# **Configure ISE 3.3 pxGrid Context-In**

### Contents

Introduction
<u>Prerequisites</u>
Requirements
Components Used
Background Information
<u>Initial Steps</u>
Enable Open API on ISE
Enable Custom Attribute for Profiling Enforcement on ISE
Swagger UI
Configure Endpoint Custom Attributes using Open API
Create Endpoint Custom Attribute
Verify Custom Attribute Creation
Context-In API for Single Endpoint
Profiling Policy for Custom Attribute
Create Endpoint
Verify Endpoint Creation
Update Endpoint
Verify Endpoint Update
Context-In API Bulk
Authorization Policy Configuration with Endpoint Identity Group
Update Endpoint in Bulk
Verify Endpoint Bulk Update
Troubleshoot

### Introduction

This document describes how to configure Cisco Identity Service Engine 3.3 pxGrid Context-in using Open API.

# Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Identity Service Engine (ISE) 3.3
- Advance REST API

### **Components Used**

- Cisco ISE 3.3
- Insomnia REST API client

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# **Background Information**

pxGrid Context-In solution through REST APIs. This is because the Context-In pubsub model has some limitations with respect to using custom attributes in profiling and authorization policies.

Custom attributes are user-defined attributes that do not come in as endpoint data through regular network probes. Prior to ISE 3.3, there were mainly two ways to input custom attribute values as endpoint data.

- pxGrid Context-In asset topic, where ISE acts as a consumer and consumes endpoint data published by an external third-party product.
- Endpoint Extensible RESTful Services (ERS) Create/Update APIs.

Both these channels have limitations for using custom attributes in profiling and authorization policies.

## **Initial Steps**

### **Enable Open API on ISE**

Open API is disabled by default on ISE. In order to enable it, navigate to Administration > System > API Settings > API Service Settings. Toggle the Open API options and click **Save**.



```
Enable Open API
```

### **Enable Custom Attribute for Profiling Enforcement on ISE**

Custom Attribute for Profiling Enforcement is disabled by default on ISE. In order to enable it, navigate to

 $\label{eq:Work Centers > Profiler > Settings > Profiler Settings. Enable Custom Attribute for Profiling Enforcement. Click Save.$ 

≡ :8	sco Identity	Services Engine			Work Cent	ters / Prof	iler			Q	Ø	٩	A
щ	Overview	Ext Id Sources	Network Devices	Endpoint Classification	Node Config	Feeds	Manual Scans	Policy Elements	Profiling Policies	Мо	re ~		
113 × 0 20 20	Profiler Sett	ings Subnet Exclusions alytics	Profiling  Profiler Sett CoA Type* Overlapping Cla Current custom Change custom Confirm change EndPoint At Anomalous Custom Atti Profiling for XSS Securit	ings assification Priority () SNMP community strings a SNMP community strings ad custom SNMP community str tribute Filter () Behaviour Detection () Behaviour Enforcement ibute for Profiling Enforcement MUD varder Persistence Queue y Scan Enforcement for EndPoi	No CoA Admin First ings:		Show 0 0						

Enable Custom Attribute for Profiling Enforcement



**Note**: The Custom Attribute for Profiling Enforcement flag indicates that an automatic re-profiling action takes place if any custom attribute is modified.

### Swagger UI

In order to access all Open API definitions on ISE, navigate to Administration > System > Settings > API Settings and click 'For more information on ISE Open API, please visit:'.

The URLs for the definitions used in this document are:

- Custom Attribute: <u>https://<ISE-PAN-IP>/api/swagger-ui/index.html?urls.primaryName=CustomAttributes</u>
- Endpoint: <u>https://<ISE-PAN-IP>/api/swagger-ui/index.html?urls.primaryName=Endpoints</u>



```
Swagger UI
```

# **Configure Endpoint Custom Attributes using Open API**

### **Create Endpoint Custom Attribute**

In order to create an endpoint custom attribute, it is mandatory to give it a name and type.

