# ClearPass Integration Guide

aruba

a Hewlett Packard
Enterprise company

CLAROTY

## Change Log

| Version | Date | Modified By | Comments |
|---|---|---|---|
| 1.0 | May 2019 | Arpit Bhatt | First Published Version – Phase1 |

## Copyright

© Copyright 2019 Hewlett Packard Enterprise Development LP.

## Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett- Packard Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at HPE-Aruba-gplquery@hpe.com.

## Contents

a Hewlett Packard
Enterprise company

www.arubanetworks.com
3333 Scott Blvd
Santa Clara, CA 95054
Phone: 1-800-WIFI-LAN (+800-943-4526)
Fax 408.227.4550

© 2019 Hewlett Packard Enterprise Development LP. All Rights Reserved.

## Figures

## Introduction

This Integration Guide covers the configuration and use of the integration between Claroty and ClearPass Policy Manager (CPPM). Claroty's Continuous Threat Detection product provides extreme visibility, continuous threat and vulnerability monitoring and deep insights into Industrial Control Systems (ICS) networks. This initial integration between Claroty and ClearPass Policy Manager focuses on the ability of Claroty to detect, discover and classify OT/ICS endpoints and share this classification directly with ClearPass via the ClearPass Security Exchange framework and the open APIs we expose. Claroty will automatically update the ClearPass Policy Manager endpoint database with endpoint classification data and a variety of custom security attributes.

This guide is written based on Phase1 of our planned integration with Claroty, which provides centralized visibility of network assets and endpoints across IT and OT infrastructure. From here a centralized endpoint and edge security policy can be defined and administered. Check back for updates to this integration framework.

## Software Requirements

At the time of writing, ClearPass Policy Manager version 6.8.0 is available and the recommended release. CPPM runs on hardware appliances with pre-installed software or as a Virtual Machine under the following hypervisors. Hypervisors that run on a client computer such as VMware Player are not supported.

- VMware ESXi 6.0, 6.5, 6.6 or higher
- Microsoft Hyper-V Server 2012 R2 or 2016 R2
- Hyper-V on Microsoft Windows Server 2012 R2 or 2016 R2
- KVM on CentOS 7.5 or later.

The version of Claroty that was used for writing this integration guide is 3.2.2.9734.

## Installation and Deployment Guide

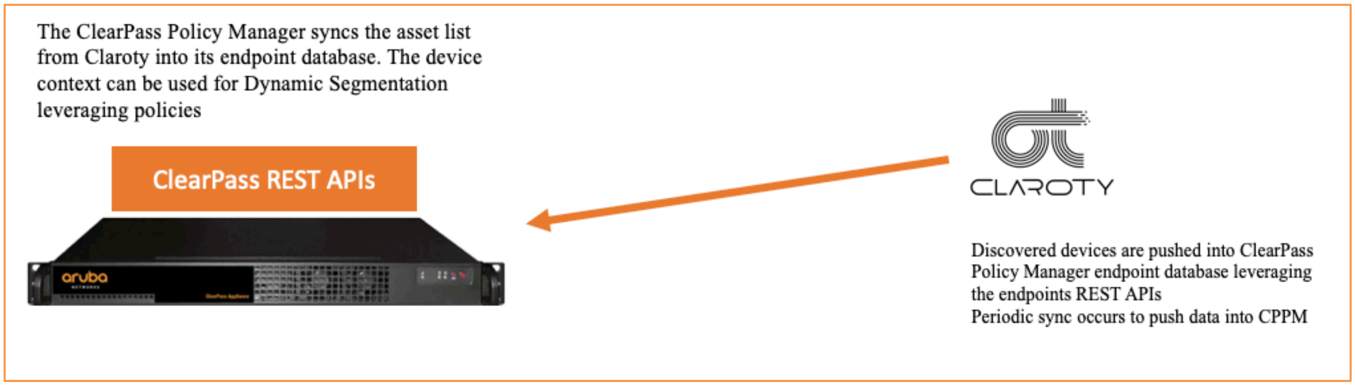
The generic ClearPass installation and deployment guide is located here:

https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Default.htm#About%20ClearPass/Intro_ClearPass.htm

## Pictorial view of the Integration

The diagram below shows a pictorial overview of the components and how they interact with each other.

***Figure 1:*** *Pictorial view of ClearPass Policy Manager integration with Claroty*



The ClearPass Policy Manager syncs the asset list from Claroty into its endpoint database. The device context can be used for Dynamic Segmentation leveraging policies

Discovered devices are pushed into ClearPass Policy Manager endpoint database leveraging the endpoints REST APIs
Periodic sync occurs to push data into CPPM

# Configuration

## ClearPass Configuration

Prior to creating and enabling the integration in Claroty a number of configuration elements need to be pre-created in ClearPass Policy Manager. Follow the below configuration steps carefully, collecting data as highlighted which will be needed in the following section when configuring Claroty to establish an integration with CPPM.

### Create a ClearPass User

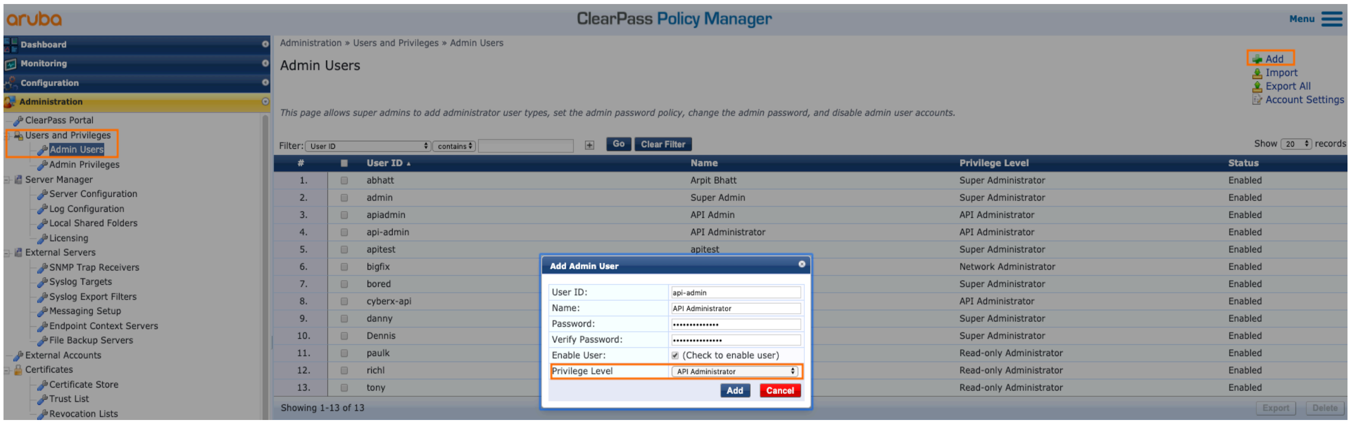
As part of the communications channel between the two products, Claroty will use a number of APIs. Access to the TIPS API is validated via Username/Password combination credentials. This user needs to have minimum levels of access, do not use a Super Administrator profile.

