
cisco
You make possible

A to Z of MUD

Enabling Secure IoT Onboarding

Vinay Saini , Solutions Architect @vinsaini
Rishikesh Radhakrishnan , Software Architect @rishikeshr

DEVNET-1343

Barcelona | January 27-31, 2020

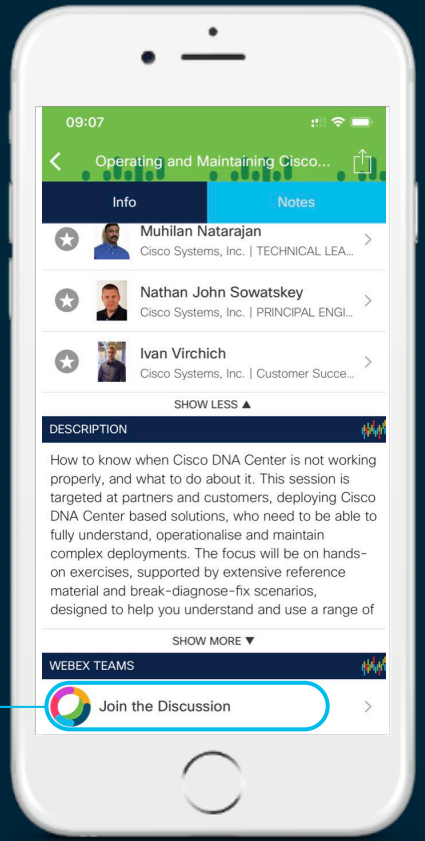
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



Agenda

- Introduction to MUD
  - IoT security challenges & MUD
  - MUD Architecture & Components
- Packet Flows
  - Using DHCP & AAA accounting as transport
  - Using LLDP & AAA accounting as transport
- Creating ISE policies
  - Using MUD in ISE Authorization Policies
- Creating MUD URL and File
  - File Creation and use with DHCP and LLDP
- MUD simulation tools and setup
  - Linux based MUD clients,
  - Scripts to send MUD URI in lldp and DHCP.

Your presenters today

- Vinay Saini
- Solutions Architect

- 15+ years in Networking and IoT
- CCIE Wireless#38448, CWNE#69
- Active Contributor to Cisco certification programs.

- Rishikesh Radhakrishnan
- Software Architect

- 15+ years in Software Architecture, Design & Development.
- Focused on IoT, Infra Automation, Multi-Cloud Orchestration.

Security Challenges in IoT Environment

Antiquated Systems
Unpatched, legacy systems

Insecure Design
Lack of segmentation

OT Security Skills
IT sec ⇔ Ops knowledge

Lack of Visibility
What's out there, who is talking to who, what are they saying

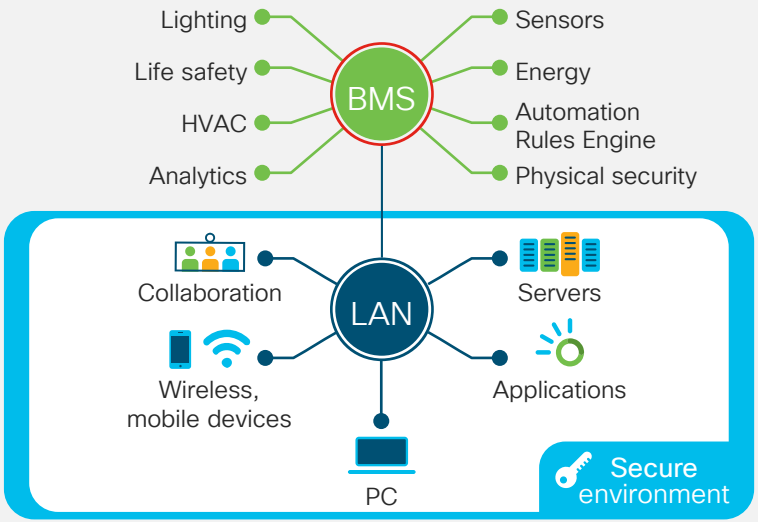
Access Control
Access needs evolving

Change Control
24/7/365 Operations

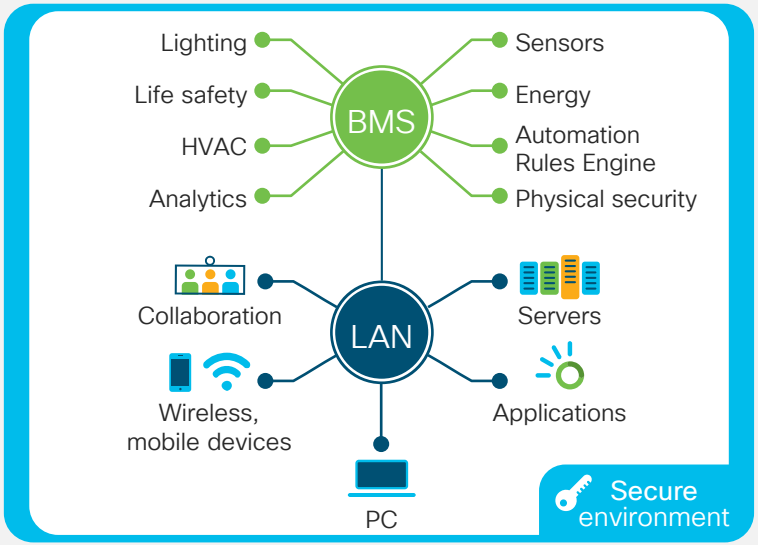
Business Needs
Real-time Information, no downtime, quick access

IoT in the Enterprise

Traditional – Isolated BMS & IoT



New Approach – Converged



Questions that need answering

What is this thing?

Who is responsible for it?

