在ISE 3.2中配置被動ID會話的授權流

目錄

簡介

本文檔介紹如何配置被動ID事件的授權規則以將SGT分配給會話。

背景資訊

被動身份服務（被動ID）不會直接對使用者進行身份驗證，而是從外部身份驗證伺服器(例如Active Directory(AD)，即提供商收集使用者身份和IP地址，然後與訂閱者共用該資訊。

ISE 3.2引入了一項新功能，允許您配置授權策略以根據Active Directory組成員資格向使用者分配安全組標籤(SGT)。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ISE 3.X
- 與任何提供商的無源ID整合
- Active Directory(AD)管理
- 分段(Trustsec)
- PxGrid（平台交換網格）

採用元件

- 身分識別服務引擎(ISE)軟體版本3.2
- Microsoft Active Directory
- 系統日誌

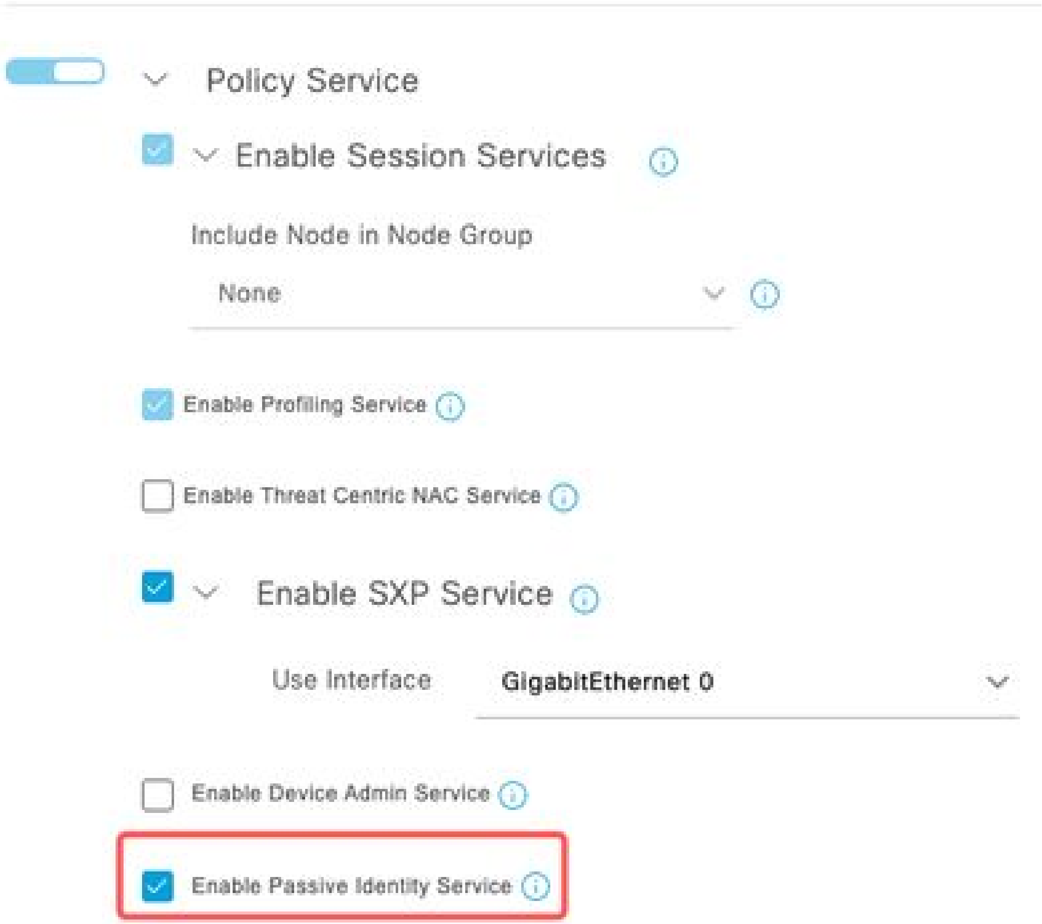
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

組態

步驟1.啟用ISE服務。

1. 在ISE上，導航到Administration > **Deployment**，選擇ISE節點並按一下**Edit**，啟用**Policy Service**，然後選擇Enable Passive Identity Service。可選，如果需要通過每個SXP和PxGrid發佈被動ID會話，則可以啟用SXP和PxGrid。按一下「**Save**」。

   警告：無法向SXP發佈由API提供程式驗證的PassiveID登入使用者的SGT詳細資訊。但是，這些使用者的SGT詳細資訊可以通過pxGrid和pxGrid Cloud發佈。



Policy Service

☑ Enable Session Services

Include Node in Node Group: None

☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

☑ Enable SXP Service

Use Interface: GigabitEthernet 0

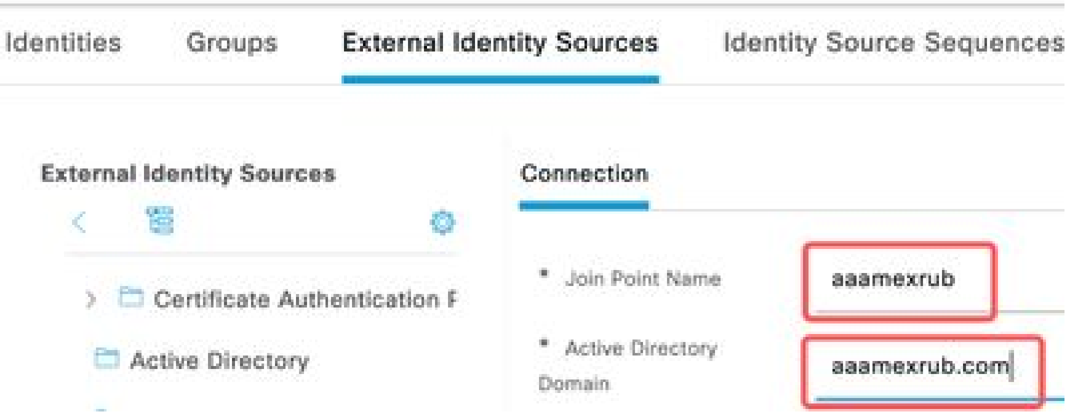
□ Enable Device Admin Service

☑ Enable Passive Identity Service

已啟用服務

步驟2.配置Active Directory。

1. 導航到Administration > **Identity Management** > **External Identity Sources**，然後選擇**Active directory**，然後點選Add按鈕。
2. 輸入**加入點名稱**和**Active Directory域**。按一下「**Submit**」。



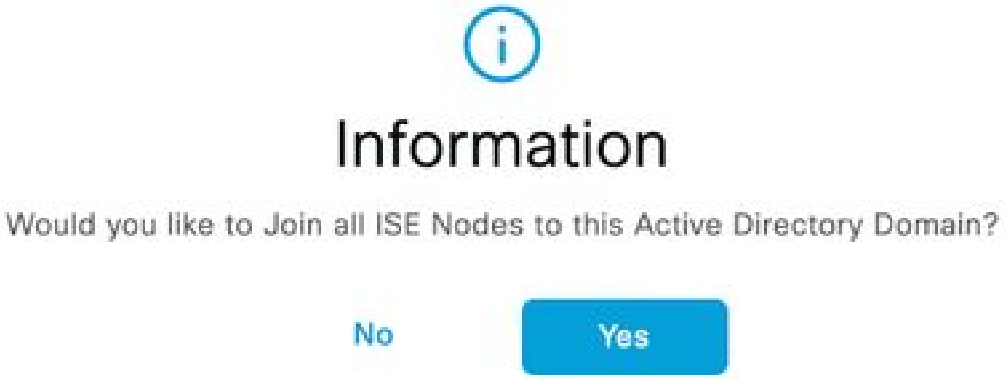
Identities
Groups
External Identity Sources
Identity Source Sequences
External Identity Sources
Certificate Authentication F
Active Directory
Connection

* Join Point Name: aaamexrub

* Active Directory Domain: aaamexrub.com

新增Active Directory

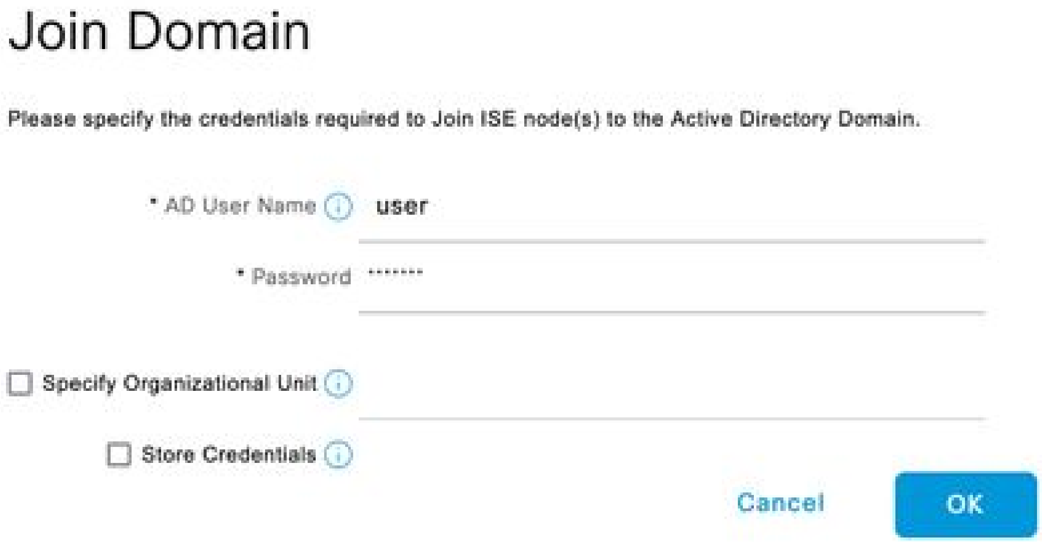
3.彈出視窗會將ISE加入AD。按一下「**Yes**」。輸入**Username**和**Password**。按一下「OK」（確定）。



Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

繼續加入



Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name: user

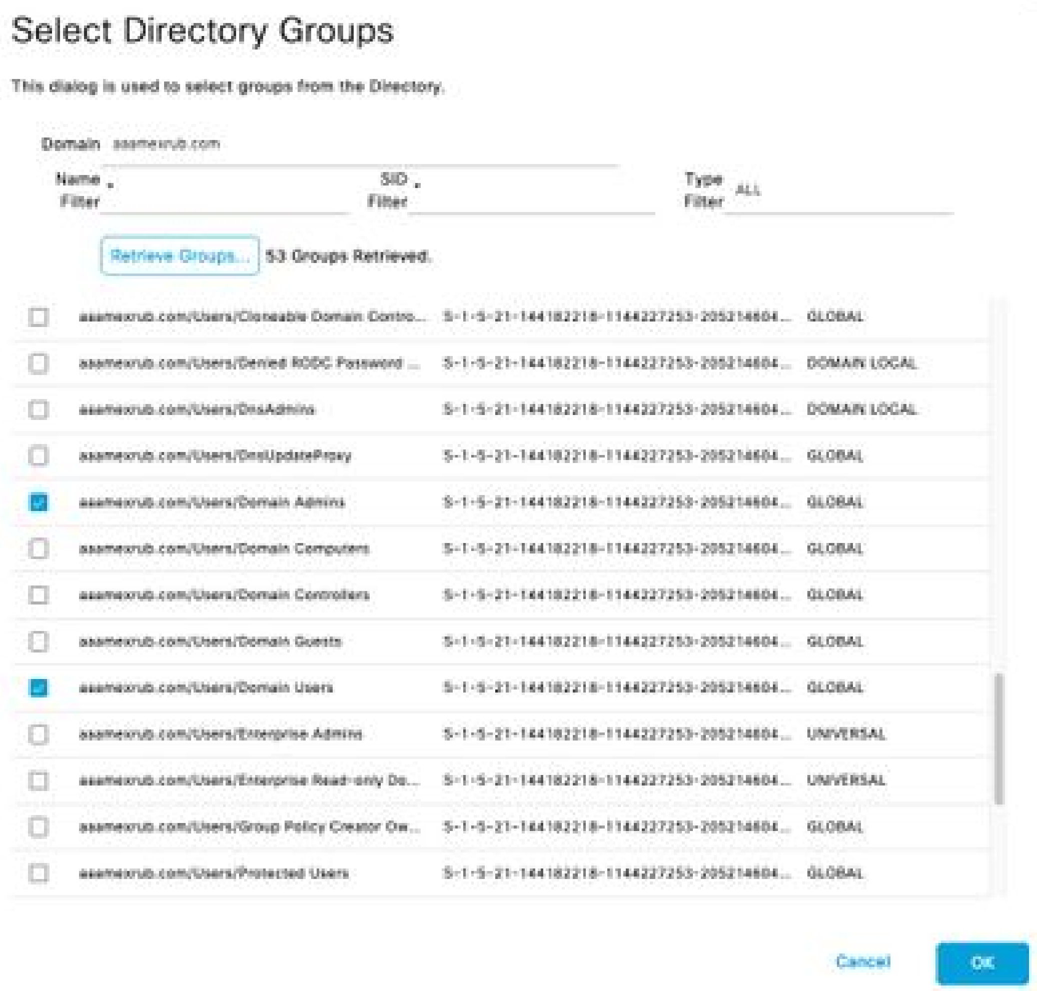
* Password: *******

□ Specify Organizational Unit

□ Store Credentials

ISE 加入Active Directory

4.檢索AD組導航到**Groups**，按一下**Add**，然後按一下**Retrieve Groups**，然後選擇所有感興趣的組，然後按一下**OK**。



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain aaamexrub.com

Name Filter *

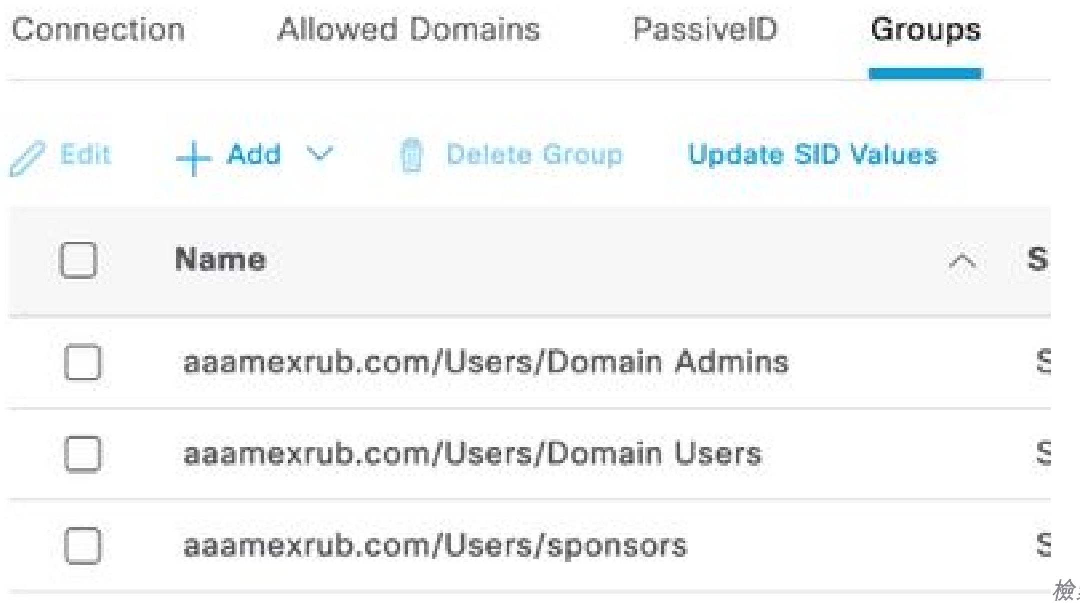
SID Filter *

Type Filter ALL

53 Groups Retrieved.

□	aaamexrub.com/Users/Cloneable Domain Contro...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
□	aaamexrub.com/Users/Denied RODC Password ...	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
□	aaamexrub.com/Users/DnsAdmins	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
□	aaamexrub.com/Users/DnsUpdateProxy	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
☑	aaamexrub.com/Users/Domain Admins	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
□	aaamexrub.com/Users/Domain Computers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
□	aaamexrub.com/Users/Domain Controllers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
□	aaamexrub.com/Users/Domain Guests	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
☑	aaamexrub.com/Users/Domain Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
□	aaamexrub.com/Users/Enterprise Admins	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
□	aaamexrub.com/Users/Enterprise Read-only Do...	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
□	aaamexrub.com/Users/Group Policy Creator Ow...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
□	aaamexrub.com/Users/Protected Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL

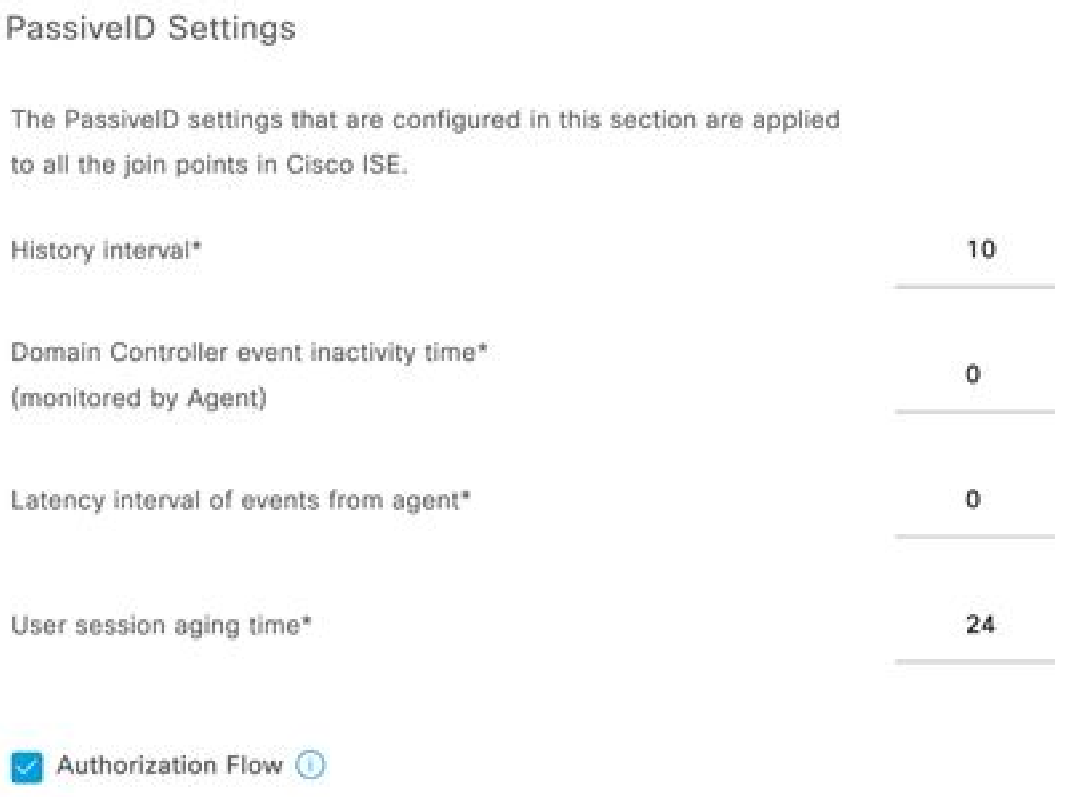
檢索AD組



□	Name	S
□	aaamexrub.com/Users/Domain Admins	S
□	aaamexrub.com/Users/Domain Users	S
□	aaamexrub.com/Users/sponsors	S

檢索的組

5.啟用授權流。導航到**高級設定**，然後在**PassiveID設定**部分中選中**Authorization Flow**覈取方塊。按一下「**Save**」。



PassiveID Settings

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

History interval* 10

Domain Controller event inactivity time* (monitored by Agent) 0

Latency interval of events from agent* 0

User session aging time* 24

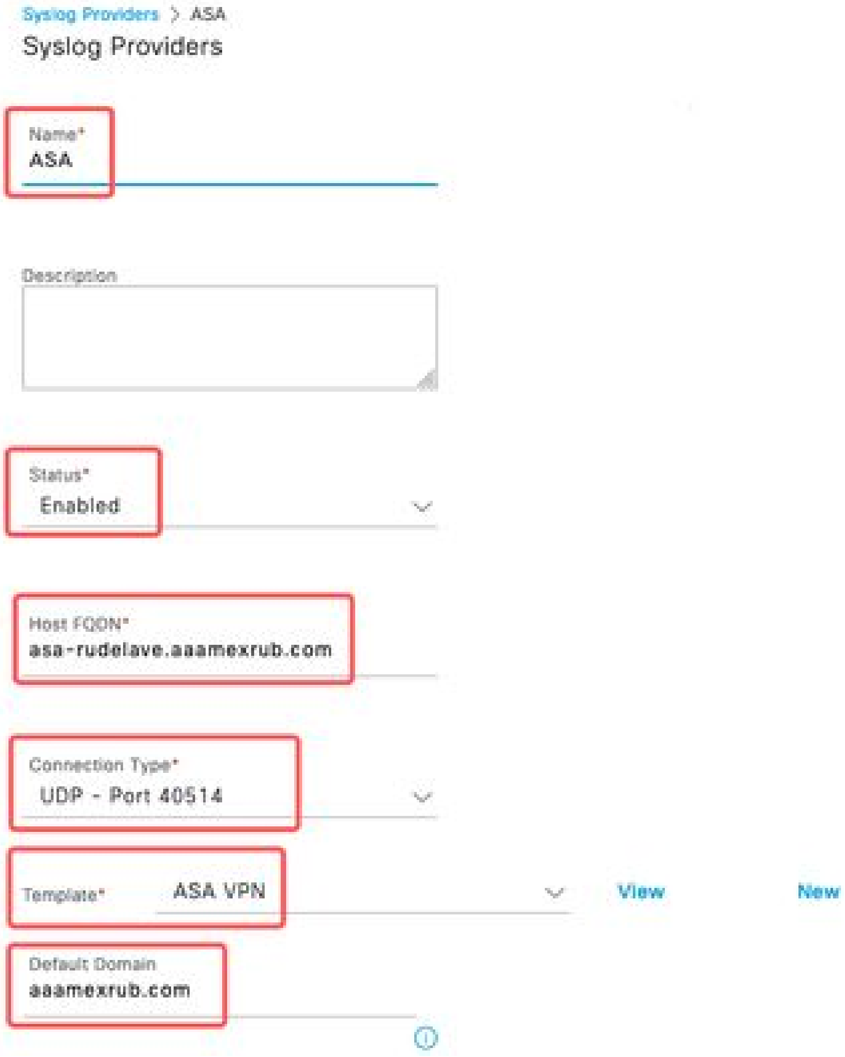
☑ Authorization Flow

啟用授權流

步驟3.配置Syslog提供程式。

1. 導航到Work Centers > **PassiveID** > **Providers**，選擇**Syslog Providers**，按一下**Add**並填寫資訊。按一下「**Save**」

   注意：在這種情況下，ISE從ASA中成功的VPN連線收到系統日誌消息，但本文檔不描述該配置。



Syslog Providers > ASA

Syslog Providers

Name*
ASA

Description

Status*
Enabled

Host FQDN*
asa-rudelave.aaamexrub.com

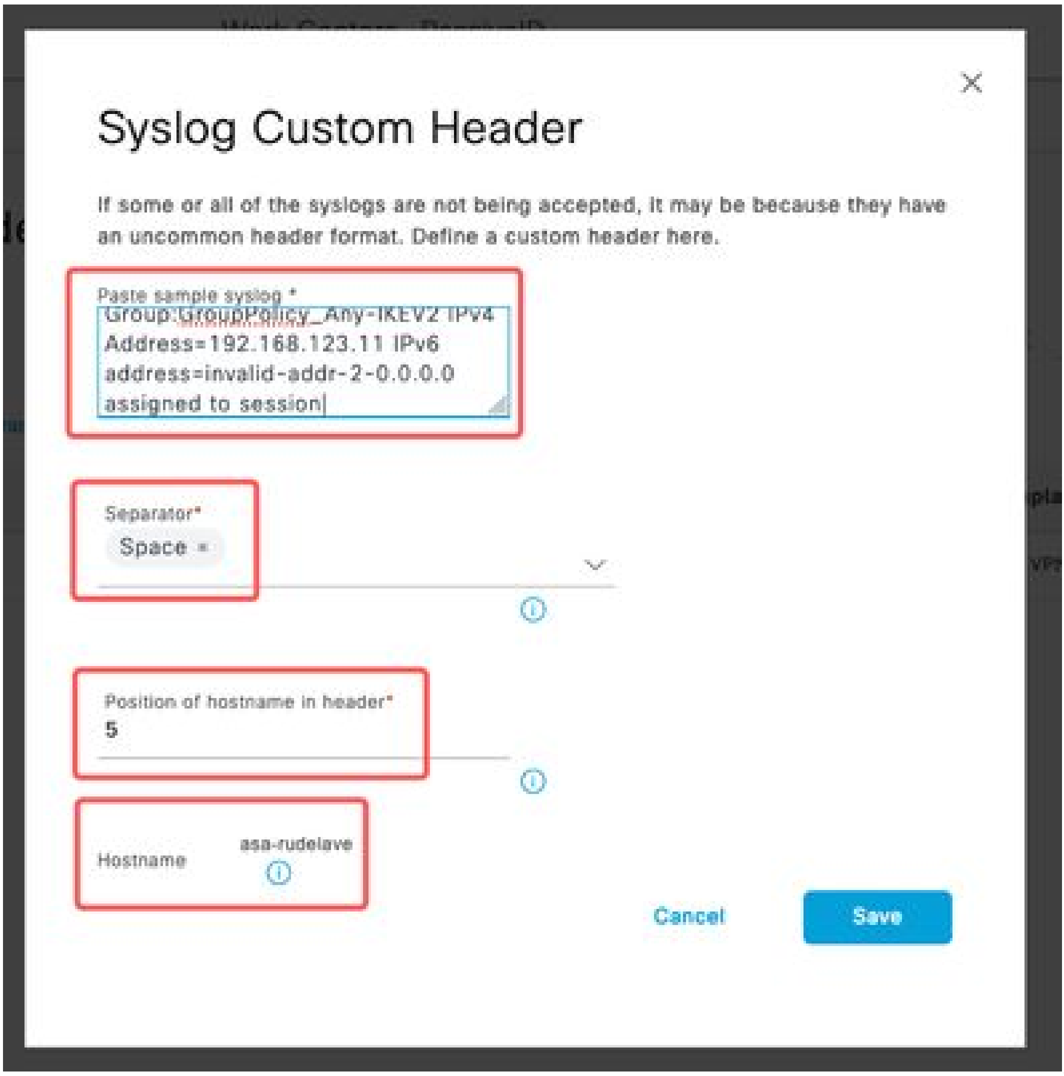
Connection Type*
UDP - Port 40514

Template* ASA VPN

Default Domain
aaamexrub.com

配置系統日誌提供程式

2. 按一下**Custom Header**。貼上示例系統日誌並使用分隔符或頁籤查詢裝置主機名。如果正確，則顯示主機名。按一下「**Save**」



Syslog Custom Header

If some or all of the syslogs are not being accepted, it may be because they have an uncommon header format. Define a custom header here.

Paste sample syslog *

```
Group:GroupPolicy_Any-IKEV2 IPv4
Address=192.168.123.11 IPv6
address=invalid-addr-2-0.0.0.0
assigned to session
```

Separator*: Space

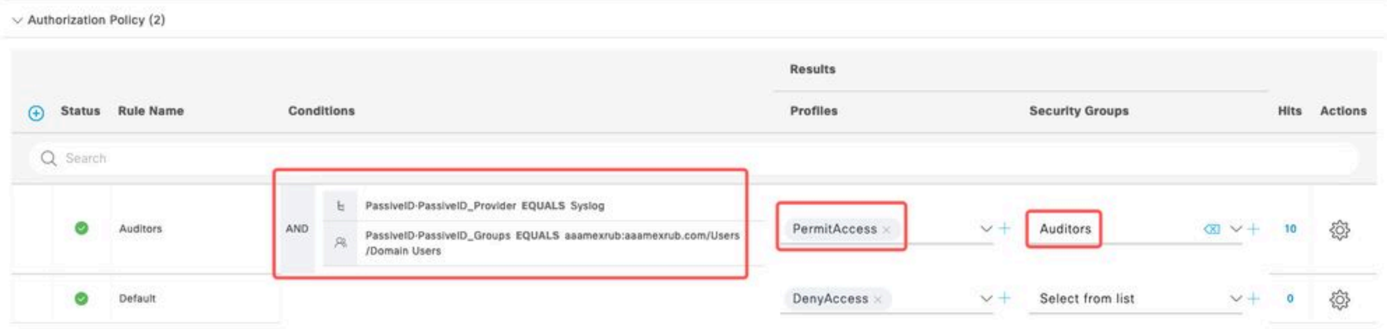
Position of hostname in header*: 5

Hostname: asa-rudelave

配置自定義報頭

步驟4.設定授權規則

1. 導覽至**Policy** > **Policy Sets**。 在這種情況下，它使用預設策略。按一下**Default**策略。在**Authorization Policy**中新增新規則。在PassiveID策略中，ISE具有所有提供程式。可以將此組與PassiveID組組合。選擇**Permit Access** as Profile，然後在**Security Groups**中選擇need it SGT。



Authorization Policy (2)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Auditors	AND PassiveID·PassiveID_Provider EQUALS Syslog PassiveID·PassiveID_Groups EQUALS aaamexrub:aaamexrub.com/Users/Domain Users	PermitAccess	Auditors	10	⚙
✓	Default		DenyAccess	Select from list	0	⚙

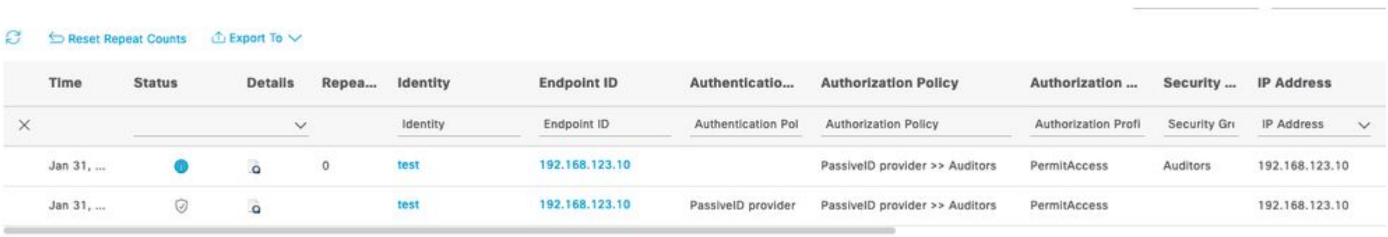
設定授權規則

驗證

ISE收到系統日誌後，您可以檢查Radius Live Logs以檢視授權流。導覽至**Operations** > **Radius** > **Live logs**。

在日誌中，您可以看到Authorization事件。該標籤包含與其關聯的使用者名稱、授權策略和安全組

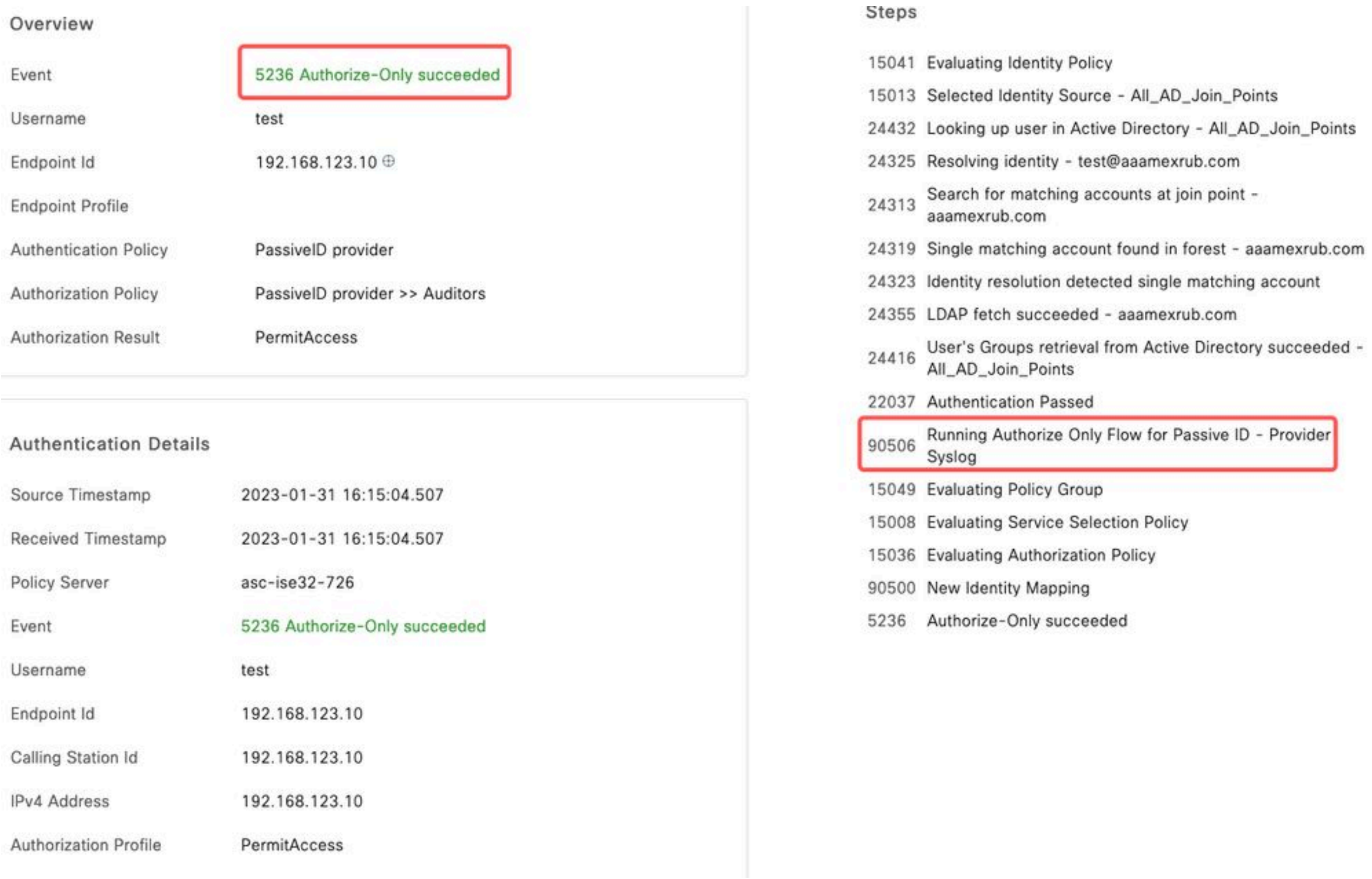
標籤。



Time	Status	Details	Repea...	Identity	Endpoint ID	Authenticatio...	Authorization Policy	Authorization ...	Security ...	IP Address
				Identity	Endpoint ID	Authentication Pol	Authorization Policy	Authorization Profi	Security Gr	IP Address
Jan 31, ...	●		0	test	192.168.123.10		PassiveID provider >> Auditors	PermitAccess	Auditors	192.168.123.10
Jan 31, ...				test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess		192.168.123.10

Radius即時日誌

要檢查更多詳細資訊，請按一下**Detail Report**。此處您可以看到評估策略以分配SGT的Authorize-Only流。



Overview

Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Endpoint Profile	
Authentication Policy	PassiveID provider
Authorization Policy	PassiveID provider >> Auditors
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2023-01-31 16:15:04.507
Received Timestamp	2023-01-31 16:15:04.507
Policy Server	asc-ise32-726
Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Calling Station Id	192.168.123.10
IPv4 Address	192.168.123.10
Authorization Profile	PermitAccess

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 - test@aaamexrub.com
24313	Search for matching accounts at join point - aaamexrub.com
24319	Single matching account found in forest - aaamexrub.com
24323	Identity resolution detected single matching account
24355	LDAP fetch succeeded - aaamexrub.com
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 Syslog
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15036	Evaluating Authorization Policy
90500	New Identity Mapping
5236	Authorize-Only succeeded

Radius即時日誌報告

疑難排解

在本例中，它使用兩個流：passiveID會話和授權流。要啟用調試，請導航到**操作** > **故障排除** > **調試嚮導**> **調試日誌配置**，然後選擇ISE節點。

對於PassiveID，將下一個元件啟用到**DEBUG**級別：

- 被動ID

要根據被動ID提供方和要檢查此情況的檔案檢查日誌，您需要檢視其他提供方的檔案passiveid-syslog.log:

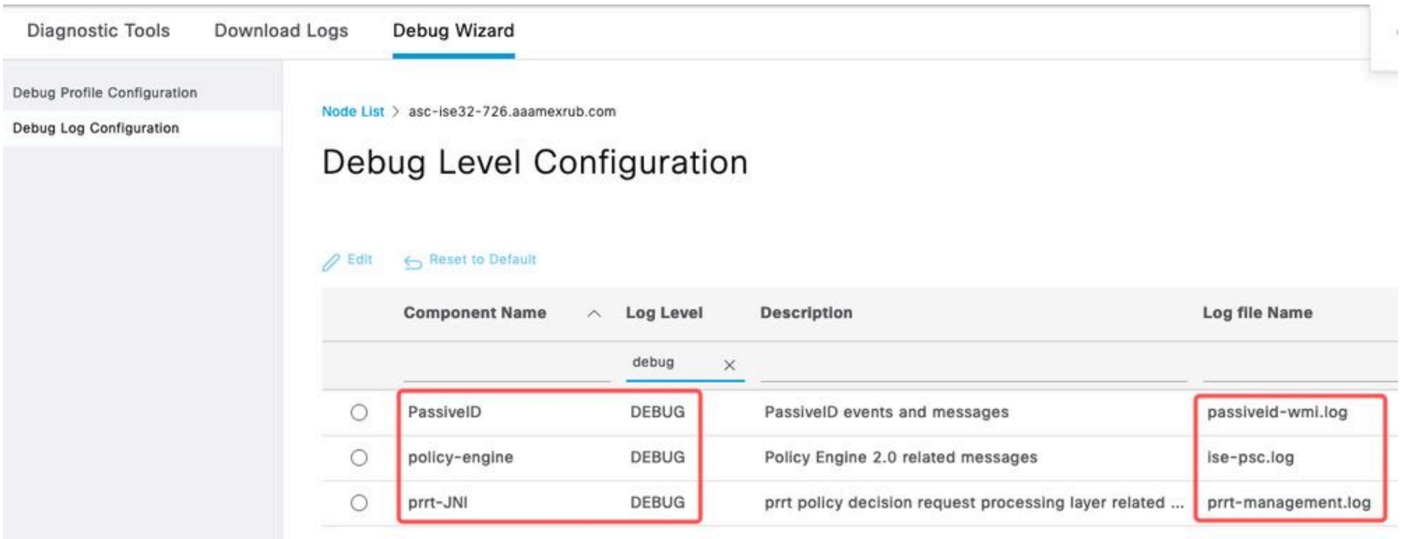
- passiveid-agent.log
- passiveid-api.log
- passiveid-endpoint.log

- passiveid-span.log
- passiveid-wmilog

對於授權流，啟用下一個元件到**DEBUG**級別：

- policy-engine
- prrt-JNI

範例：



Debug Level Configuration

	Component Name	Log Level	Description	Log file Name
		debug ×		
○	PassiveID	DEBUG	PassiveID events and messages	passiveid-wmi.log
○	policy-engine	DEBUG	Policy Engine 2.0 related messages	ise-psc.log
○	prrt-JNI	DEBUG	prrt policy decision request processing layer related ...	prrt-management.log

啟用調試

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）。