

# ISE 3.3 pxGrid Directの設定およびトラブルシューティング

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[pxGridダイレクトコネクタの設定](#)

[ステップ 1: 新しいpxGrid Directコネクタの追加](#)

[ステップ 2: pxGrid Directコネクタの定義](#)

[ステップ 3: URL](#)

[ステップ 4: Schedule](#)

[ステップ 5: 親オブジェクト](#)

[手順 6: 属性](#)

[手順 7: 識別子](#)

[ステップ 8: 要約](#)

[ステップ 9: 検証](#)

[Context Visibility pxGrid Directダッシュボード](#)

[pxGridダイレクトディクショナリを使用した許可ポリシーの設定](#)

[トラブルシューティング](#)

---

## はじめに

このドキュメントでは、Cisco Identity Service Engine(ISE)3.3 pxGridダイレクトコネクタを外部 REST APIを使用して設定し、エンドポイントデータを取得する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco ISE 3.3
- REST API

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE 3.3
- エンドポイント属性のJSONデータを提供するREST APIサーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

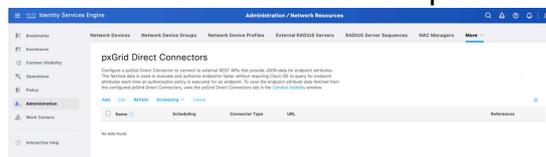
Cisco pxGrid Directを使用すると、エンドポイント属性のJSONデータを提供する外部REST APIに接続して、このデータをCisco ISEデータベースに取得できるため、エンドポイントの評価と認可を迅速に行えます。この機能を使用すると、エンドポイントを承認する必要があるたびにエンドポイント属性データを照会する必要がなくなります。取得したデータは、認可ポリシーで使用できます。

pxGrid Directは、pxGrid Direct構成で指定した属性に基づいてデータを収集するのに役立ちます。Unique IdentifierとCorrelation Identifierという2つの必須フィールドは、関連データを取得するために使用されます。コネクタにこれらのフィールドの値が含まれていない場合、コネクタからのデータの取得と保存に誤りがある可能性があります。

## pxGridダイレクトコネクタの設定

### ステップ 1：新しいpxGrid Directコネクタの追加

pxGrid Direct Connectorを設定するには、ISEからAdministration > Network Resources > pxGrid



Direct Connectorsに移動します。[Add] をクリックします。

pxGrid Direct Connectウィザードのウェルカムページが開いたら、

Let's Do It

Identity Services Engine Add pxGrid Direct Connector

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

## Welcome

Add an pxGrid Direct connector to Cisco ISE through this workflow. Configure Cisco ISE to receive from an pxGrid Direct connector additional endpoint data that might not be directly accessible to Cisco ISE from the endpoint. You can then use the advanced attribute data to create authorization policies that better meet your organizational needs.



[Exit Wizard](#) [Let's Do It](#)

## ステップ 2 : pxGrid Directコネクタの定義

必要に応じて、コネクタの名前と説明を入力します。[Next] をクリックします。

Identity Services Engine Add pxGrid Direct Connector

1 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

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：ホスト名やその他の詳細を確認せずにサーバから提示される証明書をCisco ISEが受け入れることができるようにするには、Skip Certificate Validationsチェックボックスをオンにします。このチェックボックスは、テスト環境の場合、または接続されたサーバが高いセキュリティを持つと信頼する場合にのみオンにする必要があります。通常、証明書検証をスキップすると、ネットワークがMachine-in-the-Middle攻撃に対して脆弱になる可能性があります。

---

### ステップ 3 : URL

- endpoints属性にJSONデータを提供する外部REST APIのURLを入力します。
- [認証]で、外部REST APIサーバのユーザ名とパスワードを入力します。
- Test Connectionを選択し、Successfulメッセージが表示されるまで待つから、Nextをクリックします。

- 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

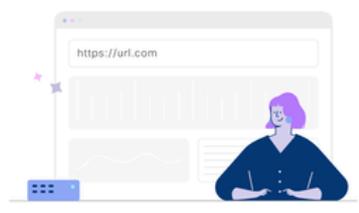
Specify the URLs that Cisco ISE must use to fetch the required endpoint data from the pxGrid Direct connector.

