Cisco API Series

Cyber Vision

2024. 6

Cisco API Series (English)

Cisco Product		
Nexus Dashboard	https://youtu.be/Zu2ZmgCRJxM	2024.2
Webex	https://youtu.be/5ugMry3pmWI https://youtu.be/W-nhsNXx72E	2023. 12 2020. 5
ACI	https://youtu.be/sbpfFfHKp68	2023. 5
NX-API	https://youtu.be/2uaKC5QOPgo	2022. 11
SD-WAN API	https://youtu.be/VY9k4qXfMX8	2022. 2
DCNM	https://youtu.be/H6yni8d4rMA	2021. 8
ASA	https://youtu.be/ynb3suFJSak	2021. 6
DNA Center (Cisco Center)	https://youtu.be/qy2zkGvfKbc	2020. 12
ISE	https://youtu.be/4PsMwKHcq7g	2020. 6
Meraki	https://youtu.be/eoiq45GID4U	2020. 3

Cisco API Series (Korean / 한국어)

Cisco Product			
Nexus Dashboard	https://youtu.be/bhY6fjBZxb4	2024.2	
Webex	https://youtu.be/_fV3c3Piq7A https://youtu.be/CIYY2_8m3rA	2023. 12 2020. 5	
ACI	https://youtu.be/ElM_a-ZnoEk	2023. 5	
NX-API	https://youtu.be/EcDtYCcKS-Q	2022. 11	
SD-WAN	https://youtu.be/W0l0Xf63vj4	2022. 2	
DCNM	https://youtu.be/MlChhs-zhFE	2021. 8	
ASA	https://youtu.be/QNsDo7wcJs8	2021. 6	
DNA Center (Cisco Center)	https://youtu.be/p5HRJGifaZg	2020. 12	
ISE	https://youtu.be/XvfDalrlFVQ	2020. 6	
Meraki	https://youtu.be/LDf9pmqPGNI	2020. 3	

Cyber Vision ?

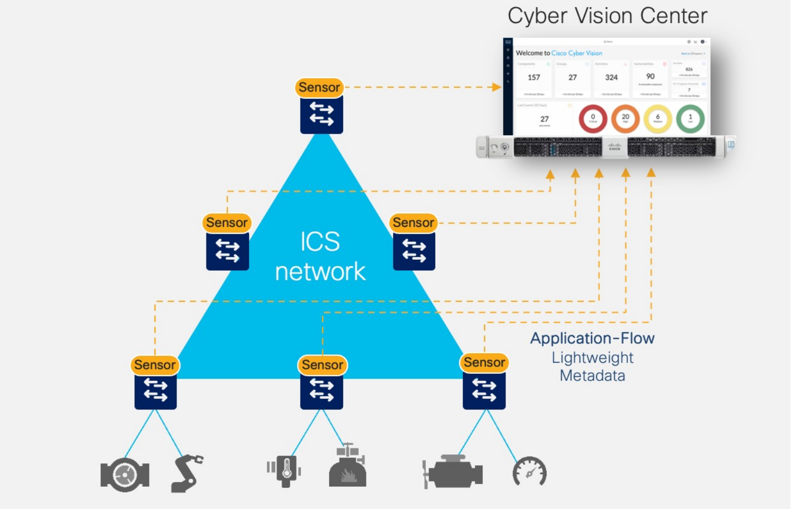
In, fact, nobody knows what are there.

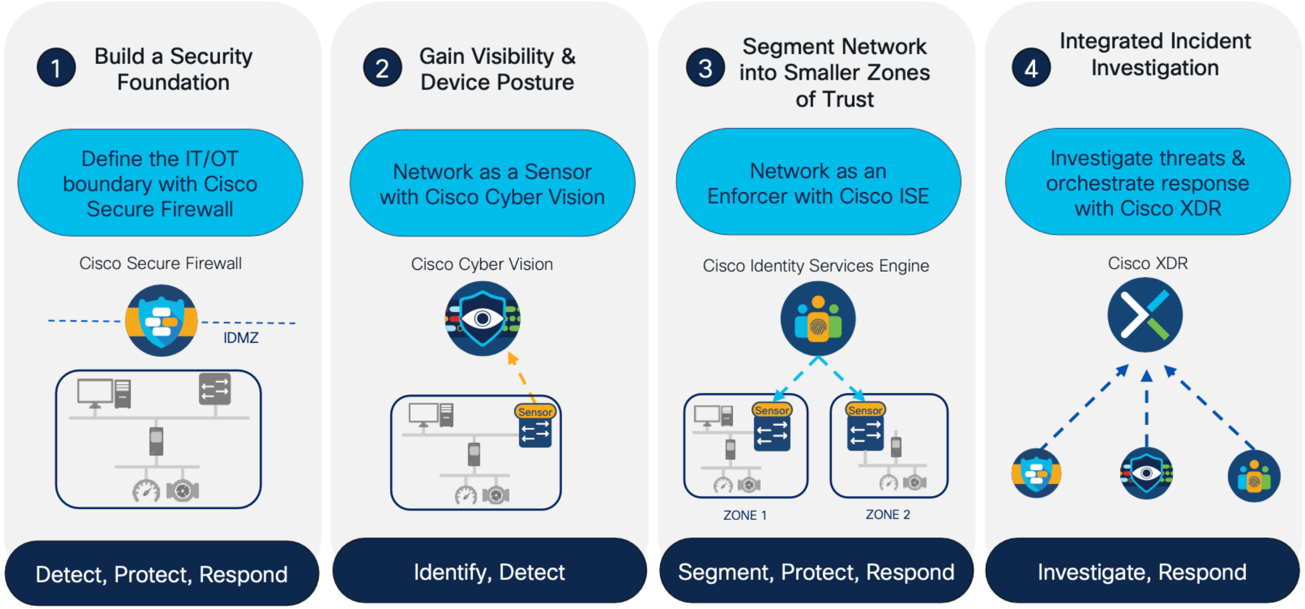
The role of the Cyber Vision Sensor

Collects Industrial Network Traffic

Decodes Industrial Protocols (DPI)

Sends Metadata to the Cyber Vision Center





1 Build a Security Foundation

Define the IT/OT boundary with Cisco Secure Firewall

Cisco Secure Firewall

Detect, Protect, Respond

2 Gain Visibility & Device Posture

Network as a Sensor with Cisco Cyber Vision

Cisco Cyber Vision

Identify, Detect

3 Segment Network into Smaller Zones of Trust

Network as an Enforcer with Cisco ISE

Cisco Identity Services Engine

Segment, Protect, Respond

4 Integrated Incident Investigation

Investigate threats & orchestrate response with Cisco XDR

Cisco XDR

Investigate, Respond

Cybervision API Summary

Easy to Use!!!

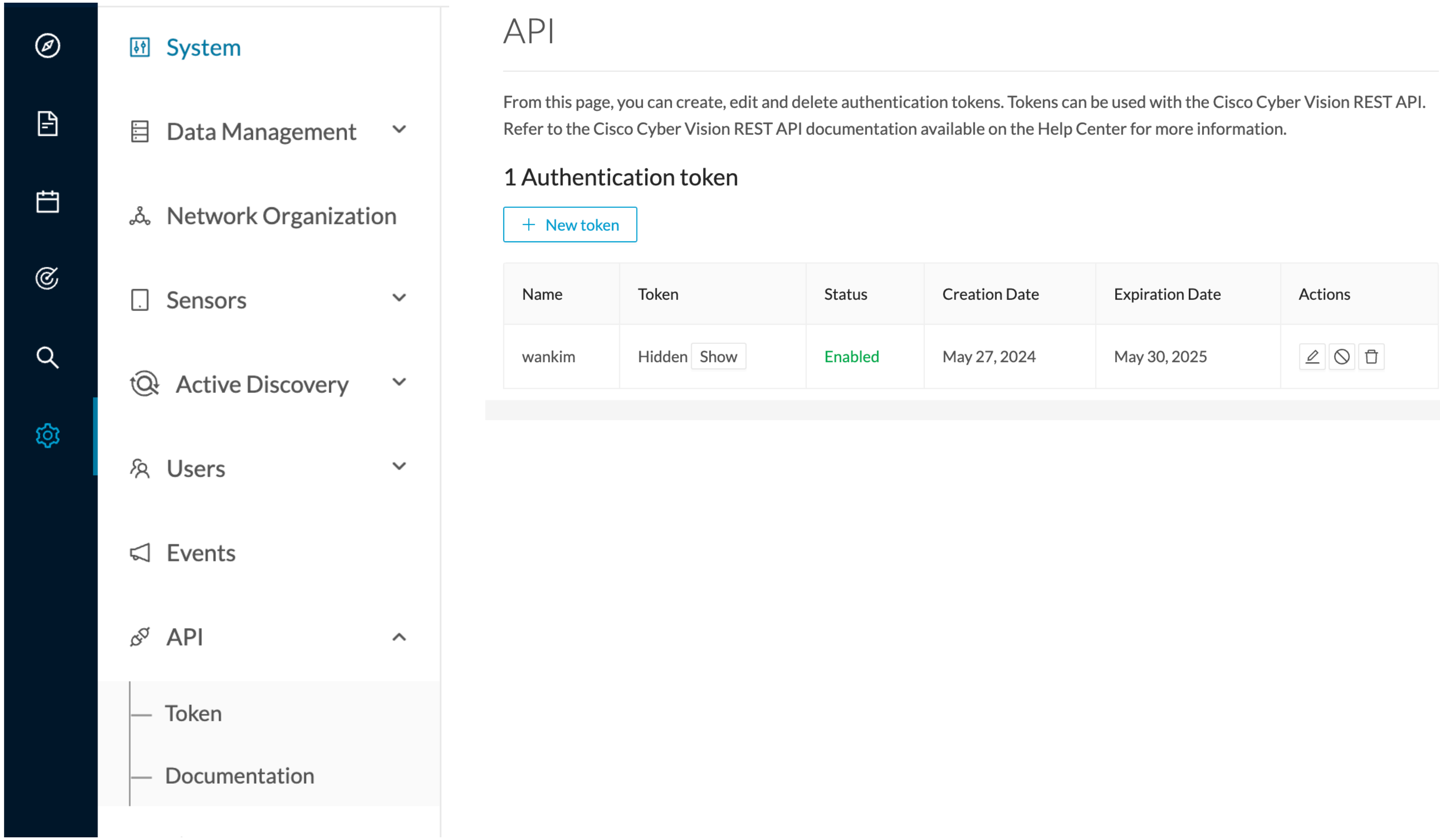
- Authentication : token
- Token : Cybervsion - web page
- Token period : as long as you want
- API Guide : Cybervsion – web page
- API test : Cybervsion – web page
- Sample code type : curl @Cybervsion – web page

Cyber Vision API guide

4.3 is used.

- https://developer.cisco.com/learning/modules/iot-cyber-vision/iot-cybervision-api-python-v4/setting-up-a-sample-script/

