Configure ISE 3.3 pxGrid Context-In

Contents

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

The information in this document is based on these software and hardware versions:

- 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.

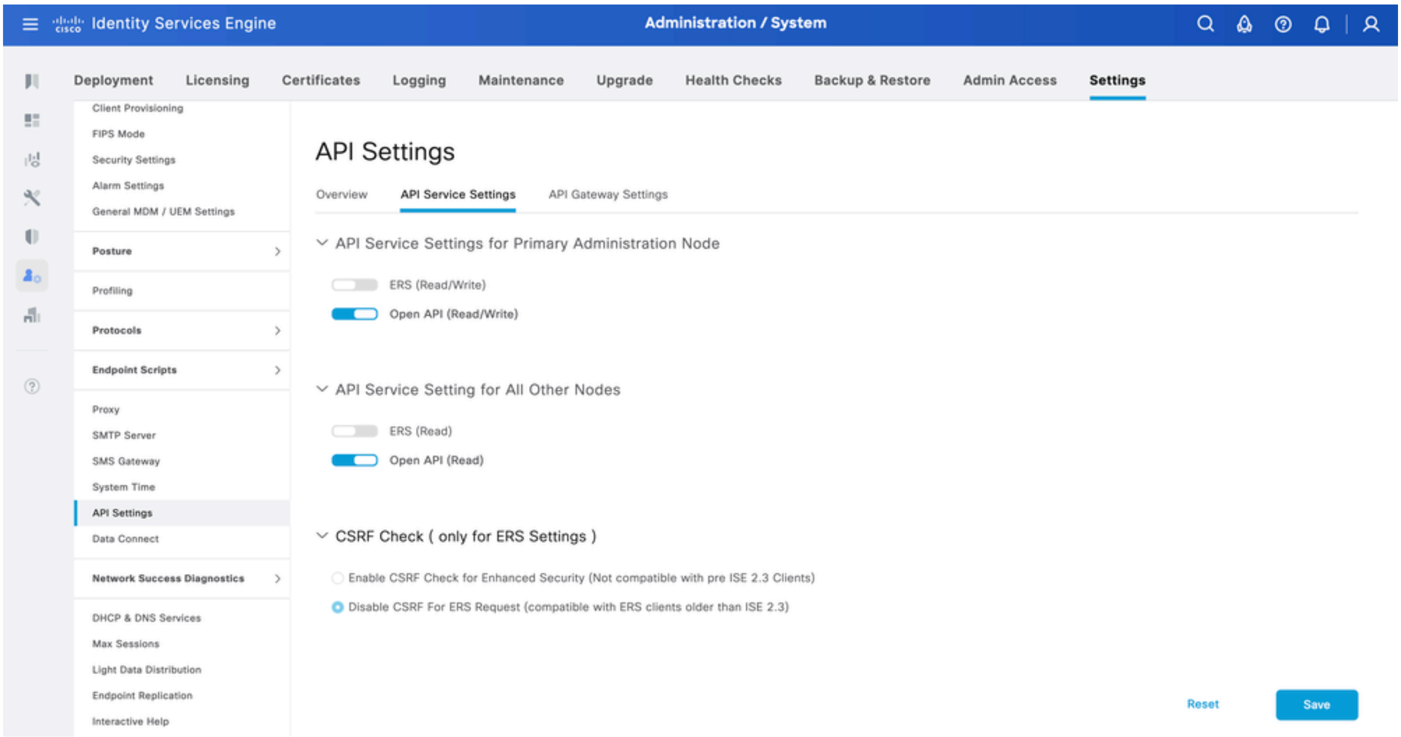
- pxGrid Context-In asset topic, where ISE acts as a consumer and consumes endpoint data published by an external third-party product.
- Endpoint Extensible RESTful Services (ERS) Create/Update APIs.

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**.



API Settings

API Service Settings for Primary Administration Node

☐ ERS (Read/Write)

☑ Open API (Read/Write)

API Service Setting for All Other Nodes

☐ ERS (Read)

☑ Open API (Read)

CSRF Check (only for ERS Settings)

○ Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)

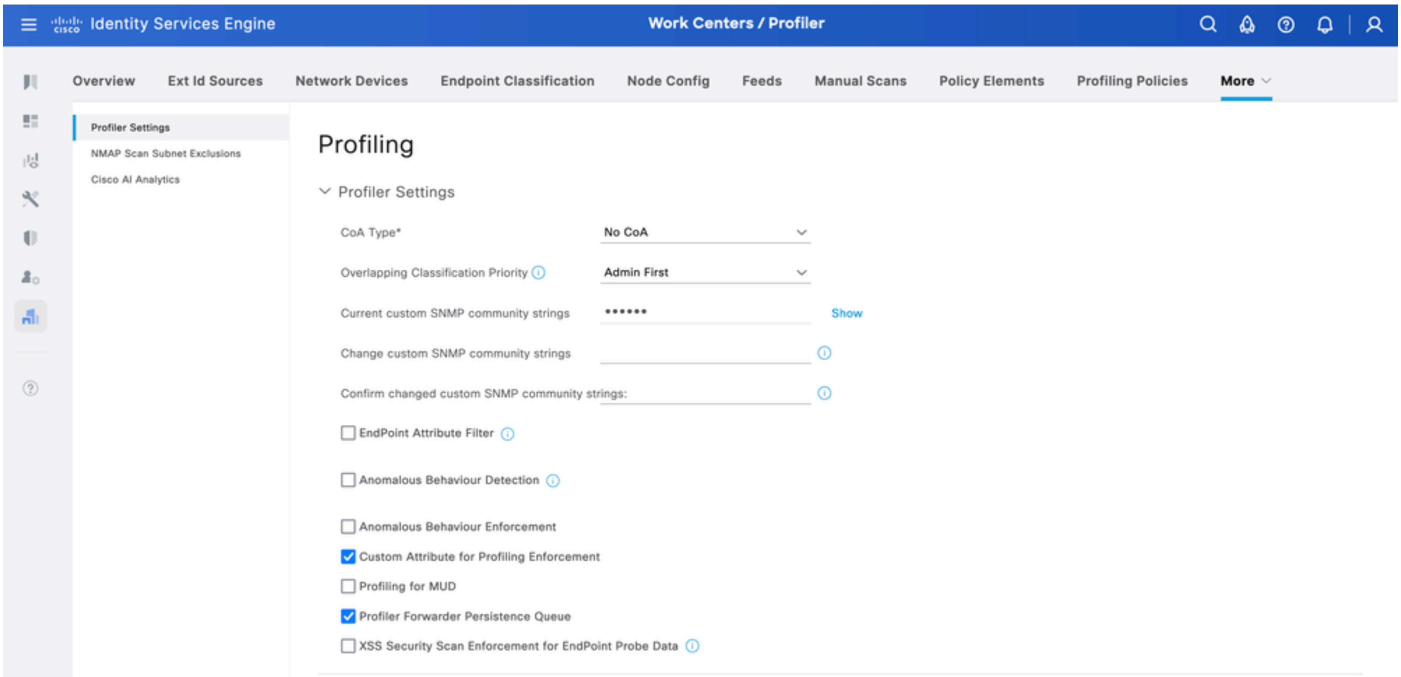
● Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)

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

Work Centers > Profiler > Settings > Profiler Settings. Enable Custom Attribute for Profiling Enforcement. Click **Save**.



Profiling

Profiler Settings

CoA Type* No CoA

Overlapping Classification Priority Admin First

Current custom SNMP community strings ••••••

Change custom SNMP community strings

Confirm changed custom SNMP community strings:

□ EndPoint Attribute Filter

□ Anomalous Behaviour Detection

□ Anomalous Behaviour Enforcement

☑ Custom Attribute for Profiling Enforcement

□ Profiling for MUD

☑ Profiler Forwarder Persistence Queue

□ XSS Security Scan Enforcement for EndPoint Probe Data

Enable Custom Attribute for Profiling Enforcement

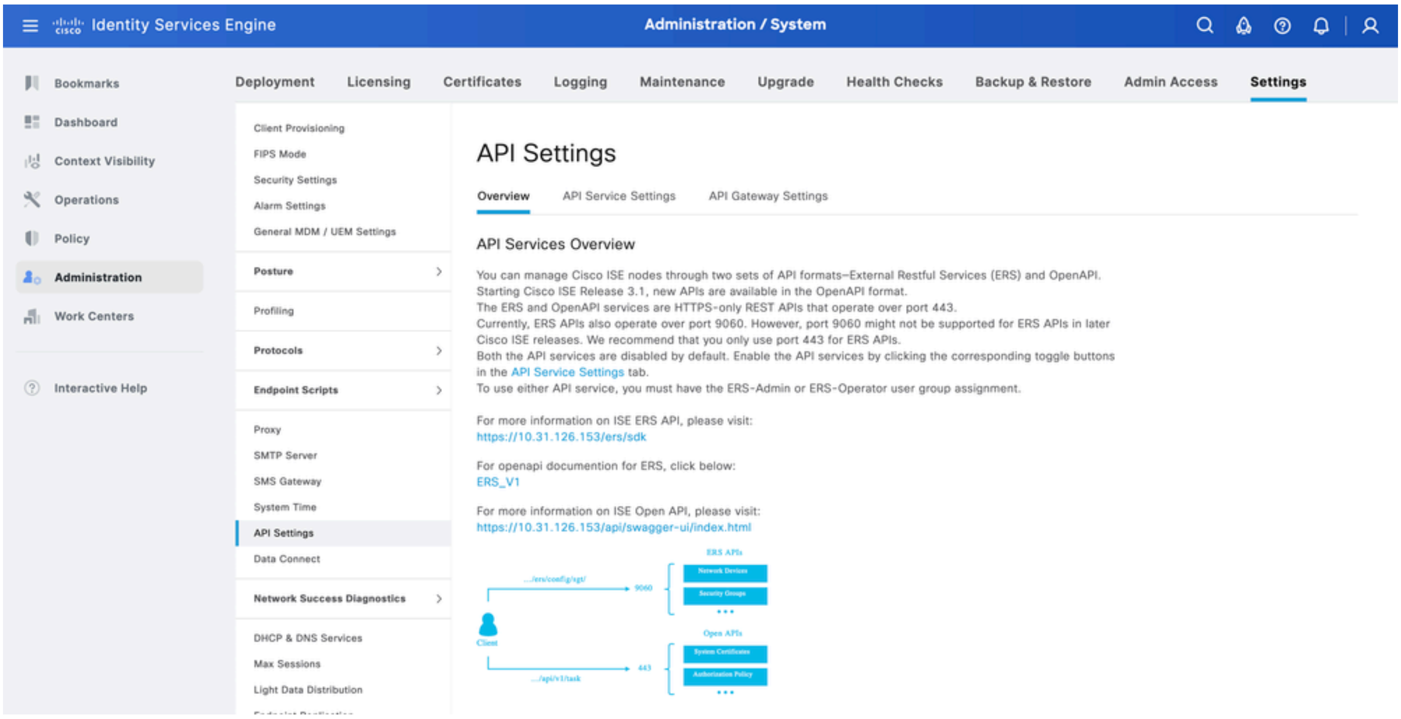
Note: The Custom Attribute for Profiling Enforcement flag indicates that an automatic re-profiling action takes place if any custom attribute is modified.