The types that can be used are:

- String
- Int
- Boolean
- Float
- Long
- IP
- Date

Method	POST
URL	https:// <ise-pan-ip>:443/api/v1/endpoint-custom-attribute</ise-pan-ip>
Authentication Type	Basic
Credentials	Use Open API account credentials
Headers	Accept:application/json Content-Type:application/json

Body	{ "attributeName": "DeviceType", "attributeType": "String" }
------	---

#### Body:

POST ▼ https://10.31.126.153/api/v1/endpoint-custom-attribute							
JSON -	Basic 👻 Qu	uery Headers 2	Docs				
1 <del>√</del> { 2 "attributeName": "DeviceType", 3 "attributeType": "String" 4 }							

Body Endpoint Custom Attribute

#### Authentication:

POST - https://10.31.126.153/api/v1/endpoint-custom-attribute					•
JSON 🗕 🛛 Ba	sic 🗕 Query	Headers 2	Docs		
ENABLED					
USERNAME	admin				
PASSWORD				•	૭
USE ISO 8859-1 🚱					

Authentication Endpoint Custom Attribute

#### Headers:



Headers Endpoint Custom Attribute

#### Expected Output:



Expected Output Endpoint Custom Attribute

### Verify Custom Attribute Creation

From ISE, navigate to Administration > Identity Management > Settings > Endpoint Custom Attributes. Verify that the attribute was created.

≡	dentity Services Eng	gine Administration / Identity Management	Q	۵	@ Ç	4   A
Ц	Identities Groups	External Identity Sources Identity Source Sequences Settings				
	User Custom Attributes	Mandatory Attribute Name Data Type				
1d	User Authentication Settings	MFCInIoHardwareManufacturer STRING				
$\times$	Endpoint Custom Attributes	MFCInfoHardwareModel STRING				
U	REST ID Store Settings	MFCInfoOperatingSystem STRING				
20		MFCInfoEndpointType STRING				
4		PostureApplicable STRING				
		LogicalProfile STRING				
		EndPointPolicy STRING				
		AnomalousBehaviour STRING				
		OperatingSystem STRING				
		BYODRegistration STRING				
		PortalUser STRING				
		LastAUPAcceptanceHours INT				
		Endpoint Custom Attributes				
		Attribute Name Type				
		DeviceType String V 🔋 +				
		Reset Save				

Endpoint Custom Attribute GUI



**Note**: The Endpoint Custom Attributes can be added manually. From ISE, navigate to Administration > Identity Management > Settings > Endpoint Custom Attributes. Click +, then enter the **Attribute Name**, and choose the **Type**.

# **Context-In API for Single Endpoint**

### **Profiling Policy for Custom Attribute**

 $From \ ISE, \ navigate \ to \ {\sf Work} \ {\sf Centers} > {\sf Profiler} > {\sf Profiling} \ {\sf Policies}. \ Click \ {\sf Add}.$ 

Enter Name of the profiling policy.

Under Rules, navigate to Attributes > Create New Condition > CUSTOMATTRIBUTE. Choose the custom attribute created, choose Operator, and enter the value to be matched. Click **Submit.** 

In this example, the DevicTypeA profiling policy is defined with CUSTOMATTRIBUTE\_DeviceType.