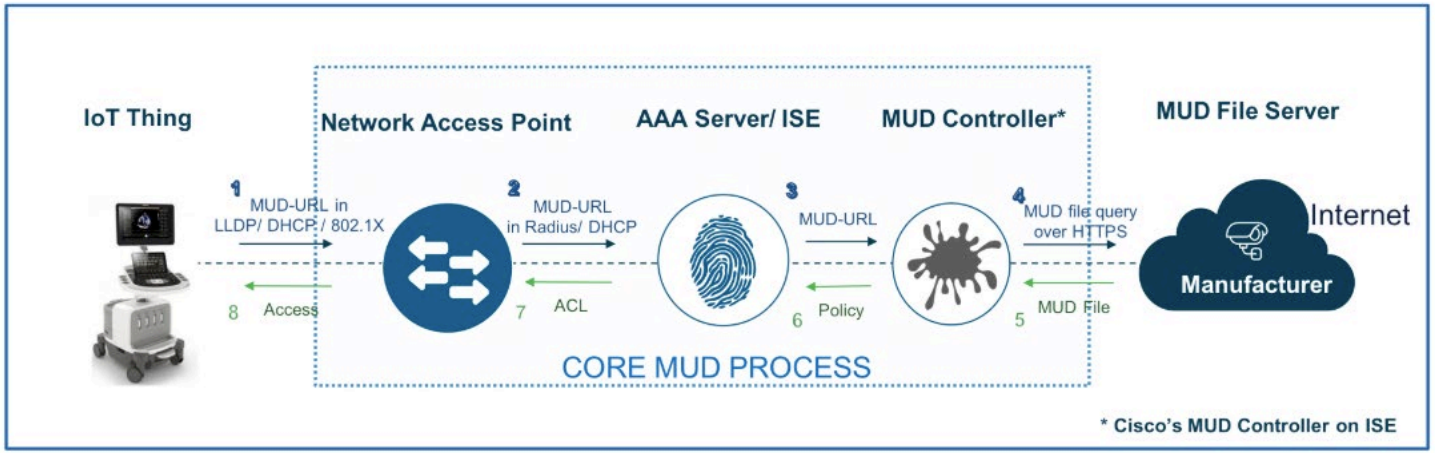
What access does it need?

Is it doing what it should be doing?

