

配置ISE 3.3 pxGrid Direct並對其進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[配置pxGrid直接聯結器](#)

[步驟 1.增加新的pxGrid直接聯結器](#)

[步驟 2.定義pxGrid直接聯結器](#)

[步驟 3.URL](#)

[步驟 4.排程](#)

[步驟 5.父物件](#)

[步驟 6.屬性](#)

[步驟 7.辨識碼](#)

[步驟 8.摘要](#)

[步驟 9.驗證](#)

[環境可視性pxGrid直接儀表板](#)

[使用pxGrid Direct Dictionary的授權策略配置](#)

[疑難排解](#)

簡介

本文檔介紹如何配置帶有外部REST API的思科身份服務引擎3.3 pxGrid直接聯結器以獲取終端資料。

必要條件

需求

思科建議您瞭解以下主題：

- 思科ISE 3.3
- REST API

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科ISE 3.3
- 為終端屬性提供JSON資料的REST API伺服器

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pxGrid Direct透過使您能夠連線到外部REST API（為終端屬性提供JSON資料）並將這些資料提取到思科ISE資料庫，幫助您更快地評估和授權終端。此功能無需在每次必須授權終端時查詢終端屬性資料。然後，您可以在授權策略中使用提取的資料。

pxGrid Direct有助於根據您在pxGrid Direct配置中指定的屬性收集資料。兩個必填欄位「唯一識別符號」和「關聯識別符號」用於提取相關資料。如果連結器不包含這些欄位的值，則從連結器擷取和儲存資料可能會出錯。