URL

Incremental URL (optional)

Authentication  
 Login  
  
 Password

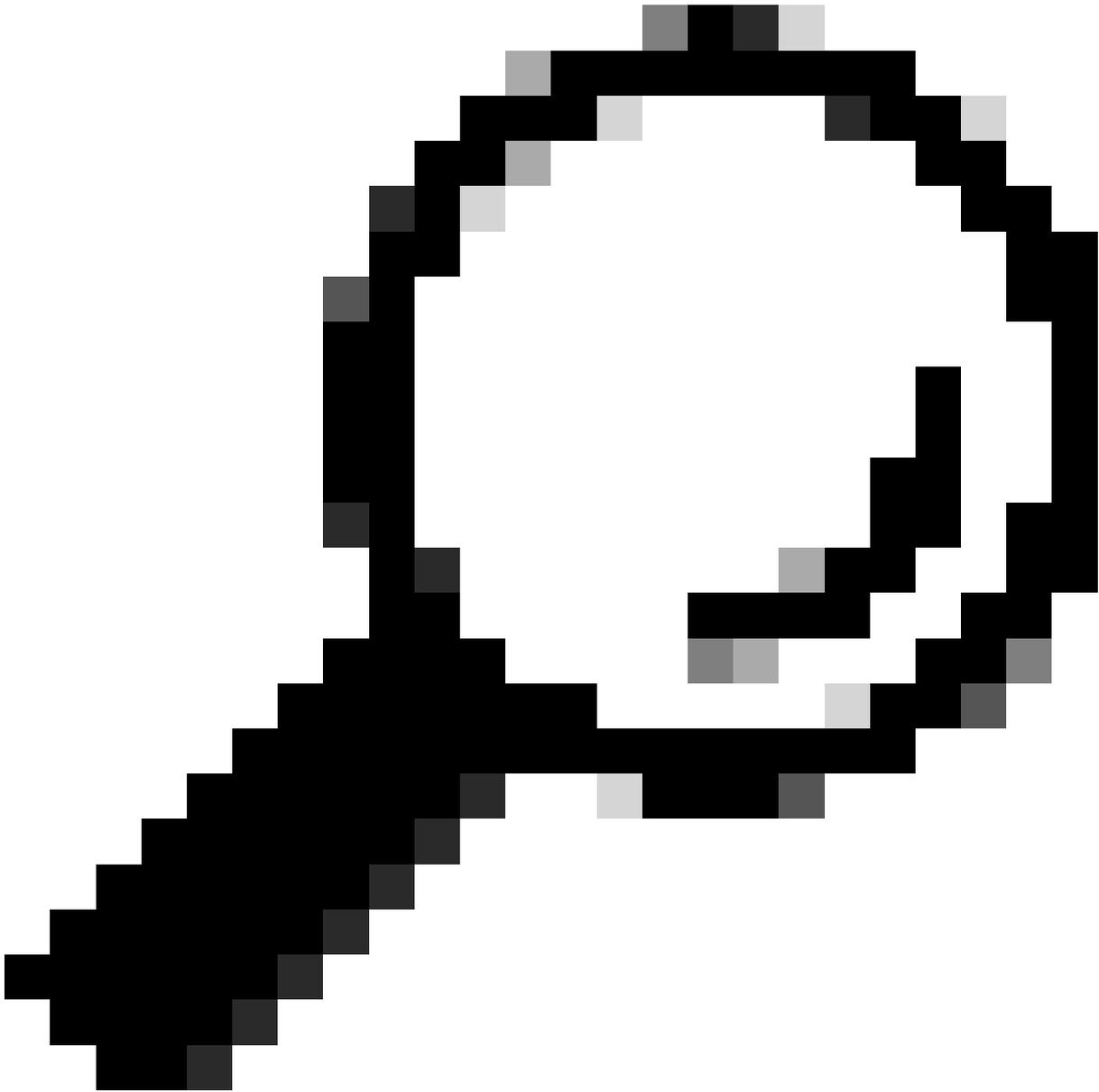
[Test Connection](#) ✔ Successful



[Exit Wizard](#)