Manufacturer Usage Description

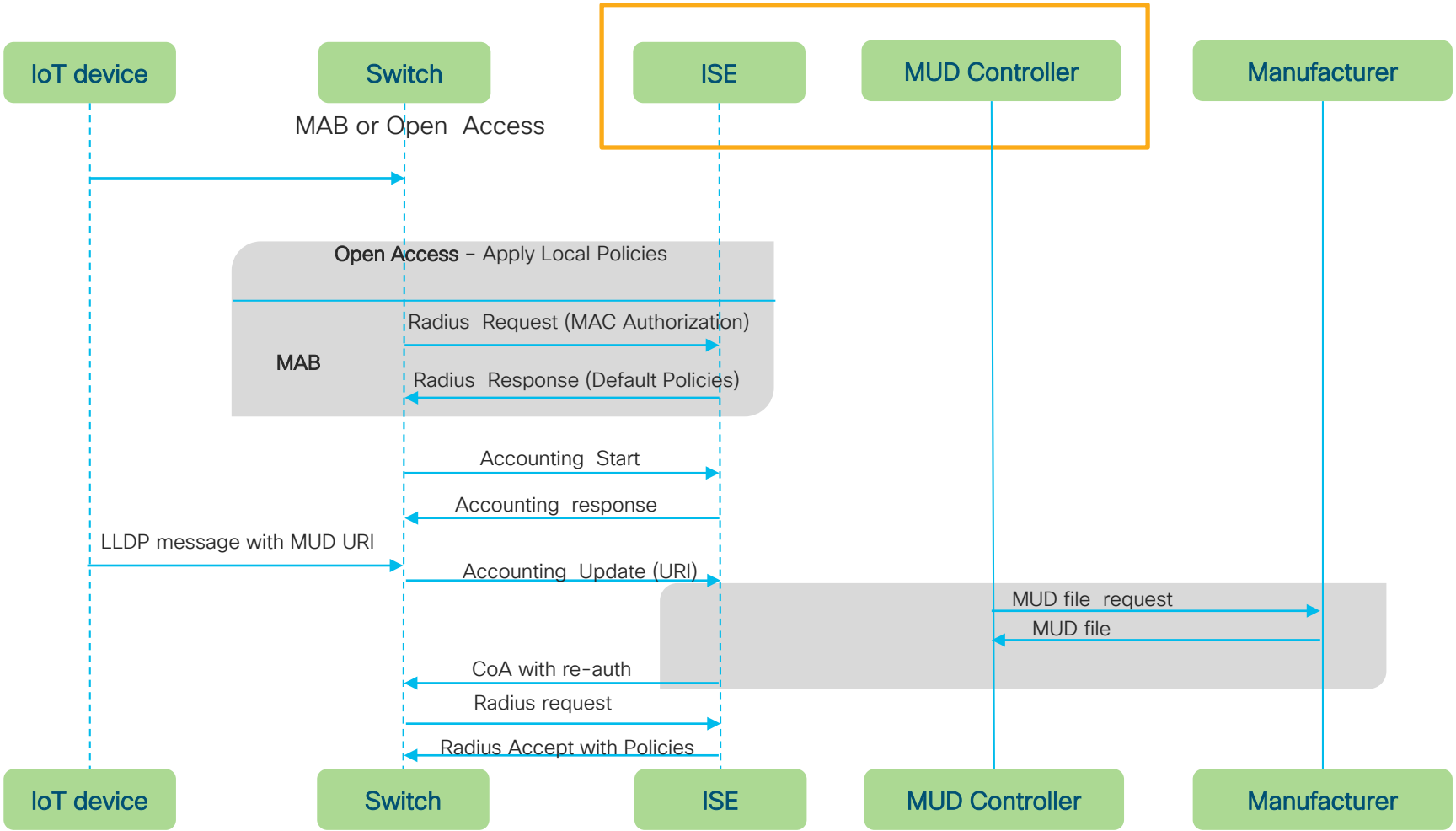
MUD Architecture and Components

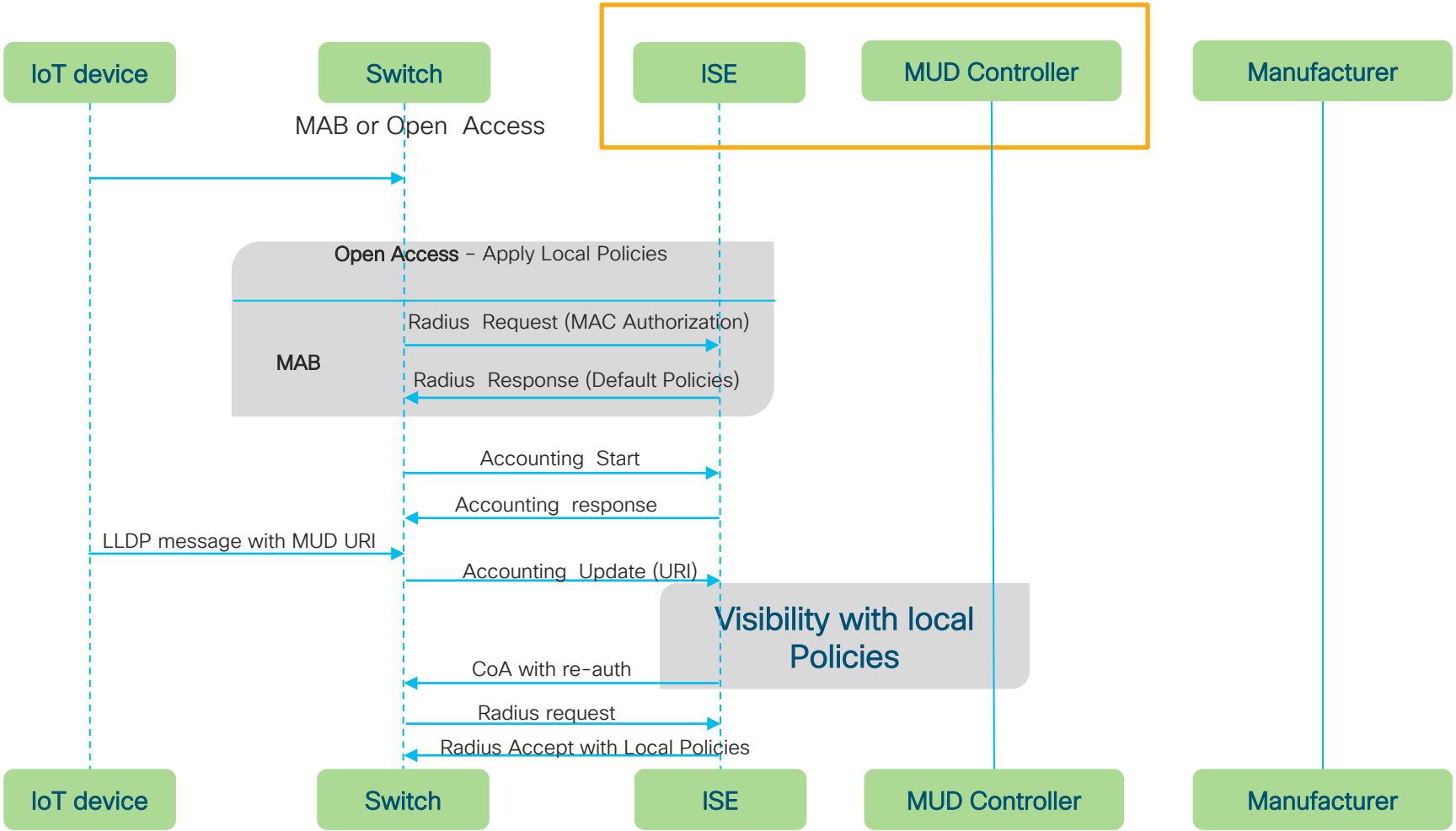
MUD Architecture and Components

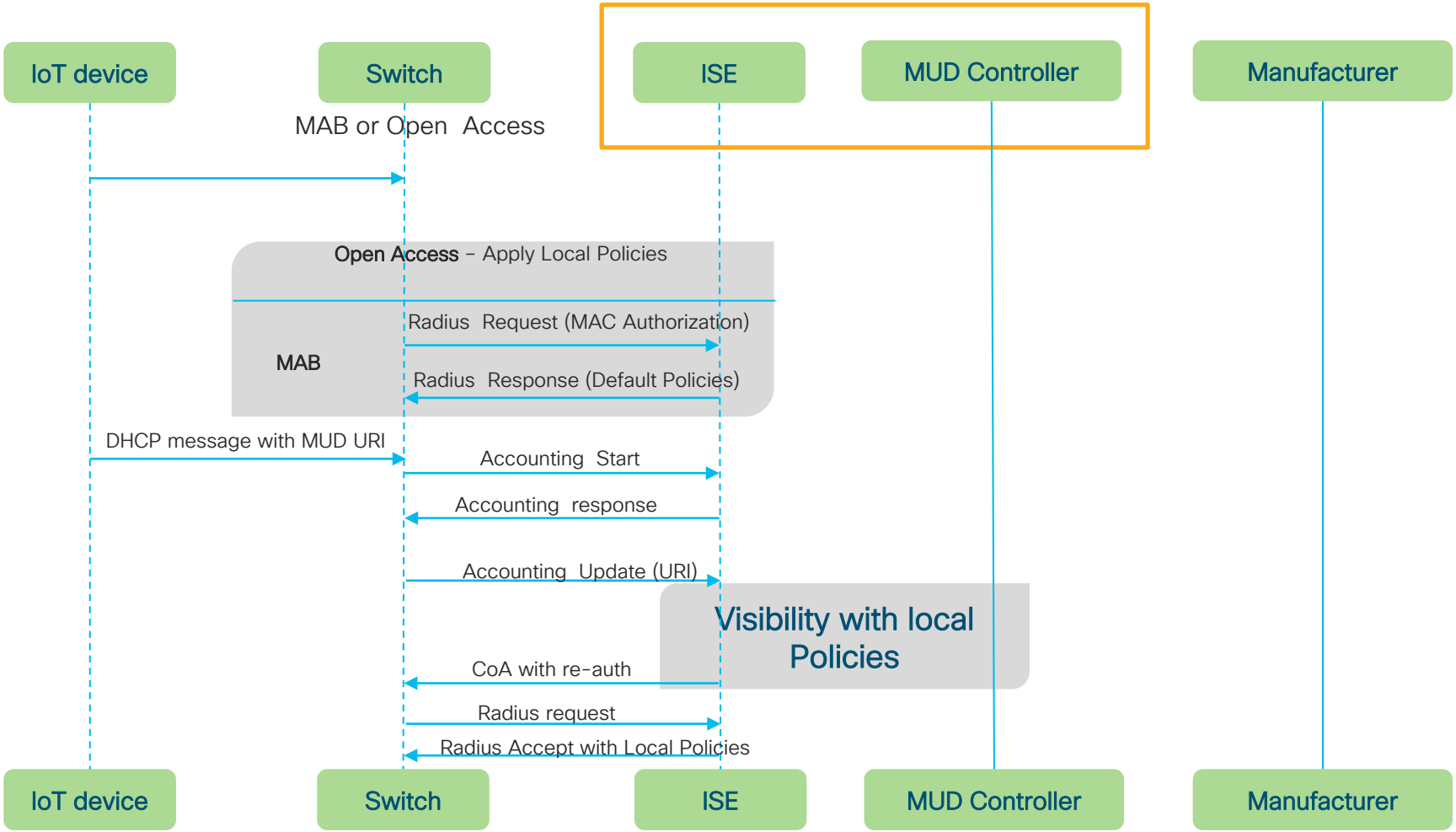


Packet Flows

MUD with LLDP & DHCP







MUD is supported on

Catalyst 9000 series Switches

IE4000

- Both LLDP and DHCP methods are supported.
- RADIUS accounting needs to be enabled.

Wireless MUD support

MUD Support on 9800 series WLC

Version 16.10.1 or above

Only DHCP Method is supported.

Only Central Switching is supported

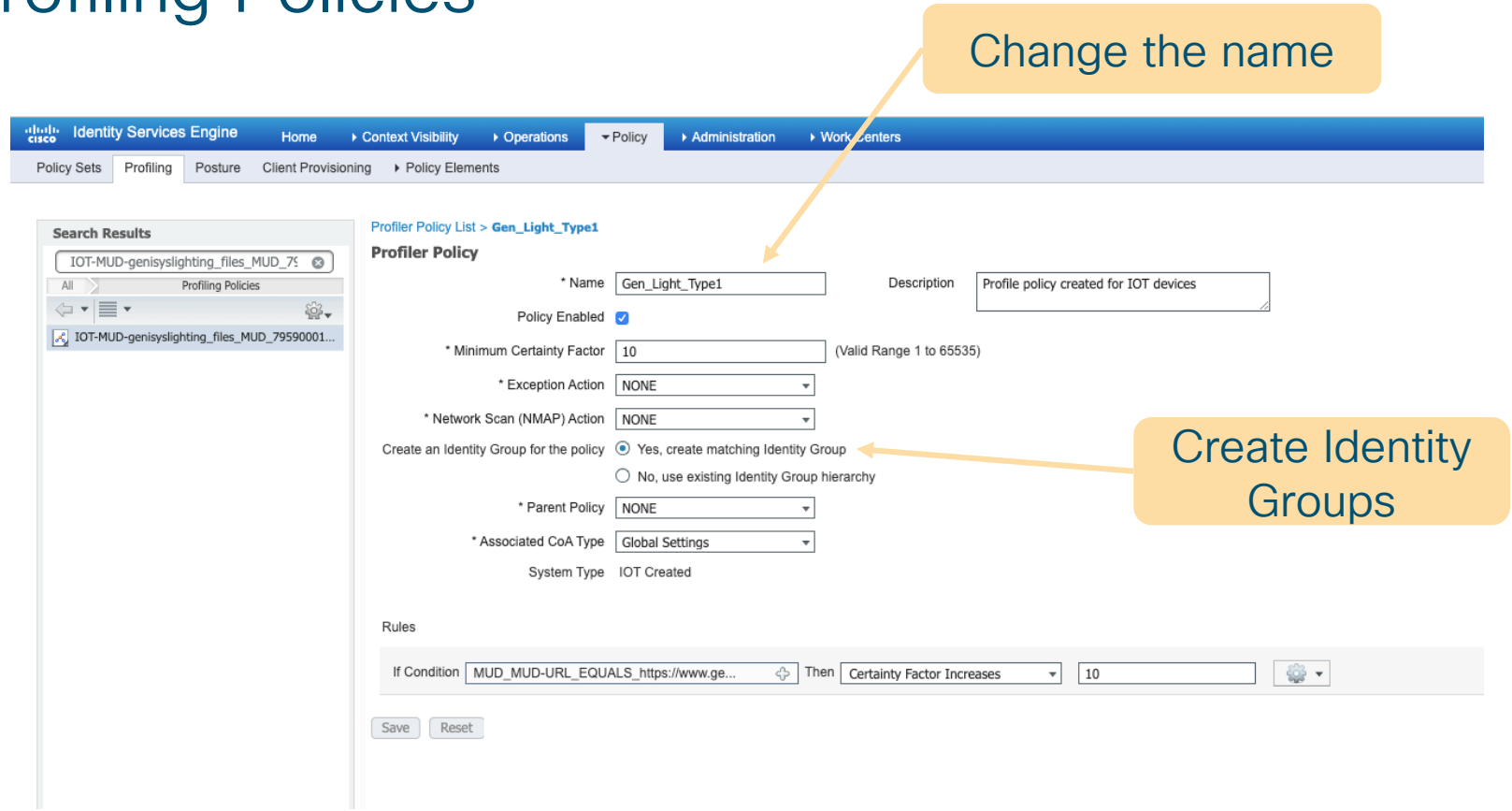
MUD URI sent in RADIUS accounting

```
  Radio Signal Strength Indicator : -29 dBm
  Signal to Noise Ratio : 47 dB
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
EoGRE : No/Simple client
Protocol          : DHCP
Type              : 12   15
Data              : 0f
00000000  00 0c 00 0b 72 61 73 70  62 65 72 72 79 70 69      |....raspberrypi |
Type              : 55   18
Data              : 12
00000000  00 37 00 0e 01 1c 02 03  0f 06 77 0c 2c 2f 1a 79  |.7........w.,/.y|
00000010  2a a1                                             |*.              |
Type              : 161  41
Data              : 29
00000000  00 a1 00 25 68 74 74 70  3a 2f 2f 31 30 2e 36 34  |...%http://10.64|
00000010  2e 36 39 2e 32 30 39 3a  38 30 38 30 2f 62 6c 69  |.69.209:8080/bli|
00000020  6e 64 76 31 2e 6a 73 6f  6e                      |ndv1.json       |
```