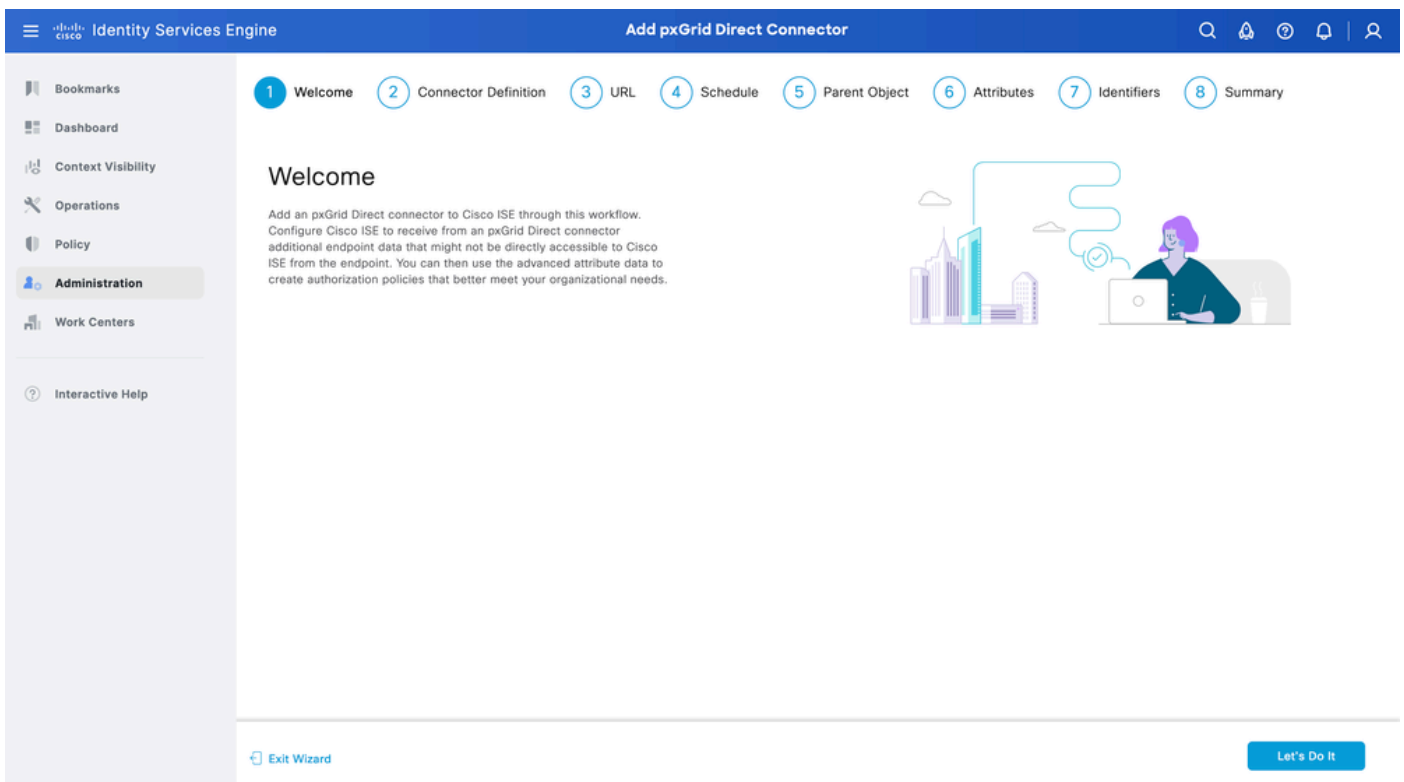
配置pxGrid直接連結器

步驟 1. 增加新的pxGrid直接連結器

要配置pxGrid Direct連結器，請從ISE導航到管理>網路資源> pxGrid直接連結器。按一下Add。



打開pxGrid直接連線嚮導的歡迎頁面後，按一下



步驟 2. 定義pxGrid直接連結器

為連結器指定名稱，並在需要時提供說明。按「Next」（下一步）。

- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy
- Administration**
- Work Centers
- Interactive Help

- Welcome
- 2 Connector Definition**
- 3 URL
- 4 Schedule
- 5 Parent Object
- 6 Attributes
- 7 Identifiers
- 8 Summary

Define Connector

A new Cisco ISE Dictionary is created at a later step to store the attributes and values that Cisco ISE retrieves from the pxGrid Direct connector. The name that you provide here is the name of the Cisco ISE Dictionary folder for the connector.

Name
pxGridConnectorFLSK

Description (optional)

Connector type: URL Fetcher

Certificate Validations

Check the Skip Certificate Validations check box to allow Cisco ISE to accept any certificate that a server presents without verifying the hostname or other details. You must check this check box only in a test environment or if you trust the connected server to be highly secure. Typically, skipping certificate validations could make your network vulnerable to machine-in-the-middle attacks.

Skip Certificate Validations



[Exit Wizard](#)

[Back](#)

[Next](#)



警告：選中Skip Certificate Validations 覈取方塊以允許Cisco ISE接受伺服器提供的任何證書而不驗證主機名或其他詳細資訊。只有在測試環境中或您信任連線的伺服器高度安全時，才能選中此覈取方塊。通常，跳過證書驗證會使您的網路易受中間機器攻擊。

步驟 3.URL

- 鍵入向終端屬性提供JSON資料的外部REST API的URL。
- 在Authentication下，輸入外部REST API伺服器的使用者名稱和密碼。
- 選擇測試連線，等待成功消息，然後按一下下一步。

- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy
- Administration**
- Work Centers
- Interactive Help

- Welcome
- Connector Definition
- 3 URL**
- 4 Schedule
- 5 Parent Object
- 6 Attributes
- 7 Identifiers
- 8 Summary

Add URL

Specify the URLs that Cisco ISE must use to fetch the required endpoint data from the pxGrid Direct connector.

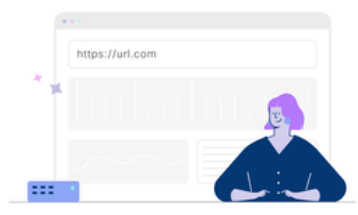
URL

Incremental URL (optional)

Authentication
 Login

 Password

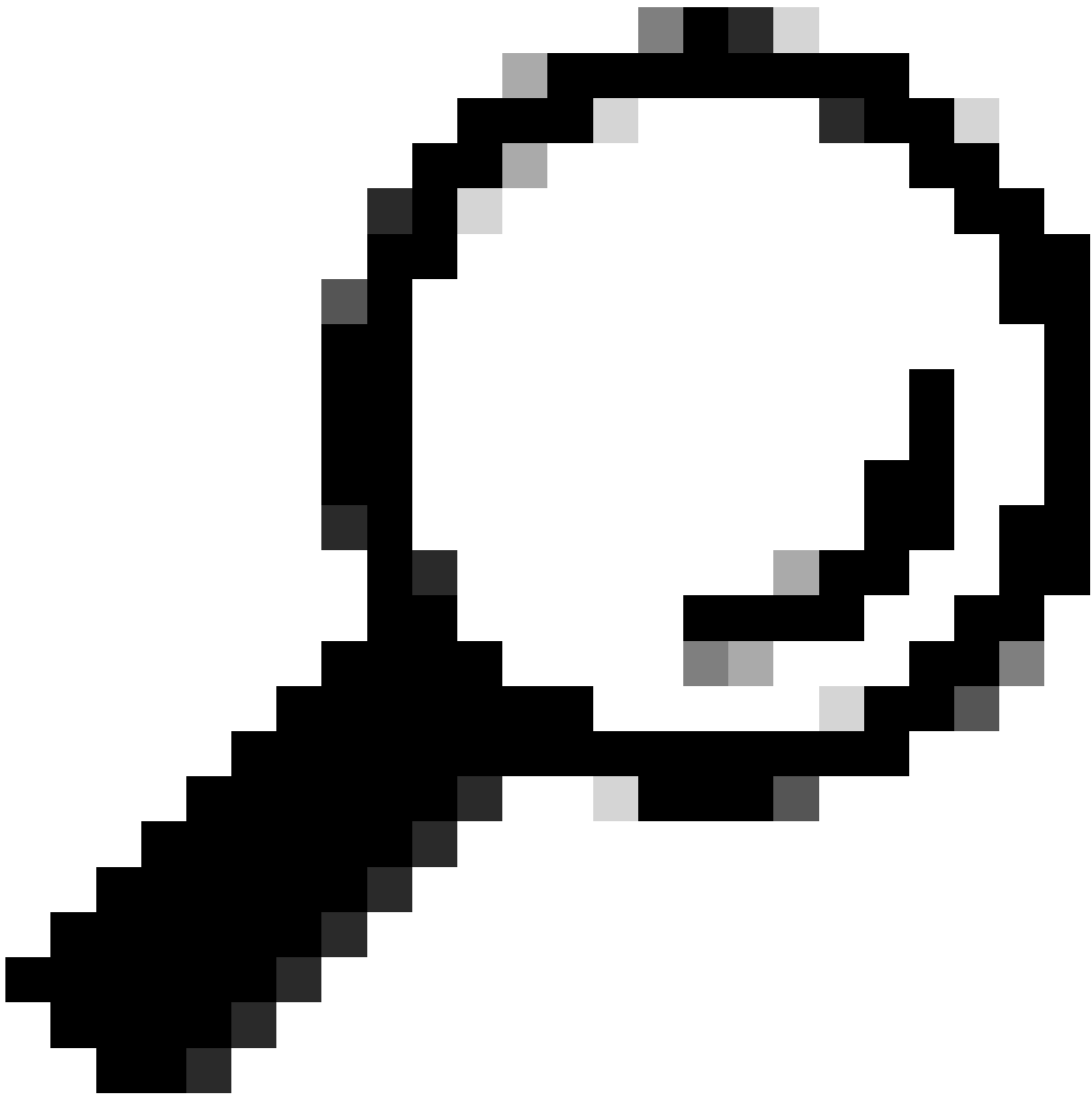
[Test Connection](#) ✔ Successful



[Exit Wizard](#)

[Back](#)

[Next](#)



提示：增量URL對於配置是可選的。如果外部REST API具有「請求引數」，則可以使用特定引數進行過濾來獲取最新資訊，而不是請求所有資料。請確認外部REST API伺服器的檔案內有Request引數。

步驟 4.排程

選取「完全同步排程」。

- 預設值- 1週
- 最小值- 12小時
- 最大值- 1個月

選取增量同步的排程。僅當在步驟3中配置了此選項時，此選項才會顯示。

- 預設值- 1天
- 最小值- 1小時
- 最大值- 1週

按「Next」（下一步）。

Identity Services Engine Add pxGrid Direct Connector

Welcome Connector Definition URL **4** Schedule 5 Parent Object 6 Attributes 7 Identifiers 8 Summary

Set Up Synchronization Schedule

Schedule the sync interval with the connector. The time that you choose is configured in the system time zone.
System time zone: Etc/GMT-6

SCHEDULE FULL SYNC

Cisco ISE retrieves all the endpoint data that is available with the pxGrid Direct connector at the time of the sync.

Synchronize Every
1 Week(s)

Start Date Start Time
09/26/2023 4:00 AM

SCHEDULE INCREMENTAL SYNC

Cisco ISE retrieves specific endpoint data from the pxGrid Direct connector, based on additional parameters defined by you. For example, you could only retrieve data that has been updated since the last full sync.