≡	diale Ident	ity Services Engine				Work Cen	ters / Pro	filer			Q 🖉	?	Q   2
н	Overviev	Ext Id Sources	Network	Devices	Endpoint Classification	Node Config	Feeds	Manual Scans	Policy Elements	Profiling Policies	More ~	,	
	Overview	<ul> <li>Ext Id Sources</li> <li>C</li> <li>Profiling Policies</li> <li>C Logical Profiles</li> <li>Al Profiles</li> </ul>	©	Devices Profiler Po * Name Policy Enab * Minimum * Exception * Network 3 Create an I * Parent Po * Associate System Typ Rules If Cond	Indpoint Classification licy led Certainty Factor Action Scan (NMAP) Action dentity Group for the policy licy d CoA Type be liten CustomATTRIBUTE_Devia Condition Na	Node Config DeviceTypeA  P DeviceTypeA  P DeviceTypeA  P DeviceTypeA  P DeviceTypeA P	rtainty Factor	Manual Scans Description id Range 1 to 65535 ) oup hierarchy Nereases $\vee$ 100 DNTAIN $\sim$	Policy Elements	Profiling Policies	More ~	Can	cel

Profiler Policy

### **Create Endpoint**

Method	POST
URL	https:// <ise-pan-ip>:443/api/v1/endpoint</ise-pan-ip>
Authentication Type	Basic
Credentials	Use Open API account credentials
Headers	Accept:application/json Content-Type:application/json
Body	{ "name": "94:DA:5F:96:74:63", "customAttributes": {"DeviceType":"A"}, "description": null, "connectedLinks": null, "mdmAttributes": null, "groupId": "aa0e8b20-8bff-11e6-996c-525400b48521", "identityStore": "", "identityStoreId": "", "mac": "94:DA:5F:96:74:63",

In this example, an endpoint with the mac address 94:DA:5F:96:74:63 and DeviceType set to A is created.

<pre>"productId": null, "serialNumber": null, "deviceType": null, "softwareRevision": null, "hardwareRevision": null, "protocol": null, "staticGroupAssignment": false, "staticProfileAssignment": false }</pre>
--

### Body:

POST 🔻	https://10.31.126.153/api/v1/endpoint	Send	-							
JSON <del>-</del>	Basic - Query Headers 2 Docs									
1- <u>{</u>										
2	"name": "94:DA:5F:96:74:63",									
3	<pre>"customAttributes": {"DeviceType":"A"},</pre>									
4	"description": null,									
5	"connectedLinks": null,									
6	"mdmAttributes": null,									
7	"groupId": "aa0e8b20-8bff-11e6-996c-525400b48521",									
8	"identityStore": "",									
9	"identityStoreId": "",									
10	"mac": "94:DA:5F:96:74:63",									
11	"portalUser": "",									
12	"profileId": "",									
13	"ipAddress": null,									
14	"vendor": null,									
15	"productId": null,									
16	"serialNumber": null,									
17	"deviceType": null,									
18	"softwareRevision": null,									
19	"hardwareRevision": null,									
20	"protocol": null,									
21	"staticGroupAssignment": false,									
22	"staticProfileAssignment": false									
23 }										

Body Endpoint

#### Authentication:

POST ▼ https://10.31.126.153/api/v1/endpoint							•
JSON 🔻	Basic 🔻	Query	Headers 2	Docs			
ENABLED							
USERNAME	admin	1					
PASSWORD		••				•	9

Authentication Endpoint

#### Headers:

POST ▼ https://10.31.126.153/api/v1/endpoint					
JSON - Basic - Query	Headers 2	Docs			
Add Delete All Toggle Descri	ption				
Content-Type		application/json		Ô	
Accept		application/json		Ô	

Headers Endpoint

#### Expected Output:



Expected Output Endpoint

### **Verify Endpoint Creation**

From ISE, navigate to Context Visibility > Endpoints. Filter with the name of the profiling policy created under **Endpoint Profile** column.