[Back](#)

[Next](#)



ヒント：この設定では、インクリメンタルURLはオプションです。外部REST APIに要求引数がある場合、すべてのデータを要求する代わりに、これらの引数を使用して特定の引数でフィルタリングすることにより、最新の情報を取得できます。要求引数が外部REST APIサーバのドキュメントに存在することを確認します。

---

## ステップ 4：Schedule

完全同期のスケジュールを選択します。

- デフォルト値：1週間
- 最小値：12時間
- 最大値 - 1か月

差分同期のスケジュールを選択します。このオプションは、ステップ3で設定した場合にのみ表示

されます。

- デフォルト値：1日
- 最小値 – 1時間
- 最大値 – 1週間

[Next] をクリックします。

Identity Services Engine Add pxGrid Direct Connector

1 Welcome 2 Connector Definition 3 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: 09 / 26 / 2023 Start Time: 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: 09 / 26 / 2023 Start Time: 4:00 AM

Exit Wizard Back Next

## ステップ 5：親オブジェクト

属性を検索するには、JSONキーを入力する必要があります。

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": ""
}
```

## 手順 6 : 属性

ポリシーに使用できる辞書項目を設定するには、JSONの属性を選択します。

このシナリオでは、Dictionaryに含まれる属性は次のとおりです。

- 資産
- IPアドレス
- mac\_address ( オプション )
- os\_バージョン
- システムID
- sys\_update
- u\_segmentation\_group\_tag ( セグメンテーショングループ\_タグ )

[Next] をクリックします。

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](#)

## 手順 7 : 識別子

- CMDBデータベースのエンドポイントに固有で、外部REST APIサーバがJSONを取得する場所である固有識別子属性を選択します。
- ISEに固有で、エンドポイントを認可ポリシーに一致させることができる関連識別子属性を選択します。

[Next] をクリックします。

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](#)

## ステップ 8 : 要約

pxGrid Directコネクタが正しく設定されていることを確認します。[Done] をクリックします。

The screenshot shows the 'Add pxGrid Direct Connector' wizard in the Cisco Identity Services Engine (ISE) interface. The breadcrumb trail at the top indicates the current step is 'Summary'. The left sidebar shows the 'Administration' menu. The main content area displays a 'Summary' section with several expandable items: 'Connector Definition', 'URL', 'Set Up Synchronization Schedule', 'Parent Object', and 'Select Attributes Configure Dictionary Items'. The 'Identifiers' section is expanded, showing 'Unique Identifier' as 'sys\_id' and 'Correlation Identifier' as 'mac\_address'. At the bottom right, there is a 'Done' button.

コネクタが完成すると、「pxGridダイレクトコネクタ」ページの下に表示されます。

The screenshot shows the 'Administration / Network Resources' page in the Cisco Identity Services Engine (ISE) interface. The breadcrumb trail indicates the current page is 'Administration / Network Resources'. The left sidebar shows the 'Administration' menu. The main content area displays the 'pxGrid Direct Connectors' page. It includes a description of the connector and a table listing the configured connectors. The table has columns for 'Name', 'Scheduling', 'Connector Type', 'URL', and 'References'. One connector is listed: 'pxGridConnectorFLSK' with 'Scheduling' set to 'Enabled', 'Connector Type' as 'URLFETCHER', and 'URL' as 'http://10.31.126.232:5000/endpoints'. There are 'Add', 'Edit', 'Refresh', 'Scheduling', and 'Delete' buttons above the table.