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



API Settings

API Services Overview

You can manage Cisco ISE nodes through two sets of API formats–External Restful Services (ERS) and OpenAPI.
Starting Cisco ISE Release 3.1, new APIs are available in the OpenAPI format.
The ERS and OpenAPI services are HTTPS-only REST APIs that operate over port 443.
Currently, ERS APIs also operate over port 9060. However, port 9060 might not be supported for ERS APIs in later Cisco ISE releases. We recommend that you only use port 443 for ERS APIs.
Both the API services are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the API Service Settings tab.
To use either API service, you must have the ERS-Admin or ERS-Operator user group assignment.

For more information on ISE ERS API, please visit:
https://10.31.126.153/ers/sdk

For openapi documention for ERS, click below:
ERS_V1

For more information on ISE Open API, please visit:
https://10.31.126.153/api/swagger-ui/index.html

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.

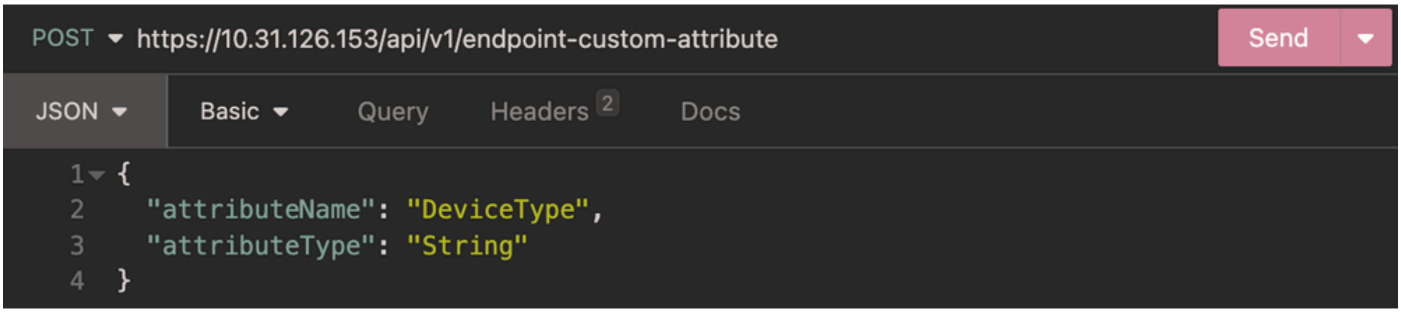
The types that can be used are:

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

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

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

Body:

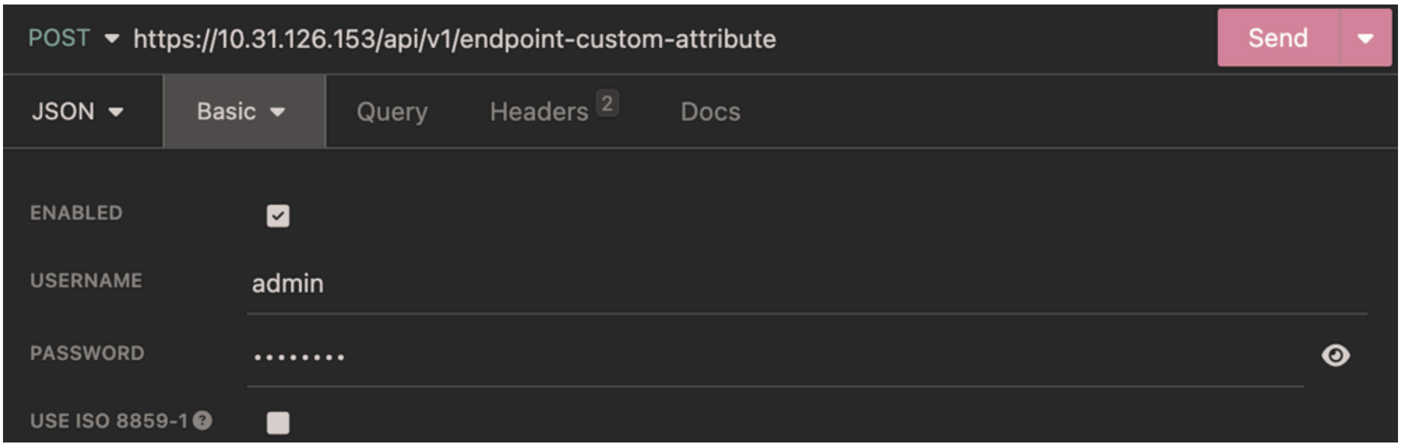


POST https://10.31.126.153/api/v1/endpoint-custom-attribute

```
{
  "attributeName": "DeviceType",
  "attributeType": "String"
}
```

Body Endpoint Custom Attribute

Authentication:



POST https://10.31.126.153/api/v1/endpoint-custom-attribute

ENABLED ☑

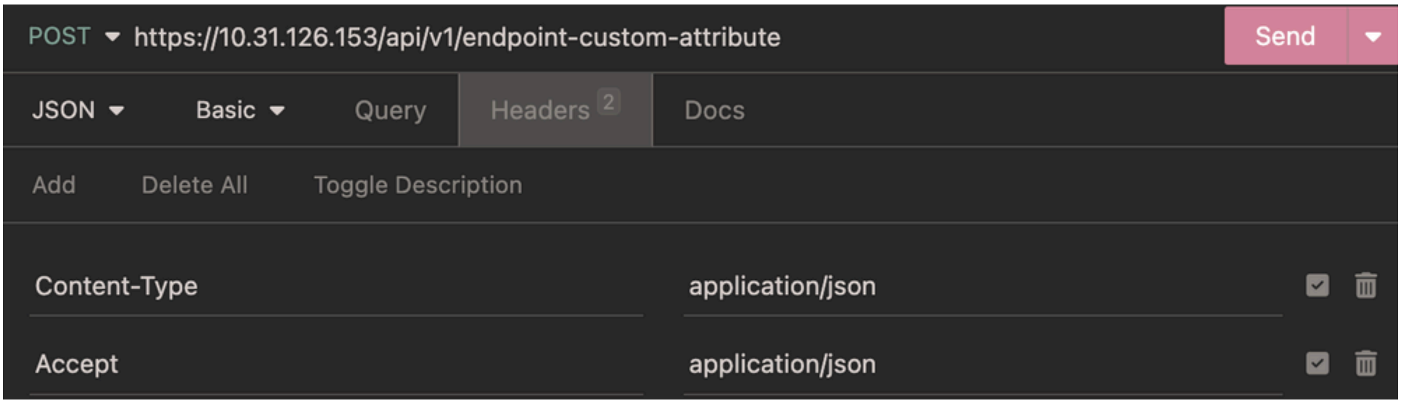
USERNAME admin

PASSWORD •••••••••

USE ISO 8859-1 □

Authentication Endpoint Custom Attribute

Headers:

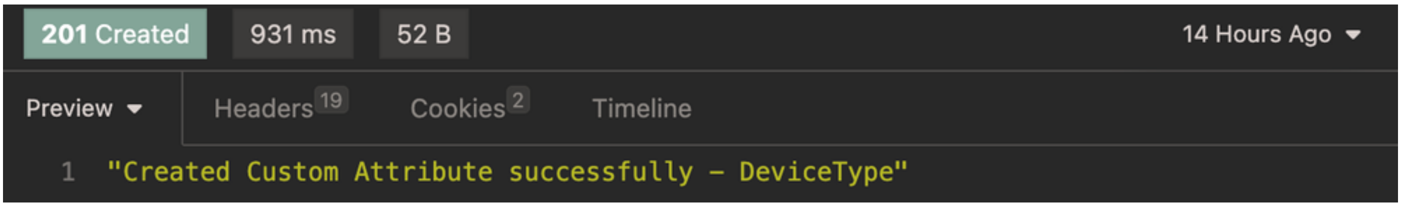


POST https://10.31.126.153/api/v1/endpoint-custom-attribute

Content-Type	application/json	☑
Accept	application/json	☑

Headers Endpoint Custom Attribute

Expected Output:

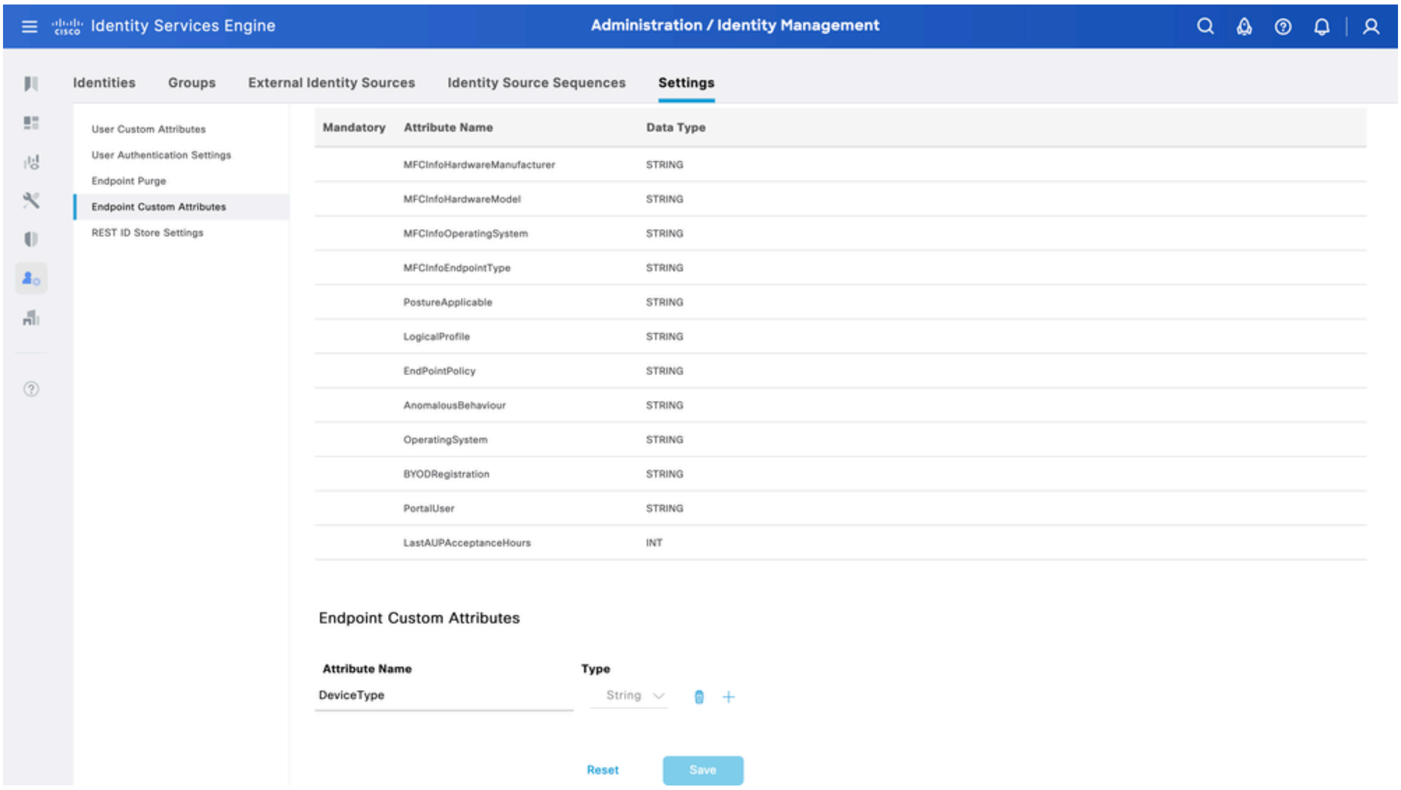


```
1  "Created Custom Attribute successfully - DeviceType"
```

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.



