Setting Operator Name and CUI in Clearpass
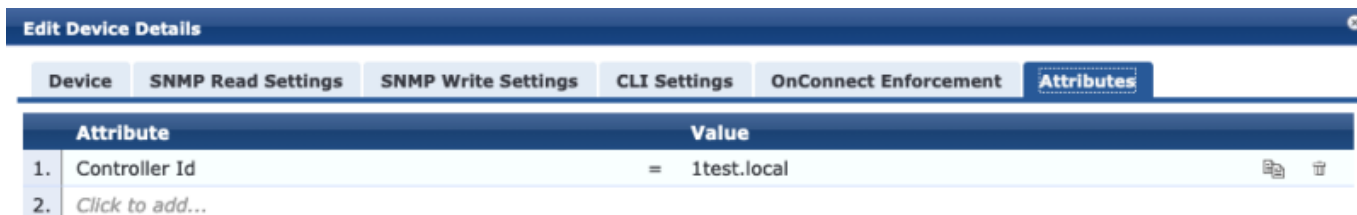
Background

Operator-Name (O-N) and Chargeable-User-Identity (CUI) are two attributes that provide a Govroam operators with useful audit information. Operator-Name identifies the sending site (in the form of their realm) and CUI contains the MAC address and username of the user device, encoded.

The approach below is fairly straight-forward: An attribute is attached to the NAS device which contains the value which we wish O-N to be set to. An Enforcement Policy and Profile are created which sets Operator-Name to the value of the Attribute. The Enforcement Policy is attached to the Service which forwards unknown realms (visitor authentication requests) to the NRPS.

This means that each NAS can have a different realm associated with it. This could be useful if the NASes are different RADIUS servers at different sites.

Setting O-N

- In **Configuration → Network → Devices** choose the device you want to apply an O-N to.
- Go to the **Attributes** page
- Add an attribute of **Controller ID** with a value of **1realm.name** where 'realm.name' is your realm name e.g. 'jisc.ac.uk'. The format always starts with a '1'.

- Save and exit.

- In **Configuration → Enforcement → Profiles Add** a new profile.
- Create a new Attribute, type **Radius:IETF**, name **Operator-Name** and value **%{Device:Controller Id}**.

Enforcement Profiles - Set O-N to Controller ID value.

Summary | Profile | Attributes

Profile:

Name:	Set O-N to Controller ID value.
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Operator-Name	=	%{Device:Controller Id}

- Save and exit

- In **Configuration → Enforcement → Policy Add** a new policy
- **Enforcement Type** is **RADIUS**.
- **Default** is **Allow Access Profile**.
- Add a new rule **Device:Controller Id**, **EXISTS**
- Choose the Enforcement Profile created above.

Enforcement Policies - Set O-N

Summary | Enforcement | Rules

Enforcement:

Name:	Set O-N
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Allow Access Profile]

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Device:Controller Id *EXISTS*)	Set O-N to Controller ID value.

- Save and exit.

- In **Configuration → Services** pick the rule that you want to apply this too - normally the rule which sends default traffic to the NRPS.
- Under **Enforcement** choose the **Enforcement Policy** created above.

Services - Shared Proxy unknown to NRPS

| Summary | Service | Roles | Proxy Targets | Enforcement |

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Set O-N   **Modify**

Enforcement Policy Details

Description:	
Default Profile:	[Allow Access Profile]
Rules Evaluation Algorithm:	first-applicable

Conditions	Enforcement Profiles
1. (Device:Controller Id *EXISTS*)	Set O-N to Controller ID value.

- Save and exit.

- Attempts to authenticate with an unknown realm should use the above Service and create an entry in the Access Tracker which looks like this:

| Summary | Input | **Output** | Alerts |

Enforcement Profiles:	Set O-N to Controller ID value.
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:IETF:Operator-Name	1test.local

Setting CUI

TBD

From:
https://wiki.govroam.uk/ - **Govroam**

Permanent link:
https://wiki.govroam.uk/doku.php?id=siteadmin:clearpass_-_setting_o-n_and_cui_wrong

Last update: **2024/05/15 12:46**