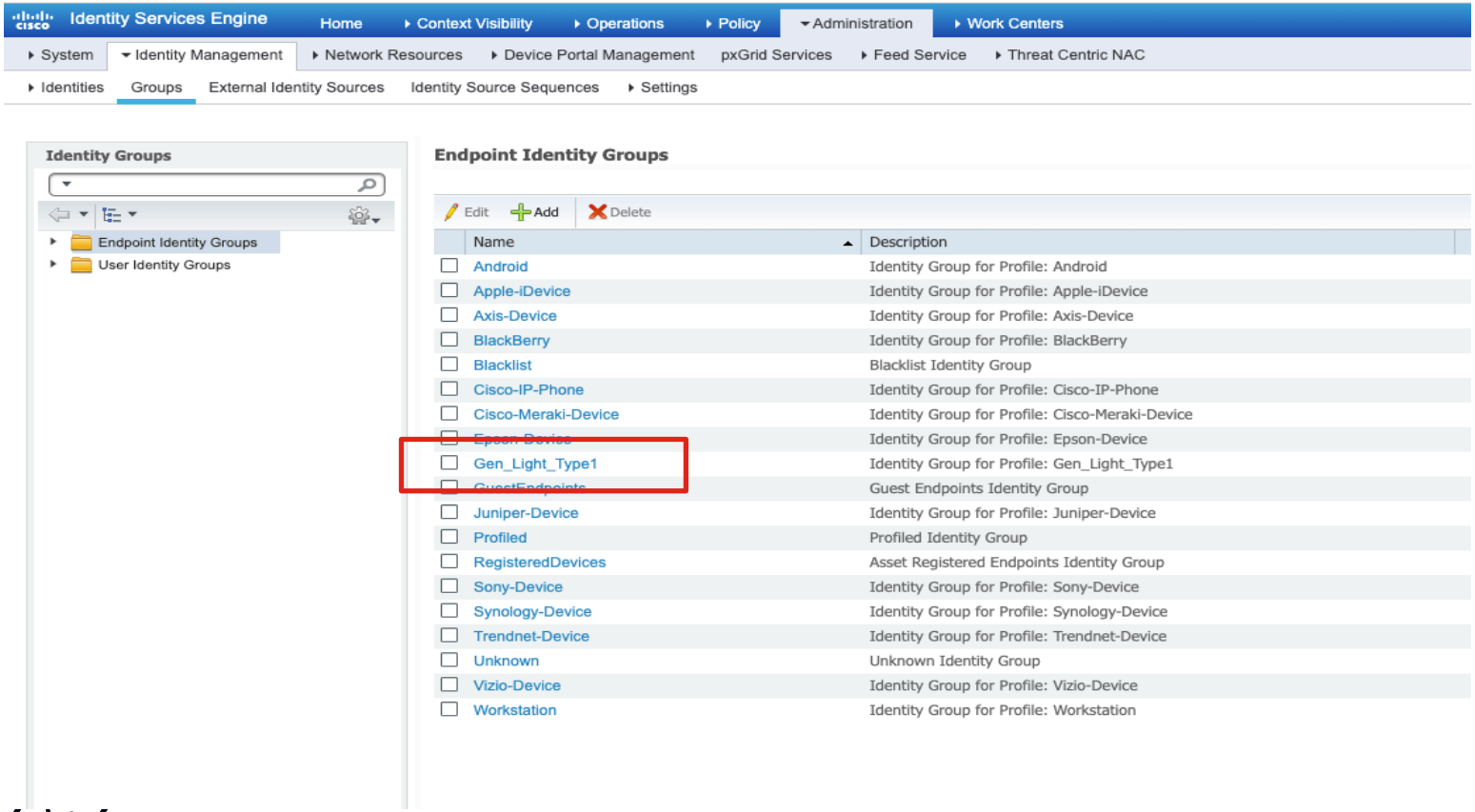
Show wireless client detail

Creating ISE policies

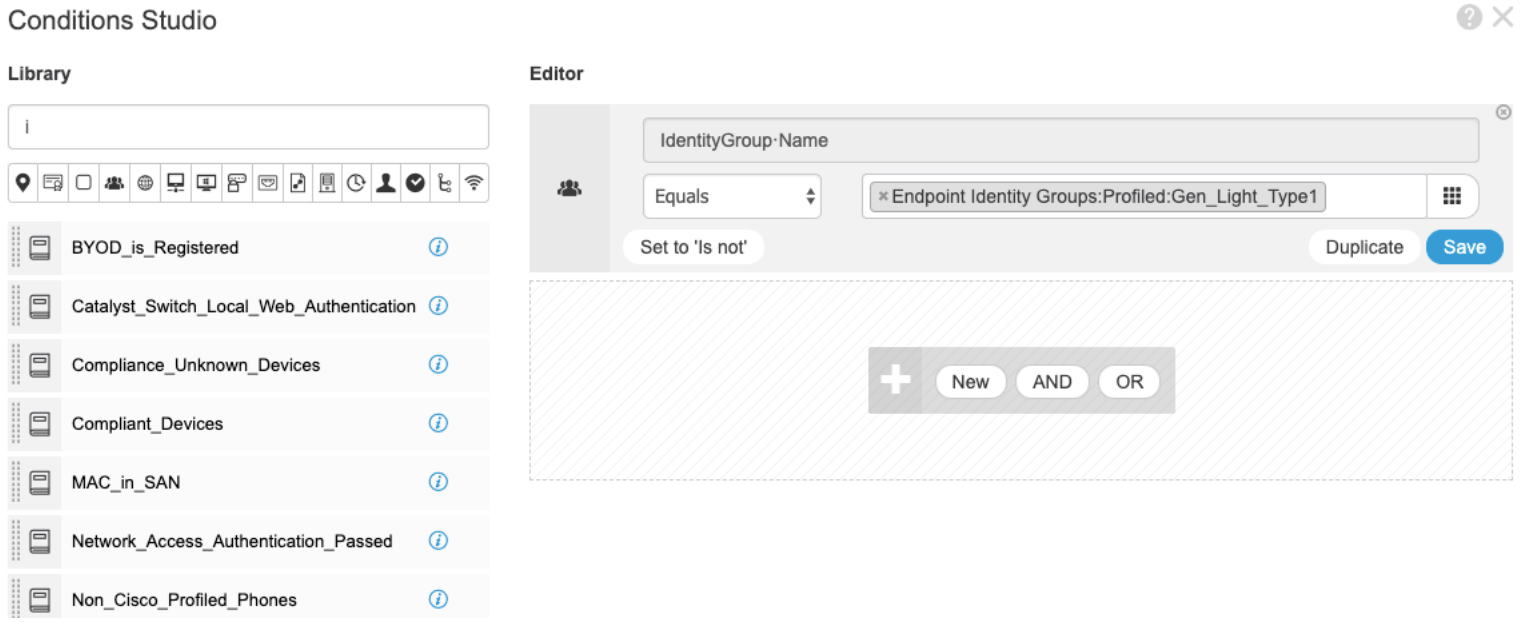
Profiling Policies



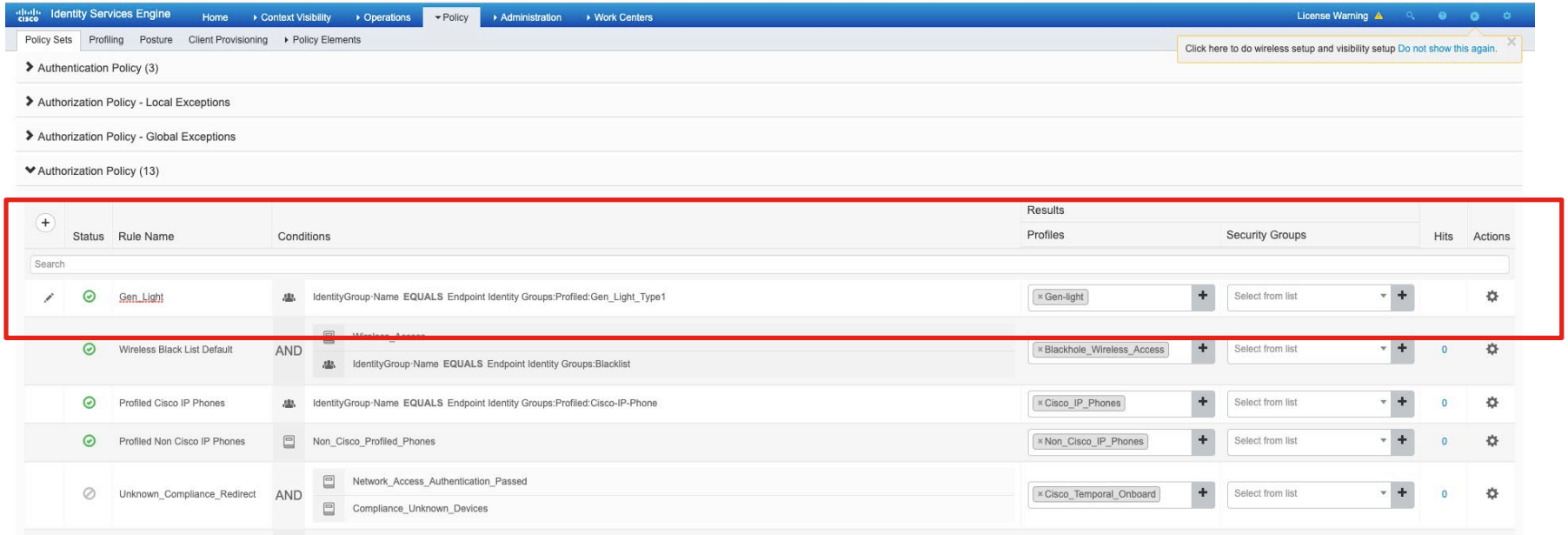
Identity Groups



Authorization Policy



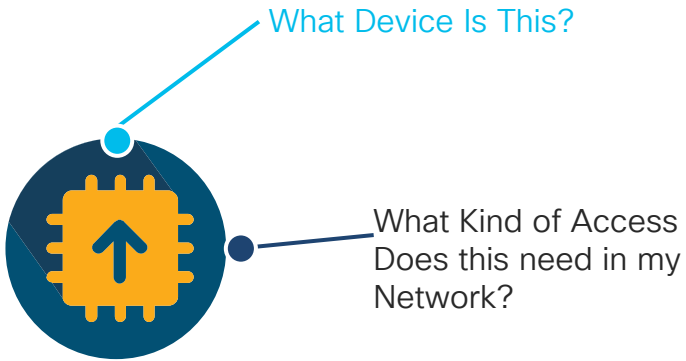