Create a user from **Administration -> Users and Privileges -> +ADD ->** {Create a user, ensure that you use a privilege level of **API Administrator**}

NOTE

*Make a note of the User ID and Password that was configured, ensure Privilege level is API Administrator*

***Figure 2:*** *Create an API level account in ClearPass*



Administration » Users and Privileges » Admin Users

Admin Users

*This page allows super admins to add administrator user types, set the admin password policy, change the admin password, and disable admin user accounts.*

Filter: User ID contains

Show 20 records

| # | | User ID ▴ | Name | Privilege Level | Status |
|---|---|---|---|---|---|
| 1. | □ | abhatt | Arpit Bhatt | Super Administrator | Enabled |
| 2. | □ | admin | Super Admin | Super Administrator | Enabled |
| 3. | □ | apiadmin | API Admin | API Administrator | Enabled |
| 4. | □ | api-admin | API Administrator | API Administrator | Enabled |
| 5. | □ | apitest | apitest | Super Administrator | Enabled |
| 6. | □ | bigfix | | Network Administrator | Enabled |
| 7. | □ | bored | | Super Administrator | Enabled |
| 8. | □ | cyberx-api | | API Administrator | Enabled |
| 9. | □ | danny | | Super Administrator | Enabled |
| 10. | □ | Dennis | | Super Administrator | Enabled |
| 11. | □ | paulk | | Read-only Administrator | Enabled |
| 12. | □ | richl | | Read-only Administrator | Enabled |
| 13. | □ | tony | | Read-only Administrator | Enabled |

Showing 1-13 of 13

**Add Admin User**

| | |
|---|---|
| User ID: | api-admin |
| Name: | API Administrator |
| Password: | •••••••••••••• |
| Verify Password: | ••••••••••••••• |
| Enable User: | ☑ (Check to enable user) |
| Privilege Level | API Administrator |

Add Cancel

### Create an Operator Profile

To securely access the REST APIs for the API Client, create a restricted access Operator Profile. Navigate to **ClearPass Guest > Administration > Operator Logins > Profiles.**

Click on **"Create a new operator profile"** on the top right corner of the page and define an operator profile as shown below.

Pick and choose the necessary access for Claroty to update CPPM endpoint database with the device context. In summary all options are set as 'No Access' except for the following.

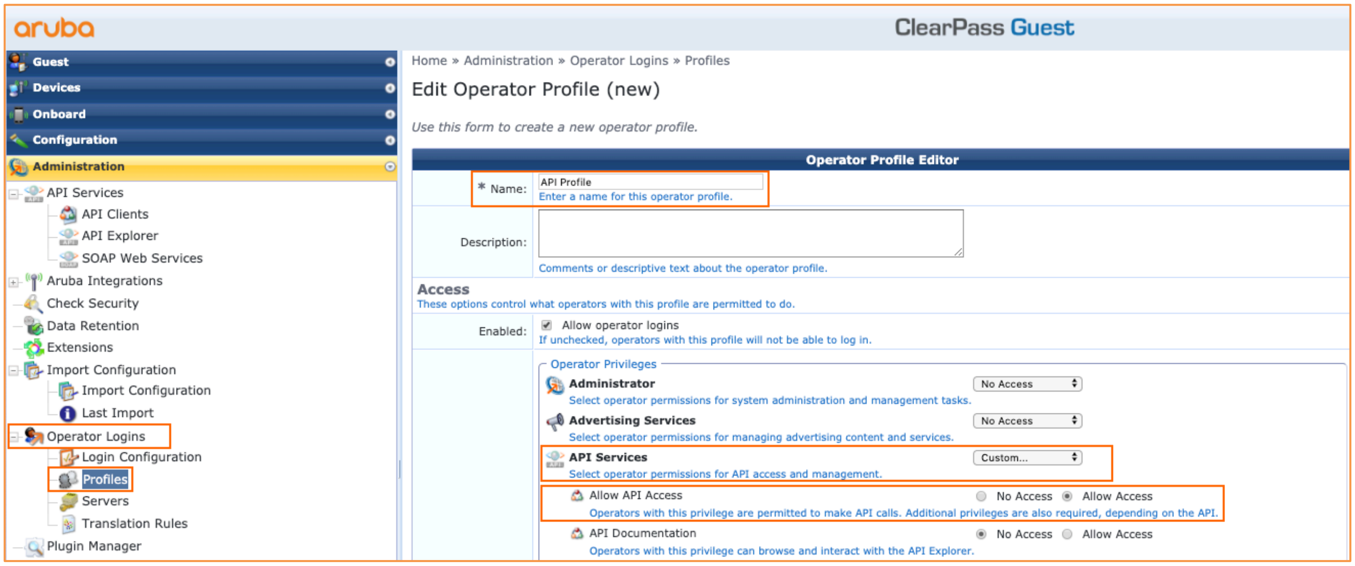
For API Services, select custom and then grant the following access

- **Allow API Access = Allow Access**

For Policy Manager, select custom and then grant the following access

- **Dictionary – Attributes = Read, Write, Delete**
- **Dictionary – Fingerprints = Read, Write, Delete**
- **Identity – Endpoints = Read, Write, Delete**

***Figure 3:*** *Operator Profile - Access restrictions 1*



Home » Administration » Operator Logins » Profiles

Edit Operator Profile (new)

*Use this form to create a new operator profile.*

Operator Profile Editor

* Name: API Profile
Enter a name for this operator profile.

Description:
Comments or descriptive text about the operator profile.

Access
These options control what operators with this profile are permitted to do.

Enabled: ☑ Allow operator logins
If unchecked, operators with this profile will not be able to log in.

Operator Privileges

Administrator — No Access
Select operator permissions for system administration and management tasks.