$\equiv rac{\mathrm{obslit}}{\mathrm{cisco}}$ Identity Services Engine	Context Visibility / Endpoints	
Authentication BYOD Cor	oliance Compromised Endpoints Endpoint Classification Guest Vulnerable Endpoints	Hardware 5G Endpoints More – Manage – – – – – – – – – – – – – – – – – – –
INACTIVE ENDPOINTS       Image: state s	C     AUTHENTICATION STATUS     C     C     AUTHENTICATION SO       2     • connected - 50%     • disconnected - 50%	C O     NETWORK DEVICES O       dentity droup     Location       available.     Type       Device Name
Add     Edit     ●     ANC ~       MAC Address     Status       ×     MAC Address     Status       ● 94:DA:5F:96:74:63	Rows/Page     3I<       Change Authorization >     Clear Threats & Vulnerabilities     Export >     Import >     MDM Actions >     Release Rejected     Rev       IP Address     Username     Hostname     Location     Endpoint Profile     Authentication Failure Ress        IP Address     Username     Hostname     Location     Endpoint Profile     Authentication Failure Ress        IP Address     Username     Hostname     Location     Endpoint Profile     Authentication Failure Ress	1     Image: Constraint of the second s

Context Visibility DeviceTypeA

### **Update Endpoint**

In order to update endpoints via Open API, the URL path requires the parameter value. This parameter can be the **ID** or **MAC address** of the endpoint.

In this example, a new profiling policy DeviceTypeB was defined in order to update the custom attribute **DeviceType** set to **B** and the **value** is set as the **MAC address**.

Method	PUT
URL	https:// <ise-pan-ip>:443/api/v1/endpoint/{value}</ise-pan-ip>
Authentication Type	Basic
Credentials	Use Open API account credentials
Headers	Accept:application/json Content-Type:application/json
Body	{ "name": "94:DA:5F:96:74:63", "customAttributes": {"DeviceType":"B"}, "description": null, "connectedLinks": null, "mdmAttributes": null, "groupId": "aa0e8b20-8bff-11e6-996c-525400b48521", "identityStore": "",

"identityStoreId": "",
"mac": "94:DA:5F:96:74:63",
"portalUser": "",
"profileId": "",
"ipAddress": null,
"vendor": null,
"productId": null,
"serialNumber": null,
"deviceType": null,
"softwareRevision": null,
"hardwareRevision": null,
"protocol": null,
"staticGroupAssignment": false,
"staticProfileAssignment": false
}

### Body:

PUT 🔻 ł	https://10.31.126.153/api/v1/endpoint/94:DA:5F:96:74:63	Send	-
JSON 🗕	Basic - Query Headers Docs		
1- [			
2	"name": "94:DA:5F:96:74:63",		
3	<pre>"customAttributes": {"DeviceType":"B"},</pre>		
	"description": null,		
5	"connectedLinks": null,		
6	"mdmAttributes": null,		
7	"groupId": "aa0e8b20-8bff-11e6-996c-525400b48521",		
8	"identityStore": "",		
9	"identityStoreId": "",		
10	"mac": "94:DA:5F:96:74:63",		
11	"portalUser": "",		
12	"profileId": "",		
13	"ipAddress": null,		
14	"vendor": null,		
15	"productId": null,		
16	"serialNumber": null,		
17	"deviceType": null,		
18	"softwareRevision": null,		
19	"hardwareRevision": null,		
20	"protocol": null,		
21	"staticGroupAssignment": false,		
22	"staticProfileAssignment": false		
23 }			

Body Update Endpoint

Authentication:

PUT - https://10.31.126.153/api/v1/endpoint/94:DA:5F:96:74:63							•
JSON 🗕	Basic 🔻	Query	Headers 2	Docs			
ENABLED							
USERNAME	admii	า					
PASSWORD						•	0

Authentication Update Endpoint

#### Headers:

PUT - https://10.31.126.153/api/v1/endpoint/94:DA:5F:96:74:63						
JSON - Basic - Query	Headers <sup>2</sup>	Docs				
Add Delete All Toggle Descr	iption					
Content-Type		application/json		Ô		
Accept		application/json		Ē		

Headers Update Endpoint

Expected Output:

<b>200</b> OK	1.36 s 670 B	12 Hours Ago 🔻
Preview 👻	Headers <sup>17</sup> Cookies Timeline	
1- {		
2 "	id": "2c816dc0-5da9-11ee-90b9-0a0622fef326",	
3 "	name": "94:DA:5F:96:74:63",	
4 "	description": "",	
5 <b>~ "</b>	customAttributes": {	
6	"DeviceType": "B"	
7 }	,	
8 "	connectedLinks": null,	
9 "	mdmAttributes": null,	
10 "	groupId": "940edf90-5d9f-11ee-90b9-0a0622fef326",	
11 "	identityStore": "",	
12 "	identityStoreId": "",	
13 "	mac": "94:DA:5F:96:74:63",	
14 "	portalUser": "",	
15 "	profileId": "942303d0-5d9f-11ee-90b9-0a0622fef326",	
16 "	ipAddress": "",	
17 "	vendor": "",	
18 "	productld": "",	
19 "	serialNumber": "",	
20	devicelype": "A",	
21 "	softwareRevision": "",	
22 "	nardwarekevision": "",	
23	protocol": "",	
24	staticGroupAssignment": Talse,	
25		
26 }		

Expected output Update Endpoint

### Verify Endpoint Update

From ISE, navigate to Context Visibility > Endpoints. Filter with the name of the profiling policy created under Endpoint Profile column.

$\equiv rac{\mathrm{disclo}}{\mathrm{cisco}}$ Identity Services Engin	e	Context Visibility / Endpoint	ts	Q & @ Q   A
Authentication BYOD	Compliance Compromised Endpoints	Endpoint Classification Guest	Vulnerable Endpoints Hardware	5G Endpoints More $\vee$ Manage $\vee$ $>$ Hide Charts
INACTIVE ENDPOINTS           %           0           &	C 2	N STATUS • C ©	AUTHENTICATIONS O Failure Reason Identity Store Identity Group No data available.	C C NETWORK DEVICES O
Add         Edit         I         I           MAC Address         S         X         MAC Address         S           94:DA:5F:96:74:63         S         S         S         S	NNC V Change Authorization V Clear Threats & Vuln Status IP Address Username Status V IP Address Username	arabilities Export Import MDM Action Hostname Location Endpoint Profile Hostname Location Endpoint Profile DeviceTypeB	tows/Page 1 → K < 1 a × Release Rejected Revole Certificate e Authentication Failure Re Authenticati Authentication Failure Reason Authenticati	11>>  Go 1 Total Rows     Filter V      Total Rows     Filter V     Authorization P Authentication     Polic Authorization Policy Authentication

Context Visibility DeviceTypeB

# **Context-In API Bulk**

### Authorization Policy Configuration with Endpoint Identity Group

From ISE, navigate to Policy > Policy Sets > Select a Policy Set > Authorization Policy. Click the gear icon in any of the Authorization Policies and choose **Insert**.

Give a name to the rule and add a new condition in order to open the Condition Studio.

Add a new attribute and navigate to Identity Group > Name > CONTAINS > Select the Endpoint Profile > USE.

Choose the profile as the result of the condition. Click Save.

In this example, the DeviceTypeA is the name of the rule.

≡ dia	le Ident	ity Servic	es Engine			Policy / Policy Se	ets			Q	۵	0	Q	8
	>4	Authorization	Policy - Global Exceptions											
PI	$\sim l$	Authorization	Policy(15)											
							Results							
×		🕂 Status	Rule Name	Con	nditions		Profiles		Security Groups		ŀ	lits	Actions	
0		Q Search	n											
#		•	Wireless Black List Default	AND	Image: Wireless_Access           R         IdentityGroup-Name EQUALS Endpoint id	dentity Groups:Blacklist	Block_Wireless_Access	<i>e</i> +	Select from list	0	+	0		
		۲	DeviceTypeA	8	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:DeviceTypeA		PermitAccess	1 +	Select from list	0	+	0	(2)	
?		٢	Profiled Cisco IP Phones	8	IdentityGroup-Name EQUALS Endpoint Identity G Phone	iroups:Profiled:Cisco-IP-	Cisco_IP_Phones	1 +	Select from list	0	+	0	(2)	
		0	Profiled Non Cisco IP Phones		Non_Cisco_Profiled_Phones		Non_Cisco_IP_Phones	/ +	Select from list	0	+	0	{ô}	
		. 0	Basic_Authenticated_Access	-	Network_Access_Authentication_Passed		PermitAccess	<i>•</i> +	Select from list	0	+	3		

Policy Sets

### **Update Endpoint in Bulk**

In order to change the attribute for different endpoints, the bulk API call is needed.

In this example, the Radius request from different endpoints does not have any custom attribute, and the **Endpoint Profile** is set as **Unknown**.

≡	diale Ident	ity Services Eng	ine			Con	text Visibility /	Endpoin	its			Q	<b>\$</b> @	0 Q   Q
	Authent	ication BYOD	Compliance	Compromise	d Endpoints	Endpoint C	Classification	Guest	Vulnerable	Endpoints	Hardware	5G Endpoints	More	✓ Manage ∨ → Hide Charts
цЫ	INAC	TIVE ENDPOINTS		63	AUTHENTICATION S	TATUS 🛈		6 8	AUTHENTICA	TIONS ()	entity Group	ජ ව	NETWORK D	EVICES ()
* • •	<			0	З		connected - 66.     disconnected - 2	57% 3.33%		No data a	vailable.		(	3
	ø	Add Edit 🏮	ANC V Change Ar	uthorization $\vee$ C	lear Threats & Vulnerab	ilities Expe	art V Import V	MDM Actio	Rows/Page <u>3</u>	I< < _1 Rejected Revo	e Certificate	0 /1>>	Go	] 3 Total Rows
		MAC Address	Status	IP Address	Username H	Hostname	Location	End	point Profile	Authorization	Policy	Authentication Failure	Re Aut	hentication
	×	MAC Address	Status ~	IP Address	Username	Hostname	Location	End	Ipoint Profile	Authorization Po	licy	Authentication Failure Re	ason Aut	thentication Polic
		94:DA:5F:96:74:61	••	10.89.210.248	94-DA-5F		Location > All Locat	ions Unkr	nown	Basic_Authentica	ted_Access		MAE	3
		94:DA:5F:96:74:62	<b>n</b> -	10.218.185.96	94-DA-5F		Location > All Locat	ions Unkr	nown	Basic_Authentica	ted_Acce	-	MAE	3
	_	94:DA:5F:96:74:65	<b>N</b>	10.112.50.171	94-DA-5F		Location > All Locat	ions Unkr	nown	Basic_Authentica	ted_Access		MAE	3

Context Visibility Uknown Profile

Method	PUT
URL	https:// <ise-pan-ip>:443/api/v1/endpoint/bulk</ise-pan-ip>
Authentication Type	Basic
Credentials	Use Open API account credentials
Headers	Accept:application/json Content-Type:application/json
Body	[ { "name": "94:DA:5F:96:74:61", "customAttributes": {"DeviceType":"A"}, "description": null, "connectedLinks": null, "mdmAttributes": null, "groupId": "aa0e8b20-8bff-11e6-996c-525400b48521", "identityStore": "", "identityStoreId": "", "identityStoreId": "", "mac": "94:DA:5F:96:74:61", "portalUser": "", "ipAddress": "94:DA:5F:96:74:61", "vendor": null,