Token



API

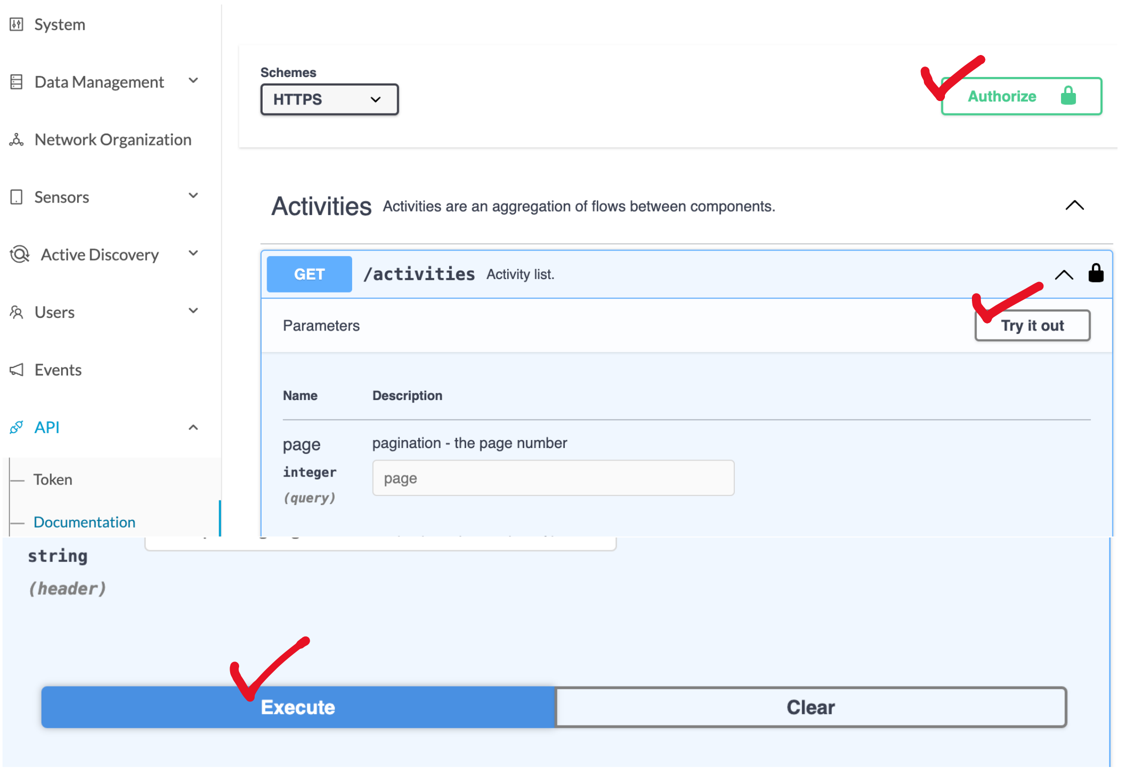
From this page, you can create, edit and delete authentication tokens. Tokens can be used with the Cisco Cyber Vision REST API. Refer to the Cisco Cyber Vision REST API documentation available on the Help Center for more information.

1 Authentication token

+ New token

Name	Token	Status	Creation Date	Expiration Date	Actions
wankim	Hidden Show	Enabled	May 27, 2024	May 30, 2025	

API document



Schemes: HTTPS

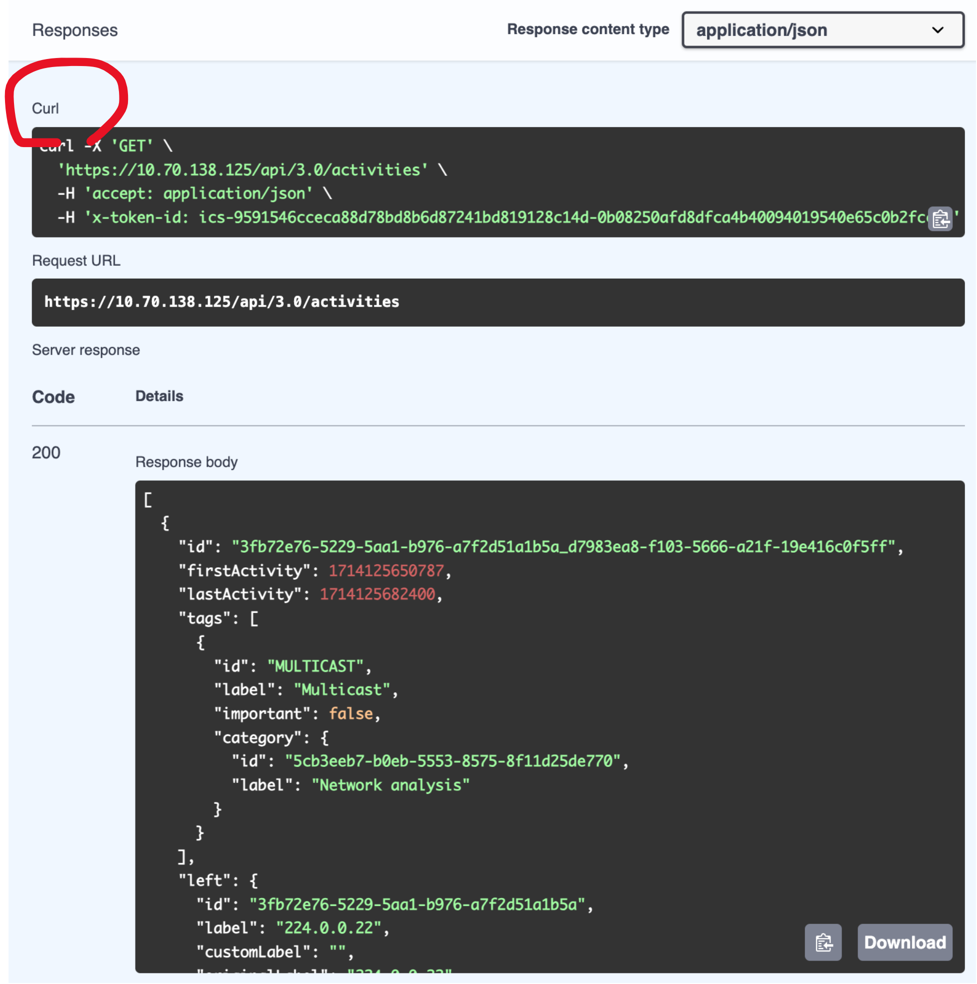
Activities Activities are an aggregation of flows between components.

GET /activities Activity list.