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

## ステップ 9 : 検証

ISEから、Policy > Policy Elements > Dictionary > System Dictionariesに移動します。pxGridダイレクトコネクタの名前でフィルタします。これを選択して、Viewをクリックします。

Identity Services Engine Policy / Policy Elements

Dictionaries Conditions Results

System Dictionaries

Selected 0 Total 1

View Quick Filter

Name	Description
pxGridConnectorFLSK	Dictionary for pxGrid Direct Connector(Type=I

Dictionary Attributesに移動し、ステップ6でDictionary Itemsとして設定した属性のリストを確認します。

Identity Services Engine Policy / Policy Elements

Dictionaries Conditions Results

Dictionary Attributes

Selected 0 Total 7

View

Name	Internal Name	Description
<input type="checkbox"/> asset	asset	Dictionary attribute for p...
<input type="checkbox"/> ip_address	ip_address	Dictionary attribute for p...
<input type="checkbox"/> mac_address	mac_address	Dictionary attribute for p...
<input type="checkbox"/> os_version	os_version	Dictionary attribute for p...
<input type="checkbox"/> sys_id	sys_id	Dictionary attribute for p...
<input type="checkbox"/> sys_updated_on	sys_updated_on	Dictionary attribute for p...
<input type="checkbox"/> u_segmentation_gro...	u_segmentation_...	Dictionary attribute for p...

## Context Visibility pxGrid Directダッシュボード

ISEから、Context Visibility > Endpoints > More > pxGrid Direct Endpointsの順に移動します。CorrelationとUnique IDに選択した値を持つエンドポイントのリストが表示されます。

関連付けIDをクリックして詳細を表示するか、特定のエンドポイントの属性をダウンロードします。

pxGrid Direct Endpoints

This window lists the endpoint attribute data that is fetched from pxGrid Direct Connectors. Click the correlation ID for an endpoint to view or download the endpoint details. To create a new pxGrid Director Connector or to update existing connector configurations, go to the [pxGrid Direct Connectors](#) window.

Correlation ID	Unique ID	Version ID	Connector
00:50:56:9B:2D:25	c50e2e34db4c85901f0f174b13961914		pxGridConn
00:C8:F2:AC:37:D3	f4ff17bcd0f01101f0f174b139619b2		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

Attributes: asset (Unknown), assigned\_to (Victoria.Stokes@example.org), attestation\_score (false), can\_print (false), category (Hardware), cd\_rom (false), change\_control, chassis\_type, checked\_in, checked\_out, comments, company.