Synchronize Every
1 Day(s)

Start Date Start Time
09/26/2023 4:00 AM

Exit Wizard Back **Next**

步驟 5.父物件

必須鍵入JSON金鑰才能搜尋屬性。

Identity Services Engine Add pxGrid Direct Connector

Navigation: Welcome Connector Definition URL Schedule **5 Parent Object** 6 Attributes 7 Identifiers 8 Summary

Parent Object

Configure the JSON data object that must be used to search for the rest of the attributes. You can read more information and example at [Page Level Help](#).

Parent Object result

✔ Successful

```
{
  "asset": "Unknown",
  "asset_tag": "",
  "assigned": "",
  "assigned_to": "Jenna.Santos@example.org",
  "assignment_group": "",
  "attestation_score": "",
  "attested": "false",
  "attested_by": "",
  "attested_date": "",
  "attributes": "",
  "can_print": "false",
  "category": "Hardware",
  "cd_rom": "false",
  "cd_speed": "",
  "change_control": "",
  "chassis_type": null,
  "checked_in": "",
  "checked_out": "",
  "comments": ""
}
```

```
{
  "Parent_Object1": {
    "Attribute1": "attribute1Value",
    "Attribute2": "attribute2Value",
    "Attribute3": "attribute3Value",
    "Attribute4": "attribute4Value",
    "Attribute5": "attribute5Value",
    "Attribute6": "attribute6Value",
    "Attribute7": "attribute7Value",
    "Attribute8": "attribute8Value"
  }
}
```

步驟 6.屬性

選擇JSON的屬性以配置可用於策略的詞典項。

在此案例中，「說明」中包含的屬性包括：

- 資產
- ip_address
- mac_address
- os_version
- sys_id
- sys_update
- u_segmentation_group_tag

按「Next」（下一步）。

Identity Services Engine Add pxGrid Direct Connector

[Welcome](#)
[Connector Definition](#)
[URL](#)
[Schedule](#)
[Parent Object](#)
6 Attributes
[7 Identifiers](#)
[8 Summary](#)

Select Attributes Configure Dictionary Items

Add the attributes that Cisco ISE must retrieve from the pxGrid Direct connector. Choose attributes that should be included to the Cisco ISE Dictionary by clicking the toggle switch next to an attribute. Enter the attribute name that you want displayed in the Cisco ISE Dictionary. All the attributes that are retrieved from the pxGrid Direct connector persist in Cisco ISE even if they are not included in the Cisco ISE Dictionary.

[Add Attribute](#)
[Delete](#)
[Exclude all from Dictionary](#)

External Name	Include in Dictionary	Name in Dictionary
<input type="checkbox"/> \$.asset	<input checked="" type="checkbox"/>	asset
<input type="checkbox"/> \$.ip_address	<input checked="" type="checkbox"/>	ip_address
<input type="checkbox"/> \$.mac_address	<input checked="" type="checkbox"/>	mac_address
<input type="checkbox"/> \$.model_id	<input type="checkbox"/>	model_id
<input type="checkbox"/> \$.os_version	<input checked="" type="checkbox"/>	os_version
<input type="checkbox"/> \$.sys_id	<input checked="" type="checkbox"/>	sys_id
<input type="checkbox"/> \$.sys_updated_on	<input checked="" type="checkbox"/>	sys_updated_on
<input type="checkbox"/> \$.u_segmentation_group_te	<input checked="" type="checkbox"/>	u_segmentation_group_tag

[Exit Wizard](#)
[Back](#)
[Next](#)

步驟 7. 辨識碼

- 從CMDB資料庫中選擇一個端點所獨有的唯一識別符號屬性，外部REST API伺服器將在其中獲取JSON。
- 選擇ISE獨有的能夠將終端與授權策略匹配的關聯識別符號屬性。

按「Next」（下一步）。

Identity Services Engine Add pxGrid Direct Connector

[Welcome](#)
[Connector Definition](#)
[URL](#)
[Schedule](#)
[Parent Object](#)
[Attributes](#)
7 Identifiers
[8 Summary](#)

Identifiers

Unique Identifiers: Attributes that are unique keys to CMDB database. For example, sys_id .


Version Identifiers: Attributes that help record the version of the endpoint data. For example, the timestamp of a data update. You can use version identifiers to better schedule incremental updates from a connector.

Correlation Identifiers: Attributes that are unique to ise and that can be used to match endpoint auth policy. For example, mac-address, ip-address, serial-number, and so on.