Parameters

Name	Description
page integer *(query)*	pagination - the page number page

string
(header)



Responses

Response content type: application/json

Curl

```
curl -X 'GET' \
  'https://10.70.138.125/api/3.0/activities' \
  -H 'accept: application/json' \
  -H 'x-token-id: ics-9591546cceca88d78bd8b6d87241bd819128c14d-0b08250afd8dfca4b40094019540e65c0b2fc'
```

Request URL

```
https://10.70.138.125/api/3.0/activities
```

Server response

Code	Details
200	Response body

```
[
  {
    "id": "3fb72e76-5229-5aa1-b976-a7f2d51a1b5a_d7983ea8-f103-5666-a21f-19e416c0f5ff",
    "firstActivity": 1714125650787,
    "lastActivity": 1714125682400,
    "tags": [
      {
        "id": "MULTICAST",
        "label": "Multicast",
        "important": false,
        "category": {
          "id": "5cb3eeb7-b0eb-5553-8575-8f11d25de770",
          "label": "Network analysis"
        }
      }
    ],
    "left": {
      "id": "3fb72e76-5229-5aa1-b976-a7f2d51a1b5a",
      "label": "224.0.0.22",
      "customLabel": "",
```

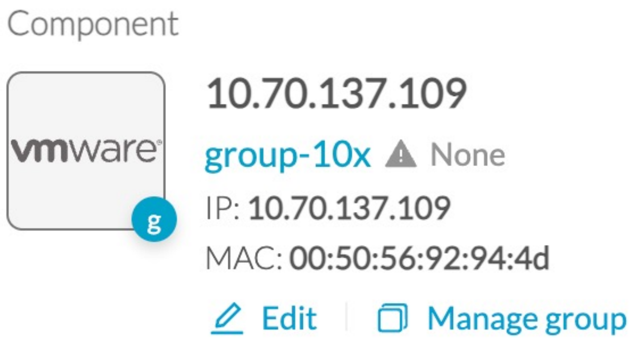
Why <Custom Properties>?

Problem 1 : IP duplication?

- There can be the multiple networks using the same network.
- So, <IP address> can’t be the primary key.
- <**Group**> is added to identity.

JSON result

```
{'aggregation':
   {'type': '', 'components': []},
 'ancestors': None,
 'credentialsCount': 0,
 'customLabel': '',
 'device': None,
 'eventsCount': 1,
 'externalCommunicationsCount': 0,
 'firstActivity': 1714124687043,
 'flowsCount': 0,
 'flowsTags': [],
 'group':
    {'id': 'f735b04b-58d4-4535-92aa-004b1c41db78',
     'label': 'group-10x',
     'description': '',
     'comments': '',
     'color': '#06a2c9',
     'locked': False,
     'groupIds': None,
     'centerID': ''},
  'icon': 'library/vmware.svg',
   'id': '2f6391a4-d104-5303-8538-f1fbb3e62278',
   'ip': '10.70.137.109',
   'label': '10.70.137.109',
   'lastActivity': 1714124964114,
    'mac': '00:50:56:92:94:4d',
```