Identity Services Engine
Administration / Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
User Custom Attributes
User Authentication Settings
Endpoint Purge
Endpoint Custom Attributes
REST ID Store Settings
Reset
Save

Mandatory	Attribute Name	Data Type
	MFCInfoHardwareManufacturer	STRING
	MFCInfoHardwareModel	STRING
	MFCInfoOperatingSystem	STRING
	MFCInfoEndpointType	STRING
	PostureApplicable	STRING
	LogicalProfile	STRING
	EndPointPolicy	STRING
	AnomalousBehaviour	STRING
	OperatingSystem	STRING
	BYODRegistration	STRING
	PortalUser	STRING
	LastAUPAcceptanceHours	INT

Endpoint Custom Attributes

Attribute Name	Type
DeviceType	String

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

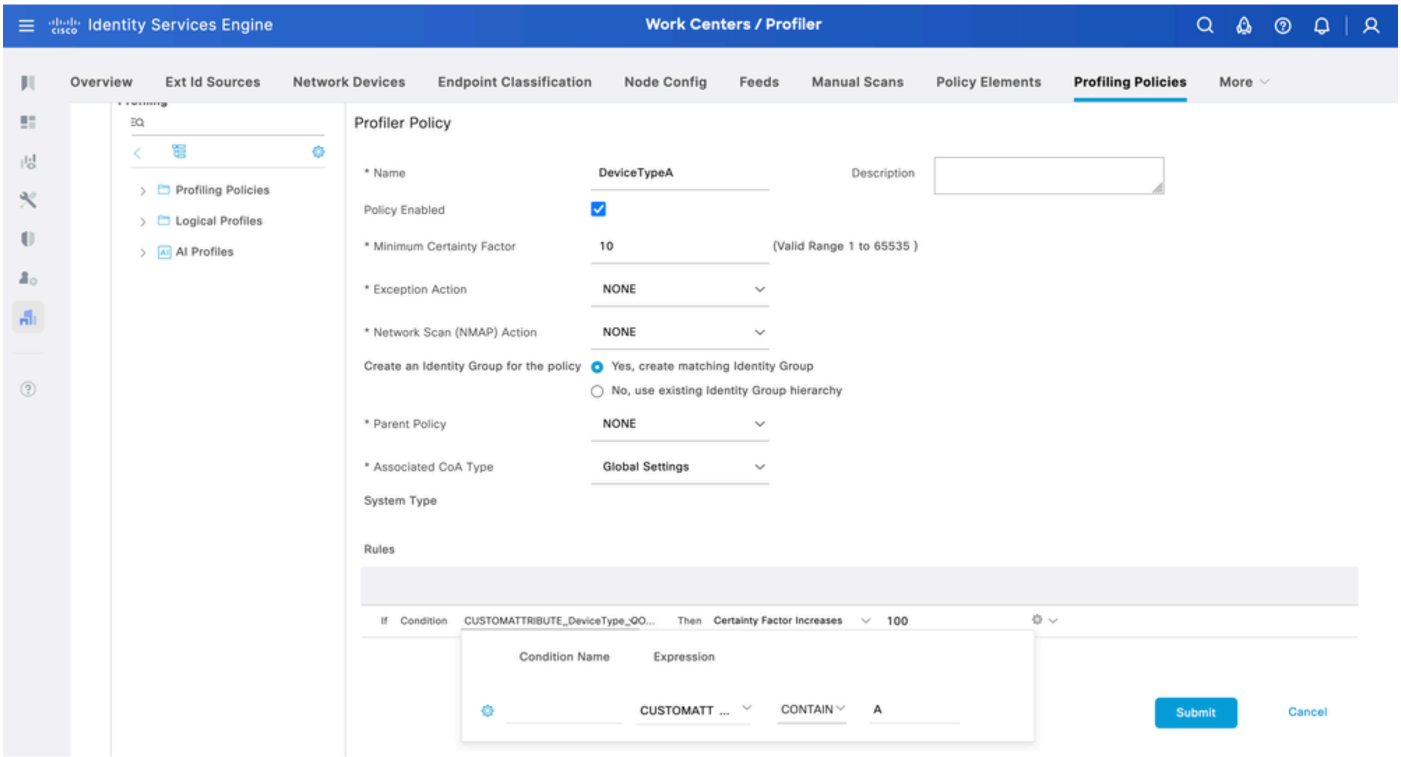
Profiling Policy for Custom Attribute

From ISE, navigate to Work Centers > Profiler > Profiling Policies. Click 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.



Profiler Policy

* Name: DeviceTypeA

Description:

Policy Enabled: ☑

* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy: ● Yes, create matching Identity Group ○ No, use existing Identity Group hierarchy

* Parent Policy: NONE

* Associated CoA Type: Global Settings

System Type

Rules

If Condition CUSTOMATTRIBUTE_DeviceType_QO... Then Certainty Factor Increases 100

Condition Name	Expression		
	CUSTOMATT ...	CONTAIN	A

Profiler Policy

Create Endpoint

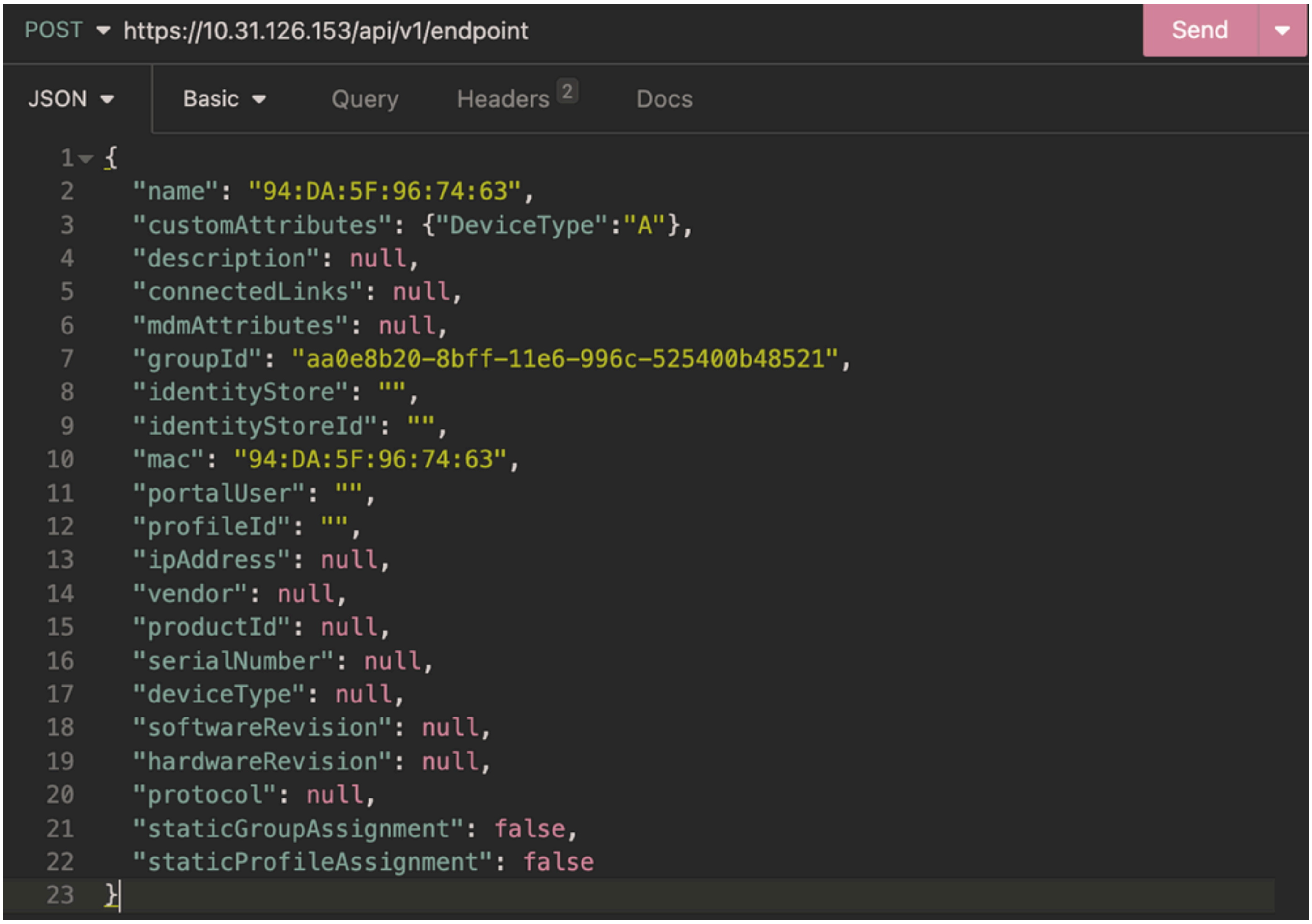
In this example, an endpoint with the mac address 94:DA:5F:96:74:63 and DeviceType set to **A** is created.