Authorization Result



Creating MUD URL and File

MUD – Manufacturer Usage Descriptions

- MUD enables us to link device classification with a policy.



MUD File explains the policies a device needs.

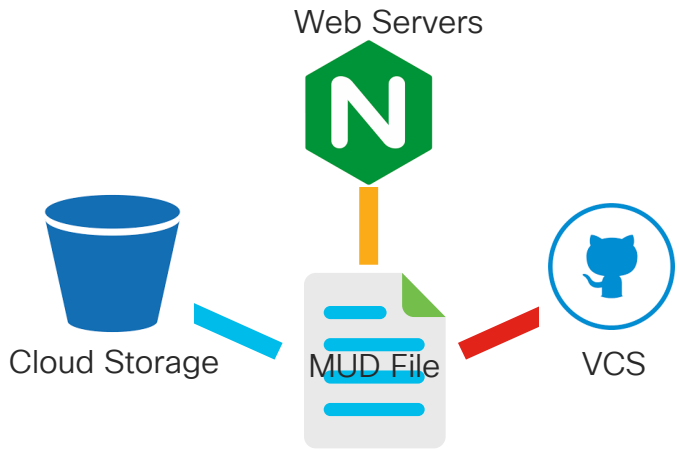
MUD File

MUD URL points to the MUD File.