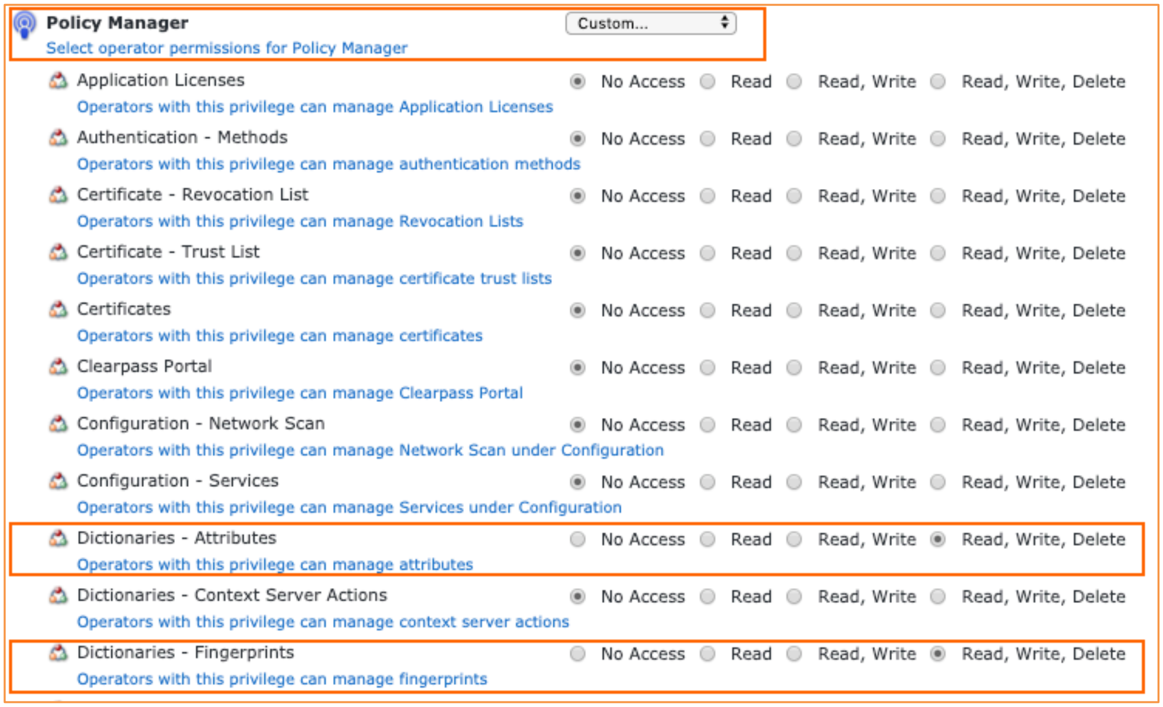
Advertising Services — No Access
Select operator permissions for managing advertising content and services.

API Services — Custom...
Select operator permissions for API access and management.

Allow API Access ○ No Access ● Allow Access
Operators with this privilege are permitted to make API calls. Additional privileges are also required, depending on the API.

API Documentation ● No Access ○ Allow Access
Operators with this privilege can browse and interact with the API Explorer.

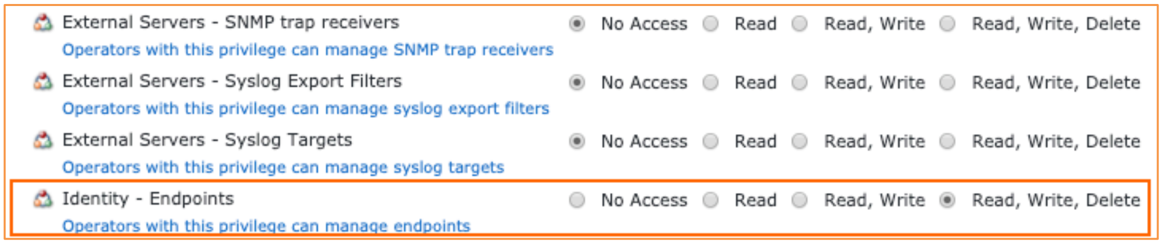
***Figure 4:*** *Operator Profile - Access restrictions 2*



Policy Manager — Custom...
Select operator permissions for Policy Manager

| | | | | |
|---|---|---|---|---|
| Application Licenses<br>Operators with this privilege can manage Application Licenses | ● No Access | ○ Read | ○ Read, Write | ○ Read, Write, Delete |
| Authentication - Methods<br>Operators with this privilege can manage authentication methods | ● No Access | ○ Read | ○ Read, Write | ○ Read, Write, Delete |
| Certificate - Revocation List<br>Operators with this privilege can manage Revocation Lists | ● No Access | ○ Read | ○ Read, Write | ○ Read, Write, Delete |
| Certificate - Trust List<br>Operators with this privilege can manage certificate trust lists | ● No Access | ○ Read | ○ Read, Write | ○ Read, Write, Delete |
| Certificates<br>Operators with this privilege can manage certificates | ● No Access | ○ Read | ○ Read, Write | ○ Read, Write, Delete |
| Clearpass Portal<br>Operators with this privilege can manage Clearpass Portal | ● No Access | ○ Read | ○ Read, Write | ○ Read, Write, Delete |
| Configuration - Network Scan<br>Operators with this privilege can manage Network Scan under Configuration | ● No Access | ○ Read | ○ Read, Write | ○ Read, Write, Delete |
| Configuration - Services<br>Operators with this privilege can manage Services under Configuration | ● No Access | ○ Read | ○ Read, Write | ○ Read, Write, Delete |
| Dictionaries - Attributes<br>Operators with this privilege can manage attributes | ○ No Access | ○ Read | ○ Read, Write | ● Read, Write, Delete |
| Dictionaries - Context Server Actions<br>Operators with this privilege can manage context server actions | ● No Access | ○ Read | ○ Read, Write | ○ Read, Write, Delete |
| Dictionaries - Fingerprints<br>Operators with this privilege can manage fingerprints | ○ No Access | ○ Read | ○ Read, Write | ● Read, Write, Delete |

***Figure 5:*** *Operator Profile - Access restrictions 3*



| | | | | |
|---|---|---|---|---|
| External Servers - SNMP trap receivers<br>Operators with this privilege can manage SNMP trap receivers | ● No Access | ○ Read | ○ Read, Write | ○ Read, Write, Delete |
| External Servers - Syslog Export Filters<br>Operators with this privilege can manage syslog export filters | ● No Access | ○ Read | ○ Read, Write | ○ Read, Write, Delete |
| External Servers - Syslog Targets<br>Operators with this privilege can manage syslog targets | ● No Access | ○ Read | ○ Read, Write | ○ Read, Write, Delete |
| Identity - Endpoints<br>Operators with this privilege can manage endpoints | ○ No Access | ○ Read | ○ Read, Write | ● Read, Write, Delete |

## Create an API Client

Claroty uses the REST APIs for this integration, REST APIs are authenticated under an OAuth2 framework. Create an API Client under **Guest > Administration > API Services > API Clients >** {Create API Client}

NOTE

***Ensure the Operator Profile previously created is used here to restrict the capabilities of the API Client.***

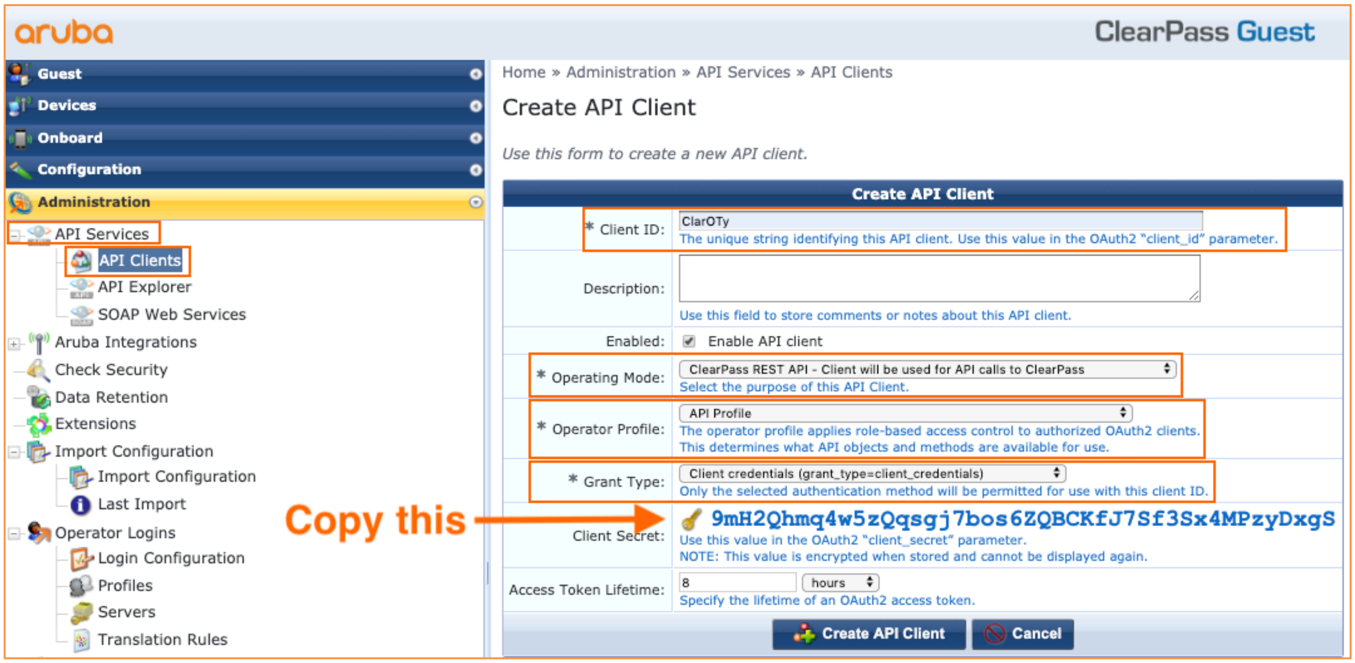
Notice the highlighted configuration options needed, and set as appropriate

- **Operating Mode = ClearPass REST API – Client will be used for API calls to ClearPass**
- **Operator Profile = Use the Operator Profile created previously**
- **Grant Type = Client credentials (grant_type=client_credentails)**

NOTE

***Record the Client Secret and the ACTUAL API Client ID i.e. ClarOTy as below***

***Figure 6:*** *Create an API Client*



Create API Client

*Use this form to create a new API client.*

| Create API Client | |
|---|---|
| * Client ID: | ClarOTy<br>The unique string identifying this API client. Use this value in the OAuth2 "client_id" parameter. |
| Description: | <br>Use this field to store comments or notes about this API client. |
| Enabled: | ☑ Enable API client |
| * Operating Mode: | ClearPass REST API - Client will be used for API calls to ClearPass<br>Select the purpose of this API Client. |
| * Operator Profile: | API Profile<br>The operator profile applies role-based access control to authorized OAuth2 clients. This determines what API objects and methods are available for use. |
| * Grant Type: | Client credentials (grant_type=client_credentials)<br>Only the selected authentication method will be permitted for use with this client ID. |
| Client Secret: | 9mH2Qhmq4w5zQqsgj7bos6ZQBCKfJ7Sf3Sx4MPzyDxgS<br>Use this value in the OAuth2 "client_secret" parameter.<br>NOTE: This value is encrypted when stored and cannot be displayed again. |
| Access Token Lifetime: | 8 hours<br>Specify the lifetime of an OAuth2 access token. |

At this time all of the necessary config has been created in Policy Manager, ensure you have the below list of information collected before proceeding to the next section.

- **CPPM API Administrator User ID**
- **CPPM API Administrator User Password**
- **CPPM OAuth2 API Client NAME**
- **CPPM OAuth2 API Client Secret**

## Claroty Configuration

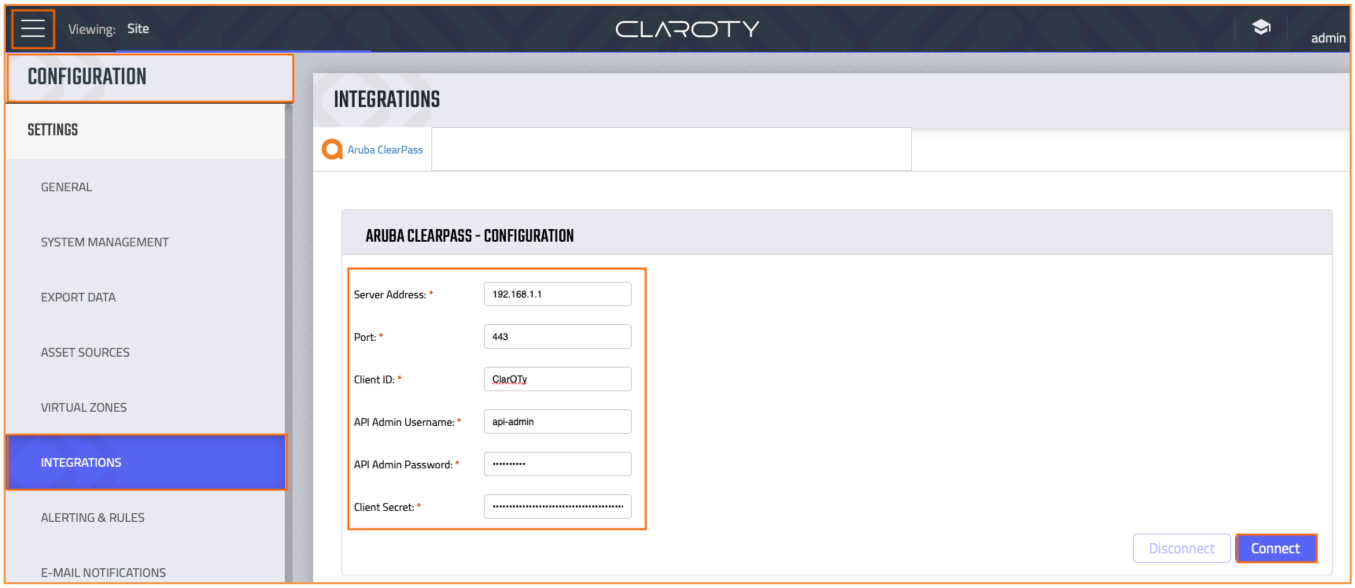
For this initial integration between the two products, there is limited configuration necessary on Claroty. After the configuration is complete the Claroty platform will continue to update the ClearPass Policy Manager endpoint database as it discovers new endpoints at a periodic schedule. Follow the steps below to configure and enable this integration.

Login as an administrator into Calroty using port 5000 (https://<IP Address>:5000). From the Claroty main console, navigate to **Configuration > Integrations > Aruba ClearPass**.

After clicking on 'Aruba ClearPass' the following screen is shown, all fields are required for the configuration. Use the values collected during ClearPass Policy Manager configuration. Once configured, click on **Connect**. A message is displayed at the bottom of the screen in a green box saying **"Added Integration Configuration"**. This is easy to miss.

The button for **Connect** changes to **Update** which indicates the configuration is saved.

***Figure 7:*** *Claroty Configuration Console*



Server Address: * 192.168.1.1

Port: * 443

Client ID: * ClarOTy

API Admin Username: * api-admin

API Admin Password: * ••••••••••

Client Secret: * ••••••••••••••••••••••••••••••••••••

Below table explains the fields used for configuration in detail.

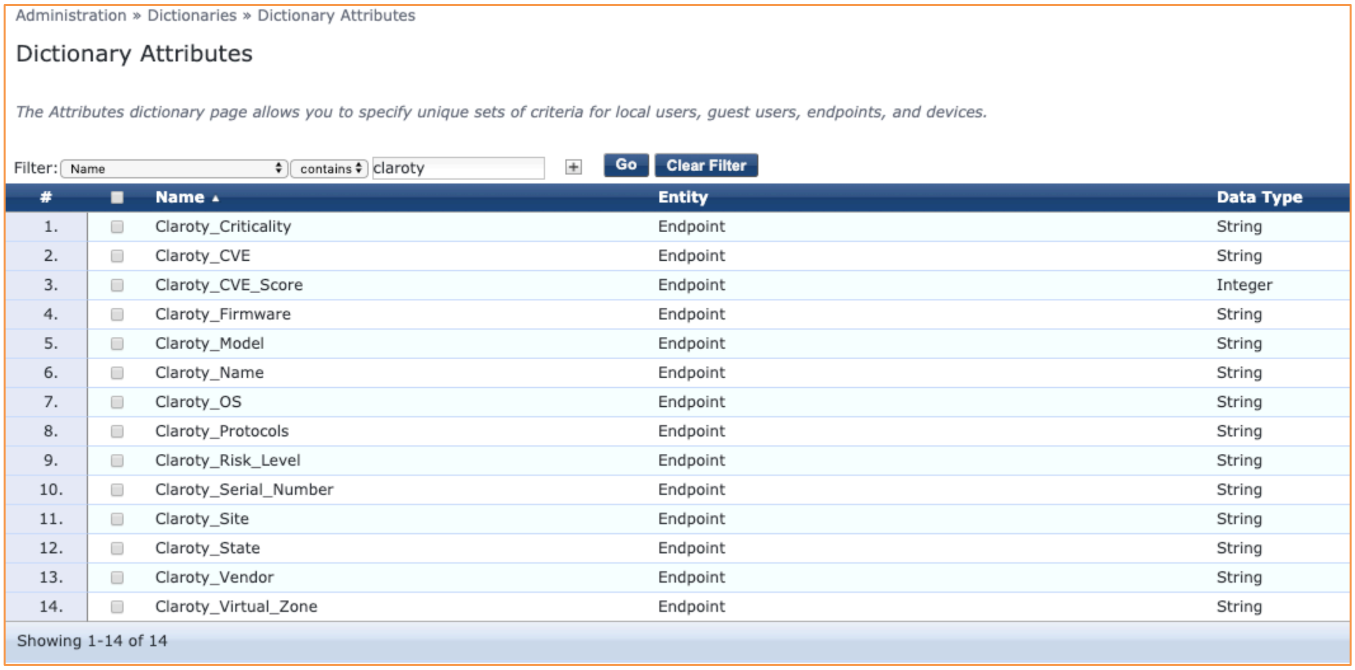
| **Field Name** | **Value/Notes** |
|---|---|
| **Server Address** | This should be the ClearPass Publisher’s IP address |
| **Port** | This should be 443 |
| **Client ID** | OAuth2 client ID created in the previous section |
| **API Admin Username** | API Administrator User ID created in the previous section |
| **API Admin Password** | API Administrator Password created in the previous section |
| **Client Secret** | OAuth2 Client Secret copied in the previous section |

## Integration Results

As part of enabling the above integration, Claroty will create a number of custom Endpoint Dictionary attributes using the ClearPass REST APIs. This is a record of the Dictionary Attributes created by Claroty.

Check under **Administration > Dictionaries > Dictionary Attributes**.

***Figure 8:*** *Endpoint Dictionary Attributes created by Claroty*



Administration » Dictionaries » Dictionary Attributes

Dictionary Attributes

*The Attributes dictionary page allows you to specify unique sets of criteria for local users, guest users, endpoints, and devices.*

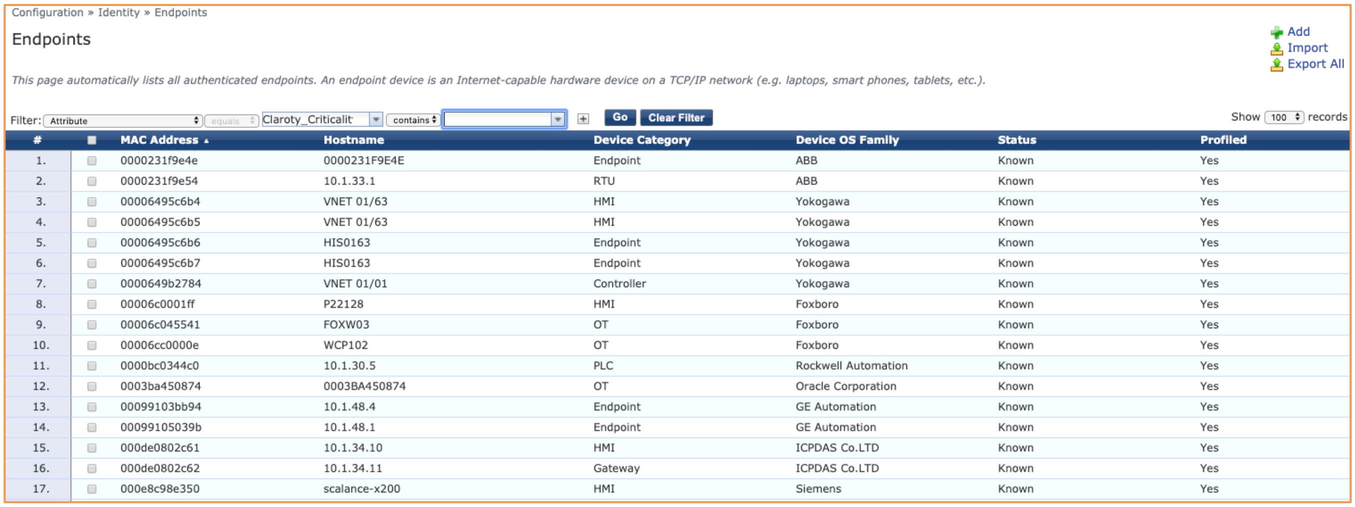
Filter: Name | contains | claroty

| # | ■ | Name ▲ | Entity | Data Type |
|---|---|---|---|---|
| 1. | □ | Claroty_Criticality | Endpoint | String |
| 2. | □ | Claroty_CVE | Endpoint | String |
| 3. | □ | Claroty_CVE_Score | Endpoint | Integer |
| 4. | □ | Claroty_Firmware | Endpoint | String |
| 5. | □ | Claroty_Model | Endpoint | String |
| 6. | □ | Claroty_Name | Endpoint | String |
| 7. | □ | Claroty_OS | Endpoint | String |
| 8. | □ | Claroty_Protocols | Endpoint | String |
| 9. | □ | Claroty_Risk_Level | Endpoint | String |
| 10. | □ | Claroty_Serial_Number | Endpoint | String |
| 11. | □ | Claroty_Site | Endpoint | String |
| 12. | □ | Claroty_State | Endpoint | String |
| 13. | □ | Claroty_Vendor | Endpoint | String |
| 14. | □ | Claroty_Virtual_Zone | Endpoint | String |

Showing 1-14 of 14

The Endpoint data is sent by Claroty, it creates the Endpoints, sets the endpoint classification and also configures some custom endpoint attributes. An example of the endpoints created are shown below.

***Figure 9:*** *Example of Endpoints created by Claroty*



Configuration » Identity » Endpoints

Endpoints

*This page automatically lists all authenticated endpoints. An endpoint device is an Internet-capable hardware device on a TCP/IP network (e.g. laptops, smart phones, tablets, etc.).*

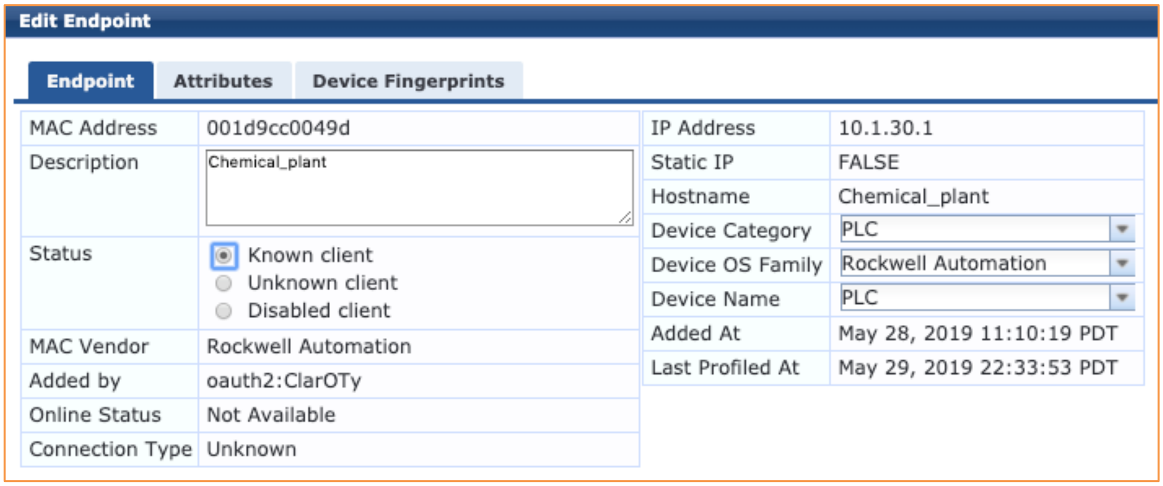
Filter: Attribute | equals | Claroty_Criticalit | contains |

