassiveID-Sitzungen konfiguriert werden. Wenn Identity Services Engine (ISE) Benutzeranmeldeereignisse von einem Anbieter wie Active Directory Domain Controllers (AD DC) WMI oder AD Agent empfängt, weist sie der PassiveID-Sitzung ein Security Group Tag (SGT) zu, das auf der Active Directory-Gruppenmitgliedschaft des Benutzers basiert. Die IP-SGT-Zuordnung und die AD-Gruppendetails für die PassiveID können über das SGT Exchange Protocol (SXP) und/oder an Abonnenten von Platform Exchange Grid (pxGrid) wie Cisco FirePOWER MANAGEMENT CENTER (FMC) und Cisco Secure Network Analytics (Stealthwatch) in der TrustSec-Domäne veröffentlicht werden.

Konfigurieren

Flussdiagramm

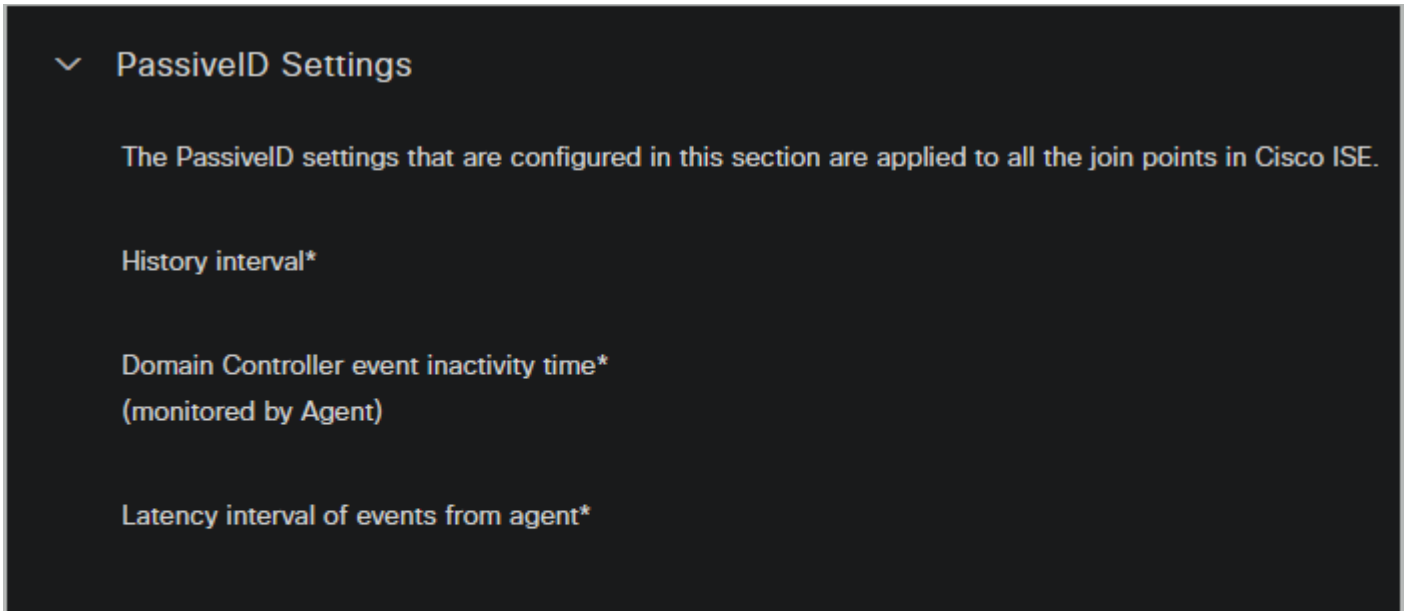


Flussdiagramm

Konfigurationen

Autorisierungsablauf aktivieren:

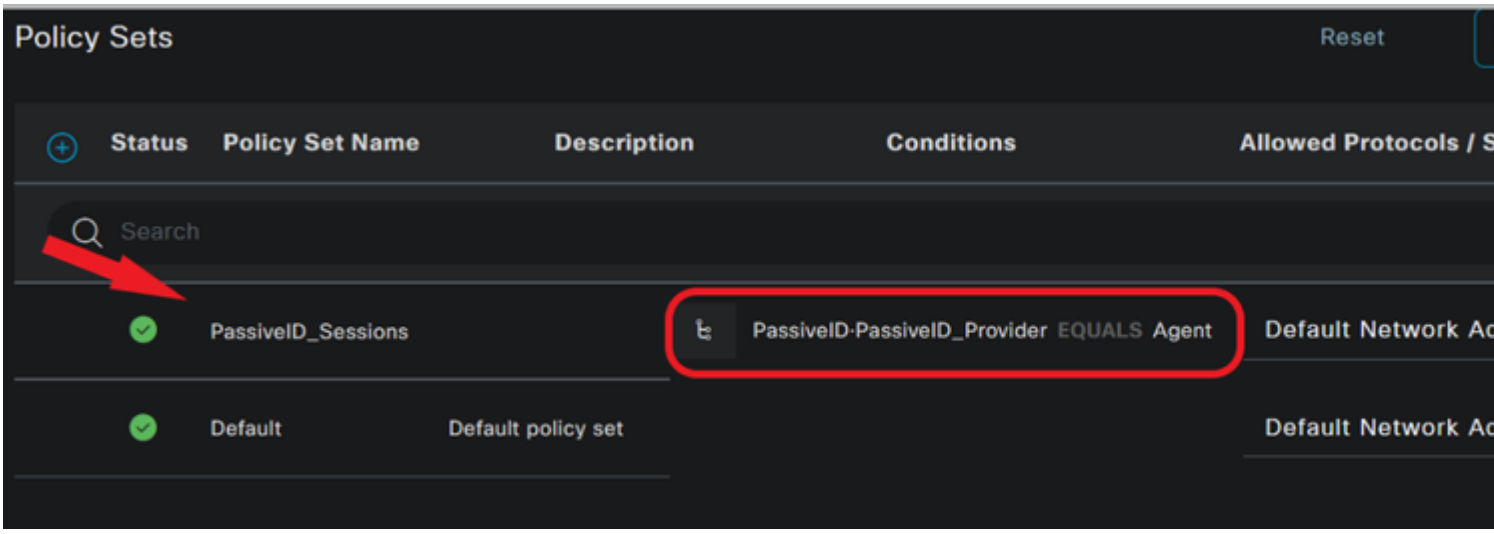
Navigieren Sie zu **Active Directory >â€¯Advanced Settings > PassiveID Settings** und überprüfen Sie **Authorization Flow** Kontrollkästchen, um Autorisierungsrichtlinien für Benutzer mit PassiveID-Anmeldung zu konfigurieren. Diese Option ist standardmäßig deaktiviert.



: Damit diese Funktion funktioniert, stellen Sie sicher, dass Sie PassiveID-, PxGrid- und SXP-Dienste in Ihrer Bereitstellung ausführen. Sie können dies überprüfen unter **Administration** > **System** > **Deployment** .

Policy Set-Konfiguration:

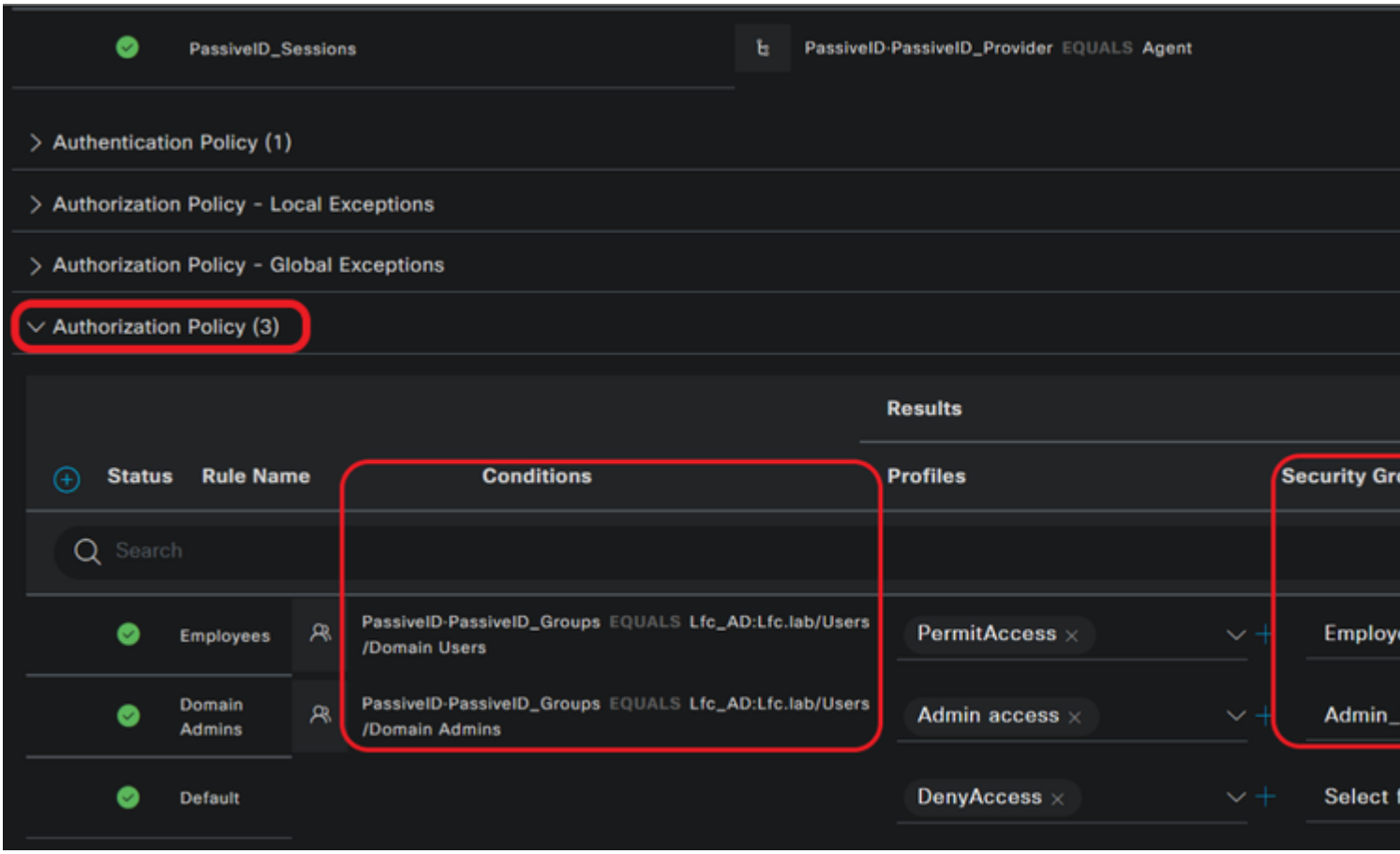
1. Erstellen Sie einen separaten Policy Set für PassiveID (empfohlen).
2. Verwenden Sie unter Bedingungen das Attribut **PassiveID·PassiveID_Provider** und wählen Sie den Anbietertyp aus.



Policy Sets

3. Autorisierungsregeln für den in Schritt 1 erstellten Richtliniensatz konfigurieren

- Erstellen Sie eine Bedingung für jede Regel, und verwenden Sie das Dictionary PassiveID auf der Grundlage von AD-Gruppen, Benutzernamen oder Beide.
- Weisen Sie jeder Regel eine Sicherheitsgruppen-Tag zu, und speichern Sie die Konfigurationen.



Autorisierungsrichtlinie

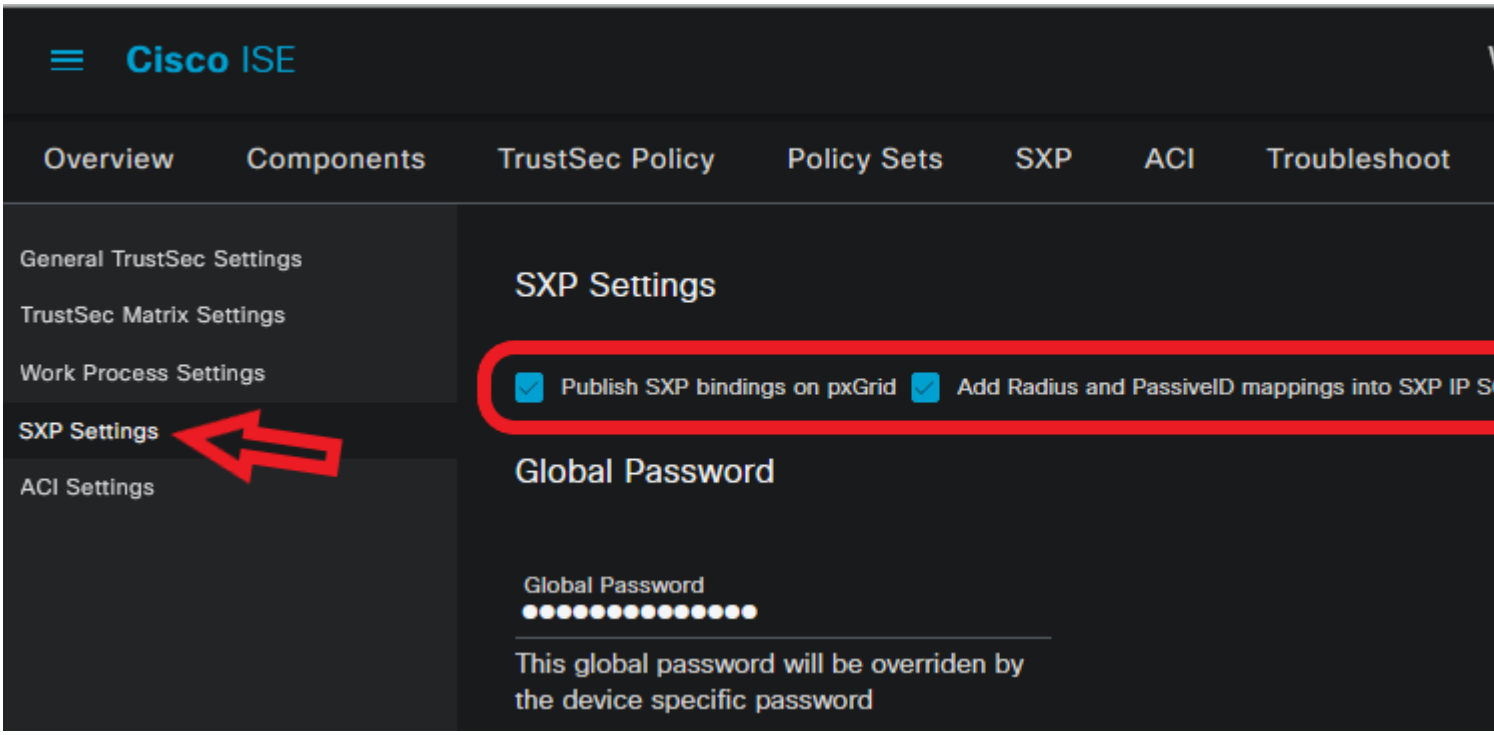
Hinweis: Die Authentifizierungsrichtlinie ist irrelevant, da sie in diesem Fluss nicht verwendet wird.

Hinweis: Sie können **PassiveID_Username, PassiveID_Groups**,Oder **PassiveID_Provider** -Attribute, um die Autorisierungsregeln zu erstellen.

---

4. Navigieren Sie zu **Work Centers > TrustSec > Settings > SXP Settings** aktivieren **Publish SXP bindings on pxGrid** und

um PassiveID-Zuordnungen mit PxGrid-Abonnenten gemeinsam zu nutzen und sie in die SXP-Zuordnungstabelle auf der ISE aufzunehmen.