"productId": null,
"serialNumber": null,
"deviceType": null,
"softwareRevision": null,
"hardwareRevision": null,
"protocol": null,
"staticGroupAssignment": false,
"staticProfileAssignment": false
}.
{
"name": "94:DA:5F:96:74:62".
"customAttributes": {"DeviceTvpe":"A"}.
"description": null.
"connectedLinks": null.
"mdmAttributes": null.
"groupId": "aa0e8b20-8bff-11e6-996c-525400b48521".
"identitvStore": "".
"identityStoreId": "".
"mac": "94:DA:5F:96:74:62".
"portalUser": "".
"profileId": "".
"ipAddress": "10.218.185.96".
"vendor": null.
"productId": null.
"serialNumber": null.
"deviceTvpe": null.
"softwareRevision": null.
"hardwareRevision": null.
"protocol": null.
"staticGroupAssignment": false.
"staticProfileAssignment": false
}
1
-

Body:

PUT 🔻 h	ttps://10.31.126.153/api/v1/endpoint/bulk	Send	-
JSON 🔻	Basic - Query Headers Docs		
1- [			
2-	{		
3	"name": "94:DA:5F:96:74:61",		
4	<pre>"customAttributes": {"DeviceType":"A"},</pre>		
5	"description": null,		
6	"connectedLinks": null,		
7	"mdmAttributes": null,		
8	"groupId": "aa0e8b20-8bff-11e6-996c-525400b48521",		
9	"identityStore": "",		
10	"identityStoreId": "",		
11	"mac": "94:DA:5F:96:74:61",		
12	"portalUser": "",		
13	"profileId": "",		
14	"ipAddress": "10.89.210.248",		
15	"vendor": null,		
16	"productId": null,		
17	"serialNumber": null,		
18	"deviceType": null,		
19	"softwareRevision": null,		
20	"hardwareRevision": null,		
21	"protocol": null,		
22	"staticGroupAssignment": false,		
23	"staticProfileAssignment": false		
24	},		



#### Authentication:

PUT - https://10.31.126.153/api/v1/endpoint/bulk								
JSON 🗕	Basic 🔻	Query	Headers 2	Docs				
ENABLED								
USERNAME	admin							
PASSWORD						a		
PASSWORD								

Authentication Endpoint Bulk

Headers:



Headers Endpoint Bulk

#### Expected Output:



Expected Output Endpoint Bulk

### Verify Endpoint Bulk Update

From ISE, navigate to Context Visibility > Endpoints. Filter with the name of the profiling policy created under the **Endpoint Profile** column.

≡ :	hale Identity Services E	ngine		Conte	oxt Visibility / End	points		۵ ۵	ଡ ଢ   ହ
jų Et	Authentication BYO	D Compliance	Compromised Endpoin	s Endpoint Cla	ssification Gue	st Vulnerable	Endpoints Hardware	5G Endpoints N	lore -> Manage ->
рġ	INACTIVE ENDPOINTS		ී ට AUTHENTIC	ATION STATUS	යි ස	AUTHENTICA Failure Reason	TIONS () Identity Store Identity Group	ී ට NETW	ORK DEVICES ()
* • •	<			3	connected - 66.67% e disconnected - 33.33%		No data available.		3
	💭 Add Edit 🏮	ANC 🗸 Change J	Authorization 🗸 🛛 Clear Threats 8	Vulnerabilities Export	∽ Import ∽ MDM	Rows/Page <u>3</u>	→ I< < <u>1</u> Rejected Revoke Certificate	<u> </u>	Go 3 Total Rows Filter V 🔕
	MAC Address	Status	IP Address Usern	me Hostname L	Location	Endpoint Profile	Authorization Policy	Authentication Failure Re	Authentication
	× MAC Address	Status ~	IP Address Userna	me Hostname	Location	Endpoint Profile	Authorization Policy	Authentication Failure Reason	Authentication Polic
	94:DA:5F:96:74:6	n n.	10.89.210.248 94:DA:	F:9 L	ocation > All Locations	DeviceTypeA	Basic_Authenticated_Acce		MAB
	94:DA:5F:96:74:6	2 °1.	10.218.185.96 94:DA:	F:9 L	ocation > All Locations	DeviceTypeA	Basic_Authenticated_Acce	-	MAB
	94:DA:5F:96:74:6	s •1.	10.112.50.171 94:DA:	F:9 L	ocation > All Locations	DeviceTypeA	Basic_Authenticated_Acce		MAB