Component

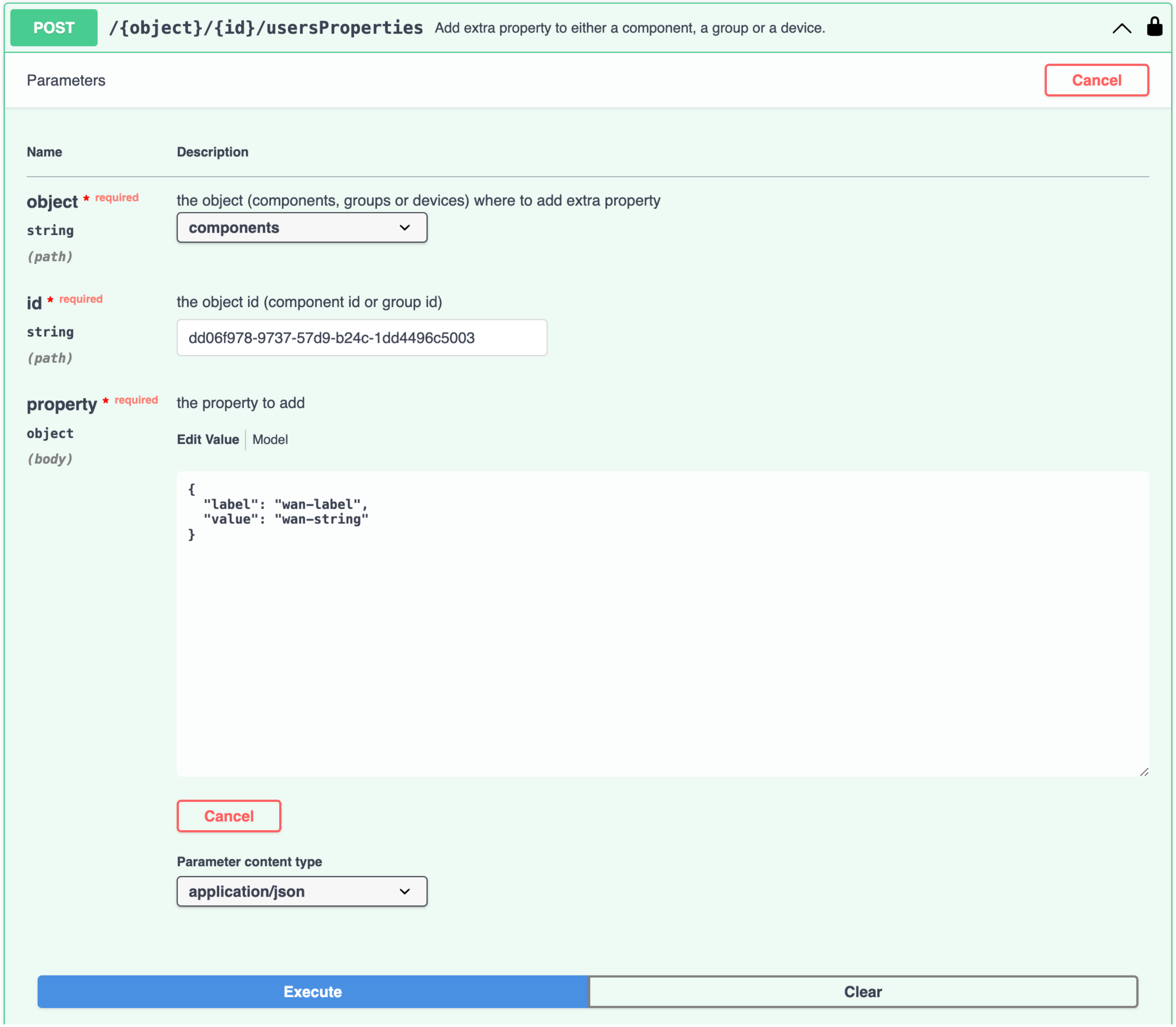
10.70.137.109

group-10x ⚠ None

IP: 10.70.137.109

MAC: 00:50:56:92:94:4d

Codes - Sample



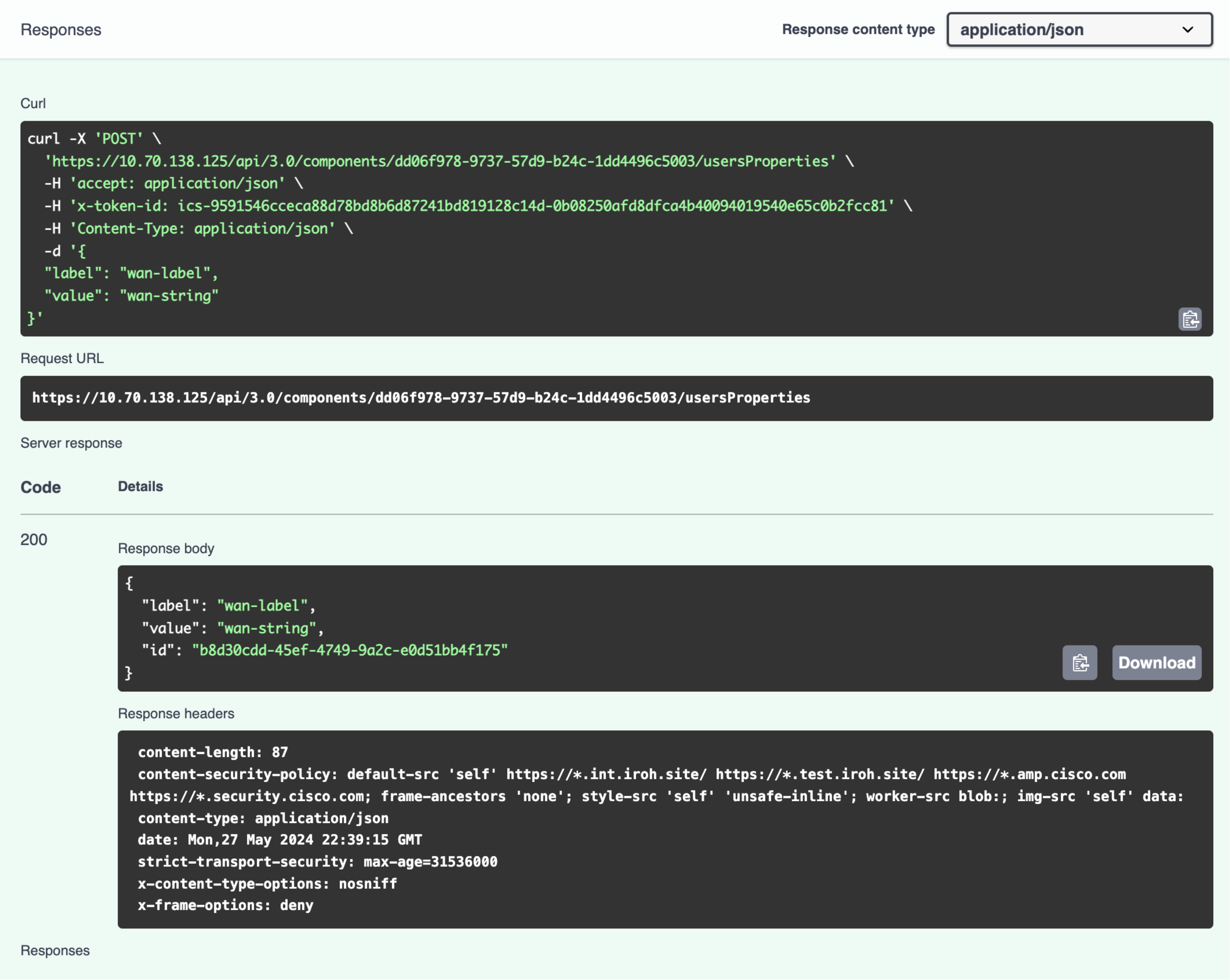
/{object}/{id}/usersProperties Add extra property to either a component, a group or a device.

Name	Description
object * required string *(path)*	the object (components, groups or devices) where to add extra property components
id * required string *(path)*	the object id (component id or group id) dd06f978-9737-57d9-b24c-1dd4496c5003
property * required object *(body)*	the property to add Edit Value | Model

```
{
  "label": "wan-label",
  "value": "wan-string"
}
```

Parameter content type

application/json



Curl

```
curl -X 'POST' \
  'https://10.70.138.125/api/3.0/components/dd06f978-9737-57d9-b24c-1dd4496c5003/usersProperties' \
  -H 'accept: application/json' \
  -H 'x-token-id: ics-9591546cceca88d78bd8b6d87241bd819128c14d-0b08250afd8dfca4b40094019540e65c0b2fcc81' \
  -H 'Content-Type: application/json' \
  -d '{
  "label": "wan-label",
  "value": "wan-string"
}'
```

Request URL

```
https://10.70.138.125/api/3.0/components/dd06f978-9737-57d9-b24c-1dd4496c5003/usersProperties
```

Server response

200

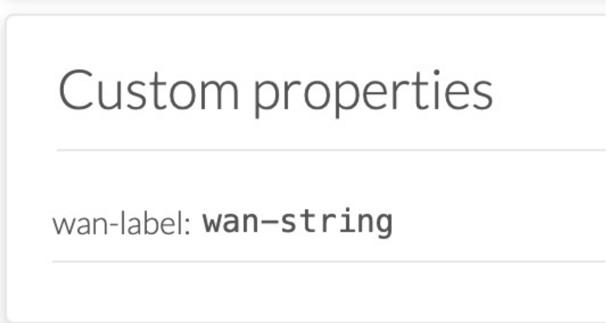
Response body

```
{
  "label": "wan-label",
  "value": "wan-string",
  "id": "b8d30cdd-45ef-4749-9a2c-e0d51bb4f175"
}
```

Response headers

```
 content-length: 87
 content-security-policy: default-src 'self' https://*.int.iroh.site/ https://*.test.iroh.site/ https://*.amp.cisco.com
https://*.security.cisco.com; frame-ancestors 'none'; style-src 'self' 'unsafe-inline'; worker-src blob:; img-src 'self' data:
 content-type: application/json
 date: Mon,27 May 2024 22:39:15 GMT
 strict-transport-security: max-age=31536000
 x-content-type-options: nosniff
 x-frame-options: deny
```

```
curl -X 'POST' \
  'https://10.70.138.125/api/3.0/components/dd06f978-9737-57d9-b24c-1dd4496c5003/usersProperties' \
  -H 'accept: application/json' \
  -H 'x-token-id: ics-9591546cceca88d78bd8b6d87241bd819128c14d-0b08250afd8dfca4b40094019540e65c0b2fcc81' \
  -H 'Content-Type: application/json' \
  -d '{
  "label": "wan-label",
  "value": "wan-string"
}’
```



Custom properties

wan-label: wan-string

```
import requests

headers = {
    'accept': 'application/json',
    'x-token-id': 'ics-9591546cceca88d78bd8b6d87241bd819128c14d-0b08250afd8dfca4b40094019540e65c0b2fcc81',
    'Content-Type': 'application/json',
}

json_data = {
    'label': 'wan-label',
    'value': 'wan-string',
}

response = requests.post(
    'https://10.70.138.125/api/3.0/components/dd06f978-9737-57d9-b24c-1dd4496c5003/usersProperties',
    headers=headers,
    json=json_data,
)
```

Custom properties

wan2-label: `wan2-string`

wan3-label: `wan3-string`

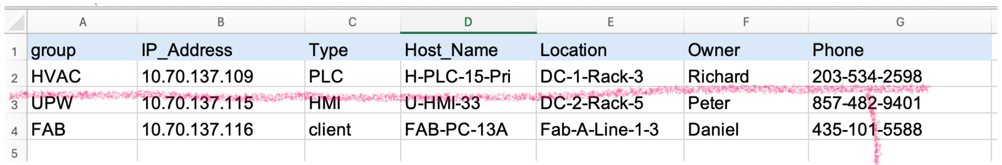
wan4-label: `wan4-string`

wan-label: `wan-string`

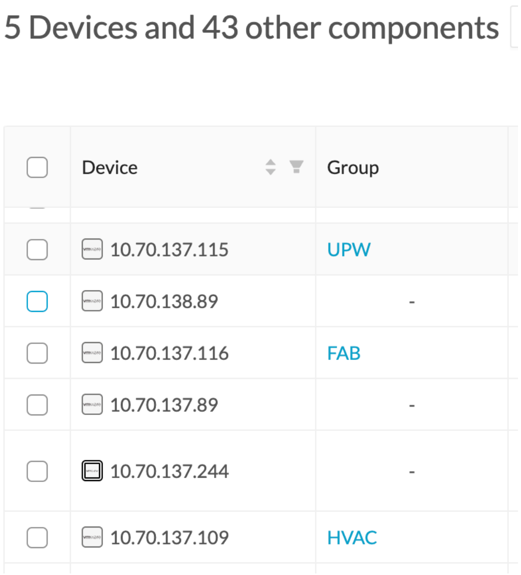
Final Codes

Result

- Before

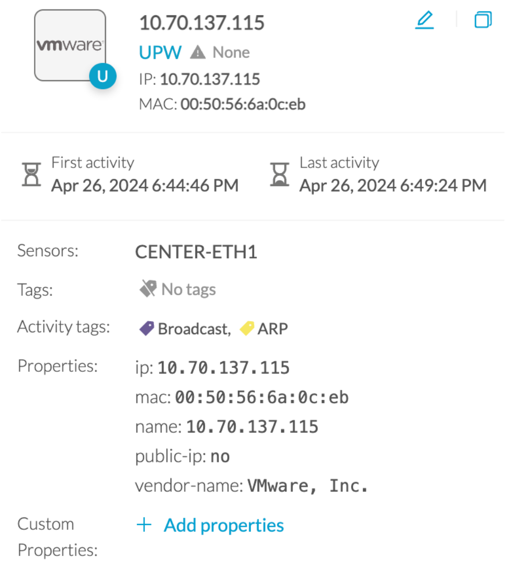


	A	B	C	D	E	F	G
1	group	IP_Address	Type	Host_Name	Location	Owner	Phone
2	HVAC	10.70.137.109	PLC	H-PLC-15-Pri	DC-1-Rack-3	Richard	203-534-2598
3	UPW	10.70.137.115	HMI	U-HMI-33	DC-2-Rack-5	Peter	857-482-9401
4	FAB	10.70.137.116	client	FAB-PC-13A	Fab-A-Line-1-3	Daniel	435-101-5588
5							



5 Devices and 43 other components

☐	Device	Group
☐	10.70.137.115	UPW
☐	10.70.138.89	-
☐	10.70.137.116	FAB
☐	10.70.137.89	-
☐	10.70.137.244	-
☐	10.70.137.109	HVAC