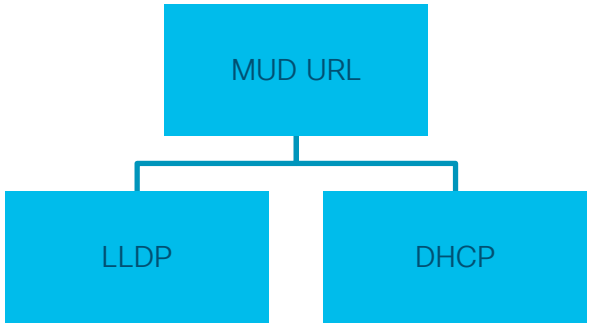
MUD URL

MUD URL

MUD URL can be any file server that can host your MUD File.



Look at Two Methods for Things to emit MUD URL



MUD File

How do I make the MUD file?

Simple Method – Use Hosted Services.

Example:
https://devnetapps.cisco.com/mudmakerui#/create

https://www.mudmaker.org/mudmaker.html

Legendary Method – Create Manually!!

Sample MUD File


```
- {
-   "ietf-mud:mud": {
      "mud-version": 1,
      "mud-url": "https://devnetapps.cisco.com/mudmakerui/1575055156038.json",
      "cache-validity": 48,
      "is-supported": true,
      "systeminfo": "1",
      "mud-signature": "https://devnetapps.cisco.com/mudmakerui/1575055156038.p7s",
-     "from-device-policy": {
-       "access-lists": {
-         "access-list": [
-           {
              "name": "mud-55835-v4fr"
            },
-           {
              "name": "mud-55835-v6fr"
            }
          ]
        }
      },
-     "to-device-policy": {
-       "access-lists": {
-         "access-list": [
-           {
              "name": "mud-55835-v4to"
            },
-           {
              "name": "mud-55835-v6to"
            }
          ]
        }
      }
    },
-   "ietf-access-control-list:access-lists": {
-     "acl": [
-       {
          "name": "mud-55835-v4to",
          "type": "ipv4-acl-type",
-         "aces": {
-           "ace": [
-             {
                "name": "cl0-todev",
-               "matches": {
-                 "ipv4": {
                    "ietf-acldns:src-dnsname": "me.me.com",
                    "protocol": 17
                  }
                },
-               "actions": {
                  "forwarding": "accept"
                }
              },
              null,
-             {
                "name": "myctl0-todev",
-               "matches": {
-                 "ietf-mud:mud": {
-                   "my-controller": [
                      null
                    ]
                  },
-                 "ipv4": {
                    "protocol": 6
                  }
                },
-               "actions": {
                  "forwarding": "accept"
                }
              },
-             {
                "name": "myman0-todev",
-               "matches": {
-                 "ietf-mud:mud": {
-                   "same-manufacturer": [
                      null
                    ]
                  },
-                 "ipv4": {
                    "protocol": 6
                  },
-                 "tcp": {
                    "source-port": {
```



```
- {
-   "ietf-mud:mud": {
      "mud-version": 1,
      "mud-url": "https://devnetapps.cisco.com/mudmakerui/1575055156038.json",
      "cache-validity": 48,
      "is-supported": true,
      "systeminfo": "1",
      "mud-signature": "https://devnetapps.cisco.com/mudmakerui/1575055156038.p7s",
-     "from-device-policy": {
-       "access-lists": {
-         "access-list": [
-           {
              "name": "mud-55835-v4fr"
            },
-           {
              "name": "mud-55835-v6fr"
            }
          ]
        }
      },
-     "to-device-policy": {
-       "access-lists": {
-         "access-list": [
-           {
              "name": "mud-55835-v4to"
            },
-           {
              "name": "mud-55835-v6to"
            }
          ]
        }
      }
    },
-   "ietf-access-control-list:access-lists": {
-     "acl": [
-       {
          "name": "mud-55835-v4to",
          "type": "ipv4-acl-type",
-         "aces": {
```

Simulation and Testing Tools

Simulation Methods

- Explore two methods here
  - DHCP
  - LLDP

- Pre-Requisites
  - ISE
  - IE4000
  - Emulate a thing (either Linux VM or Raspberry Pi)
  - NGINX – Host MUD File.
  - MUD file from either of the URLs below.
  - https://devnetapps.cisco.com/mudmakerui#/create

    or
  - https://www.mudmaker.org/mudmaker.html

    or

    Create Manually. ☺

Using DHCP

Using ISC dhclient

- Update dhclient.conf with following entries.

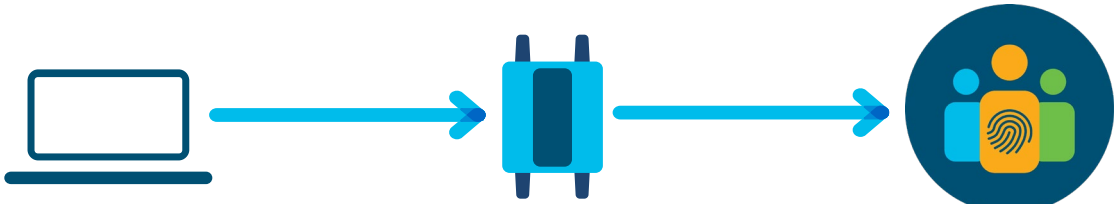
```
# for DHCPv4

option mudurl code 161 = text;
send mudurl "https://makermudurl.com/mudfile.json";


# for DHCPv6

option dhcp6.mudurl code 112 = text;

send mudurl "https://makermudurl.com/mudfile.json";
```

Using dhcpd

- Add following to dhclient.conf

```
mudurl "https://makermudurl.com/mudfile.json"
```

Simulation – Sending MUD URL



Replace the interface name, run following command.

```
dhclient -r <interface name ex: eth0, eno33559296 etc>
```

Using LLDP

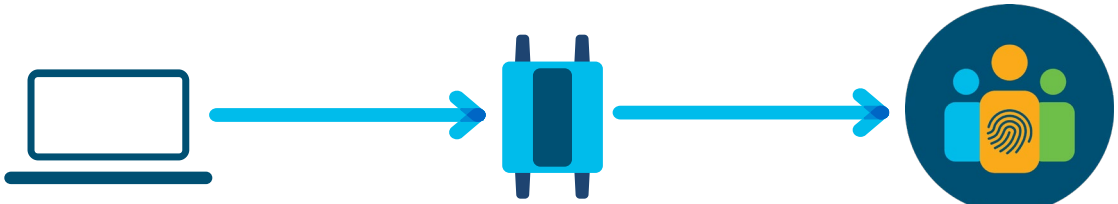
- Install lldpd.
- Enable & Start lldp service.
- Use helper script to generate and send lldp payload.

https://www.mudmaker.org/lldpmud.sh

- Run the following command.

```
sh lldpmud.sh https://makermudurl.com/mudfile.json
```

Simulation – Sending MUD URL



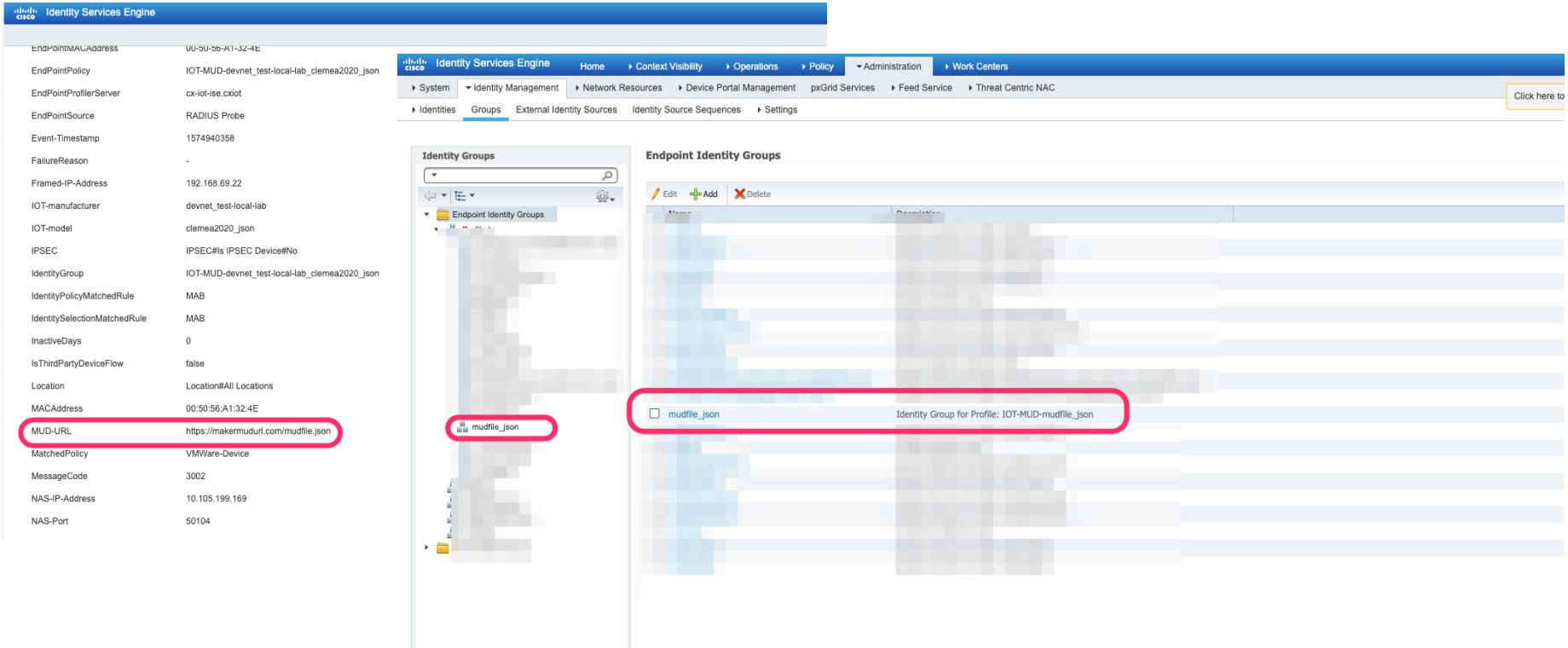
Run the following command

IE4K

ISE

```
sh lldpmud.sh https://makermudurl.com/mudfile.json
```

MUD URL Extracted In ISE



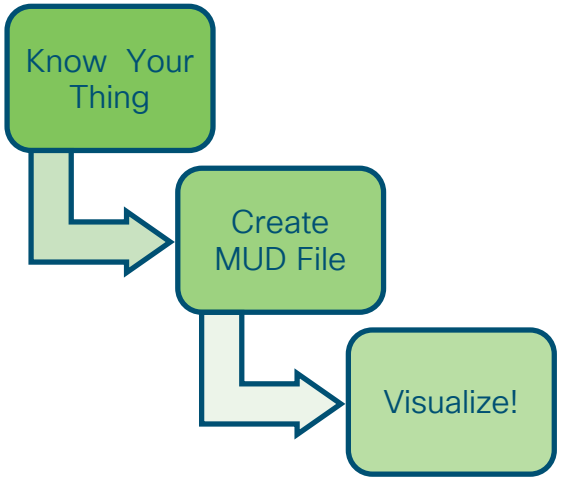
MUD visualizer

MUD Visualizer: What is the need ?

MUD files are complex to read and validate manually

MUD Visualizer

- It's Open-Source
- Shows both Incoming and outgoing traffic
- MUD Visualizer can visualize multiple MUD-files at the same time
- visualize the communications based on how their ACEs match.



Mudmaker.org

References

https://github.com/iot-onboarding/mud-visualizer

https://www.nccoe.nist.gov/sites/default/files/library/sp1800/iot-ddos-nist-sp1800-15-preliminary-draft.pdf

https://developer.cisco.com/site/mud/

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

You make **possible**

Appendices

Commands on Cisco Switches

```
device-sensor filter-list lldp list LLDP_TLV_list
! list of TLV to be filtered if any apart from TLV 127.
! TLV 127 is automatically added.
!
device-sensor filter-spec lldp include list LLDP_TLV_list
! Commands to inform Sanet about inclusion of LLDP TLVs in accounting
access-session attributes filter-list list LLDP_attrs
 lldp
access-session accounting attributes filter-spec include list LLDP_attrs
!
device-sensor notify all-changes
```

You make **possible**