

# MOP

By Don Chen

## Description

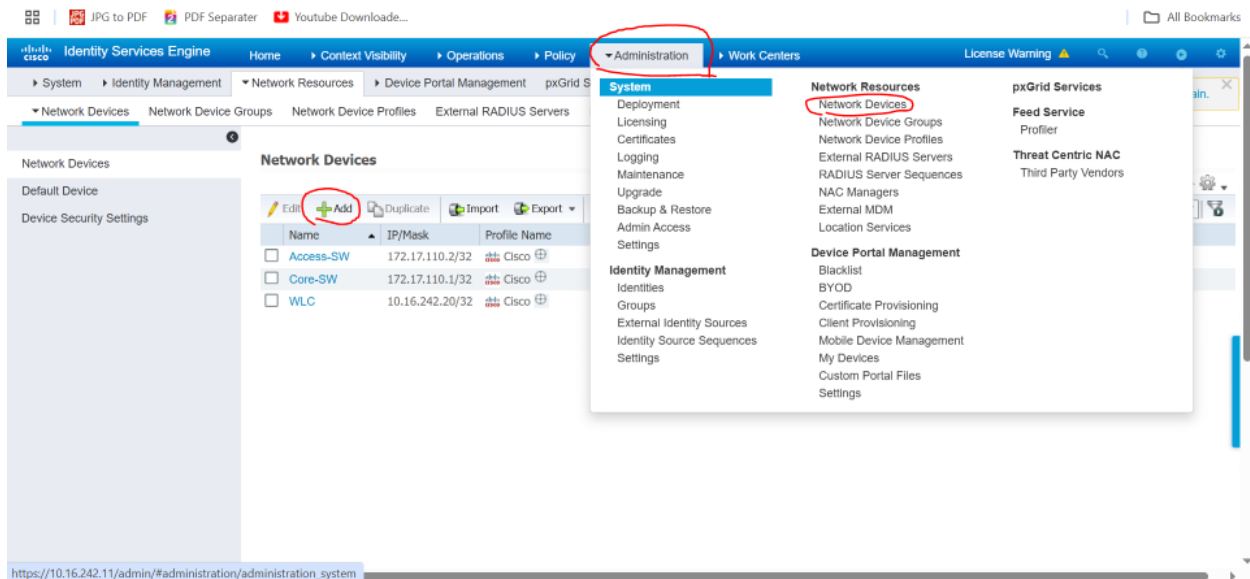
We are onboarding 2 new access switches to our network.

## Prerequisites

- Access and logins to ISE.

## Step-by-Step Instructions

1. Open the CLI of Access\_SW\_02.
2. Use the switch configuration template file included with the MOP, but make sure to replace the "<IP of Switch>" with the appropriate IP. In this case, use "172.16.101.3".
3. Copy and paste that into the switch
4. Go to the ISE GUI by typing 172.16.100.50 while in the browser.
5. Log in.
6. Go to Administration -> Network Devices. Then click Add.



7. Input the information to match the screenshots below. For the next switch, remember that the name and the IP address will be different. Click “Submit” after you matched the screenshots.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. A sub-navigation bar shows System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Center. The main content area is titled "Network Devices" and contains a form for configuring a new device. The form includes fields for Name (Access\_SW\_2), Description, IP Address (172.16.101.3), and Subnet (32). It also has dropdown menus for Device Profile (Cisco), Model Name (Unknown), and Software Version (Unknown). At the bottom, there are sections for Network Device Group, Location (All Locations), IPSEC (Is IPSEC Device), and Device Type (All Device Types), each with a "Set To Default" button.

The screenshot shows the "RADIUS Authentication Settings" page in the Cisco ISE interface. The page is divided into three main sections: RADIUS UDP Settings, RADIUS DTLS Settings, and General Settings. In the RADIUS UDP Settings section, the Protocol is set to RADIUS, the Shared Secret is cisco123, and the CoA Port is 1700. In the RADIUS DTLS Settings section, DTLS Required is unchecked, the Shared Secret is radius/dtls, and the CoA Port is 2083. In the General Settings section, Enable KeyWrap is unchecked, and the Key Input Format is set to ASCII.

**RADIUS Authentication Settings**

**RADIUS UDP Settings**

Protocol: **RADIUS**

\* Shared Secret: cisco123 [Hide]

Use Second Shared Secret: ☐ [i]

[ ] [Show]

CoA Port: 1700 [Set To Default]

**RADIUS DTLS Settings** [i]

DTLS Required: ☐ [i]

Shared Secret: radius/dtls [i]

CoA Port: 2083 [Set To Default]

Issuer CA of ISE Certificates for CoA: Select if required (optional) [i]

DNS Name: [ ]

**General Settings**

Enable KeyWrap: ☐ [i]

\* Key Encryption Key: [ ] [Show]

\* Message Authenticator Code Key: [ ] [Show]

Key Input Format: ☒ ASCII ☐ HEXADECIMAL

☒ ▼ SNMP Settings

\* SNMP Version

\* SNMP RO Community

SNMP Username

Security Level

Auth Protocol

Auth Password

Privacy Protocol

Privacy Password

\* Polling Interval  seconds (Valid Range 600 to 86400 or zero)

Link Trap Query ☒

MAC Trap Query ☒

\* Originating Policy Services Node

- Now repeat for the second switch. Remember, the second switch has a different IP address, so take extra care in steps 2 and 7.

## Verification

- Access privileged exec mode of the access switches.
- Use the command “show aaa servers”. You should see a screenshot similar to one the below.

```
ACCESS-SW1#show aaa servers
RADIUS: id 1, priority 1, host 10.16.242.11, auth-port 1812, acct-port 1813
State: current UP, duration 391s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
        Response: accept 0, reject 0, challenge 0
        Response: unexpected 0, server error 0, incorrect 0, time 0ms
        Transaction: success 0, failure 0
        Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
        Response: accept 0, reject 0, challenge 0
        Response: unexpected 0, server error 0, incorrect 0, time 0ms
        Transaction: success 0, failure 0
        Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
        Request: start 0, interim 0, stop 0
        Response: start 0, interim 0, stop 0
        Response: unexpected 0, server error 0, incorrect 0, time 0ms
        Transaction: success 0, failure 0
        Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 6m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
Requests per minute past 24 hours:
    high - 0 hours, 0 minutes ago: 0
    low  - 0 hours, 0 minutes ago: 0
```

- Access the ISE GUI and log in.

- Navigate to Operations -> Radius -> Live Logs. You should see something similar to the screenshot below. Make sure you find the IP address of the two switches we added.

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint Port	Authentication	Authorization	IP Address	Network Device	Device Port	Identity Group
Dec 26, 2024 04:23:22:723 PM	Success	...	0	9C 62 6C 3C 90 90	9C 62 6C 3C 90 90	ASTON-DO...	Wired == M...	Wired == D...	172.17.101.10	ACCESS-SW1	GigabitEthernet...	ASTON-DOWN
Dec 26, 2024 04:23:22:522 PM	Success	...	0	9C 62 6C 3C 90 90	9C 62 6C 3C 90 90	ASTON-DO...	Default == M...	Default == B...	172.17.101.10	ACCESS-SW1	GigabitEthernet...	ASTON-DOWN
Dec 26, 2024 04:23:22:301 PM	Success	...	0	9C 62 6C 3C 90 90	9C 62 6C 3C 90 90	ASTON-DO...	Default == M...	Default == B...	172.17.101.10	ACCESS-SW1	GigabitEthernet...	ASTON-DOWN
Dec 26, 2024 03:58:57:191 PM	Success	...	0	9C 62 6C 3C 90 90	9C 62 6C 3C 90 90	ASTON-DO...	Default == M...	Default == B...	172.17.101.10	ACCESS-SW1	GigabitEthernet...	ASTON-DOWN
Dec 26, 2024 03:42:31:868 PM	Success	...	0	9C 62 6C 3C 90 90	9C 62 6C 3C 90 90	ASTON-DO...	Default == M...	Default == B...	172.17.101.10	ACCESS-SW1	GigabitEthernet...	ASTON-DOWN
Dec 19, 2024 10:32:56:048 PM	Success	...	0	9C 62 6C 3C 90 90	9C 62 6C 3C 90 90	ASTON-DO...	Default == M...	Default == B...	172.17.101.10	ACCESS-SW1	GigabitEthernet...	ASTON-DOWN
Dec 19, 2024 10:30:00:463 PM	Success	...	0	9C 62 6C 3C 90 90	9C 62 6C 3C 90 90	ASTON-DO...	Default == M...	Default == B...	172.17.101.10	ACCESS-SW1	GigabitEthernet...	ASTON-DOWN

## Rollback Plan

- Factory reset the switches by logging into privileged exec mode, then using “write erase”.
- Access the ISE GUI and Log in.
- Go to Administration -> Network Devices.
- Checkmark the two new switches, then click “Delete”, select “Delete Selected”. This step will look similar to the screenshot below.

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> Access-SW	172.17.110.2/32	Cisco	All Locations	All Device Types	
<input checked="" type="checkbox"/> