配置ISE 3.2為PassiveID會話分配安全組標籤

目錄

簡介

本文檔介紹如何通過ISE 3.2中的授權策略配置安全組標籤(SGT)並將其分配給被動ID會話。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ISE 3.2
- 被動ID、TrustSec和PxGrid

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE 3.2
- FMC 7.0.1
- 運行16.12.1的WS-C3850-24P

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

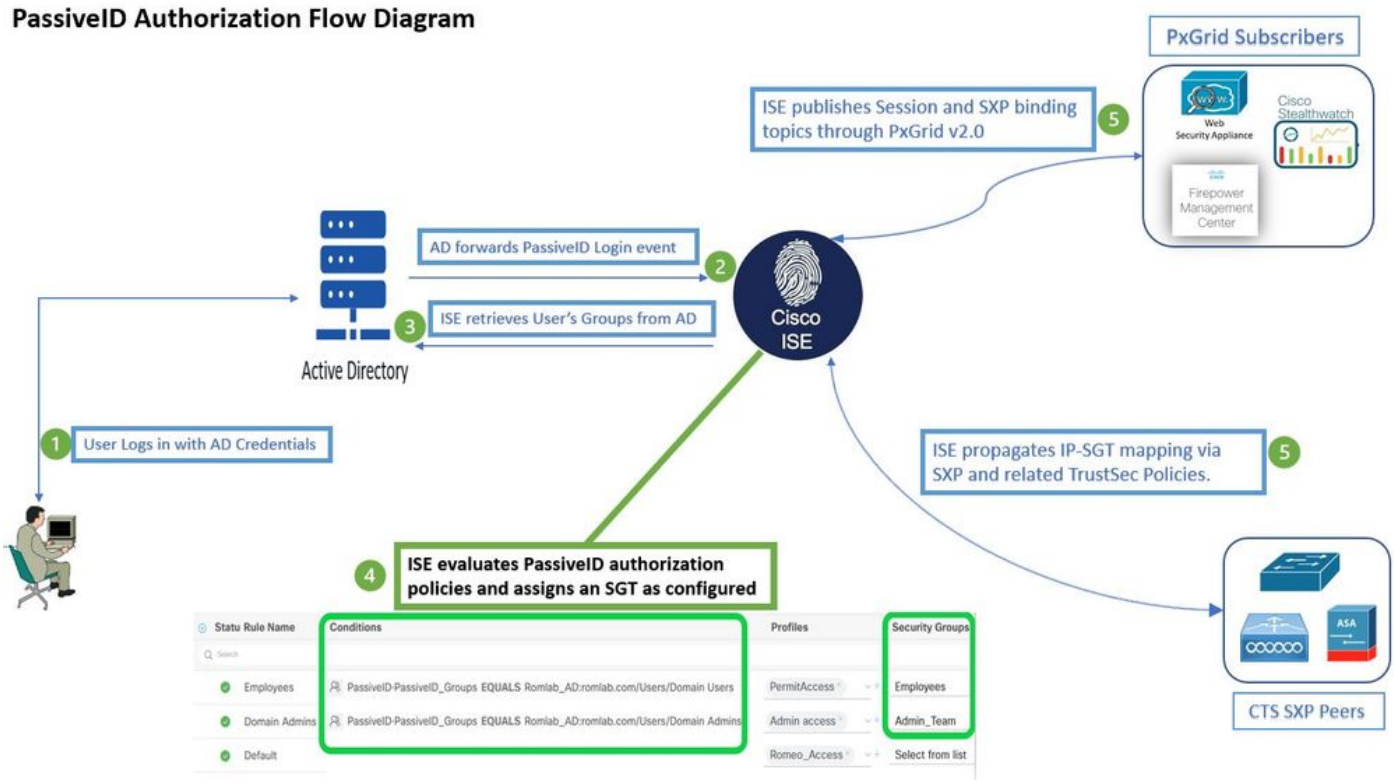
背景資訊

思科身份服務引擎(ISE)3.2是支援此功能的最低版本。 本文檔不涉及PassiveID、PxGrid和SXP配置。有關相關資訊，請參閱管理員指南。

在ISE 3.1或更舊版本中，安全組標籤(SGT)只能分配給Radius會話或主動身份驗證（例如802.1x和MAB）。在ISE 3.2中，我們可以為PassiveID會話配置授權策略，以便當身份服務引擎(ISE)從提供商(例如Active Directory域控制器(AD DC)WMI或AD代理)接收使用者登入事件時，它基於使用者Active Directory(AD)組成員身份向PassiveID會話分配安全組標籤(SGT)。PassiveID的IP-SGT對映和AD組詳細資訊可以通過SGT交換協定(SXP)發佈到TrustSec域和/或發佈到Platform Exchange Grid(pxGrid)使用者，例如Cisco Firepower管理中心(FMC)和Cisco Secure Network Analytics(Stealthwatch)。

設定

流程圖

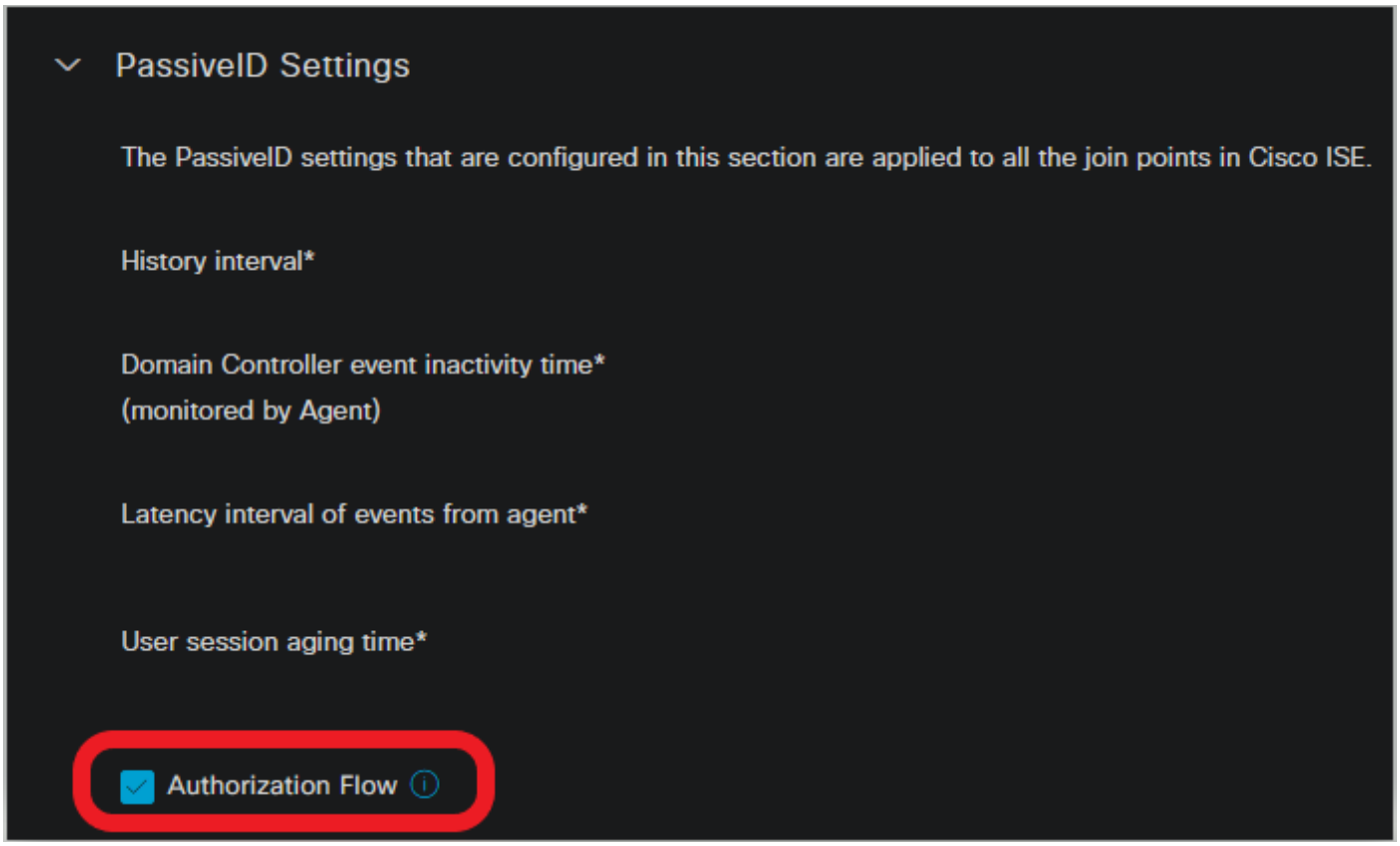


流程圖

組態

啟用授權流：

導航至 **Active Directory > Advanced Settings > PassiveID Settings** 並檢查 **Authorization Flow** 覈取方塊，以便為PassiveID登入使用者配置授權策略。預設情況下，此選項處於禁用狀態。

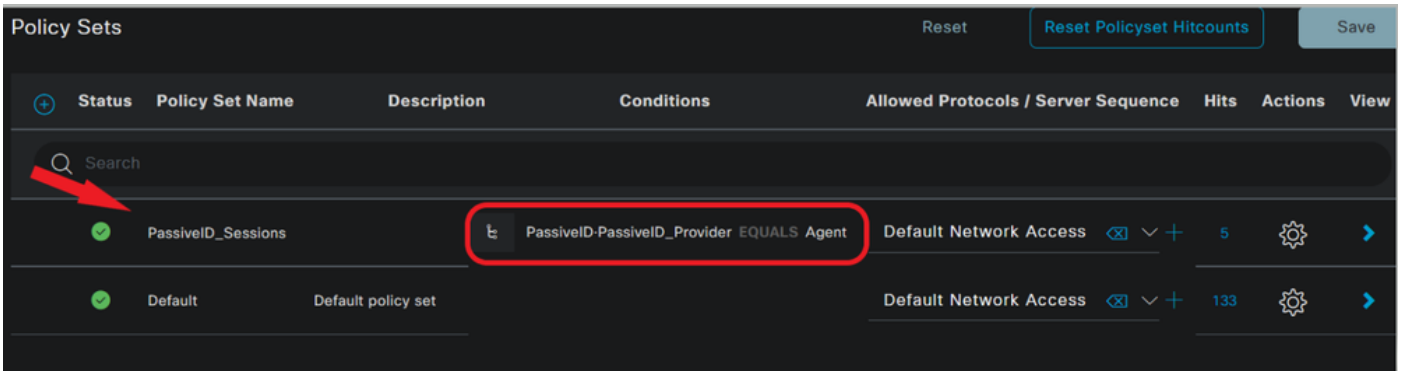


啟用授權流

註：要使用此功能，請確保在部署中運行PassiveID、PxGrid和SXP服務。您可以在以下位置驗證這一點 **Administration > System > Deployment** .

策略集配置：

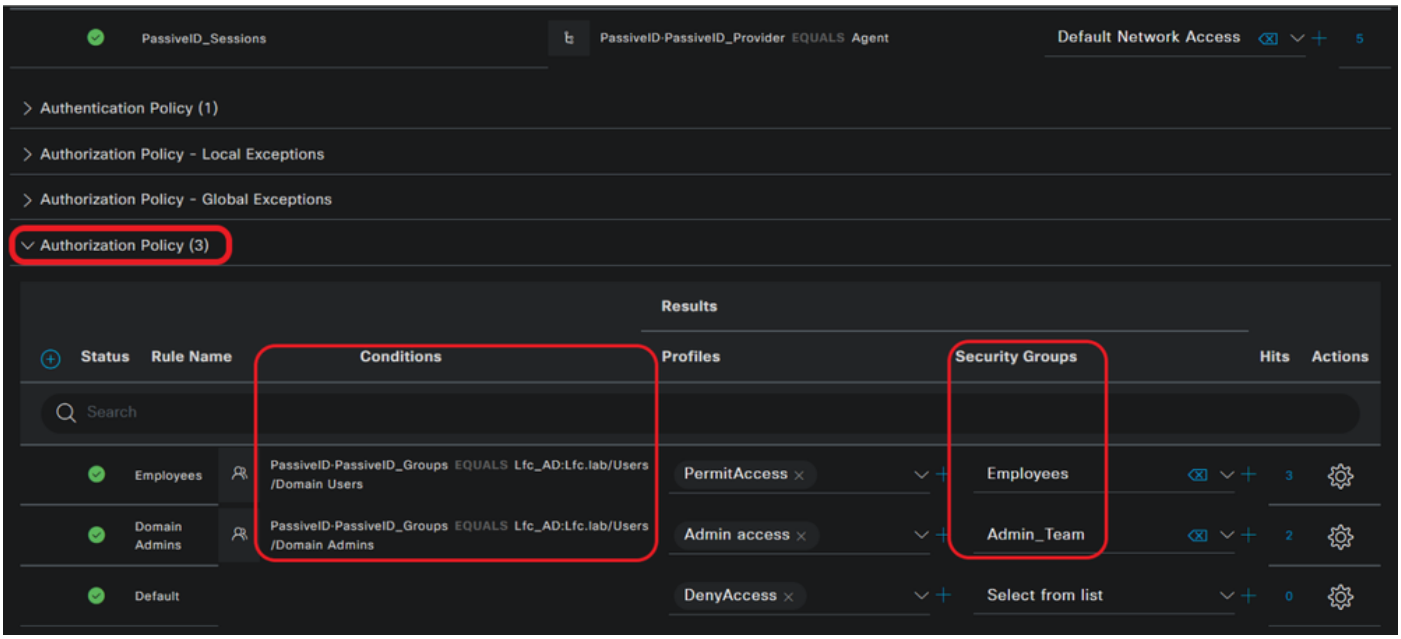
1. 為PassiveID建立單獨的策略集（推薦）。
2. 對於條件，請使用屬性 **PassiveID·PassiveID_Provider** 並選擇提供商型別。



策略集

3. 為步驟1中建立的策略集配置授權規則。

- 為每個規則建立一個條件，並基於AD組、使用者名稱或兩者使用PassiveID字典。
- 為每個規則分配一個安全組標籤並儲存配置。

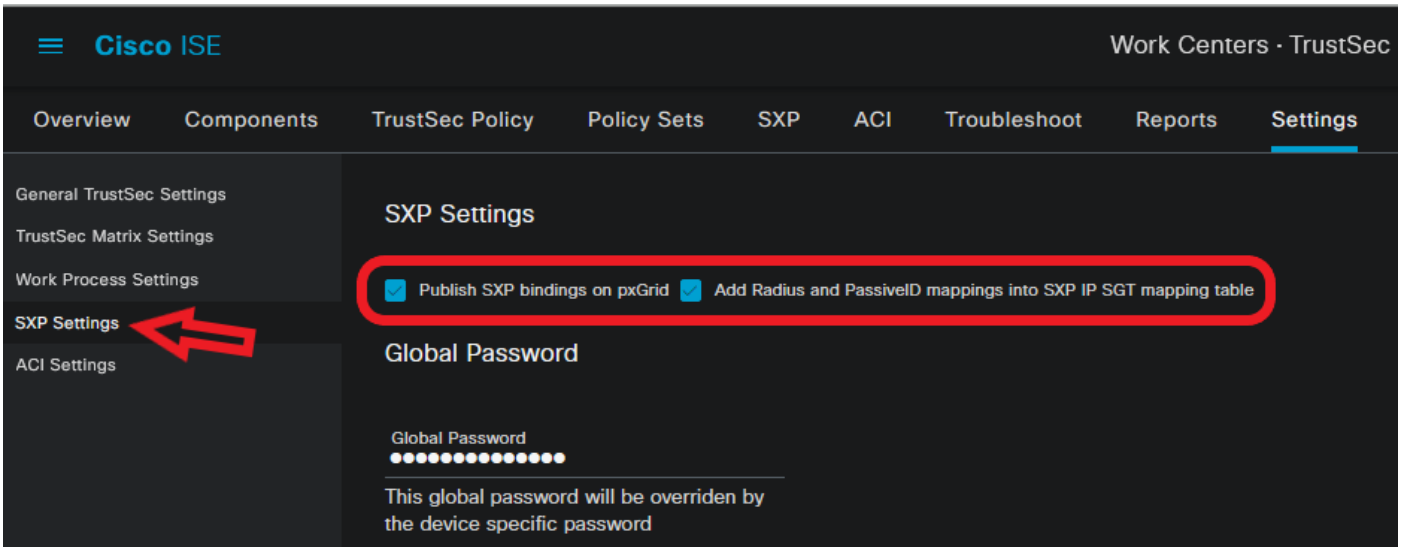


授權策略

注意：身份驗證策略不相關，因為它未在此流中使用。

註：您可以 **PassiveID_Username, PassiveID_Groups,**或 **PassiveID_Provider** 屬性來建立授權規則。

4.導航至 **Work Centers > TrustSec > Settings > SXP Settings** 啟用 **Publish SXP bindings on pxGrid** 和 **Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table** 與PxGrid使用者共用PassiveID對映，並將它們包括在ISE上的SXP對映表中。



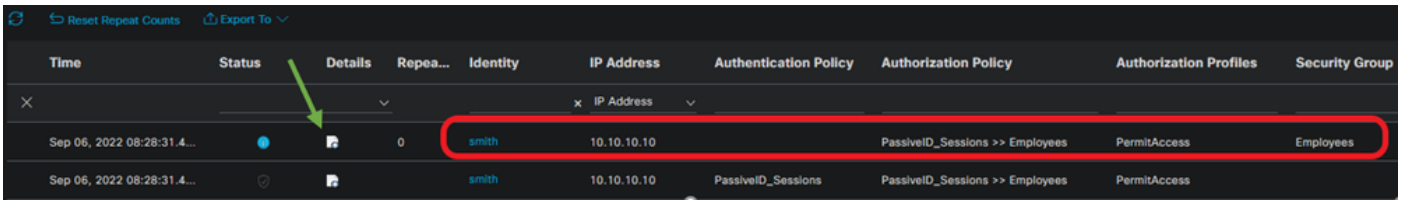
SXP設定

驗證

使用本節內容，確認您的組態是否正常運作。

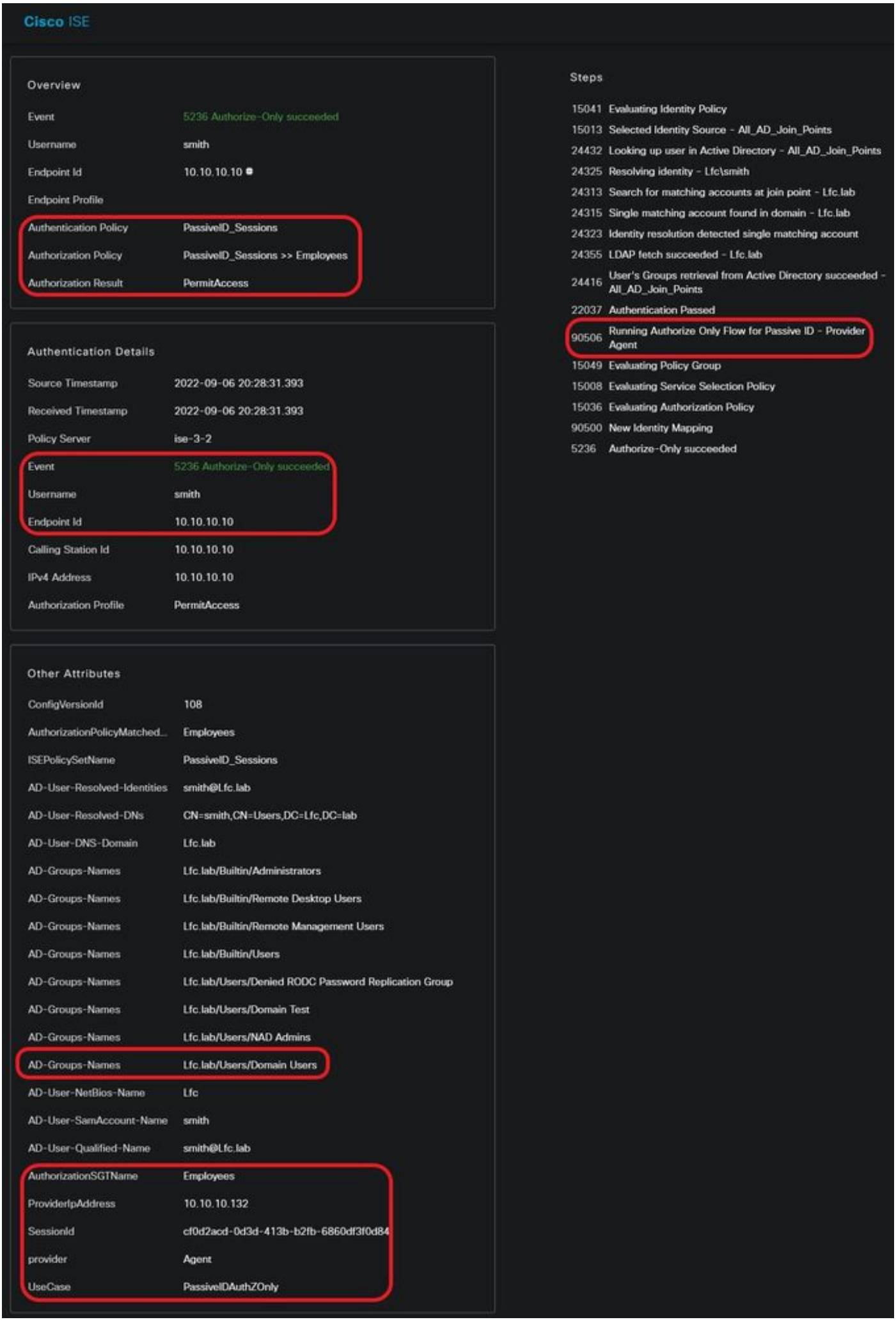
ISE驗證

使用者登入事件從Active Directory域控制器(AD DC)WMI或AD代理等提供程式傳送到ISE後，繼續檢查即時日誌。導航至 **Operations > Radius > Live Logs**.



Radius LiveLog

按一下「詳細資訊」(Details)列中的放大鏡圖示，以檢視使用者的詳細報告，在本例中為smith（域使用者），如下所示。



其他使用者（域管理員）的詳細報告，如圖所示，根據配置的授權策略分配不同的SGT。

被動ID	被動	追蹤	passiveid-*.log
Pxgrid	pxgrid	追蹤	pxgrid-server.log
SXP	sxp	偵錯	sxp.log

注意：完成故障排除後，請記得重置調試，並選擇相關節點，然後按一下 **Reset to Default**.

日誌片段

1. ISE從提供商接收登入事件：

Passiveid-*.log檔案：

```
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 loging
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檔案

2. ISE根據配置的授權策略分配SGT並將PassiveID使用者的IP-SGT對映發佈到PxGrid使用者和SXP對等體：

sxp.log檔案：

```
2022-09-06 20:28:31,587 DEBUG [sxpservice-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 [sxpservice-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, sessionExpiryTimeInMillis=-1, apic=false, routable=true, vns=[DEFAULT_VN]) to VPNs [default]
```

sxp.log檔案

pxgrid-server.log檔案：

```
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:1730
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檔案

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。