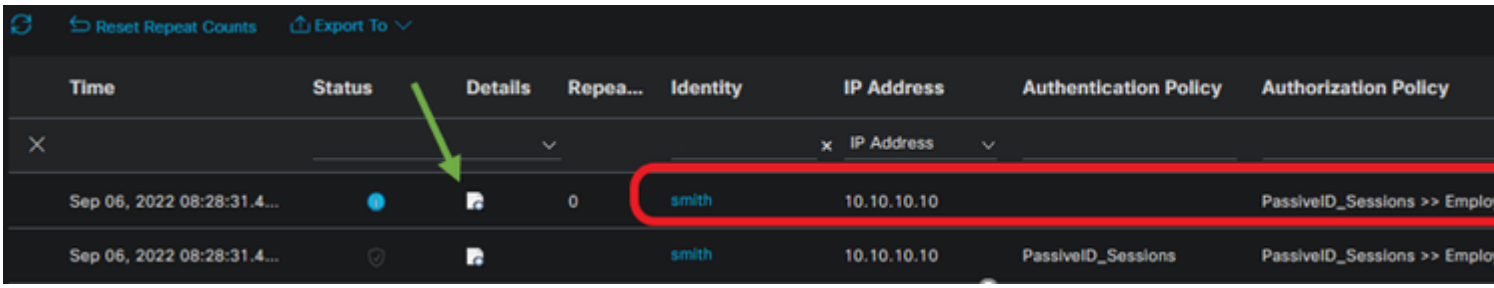
SXP-Einstellungen

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

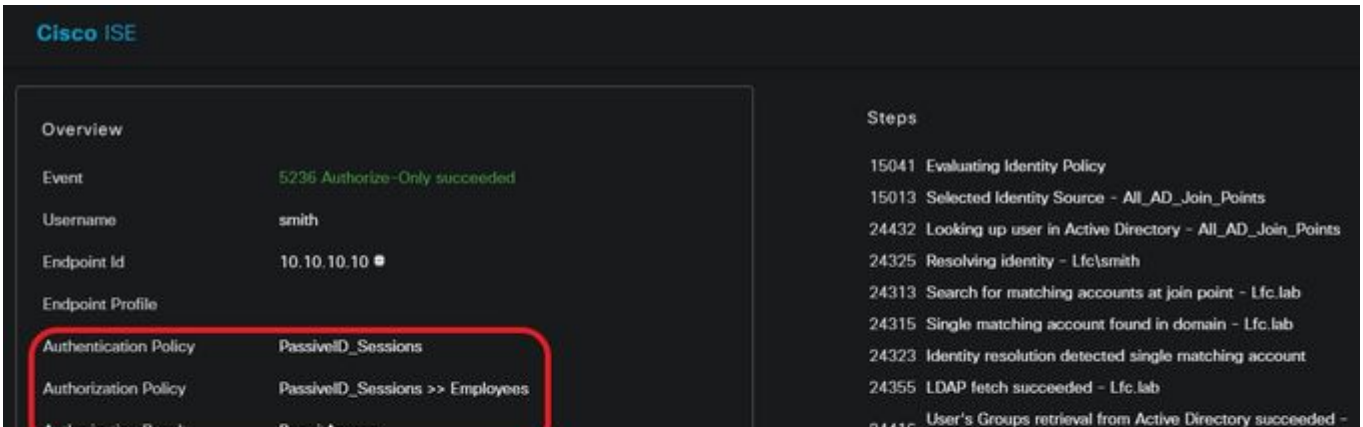
ISE-Verifizierung

Sobald die Benutzeranmeldeereignisse von einem Anbieter wie Active Directory Domain Controllers (AD DC) WMI oder AD Agent an die ISE gesendet wurden, fahren Sie mit der Überprüfung der Live-Protokolle fort. Navigieren Sie zu **Operations** > **Radius** > **Live Logs**.



Radius-LiveProtokolle

Klicken Sie in der Spalte Details auf das Lupensymbol, um einen detaillierten Bericht für einen Benutzer anzuzeigen, in diesem Beispiel Smith (Domain Users), wie hier gezeigt.



: PassiveID-Ereignisse von einem API-Anbieter können nicht auf SXP-Peers veröffentlicht werden. Die SGT-Details dieser Benutzer können jedoch über pxGrid veröffentlicht werden.