Method	**POST**
URL	https://<ISE-PAN-IP>:443/api/v1/endpoint
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",`

	"portalUser": "", "profileId": "", "ipAddress": null, "vendor": null, "productId": null, "serialNumber": null, "deviceType": null, "softwareRevision": null, "hardwareRevision": null, "protocol": null, "staticGroupAssignment": false, "staticProfileAssignment": false }

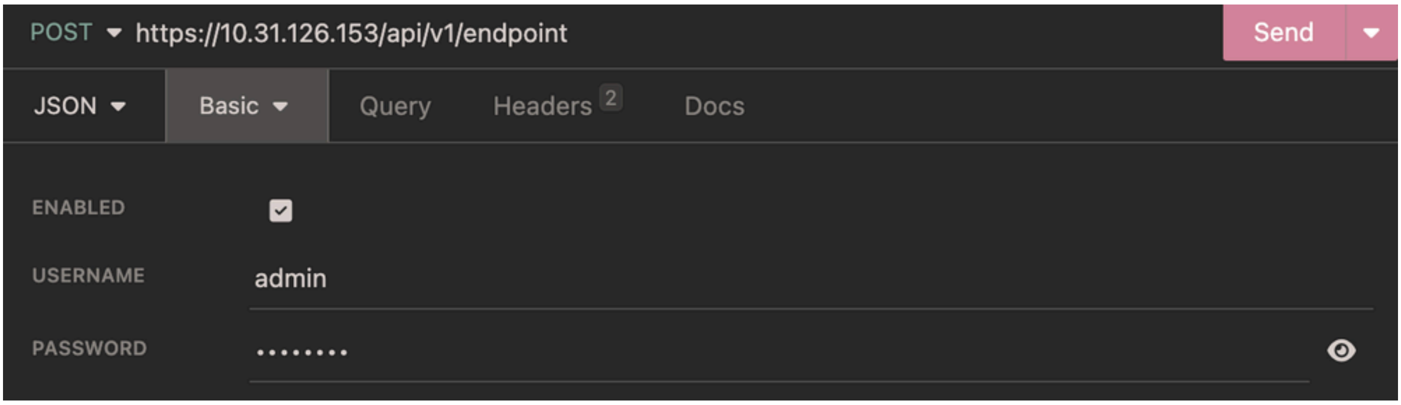
Body:



```
{
  "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",
  "portalUser": "",
  "profileId": "",
  "ipAddress": null,
  "vendor": null,
  "productId": null,
  "serialNumber": null,
  "deviceType": null,
  "softwareRevision": null,
  "hardwareRevision": null,
  "protocol": null,
  "staticGroupAssignment": false,
  "staticProfileAssignment": false
}
```

Body Endpoint

Authentication:



POST https://10.31.126.153/api/v1/endpoint

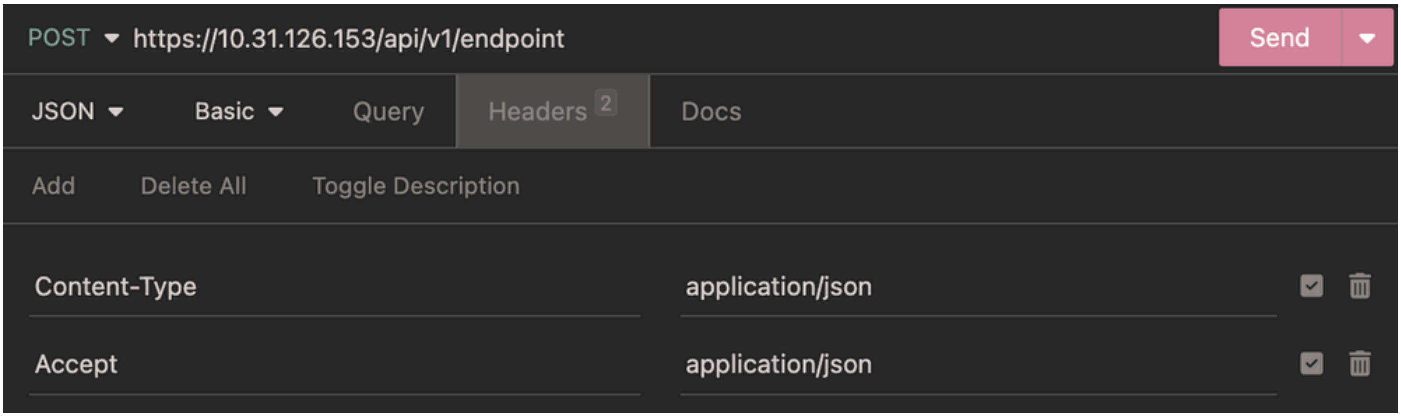
ENABLED ☑

USERNAME admin

PASSWORD ••••••••

Authentication Endpoint

Headers:

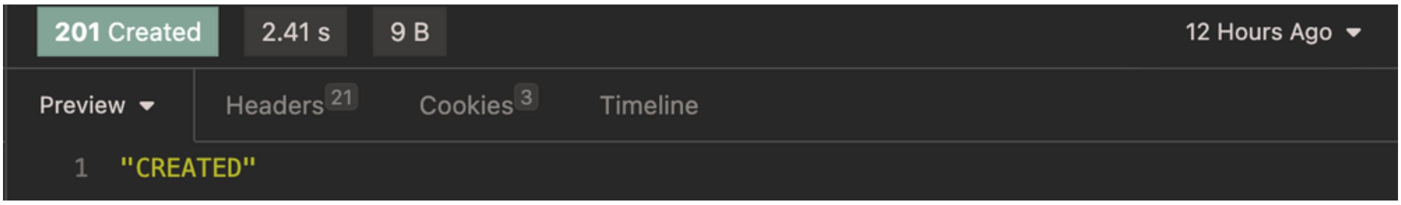


POST https://10.31.126.153/api/v1/endpoint

Content-Type	application/json	☑
Accept	application/json	☑

Headers Endpoint

Expected Output:



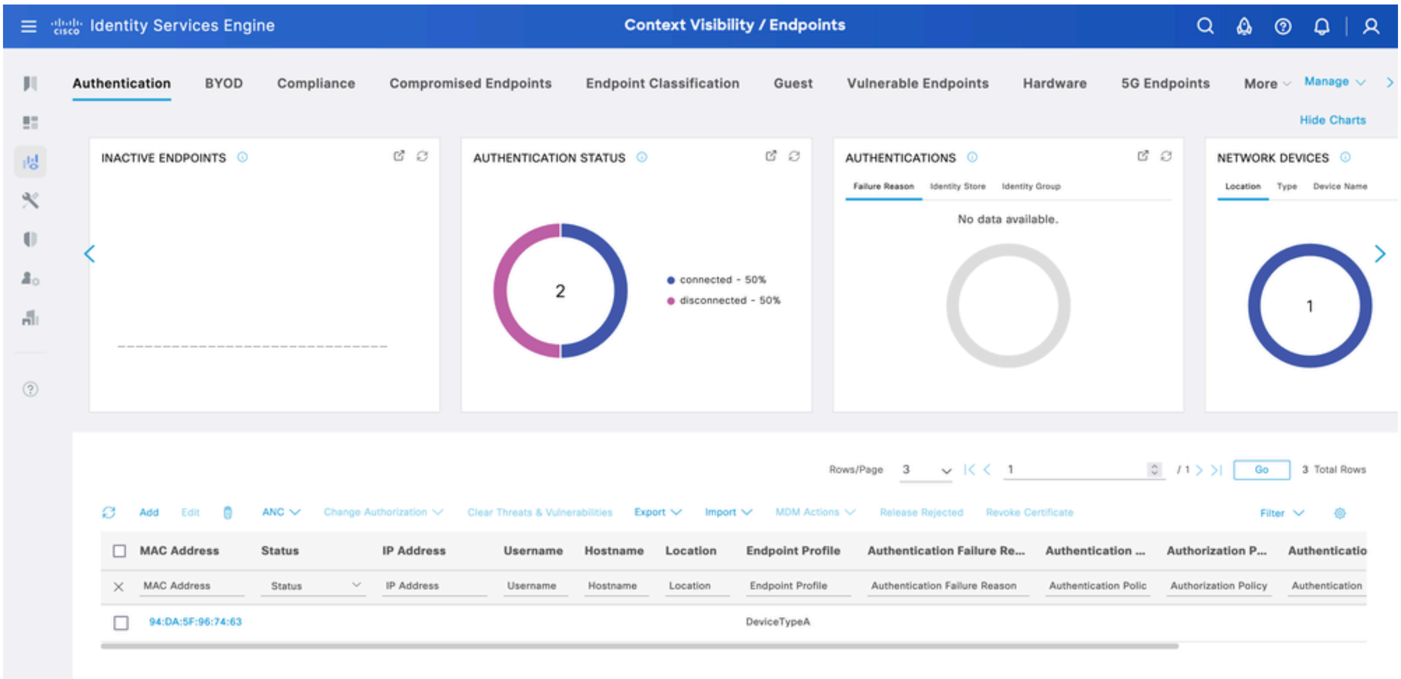
201 Created 2.41 s 9 B

```
"CREATED"
```

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.



MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Re...	Authentication ...	Authorization P...	Authenticatio
94:DA:5F:96:74:63						DeviceTypeA				

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.

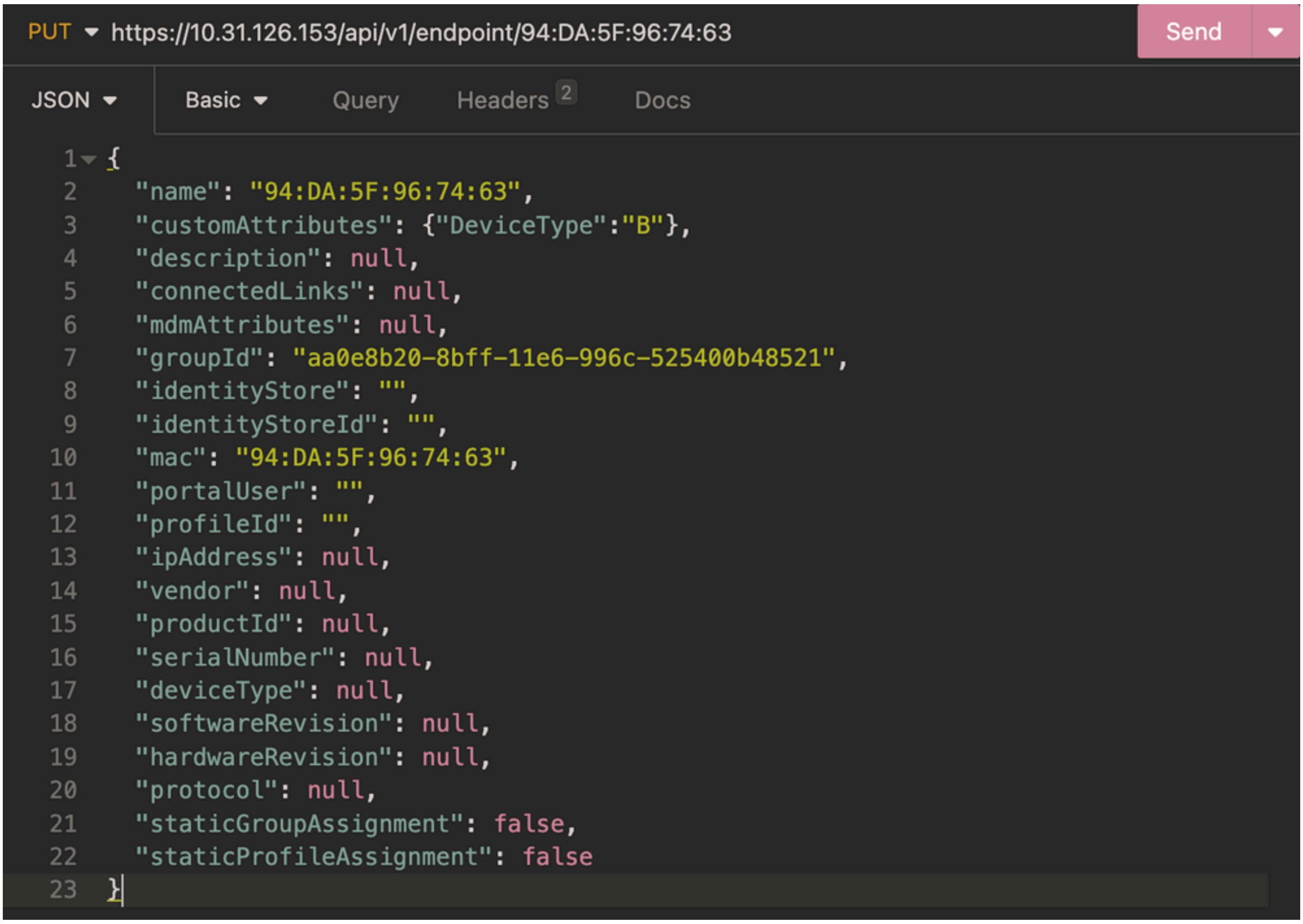
In this example, a new profiling policy DeviceTypeB was defined in order to update the custom attribute **DeviceType** set to **B** and the **value** is set as the **MAC address**.