Unique Identifier

Correlation Identifier

Version Identifier (optional)



[Exit Wizard](#)
[Back](#)
[Next](#)

步驟 8.摘要

確保pxGrid直接聯結器配置正確。按一下「完成」。

Identity Services Engine Add pxGrid Direct Connector

Summary

- Connector Definition [Edit](#)
- URL [Edit](#)
- Set Up Synchronization Schedule [Edit](#)
- Parent Object [Edit](#)
- Select Attributes Configure Dictionary Items [Edit](#)
- Identifiers [Edit](#)
 - Unique Identifier sys_id
 - Correlation Identifier mac_address

[Exit Wizard](#) [Back](#) [Done](#)

聯結器完成後，會顯示在「pxGrid直接聯結器」頁面下。

Identity Services Engine Administration / Network Resources

pxGrid Direct Connectors

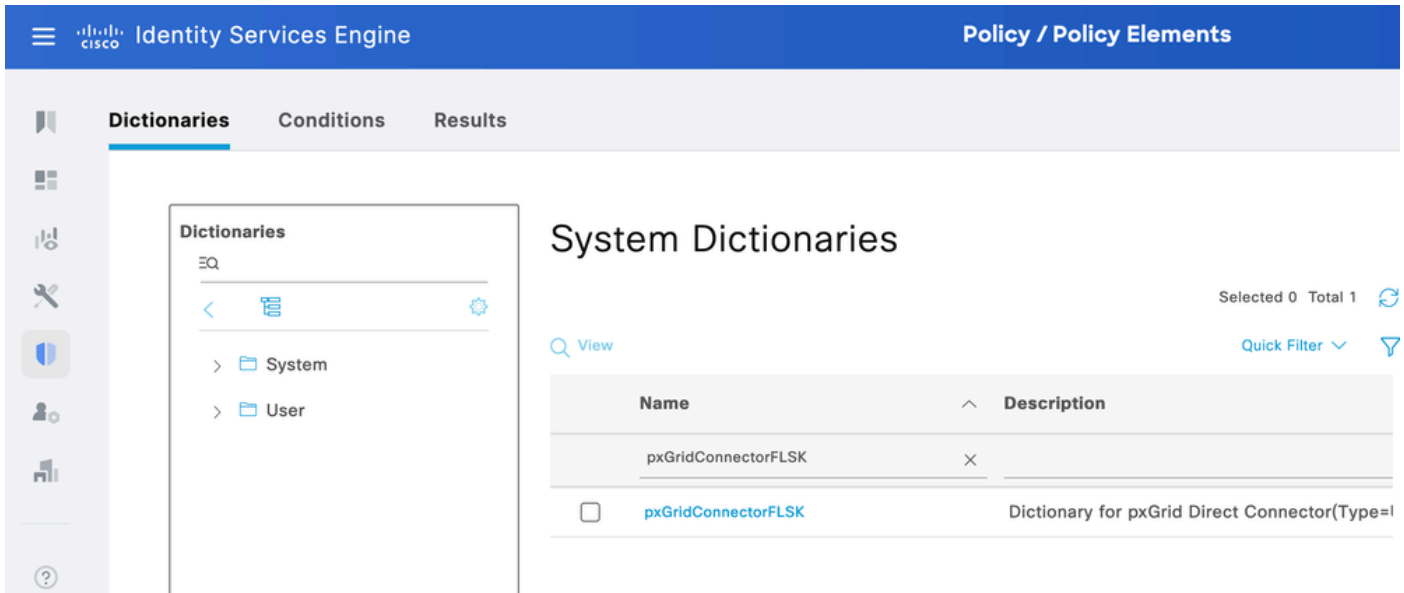
Configure a pxGrid Direct Connector to connect to external REST APIs that provide JSON data for endpoint attributes. The fetched data is used to evaluate and authorize endpoints faster without requiring Cisco ISE to query for endpoint attributes each time an authorization policy is executed for an endpoint. To view the endpoint attribute data fetched from the configured pxGrid Direct Connectors, view the pxGrid Direct Connectors tab in the [Context Visibility](#) window.