Context Visibility DevcieTypeA Endpoint Profile

For the endpoint, in order to use the correct Authorization Policy **DeviceTypeA**, the endpoint must reauthenticate.

	dentity Services Eng	ine		Con	text Visibility / End	points		Q (	0 0 0 A
Aut	hentication BYOD	Compliance	Compromised Endpoints	Endpoint C	Classification Gue	st Vulnerable	e Endpoints Har	dware 5G Endpoints	More $\vee$ Manage $\vee$ > Hide Charts
18 % 0 < 40 Ali			authentication	a a constanti a	년 유 e connected - 66.67% e disconnected - 33.33%	AUTHENTIC	Identity Store Identity Generative Construction Construct	IC O NET	WORK DEVICES ation Type Device Name
	Add         Edit         Image: Control of the state of	ANC Change Au Status Status "I. "I.	IP Address         Usernan           IP Address         Usernan           IP Address         Usernan           10.149.100.195         94-DA-51           10.193.221.131         94-DA-51           10.53.2.201         94-DA-54	ulnerabilities Expe e Hostname a	Location All Locations	Rows/Page 3 Actions V Release Endpoint Profile Endpoint Profile DeviceTypeA DeviceTypeA	IX < 1     Rejected Revoke Cert      Authorization Policy      DeviceTypeA      DeviceTypeA      DeviceTypeA	Contraction Failure Reson  Authentication Failure Reson	Go 3 Total Rows Fitter V Image: Imag

Context Visibility DevcieTypeA Authorization Policy

### Troubleshoot

This section provides information that you can use in order to troubleshoot your configuration.

From ISE, navigate to Operation > Troubleshoot > Debug Wizard > Debug Log Configuration. Choose your Primary Admin Node (PAN) and clickEdit.

Filter the Component Nameby API service and choose the Log Level needed. ClickSave.

≡	diade Identity Services E	ingine		Ope	erations / Troubl	eshoot			Q	۵	@ (	2   A
Щ	Bookmarks	Diagnostic Tools Download	Logs De	bug Wizard								
	Dashboard	Debug Profile Configuration	Nederline	N los dans 1 anno 1								
10	Context Visibility	Debug Log Configuration	Dob		nfiguratio	•						
*	Operations		Deb	ug Level CC	iniguratio							a
-0	Policy		/ Edit	← Reset to Default	Log Filter Enable	Log Filter Disable				Quic	k Filter 🗸	V
80	Administration			Component Name	A Log Level	Description		Log file Name	Log	9 Filter		
di.	Work Centers			apiservice	×							
			•	apiservice	DEBUG	ISE API Service Io	ogs	api-service.log	Dis	abled		
?	Interactive Help						Save   Cancel					

Debug Level Configuration Open API

• On ISE PAN CLI the logs are found at:

- On ISE GUI navigate to Operations > Troubleshoot > Download Logs > Select ISE PAN > Debug log > Debug Log Type > Application Logs. Download the zip files for api-service.log.
- API response codes and their possible meanings:
  - 200 (OK): Indicates the Open API successfully carried out the desired action.
  - 201 (Created): Indicates the resource was created and the request was successful.
  - 400 (Bad Request): The server is unable to process the request. Recognize client errors due to malformed request syntax, invalid parameters, and so on. Read the message details if available.
  - 401 (Unauthorised): This indicates that the action was undertaken with the wrong credentials or no credentials, or the account is not authorized to perform this action.
  - 403 (Forbidden): This indicates the server is capable of understanding the request but is not authorized.
  - 404 (Not Found): This indicates the server is unable to find the requested resource.
  - 500 (Internal Server Error): Indicates an issue on the server side. Logs on ISE can help understand the cause.