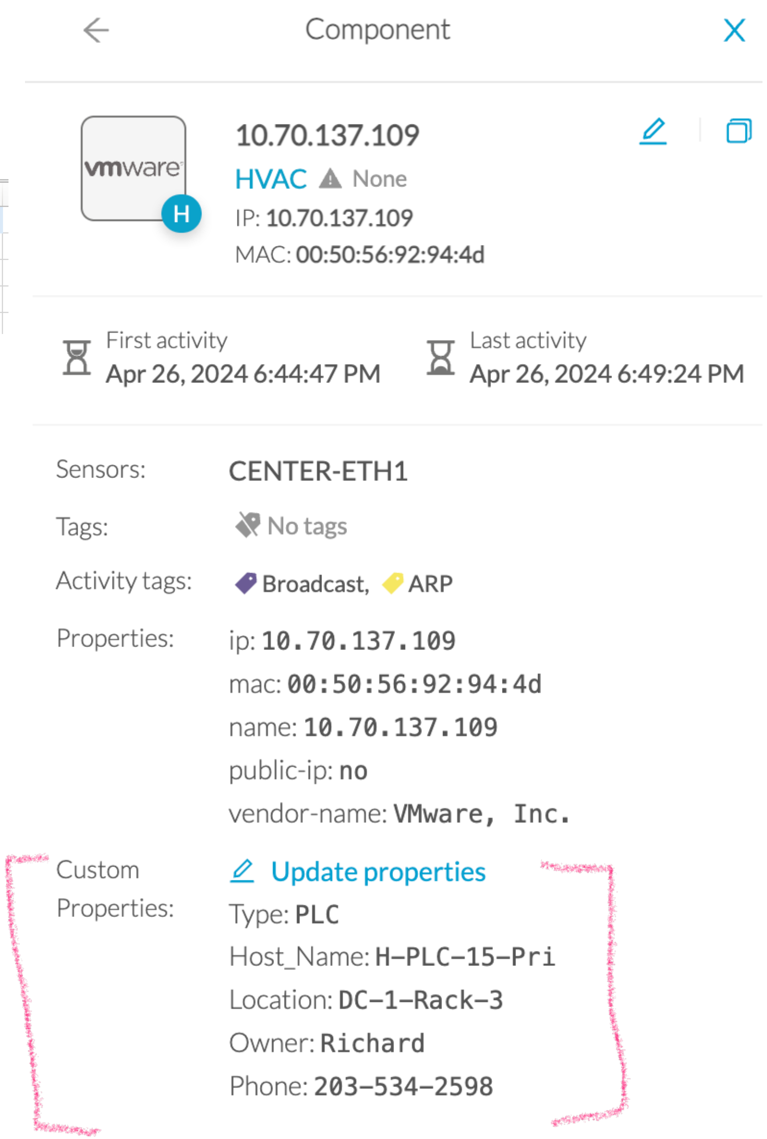


10.70.137.115
UPW ⚠ None
IP: 10.70.137.115
MAC: 00:50:56:6a:0c:eb

First activity
Apr 26, 2024 6:44:46 PM

Last activity
Apr 26, 2024 6:49:24 PM

Sensors: CENTER-ETH1
Tags: No tags
Activity tags: Broadcast, ARP
Properties:
ip: 10.70.137.115
mac: 00:50:56:6a:0c:eb
name: 10.70.137.115
public-ip: no
vendor-name: VMware, Inc.
Custom Properties: + Add properties



Component

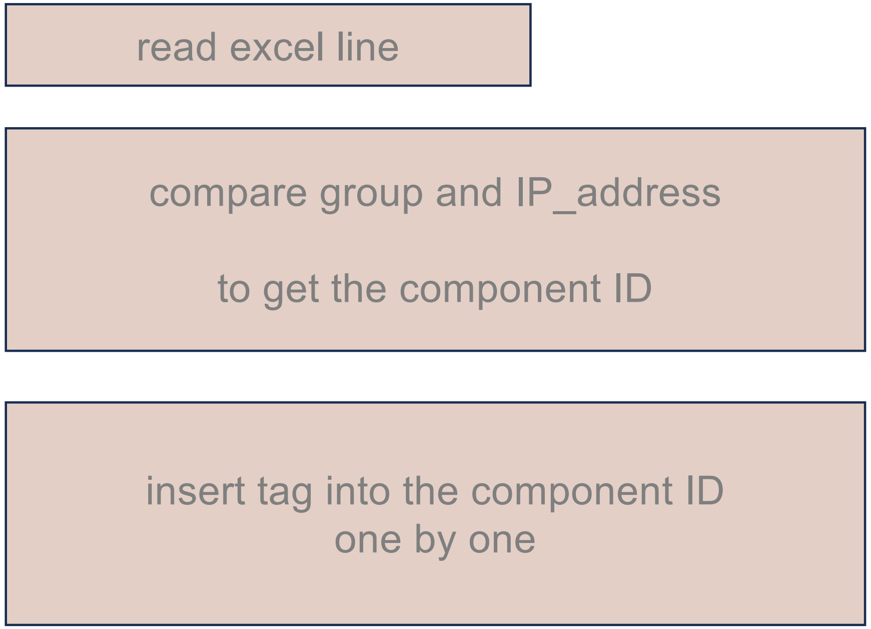
10.70.137.109
HVAC ⚠ None
IP: 10.70.137.109
MAC: 00:50:56:92:94:4d

First activity
Apr 26, 2024 6:44:47 PM

Last activity
Apr 26, 2024 6:49:24 PM

Sensors: CENTER-ETH1
Tags: No tags
Activity tags: Broadcast, ARP
Properties:
ip: 10.70.137.109
mac: 00:50:56:92:94:4d
name: 10.70.137.109
public-ip: no
vendor-name: VMware, Inc.
Custom Properties: Update properties
Type: PLC
Host_Name: H-PLC-15-Pri
Location: DC-1-Rack-3
Owner: Richard
Phone: 203-534-2598