PxGrid-Teilnehmerverifizierung

Dieser CLI-Ausschnitt überprüft, ob das FMC die IP-SGT-Zuordnungen für die zuvor erwähnten PassiveID-Sitzungen von der ISE erhalten hat.

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

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#
```

FMC CLI-Verifizierung

TrustSec SXP-Peer-Überprüfung

Der Switch hat die IP-SGT-Zuordnungen für PassiveID-Sitzungen von der ISE gelernt (siehe CLI-Auszug).

```
sw-3850#sho cts sxp connections brief
 SXP: Enabled
Default Source IP: 10.10.10.104
-------------------------------------------------------------------------------
   Peer_IP            Source_IP            Conn Status          Du
-------------------------------------------------------------------------------
10.10.10.135        10.10.10.104   On(Speaker)::On(Listener)    0:

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
```

: Die Switch-Konfiguration für AAA und TrustSec wird in diesem Dokument nicht behandelt. Informationen zu den entsprechenden Konfigurationen finden Sie im Cisco TrustSec-Leitfaden.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Debuggen auf ISE aktivieren

Navigieren Sie zu **Administration > System > Logging > Debug Log Configuration** , um die nächsten Komponenten auf die angegebene Ebene zu setzen.

Knoten	Komponentenname	Protokollstufe	Protokolldateiname
PassiveID	passiv	Nachverfolgung	passiveid-*.log
PxGrid	pxgrid	Nachverfolgung	pxgrid-server.log
SXP	SXP	Fehlersuche	sxp.log

Hinweis: Wenn Sie mit der Fehlerbehebung fertig sind, denken Sie daran, die Fehlerbehebungen zurückzusetzen, den zugehörigen Knoten auszuwählen und auf zu klicken. **Reset to Default.**

Protokolle Ausschnitte

1. ISE empfängt Anmeldeereignisse vom Anbieter:

Passiveid-*.log-Datei:

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

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

2022-09-06 20:28:31,309 DEBUG  [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Build
published to session directory.
2022-09-06 20:28:31,309 DEBUG  [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- retrie
information from Active Directory.

2022-09-06 20:28:31,326 DEBUG  [Grizzly-worker(26)][[]] com.cisco.idc.agent-probe- Forw
session directory. Identity Mapping.id-src-first-port = -1 , Identity Mapping.dc-domainnam
Mapping.id-src-port-start = -1 , Identity Mapping.probe = Agent , Identity Mapping.id-src-p
Mapping.event-user-name = smith , Identity Mapping.dc-host = /10.10.10.132 , Identity M
Identity Mapping.server = ise-3-2 , Identity Mapping.event-ip-address = 10.10.10.10 ,
```

Passiveid-.log-Datei*

2. Die ISE weist der konfigurierten Autorisierungsrichtlinie ein SGT zu und veröffentlicht die IP-SGT-Zuordnung für PassiveID-Benutzer für PxGrid-Abonnenten und SXP-Peers:

sxp.log-Datei:

```
2022-09-06 20:28:31,587 DEBUG [sxpservice-http-96443] cisco.ise.sxp.rest.SxpGlueRe
binding tag=4, ip=10.10.10.10, vns=[], vpns=[null] nasIp=10.10.10.132
2022-09-06 20:28:31,587 DEBUG [sxpservice-http-96443] cisco.ise.sxp.rest.SxpGlueRe
created for ip address : 10.10.10.10/32

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

2022-09-06 20:28:31,613 DEBUG [SxpNotificationSerializer-Thread] cisco.cpm.sxp.eng
session binding RestSxpLocalBinding(tag=4, groupName=null, ipAddress=10.10.10.1
sessionId=cf0d2acd-0d3d-413b-b2fb-6860df3f0d84, peerSequence=null, sxpBindingOp
sessionExpiryTimeInMillis=-1, apic=false, routable=true, vns=[DEFAULT_VN]) to VPNs [
```

sxp.log-Datei

pxgrid-server.log-Datei:

```
2022-09-06 20:28:31,693 TRACE  [Grizzly(1)][[]] cpm.pxgrid.ws.client.WsEndpoint -::::- Send, se
```