## pxGridダイレクトディクショナリを使用した許可ポリシーの設定

ISEから、Policy > Policy Sets > Select a Policy Set > Authorization Policyの順に移動します。任意の許可ポリシーで歯車アイコンをクリックし、[挿入]を選択します。

ルールに名前を付け、新しい条件を追加して条件スタジオを開きます。

クリックして新しい属性を追加し、未分類に移動して、pxGridダイレクトコネクタの名前で辞書

Conditions Studio

Library

Search by Name

- 5G
- BYOD\_is\_Registered
- Catalyst\_Switch\_Local\_Web\_Authentication
- Compliance\_Unknown\_Devices
- Compliant\_Devices
- EAP-MSCHAPv2
- EAP-TLS
- Guest\_Flow
- MAC\_in\_SAN
- Network\_Access\_Authentication\_Passed

Editor

Click to add an attribute

Equals

Select attribute for condition

Dictionary	Attribute	ID	Info
pxGridConnectorFLSK	asset		
pxGridConnectorFLSK	ip_address		
pxGridConnectorFLSK	mac_address		
pxGridConnectorFLSK	os_version		
pxGridConnectorFLSK	sys_id		
pxGridConnectorFLSK	sys_updated_on		
pxGridConnectorFLSK	u_segmentation_group_tag		

フィルタの下に表示します。

許可ポリシーで処理できる属性を選択し、値を設定します。Useをクリックします。



## 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

## トラブルシューティング

ISEから、Operation > Troubleshoot > Debug Wizard > Debug Log Configurationの順に移動します。Primary Admin Node (PAN)を選択して、Editをクリックします。

コンポーネント名をpxGrid Directでフィルタリングし、必要なログレベルを選択します。[Save]をクリックします。

The screenshot shows the Cisco ISE Operations / Troubleshoot interface. The 'Debug Wizard' tab is active, and the 'Debug Log Configuration' section is selected. The 'Node List' shows 'ise-demo-1.aaamex.com'. The 'Debug Level Configuration' table is displayed with the following data:

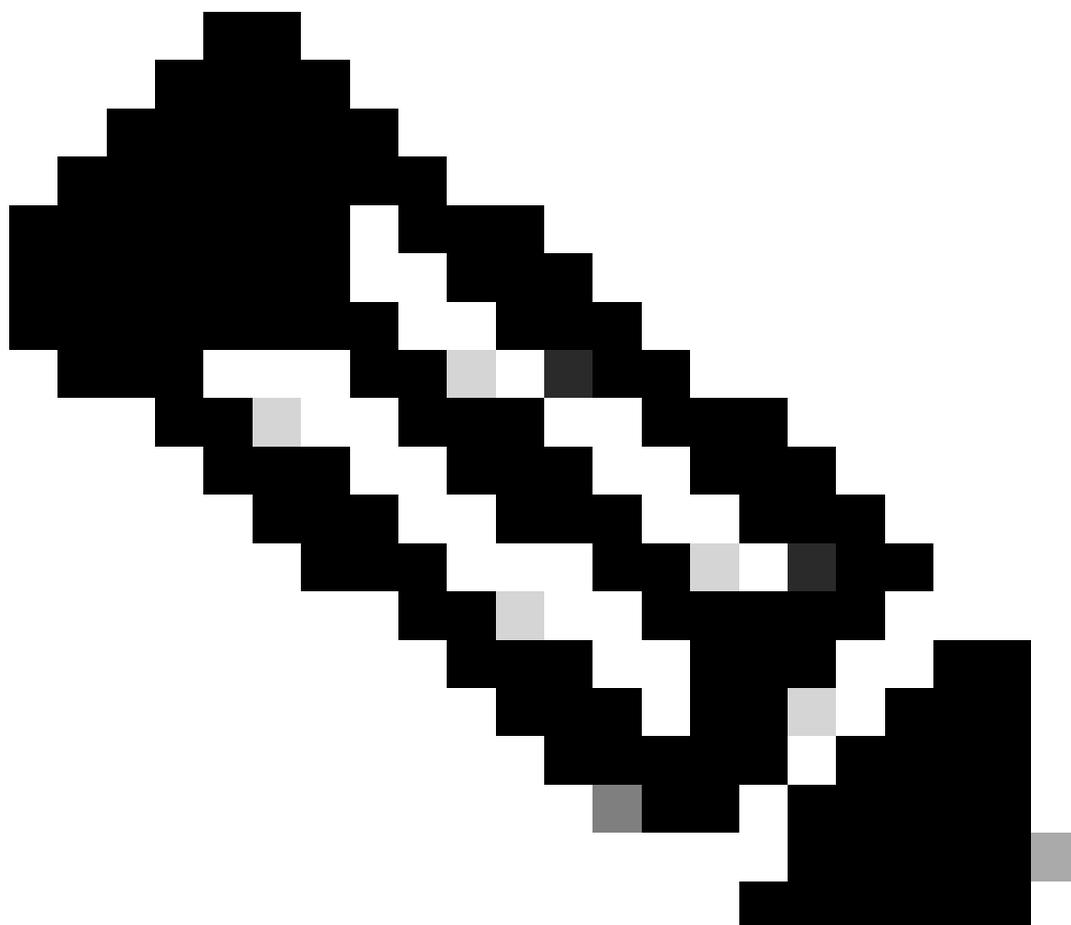
Component Name	Log Level	Description	Log file Name	Log Filter
pxgrid Direct	×			
<input type="radio"/> pxGrid Direct	DEBUG	pxGrid Direct backend and UI log messa	pxgriddirect-service.log, f	Disabled

Buttons for 'Edit', 'Reset to Default', 'Log Filter Enable', 'Log Filter Disable', and 'Quick Filter' are visible. A 'Save | Cancel' button is at the bottom.

- ISE PAN CLIでは、ログは次の場所にあります。

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

- ISE GUIで、Operations > Troubleshoot > Download Logsの順に移動し、ISE PAN > Debug log > Debug Log Type > Application Logsの順に選択します。pxgriddirect-service.logおよびpxgriddirect-connector.logのzipファイルをダウンロードします。
- 



注：

pxgriddirect-serviceのログには、フェッチされたエンドポイントデータが受信され、Cisco ISEデータベースに保存されたかどうかに関連する情報が含まれています。

pxgriddirect-connectorのログには、pxGrid DirectedコネクタがCisco ISEに正常に追加されたかどうかを示す情報が含まれています。

---

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。