Flow chart



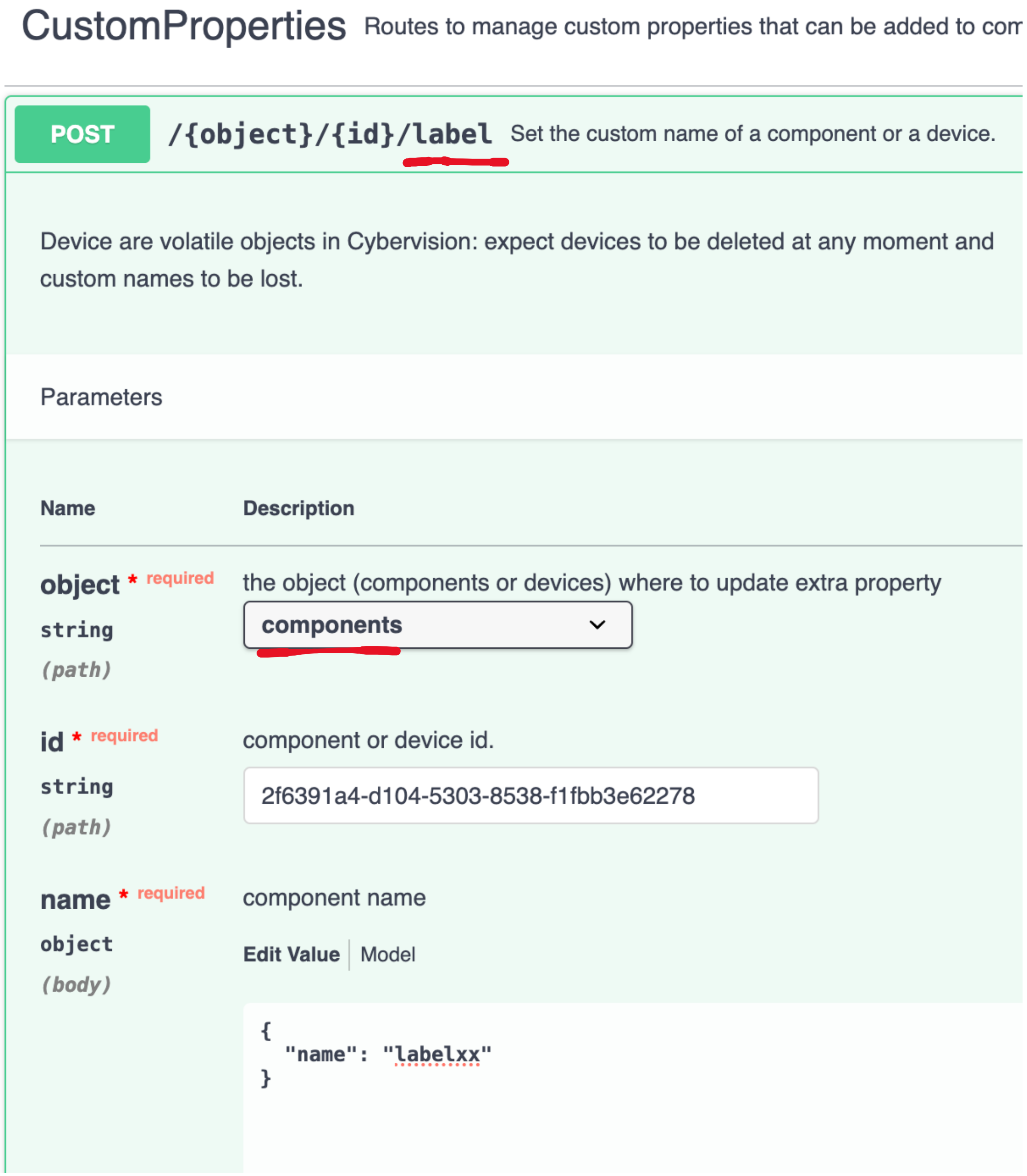
read excel line

compare group and IP_address

to get the component ID

insert tag into the component ID
one by one

CISCO



CustomProperties Routes to manage custom properties that can be added to com

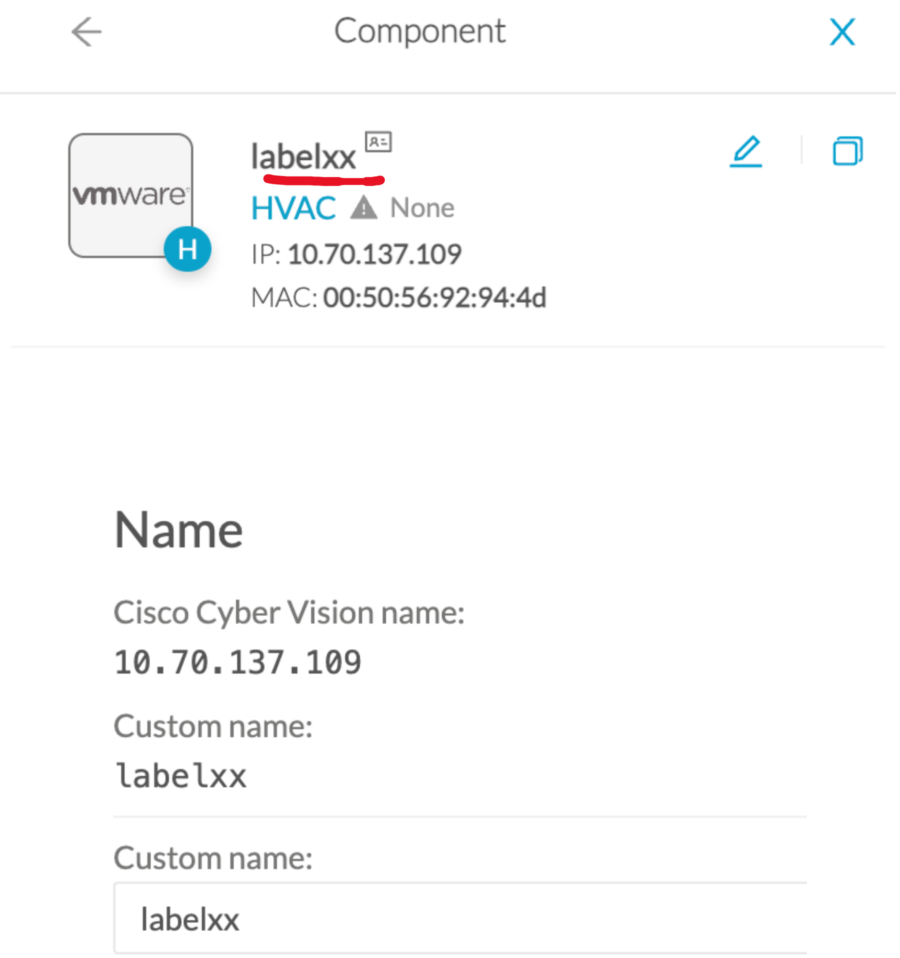
POST /{object}/{id}/label Set the custom name of a component or a device.

Device are volatile objects in Cybervision: expect devices to be deleted at any moment and custom names to be lost.

Parameters

Name	Description
object * required string *(path)*	the object (components or devices) where to update extra property components
id * required string *(path)*	component or device id. 2f6391a4-d104-5303-8538-f1fbb3e62278
name * required object *(body)*	component name **Edit Value** | Model

```
{
  "name": "labelxx"
}
```



labelxx

HVAC ⚠ None

IP: 10.70.137.109

MAC: 00:50:56:92:94:4d

Name

Cisco Cyber Vision name:

10.70.137.109

Custom name:

labelxx

Custom name:

labelxx