Method	**PUT**
URL	https://<ISE-PAN-IP>:443/api/v1/endpoint/{value}
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:

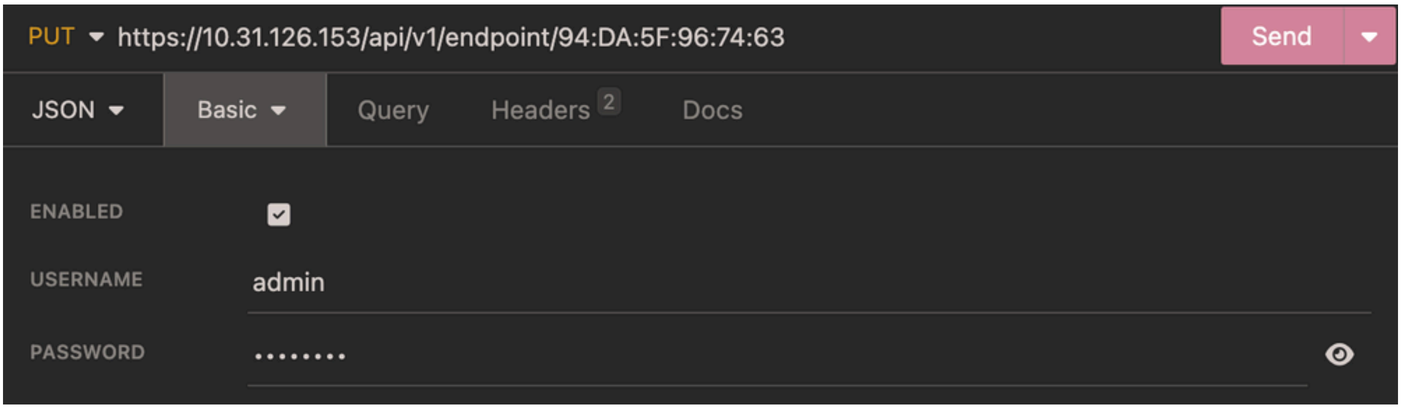


PUT https://10.31.126.153/api/v1/endpoint/94:DA:5F:96:74:63

```
{
  "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 Update Endpoint

Authentication:



PUT https://10.31.126.153/api/v1/endpoint/94:DA:5F:96:74:63

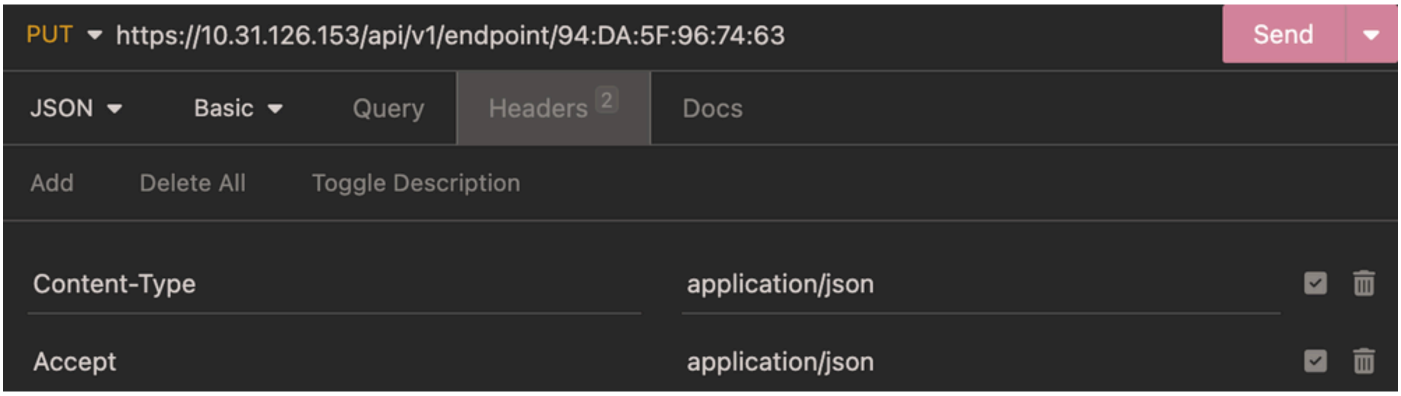
ENABLED ☑

USERNAME admin

PASSWORD •••••••••

Authentication Update Endpoint

Headers:

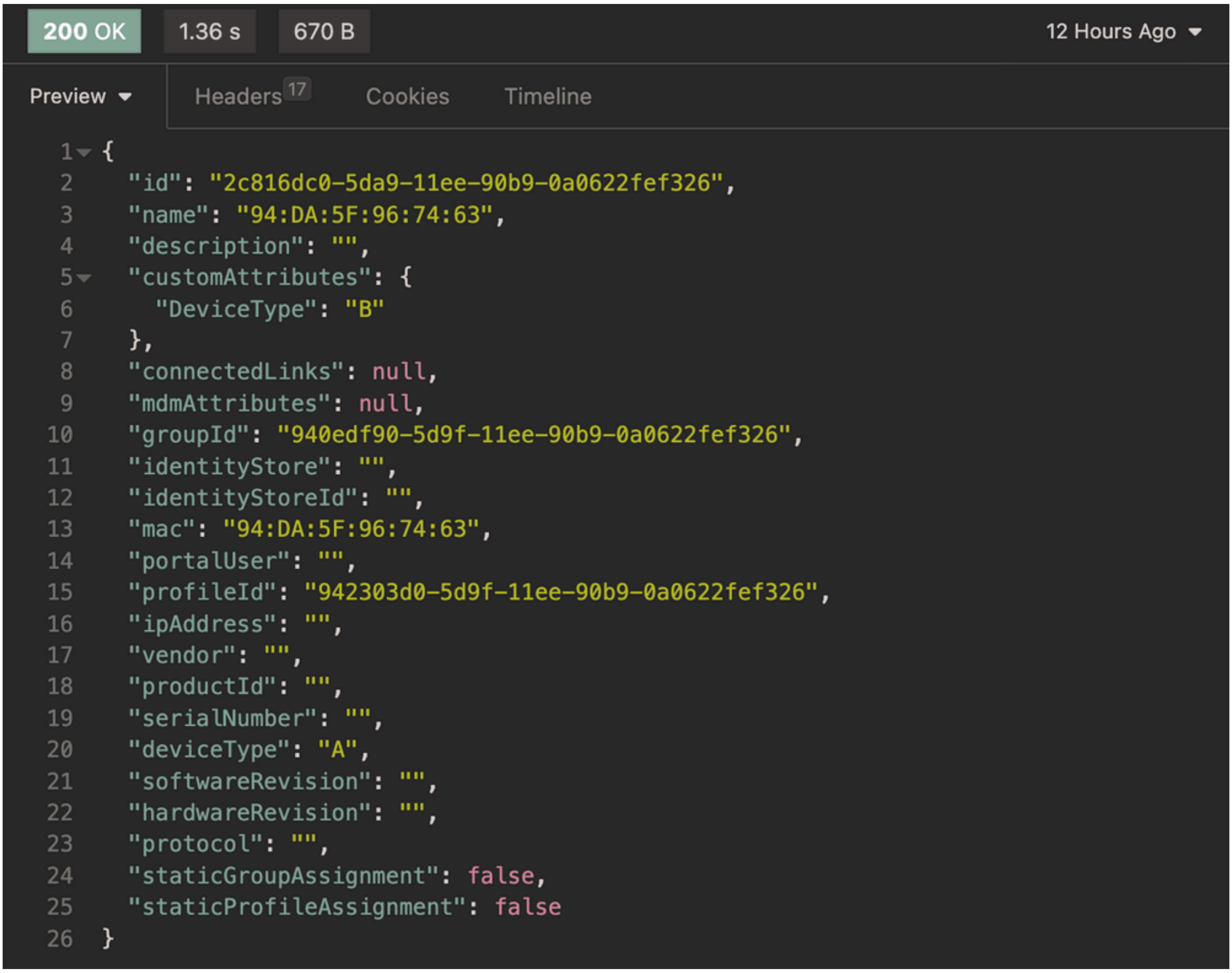


PUT https://10.31.126.153/api/v1/endpoint/94:DA:5F:96:74:63

Content-Type	application/json	☑
Accept	application/json	☑

Headers Update Endpoint

Expected Output:

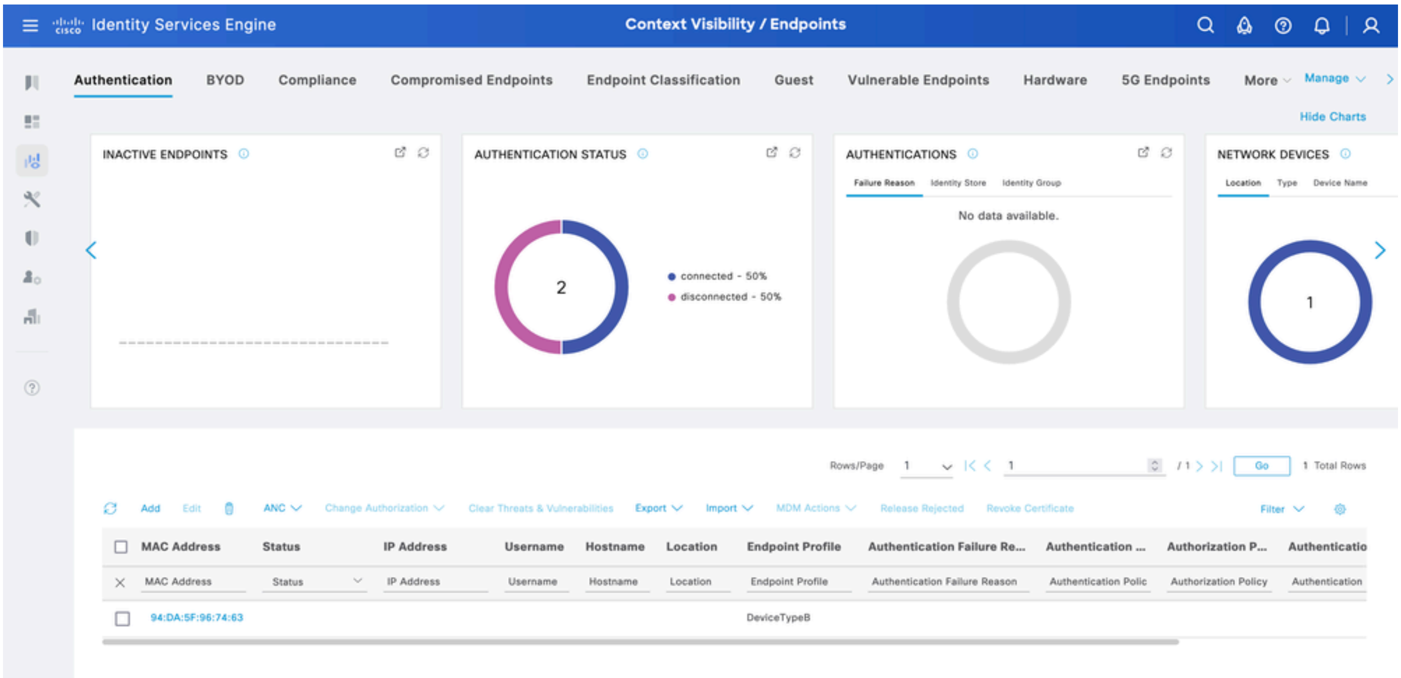


```
{
  "id": "2c816dc0-5da9-11ee-90b9-0a0622fef326",
  "name": "94:DA:5F:96:74:63",
  "description": "",
  "customAttributes": {
    "DeviceType": "B"
  },
  "connectedLinks": null,
  "mdmAttributes": null,
  "groupId": "940edf90-5d9f-11ee-90b9-0a0622fef326",
  "identityStore": "",
  "identityStoreId": "",
  "mac": "94:DA:5F:96:74:63",
  "portalUser": "",
  "profileId": "942303d0-5d9f-11ee-90b9-0a0622fef326",
  "ipAddress": "",
  "vendor": "",
  "productId": "",
  "serialNumber": "",
  "deviceType": "A",
  "softwareRevision": "",
  "hardwareRevision": "",
  "protocol": "",
  "staticGroupAssignment": false,
  "staticProfileAssignment": false
}
```

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.



MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Re...	Authentication ...	Authorization P...	Authenticatio
94:DA:5F:96:74:63						DeviceTypeB				

Context Visibility DeviceTypeB

Context-In API Bulk

Authorization Policy Configuration with Endpoint Identity Group

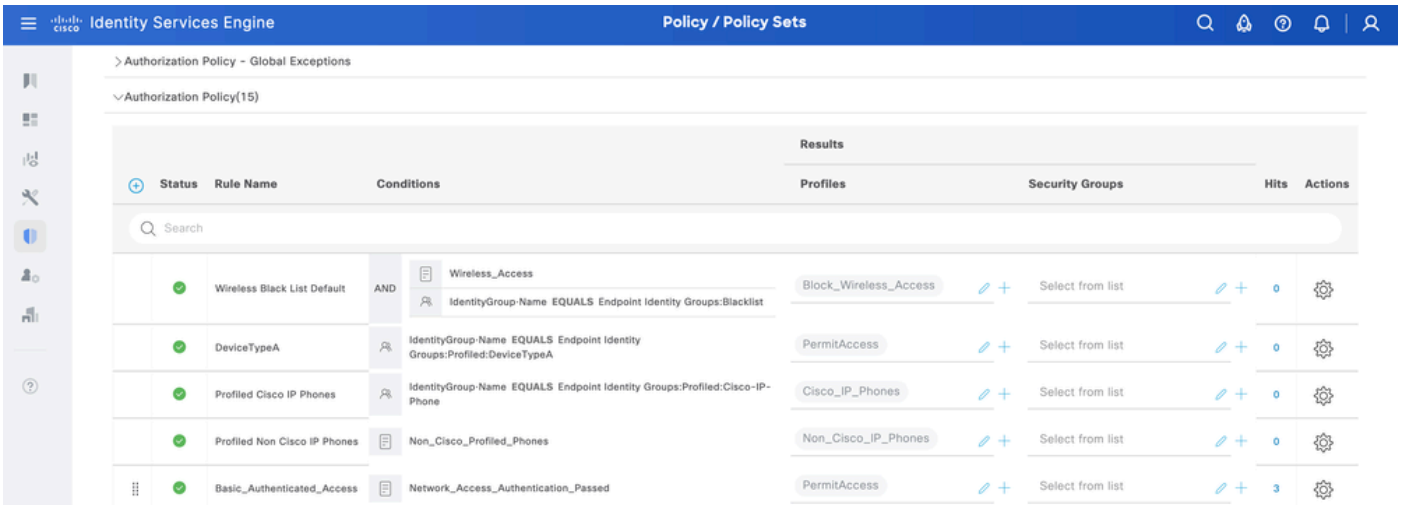
From ISE, navigate to Policy > Policy Sets > Select a Policy Set > Authorization Policy. Click the gear icon in any of the Authorization Policies and choose**Insert**.

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**.



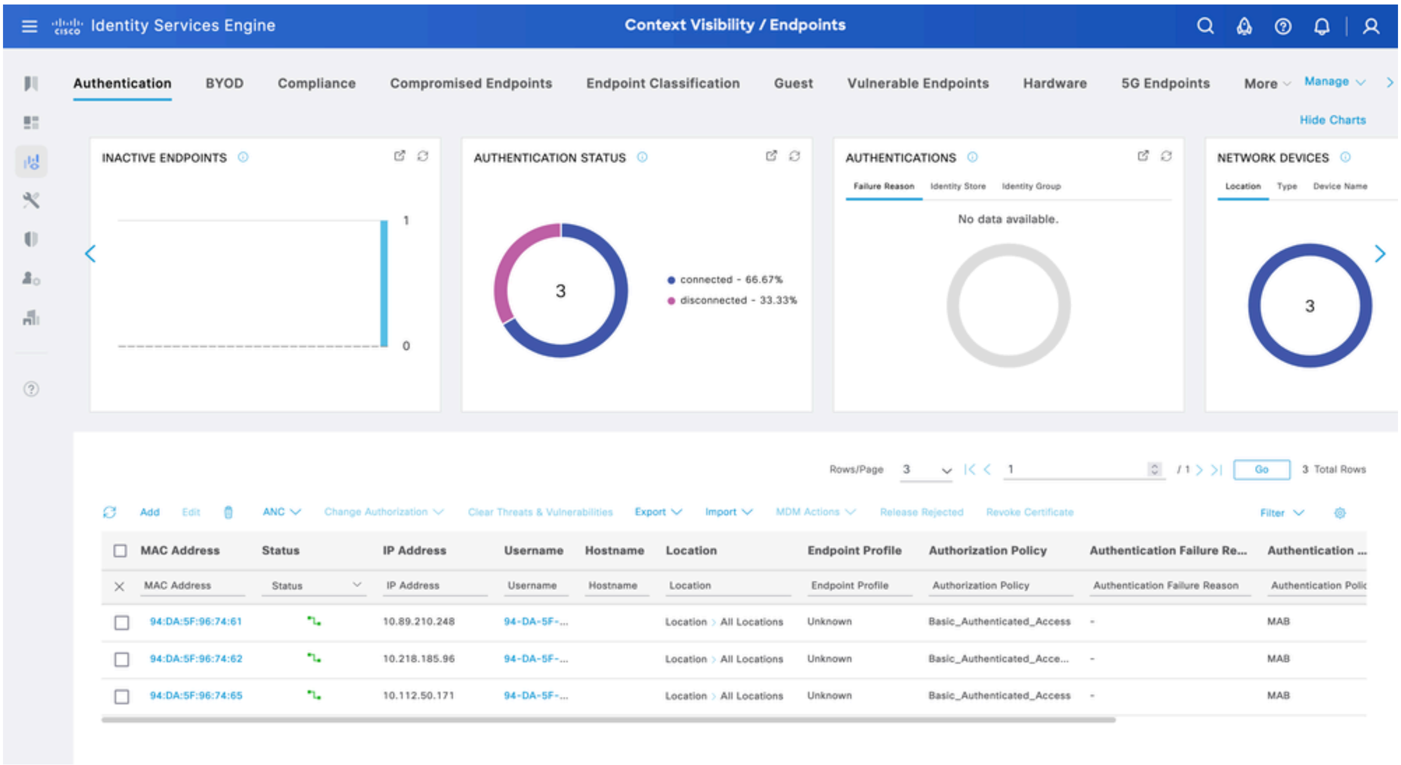
Status	Rule Name		Conditions	Results Profiles	 Security Groups	Hits	Actions
✓	Wireless Black List Default	AND	Wireless_Access IdentityGroup·Name EQUALS Endpoint Identity Groups:Blacklist	Block_Wireless_Access	Select from list	0	⚙
✓	DeviceTypeA		IdentityGroup·Name EQUALS Endpoint Identity Groups:Profiled:DeviceTypeA	PermitAccess	Select from list	0	⚙
✓	Profiled Cisco IP Phones		IdentityGroup·Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	Cisco_IP_Phones	Select from list	0	⚙
✓	Profiled Non Cisco IP Phones		Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones	Select from list	0	⚙
✓	Basic_Authenticated_Access		Network_Access_Authentication_Passed	PermitAccess	Select from list	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**.



□	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authorization Policy	Authentication Failure Re...	Authentication ...
×	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authorization Policy	Authentication Failure Reason	Authentication Polic
□	94:DA:5F:96:74:61		10.89.210.248	94-DA-5F-...		Location > All Locations	Unknown	Basic_Authenticated_Access	-	MAB
□	94:DA:5F:96:74:62		10.218.185.96	94-DA-5F-...		Location > All Locations	Unknown	Basic_Authenticated_Acce...	-	MAB
□	94:DA:5F:96:74:65		10.112.50.171	94-DA-5F-...		Location > All Locations	Unknown	Basic_Authenticated_Access	-	MAB

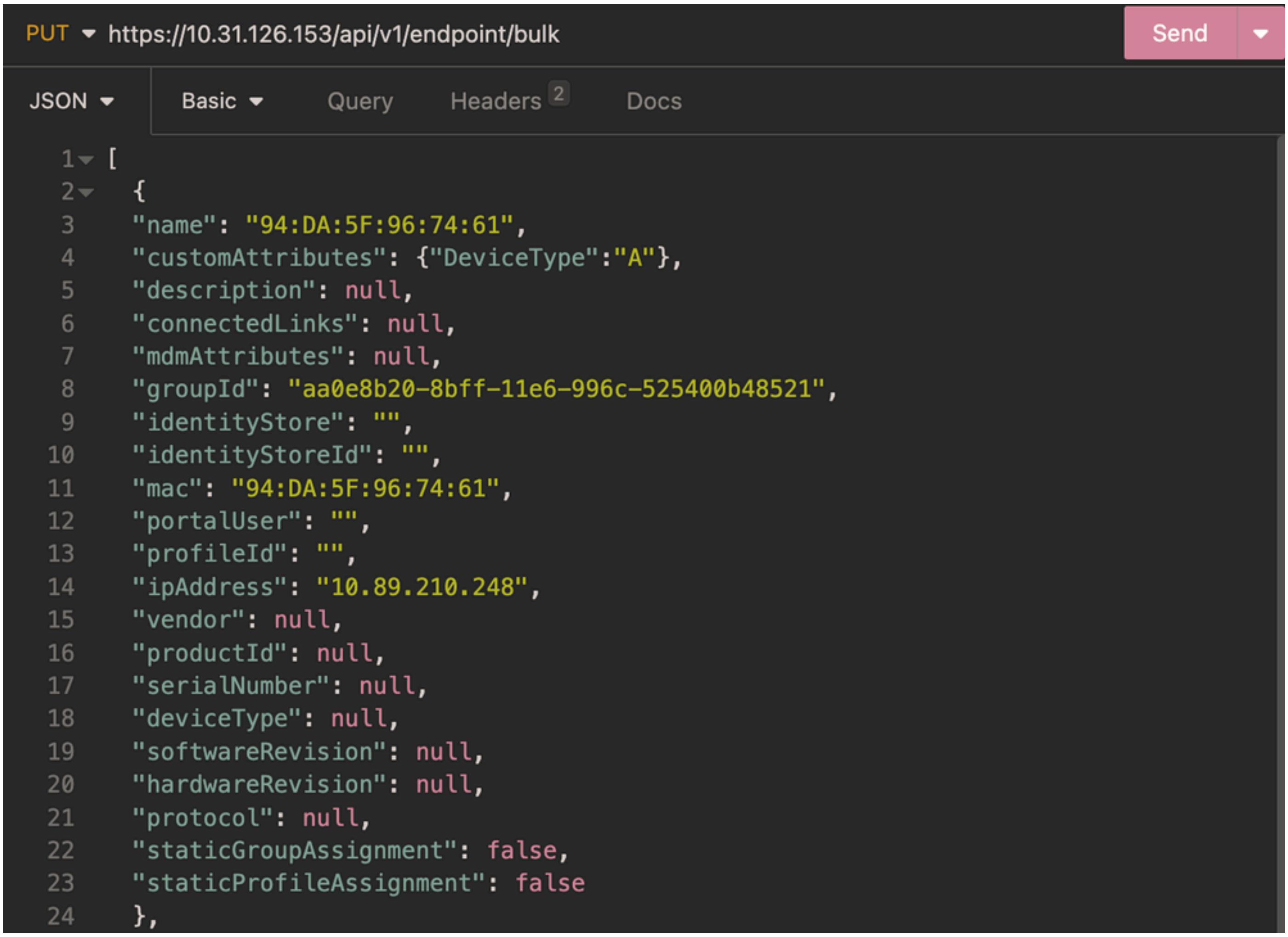
Context Visibility Uknown Profile

Method	PUT
URL	https://<ISE-PAN-IP>:443/api/v1/endpoint/bulk
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": "",`
	`"mac": "94:DA:5F:96:74:61",`
	`"portalUser": "",`
	`"profileId": "",`
	`"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": {"DeviceType":"A"}, "description": null, "connectedLinks": null, "mdmAttributes": null, "groupId": "aa0e8b20-8bff-11e6-996c-525400b48521", "identityStore": "", "identityStoreId": "", "mac": "94:DA:5F:96:74:62", "portalUser": "", "profileId": "", "ipAddress": "10.218.185.96", "vendor": null, "productId": null, "serialNumber": null, "deviceType": null, "softwareRevision": null, "hardwareRevision": null, "protocol": null, "staticGroupAssignment": false, "staticProfileAssignment": false },.......]

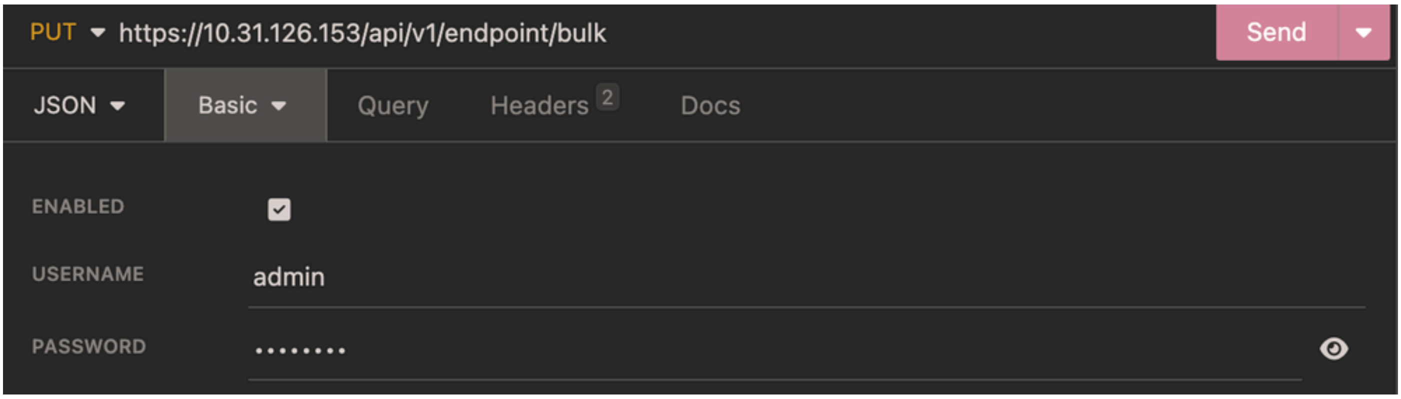
Body:



```
[
  {
  "name": "94:DA:5F:96:74:61",
  "customAttributes": {"DeviceType":"A"},
  "description": null,
  "connectedLinks": null,
  "mdmAttributes": null,
  "groupId": "aa0e8b20-8bff-11e6-996c-525400b48521",
  "identityStore": "",
  "identityStoreId": "",
  "mac": "94:DA:5F:96:74:61",
  "portalUser": "",
  "profileId": "",
  "ipAddress": "10.89.210.248",
  "vendor": null,
  "productId": null,
  "serialNumber": null,
  "deviceType": null,
  "softwareRevision": null,
  "hardwareRevision": null,
  "protocol": null,
  "staticGroupAssignment": false,
  "staticProfileAssignment": false
  },
```

Body Endpoint Bulk

Authentication:



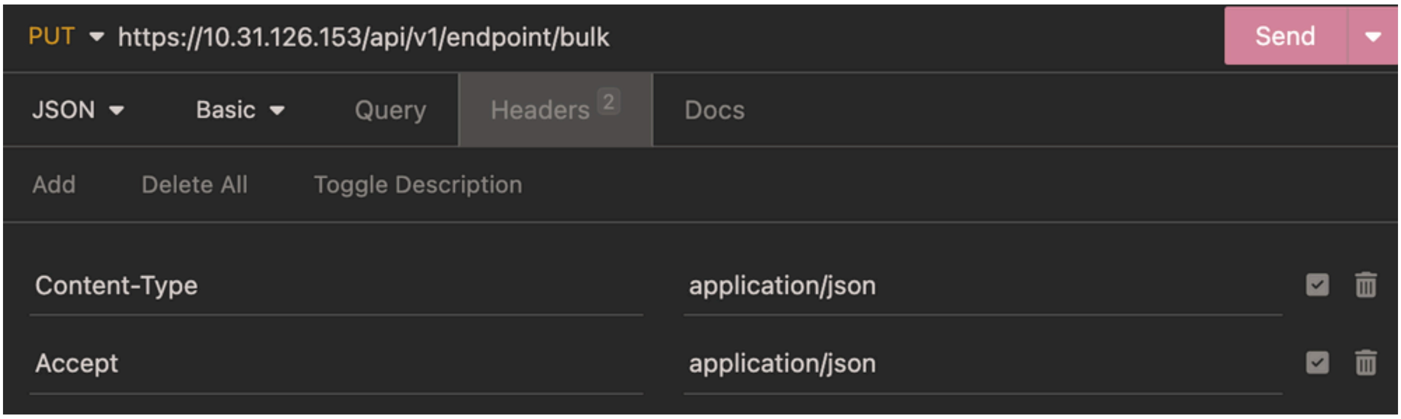
ENABLED ☑

USERNAME admin

PASSWORD ••••••••

Authentication Endpoint Bulk

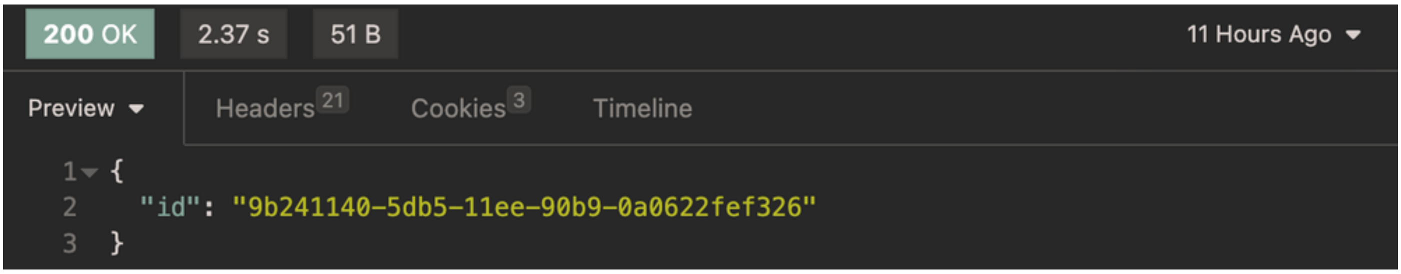
Headers:



Content-Type	application/json
Accept	application/json

Headers Endpoint Bulk

Expected Output:

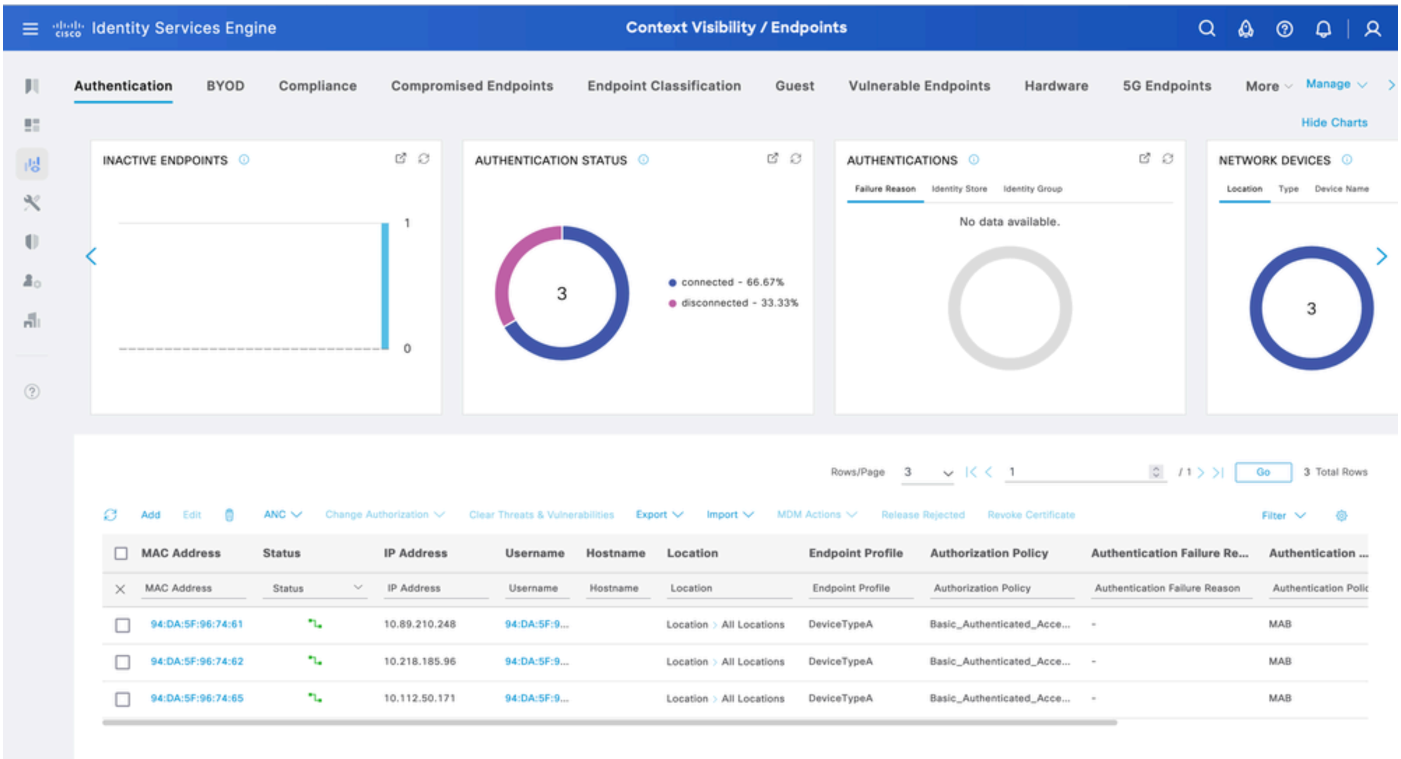