[Add](#) [Edit](#) [Refresh](#) [Scheduling](#) [Delete](#)

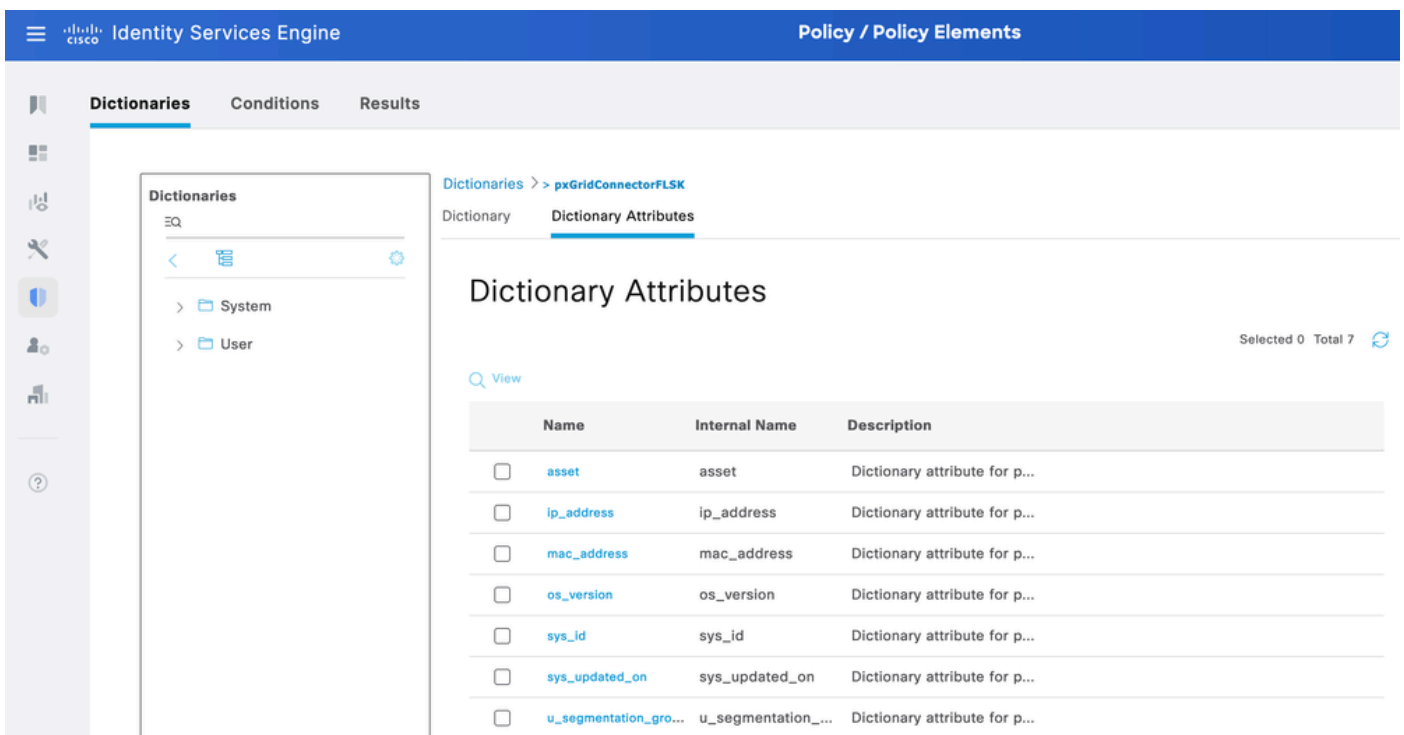
Name	Scheduling	Connector Type	URL	References
pxGridConnectorFLSK	Enabled	URLFETCHER	http://10.31.126.232:5000/endpoints	0

步驟 9.驗證

從ISE，導航到策略>策略元素>詞典>系統詞典。按pxGrid直接聯結器的名稱篩選。選擇它並按一下View。



導航到Dictionary Attributes，並檢視步驟6下配置為Dictionary Items的屬性清單。



環境可視性pxGrid直接儀表板

從ISE，導航至情景可視性>終端>更多> pxGrid直接終端。系統將顯示端點的清單，其中包含關聯和唯一識別符號的選定值。

點選相關ID以檢視詳細資訊，或下載特定終端的屬性。

The screenshot displays the Cisco ISE interface for managing endpoints. The main content area is titled "pxGrid Direct Endpoints" and shows a table of endpoint data. The table has the following columns: Correlation ID, Unique ID, Version ID, and Connector. The data rows include various correlation IDs and their corresponding unique and version IDs, all connected to a "pxGridConn" connector.