Show 100 records

| # | ■ | MAC Address ▲ | Hostname | Device Category | Device OS Family | Status | Profiled |
|---|---|---|---|---|---|---|---|
| 1. | □ | 0000231f9e4e | 0000231F9E4E | Endpoint | ABB | Known | Yes |
| 2. | □ | 0000231f9e54 | 10.1.33.1 | RTU | ABB | Known | Yes |
| 3. | □ | 00006495c6b4 | VNET 01/63 | HMI | Yokogawa | Known | Yes |
| 4. | □ | 00006495c6b5 | VNET 01/63 | HMI | Yokogawa | Known | Yes |
| 5. | □ | 00006495c6b6 | HIS0163 | Endpoint | Yokogawa | Known | Yes |
| 6. | □ | 00006495c6b7 | HIS0163 | Endpoint | Yokogawa | Known | Yes |
| 7. | □ | 0000649b2784 | VNET 01/01 | Controller | Yokogawa | Known | Yes |
| 8. | □ | 00006c0001ff | P22128 | HMI | Foxboro | Known | Yes |
| 9. | □ | 00006c045541 | FOXW03 | OT | Foxboro | Known | Yes |
| 10. | □ | 00006cc0000e | WCP102 | OT | Foxboro | Known | Yes |
| 11. | □ | 0000bc0344c0 | 10.1.30.5 | PLC | Rockwell Automation | Known | Yes |
| 12. | □ | 0003ba450874 | 0003BA450874 | OT | Oracle Corporation | Known | Yes |
| 13. | □ | 00099103bb94 | 10.1.48.4 | Endpoint | GE Automation | Known | Yes |
| 14. | □ | 00099105039b | 10.1.48.1 | Endpoint | GE Automation | Known | Yes |
| 15. | □ | 000de0802c61 | 10.1.34.10 | HMI | ICPDAS Co.LTD | Known | Yes |
| 16. | □ | 000de0802c62 | 10.1.34.11 | Gateway | ICPDAS Co.LTD | Known | Yes |
| 17. | □ | 000e8c98e350 | scalance-x200 | HMI | Siemens | Known | Yes |

Looking closer at the endpoint data we can see several important things, the mac-address, mac-vendor, and some device classification as determined by Claroty, other valuable data such as the date the endpoint was added and profiled, said another way the time Claroty updated ClearPass with the devices data.

***Figure 10:*** *Normalized Endpoint data created by Claroty*



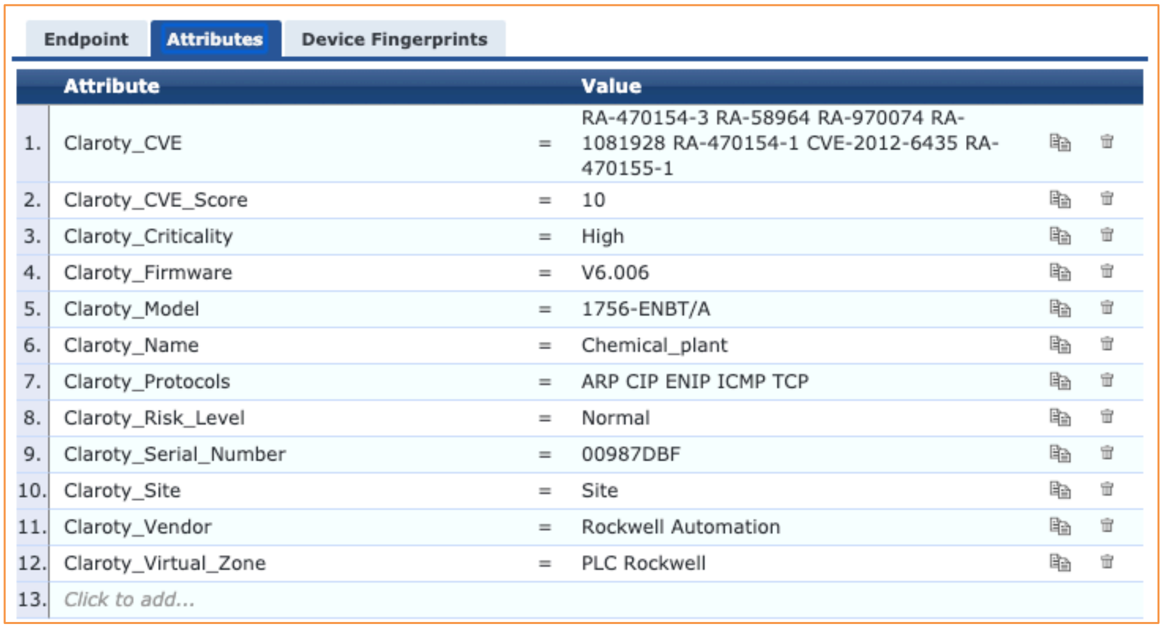
**Edit Endpoint**

| | |
|---|---|
| MAC Address | 001d9cc0049d |
| Description | Chemical_plant |
| Status | ● Known client<br>○ Unknown client<br>○ Disabled client |
| MAC Vendor | Rockwell Automation |
| Added by | oauth2:ClarOTy |
| Online Status | Not Available |
| Connection Type | Unknown |

| | |
|---|---|
| IP Address | 10.1.30.1 |
| Static IP | FALSE |
| Hostname | Chemical_plant |
| Device Category | PLC |
| Device OS Family | Rockwell Automation |
| Device Name | PLC |
| Added At | May 28, 2019 11:10:19 PDT |
| Last Profiled At | May 29, 2019 22:33:53 PDT |

In addition to the standard data, Claroty also supplies other custom attributes. Click on the **Attributes** tab to see them. Any of these attributes could be used in a Policy.

***Figure 11:*** *Custom Endpoint data created by Claroty*



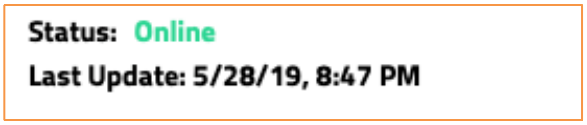
| | Attribute | | Value |
|---|---|---|---|
| 1. | Claroty_CVE | = | RA-470154-3 RA-58964 RA-970074 RA-1081928 RA-470154-1 CVE-2012-6435 RA-470155-1 |
| 2. | Claroty_CVE_Score | = | 10 |
| 3. | Claroty_Criticality | = | High |
| 4. | Claroty_Firmware | = | V6.006 |
| 5. | Claroty_Model | = | 1756-ENBT/A |
| 6. | Claroty_Name | = | Chemical_plant |
| 7. | Claroty_Protocols | = | ARP CIP ENIP ICMP TCP |
| 8. | Claroty_Risk_Level | = | Normal |
| 9. | Claroty_Serial_Number | = | 00987DBF |
| 10. | Claroty_Site | = | Site |
| 11. | Claroty_Vendor | = | Rockwell Automation |
| 12. | Claroty_Virtual_Zone | = | PLC Rockwell |
| 13. | *Click to add...* | | |

**Claroty_Criticality, Claroty_Firmware, Claroty_Risk_Level, Claroty_CVE_Score** are some of the very useful attributes that can be used within the enforcement policy. For example, a known vulnerable Firmware for a device category can be blocked. If the Criticality is High, an endpoint can be quarantined.

## Monitoring/Reviewing ClearPass and Claroty communications

Once the sync has started endpoint data will be populated directly into the Policy Manager endpoint database, view the last update time from the integration configuration screen, see below for an example.

***Figure 12:*** *Reviewing 'Last Update' time to ClearPass*

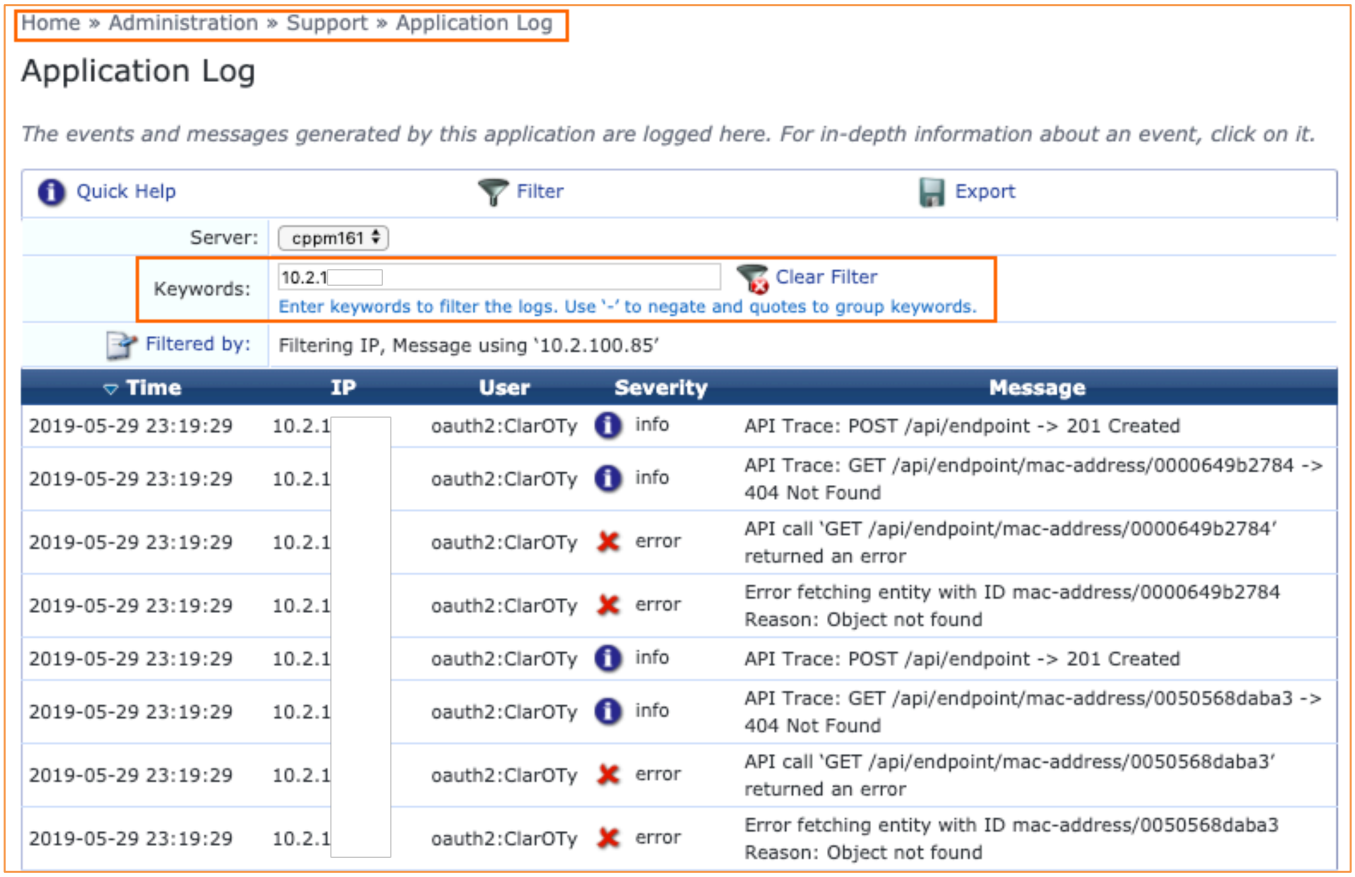


**Status:** Online

**Last Update: 5/28/19, 8:47 PM**

If the sync is not working or shows an error then it's likely you've missed capturing the information correctly, recheck the data recorded, additionally you can view the API calls between Claroty and ClearPass from **ClearPass Guest > Administration > Support > Application Log.** Below is an example of logs from Claroty to ClearPass. Filter using the IP address of Claroty.

***Figure 13:*** *Example of API logs between Claroty and ClearPass*



Application Log

*The events and messages generated by this application are logged here. For in-depth information about an event, click on it.*

Server: cppm161

Keywords: 10.2.1[redacted]

Enter keywords to filter the logs. Use '-' to negate and quotes to group keywords.

Filtered by: Filtering IP, Message using '10.2.100.85'

| Time | IP | User | Severity | Message |
|---|---|---|---|---|
| 2019-05-29 23:19:29 | 10.2.1[redacted] | oauth2:ClarOTy | ℹ info | API Trace: POST /api/endpoint -> 201 Created |
| 2019-05-29 23:19:29 | 10.2.1[redacted] | oauth2:ClarOTy | ℹ info | API Trace: GET /api/endpoint/mac-address/0000649b2784 -> 404 Not Found |
| 2019-05-29 23:19:29 | 10.2.1[redacted] | oauth2:ClarOTy | ✗ error | API call 'GET /api/endpoint/mac-address/0000649b2784' returned an error |
| 2019-05-29 23:19:29 | 10.2.1[redacted] | oauth2:ClarOTy | ✗ error | Error fetching entity with ID mac-address/0000649b2784 Reason: Object not found |
| 2019-05-29 23:19:29 | 10.2.1[redacted] | oauth2:ClarOTy | ℹ info | API Trace: POST /api/endpoint -> 201 Created |
| 2019-05-29 23:19:29 | 10.2.1[redacted] | oauth2:ClarOTy | ℹ info | API Trace: GET /api/endpoint/mac-address/0050568daba3 -> 404 Not Found |
| 2019-05-29 23:19:29 | 10.2.1[redacted] | oauth2:ClarOTy | ✗ error | API call 'GET /api/endpoint/mac-address/0050568daba3' returned an error |
| 2019-05-29 23:19:29 | 10.2.1[redacted] | oauth2:ClarOTy | ✗ error | Error fetching entity with ID mac-address/0050568daba3 Reason: Object not found |

Notice there are a few error logs. These errors indicate that the mac address did not exist hence a new one was created by Claroty. If it exists, it will be updated if necessary and the errors will not be seen.