```
{
  "id": "9b241140-5db5-11ee-90b9-0a0622fef326"
}
```

Expected Output Endpoint Bulk

Verify Endpoint Bulk Update

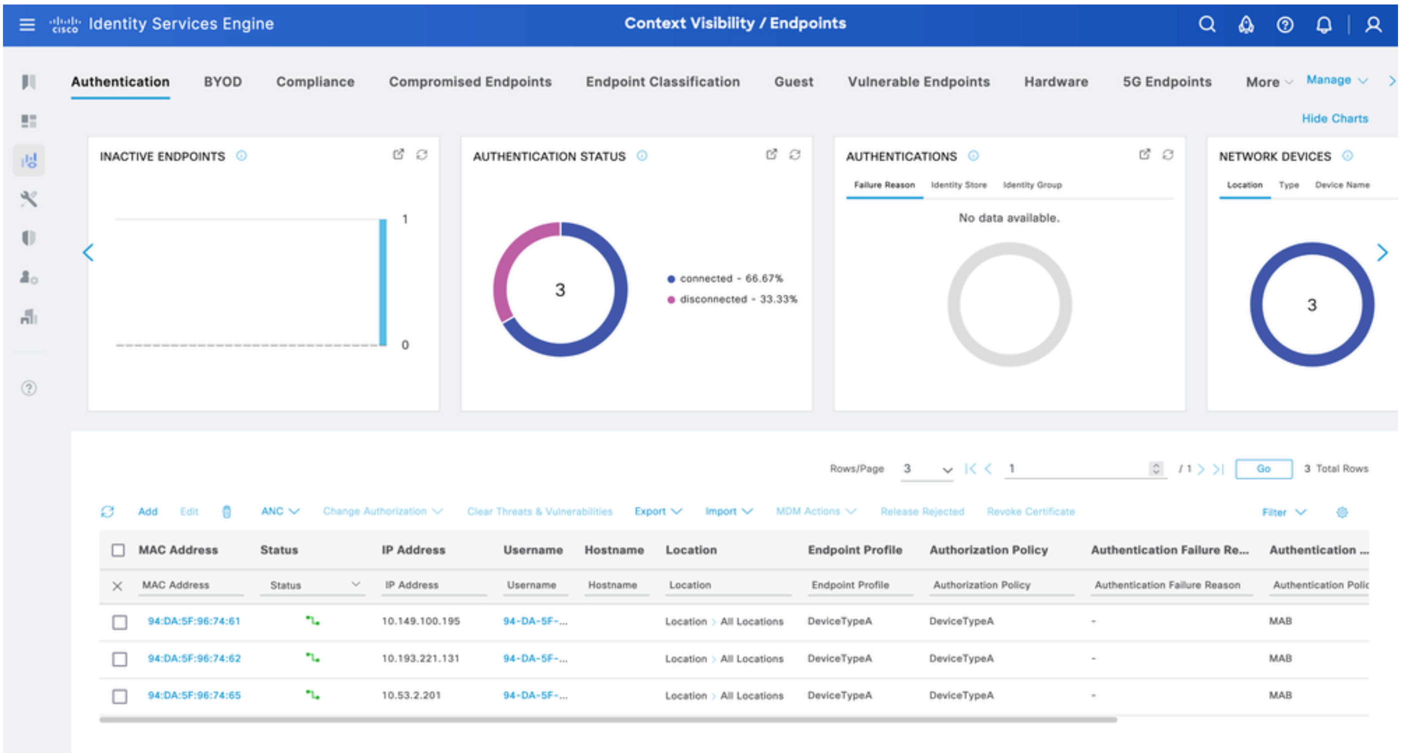
From ISE, navigate to Context Visibility > Endpoints. Filter with the name of the profiling policy created under the **Endpoint Profile** column.



□	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authorization Policy	Authentication Failure Re...	Authentication ...
×	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authorization Policy	Authentication Failure Reason	Authentication Polic
□	94:DA:5F:96:74:61		10.89.210.248	94:DA:5F:9...		Location > All Locations	DeviceTypeA	Basic_Authenticated_Acce...	-	MAB
□	94:DA:5F:96:74:62		10.218.185.96	94:DA:5F:9...		Location > All Locations	DeviceTypeA	Basic_Authenticated_Acce...	-	MAB
□	94:DA:5F:96:74:65		10.112.50.171	94:DA:5F:9...		Location > 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 re-authenticate.



MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authorization Policy	Authentication Failure Re...	Authentication ...
94:DA:5F:96:74:61		10.149.100.195	94-DA-5F-...		Location > All Locations	DeviceTypeA	DeviceTypeA	-	MAB
94:DA:5F:96:74:62		10.193.221.131	94-DA-5F-...		Location > All Locations	DeviceTypeA	DeviceTypeA	-	MAB
94:DA:5F:96:74:65		10.53.2.201	94-DA-5F-...		Location > All Locations	DeviceTypeA	DeviceTypeA	-	MAB

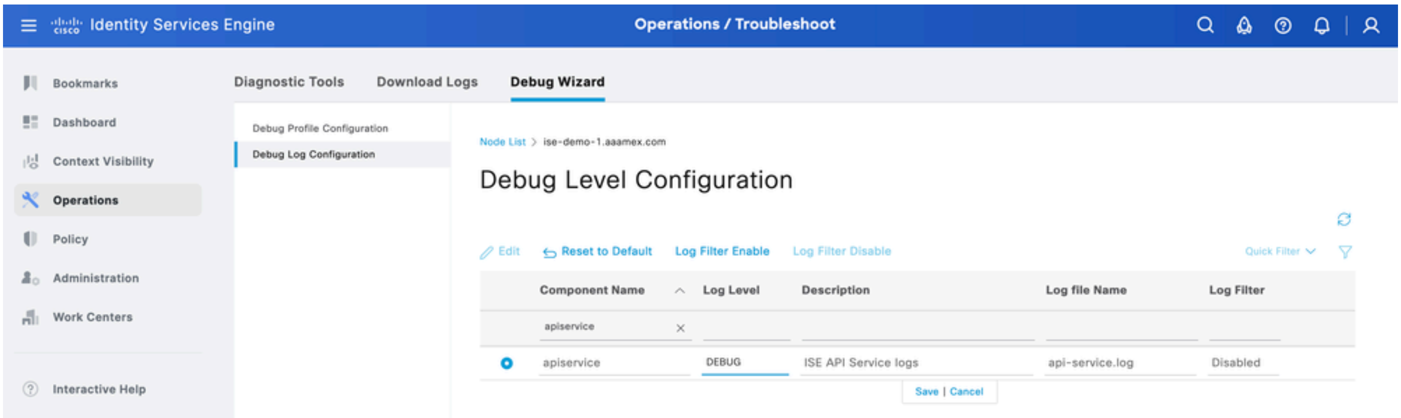
Context Visibility DevcieTypeA Authorization Policy

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 click**Edit**.

Filter the**Component Name**by API service and choose the Log Level needed. Click**Save**.



Debug Level Configuration

	Component Name	Log Level	Description	Log file Name	Log Filter
	apiservice				
●	apiservice	DEBUG	ISE API Service logs	api-service.log	Disabled

Debug Level Configuration Open API

- On ISE PAN CLI the logs are found at:

```
admin#show logging application api-service.log
```

- 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.