Correlation ID	Unique ID	Version ID	Connector
00:50:56:9B:2D:25	c50e2e34db4c85901f0f174b13961914		pxGridConn
00:C8:F2:AC:37:D3	f4ff17bcd8b0f01101f0f174b139619b2		pxGridConn
00:F0:DF:06:1C:82	e7eb377cdb8341101f0f174b13961957		pxGridConn
01:71:B2:C5:0C:42	d74ffb4dbc341101f0f174b139619b7		pxGridConn
01:7A:EB:FA:62:91	fcf697b8db4b01101f0f174b139619b7		pxGridConn
01:9C:12:FA:A3:CE	bb493b74db8341101f0f174b139619f3		pxGridConn
01:CB:06:53:F2:2F	eff30005db0741101f0f174b13961950		pxGridConn
01:ED:A1:A9:73:17	d49b5f78dbcb01101f0f174b1396191d		pxGridConn
02:02:3F:6A:9B:AE	ca4bf78db8341101f0f174b1396199b		pxGridConn
02:04:1E:0E:BC:0A	e44d2730db0341101f0f174b13961988		pxGridConn

The details panel on the right shows the following attributes for a selected endpoint:

- asset: Unknown
- asset_tag: Unknown
- assigned: Victoria.Stokes@example.org
- assignment_group: Unknown
- attestation_score: Unknown
- attested: false
- attested_by: Unknown
- attested_date: Unknown
- attributes: Unknown
- can_print: false
- category: Hardware
- cd_rom: false
- cd_speed: Unknown
- change_control: Unknown
- chassis_type: Unknown
- checked_in: Unknown
- checked_out: Unknown
- comments: Unknown
- company: Unknown

使用pxGrid Direct Dictionary的授權策略配置

從ISE，導航到策略> 策略集>選擇策略集 > 授權策略。在任何授權策略中點選齒輪圖示，然後選擇插入。

為規則指定名稱並新增條件以開啟Condition Studio。

按一下以增加新屬性，導航到未分類，在詞典下按pxGrid直接連結器的名稱進行過濾。



選擇可在授權策略下處理的屬性，並設定值。按一下Use。

Overview

Event	5200 Authentication succeeded
Username	94:DA:5F:96:74:63
Endpoint Id	94:DA:5F:96:74:63 ⓘ
Endpoint Profile	
Authentication Policy	Default >> MAB
Authorization Policy	Default >> pxGrid_Direct_attribute
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2023-09-27 09:30:44.753
Received Timestamp	2023-09-27 09:30:44.753
Policy Server	ise-demo-1
Event	5200 Authentication succeeded
Username	94:DA:5F:96:74:63
Endpoint Id	94:DA:5F:96:74:63
Calling Station Id	94:da:5f:96:74:63
Authentication Method	mab
Authentication Protocol	Lookup
Service Type	Call Check
Network Device	SPRT

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
11117	Generated a new session ID	0
11027	Detected Host Lookup UseCase (Service-Type = Call Check (10))	0
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	0
15041	Evaluating Identity Policy	10
15048	Queried PIP - Normalised Radius.RadiusFlowType	1
15013	Selected Identity Source - Internal Endpoints	4
24209	Looking up Endpoint in Internal Endpoints IDStore - 94:DA:5F:96:74:63	0
24217	The host is not found in the internal endpoints identity store	4
22056	Subject not found in the applicable identity store(s)	0
22058	The advanced option that is configured for an unknown user is used	0
22060	The 'Continue' advanced option is configured in case of a failed authentication request	0
15036	Evaluating Authorization Policy	0
24209	Looking up Endpoint in Internal Endpoints IDStore - 94:DA:5F:96:74:63	1
24217	The host is not found in the internal endpoints identity store	2
15048	Queried PIP - Radius.NAS-Port-Type	6
15048	Queried PIP - Network Access.UserName	8
15048	Queried PIP - IdentityGroup.Name	3
15048	Queried PIP - EndPoints.LogicalProfile	2
15048	Queried PIP - pxGridConnectorFLSK.mac_address	4
15016	Selected Authorization Profile - PermitAccess	4

疑難排解

從ISE，導航到操作>故障排除>調試嚮導>調試日誌配置。選擇您的主管理節點(PAN)，然後點選編輯。

按pxGrid Direct過濾元件名稱，然後選擇所需的日誌級別。按一下Save。

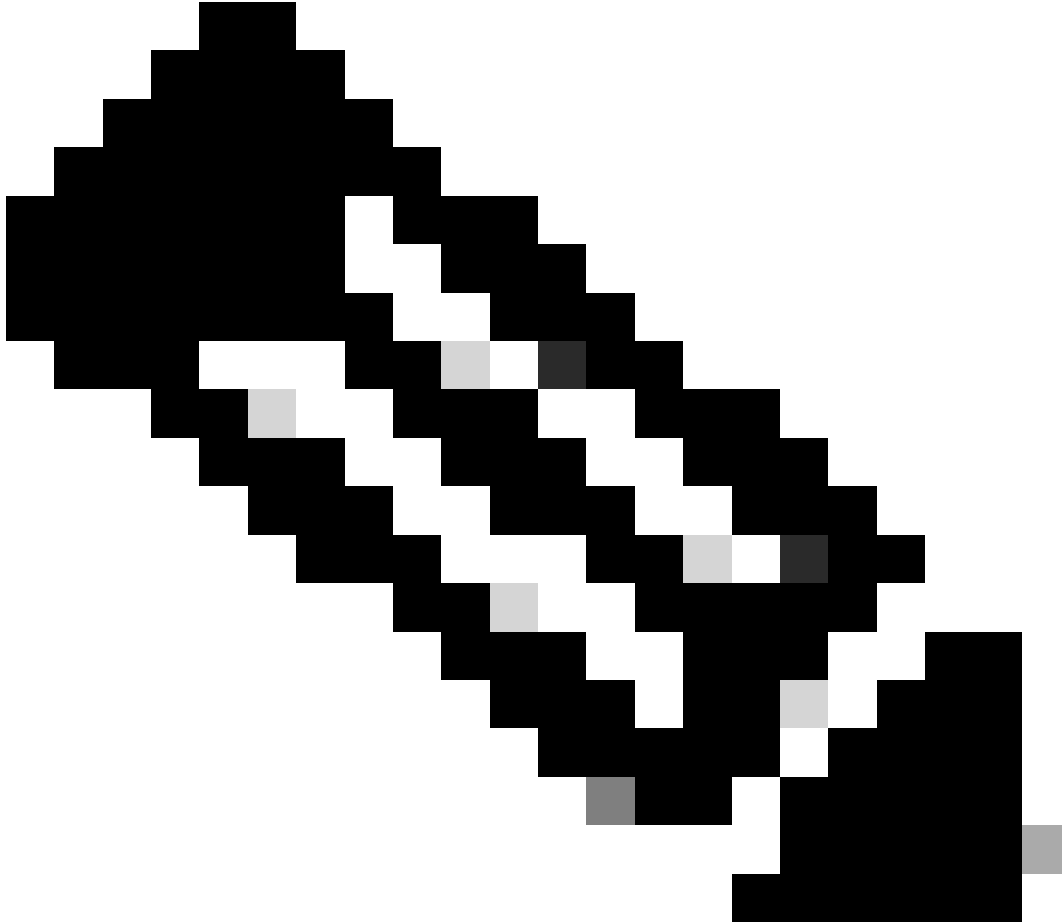
The screenshot shows the 'Debug Wizard' configuration page in the Cisco ISE Operations / Troubleshoot section. The page is titled 'Debug Level Configuration' and is for the component 'pxGrid Direct'. It features a table with columns for Component Name, Log Level, Description, Log file Name, and Log Filter. The table shows that the log level is set to 'DEBUG' and the log filter is 'Disabled'. There are buttons for 'Edit', 'Reset to Default', 'Log Filter Enable', 'Log Filter Disable', and 'Save | Cancel'.

Component Name	Log Level	Description	Log file Name	Log Filter
pxGrid Direct	DEBUG	pxGrid Direct backend and UI log messa	pxgriddirect-service.log, f	Disabled

- 在ISE PAN CLI上，可以在以下位置找到日誌：

```
admin#show logging application pxgriddirect-service.log
admin#show logging application pxgriddirect-connector.log
```

- 在ISE GUI上，導航到Operations > Troubleshoot > Download Logs > Select ISE PAN > Debug log > Debug Log Type > Application Logs。下載pxgriddirect-service.log和pxgriddirect-connector.log的zip檔案。
-



附註：

pxgriddirect-service的日誌包含有關提取的終端資料是否已經接收並儲存到Cisco ISE資料庫的資訊。

pxgriddirect-connector的日誌包含指示pxGrid Directed聯結器是否成功增加到Cisco ISE的資訊。

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）。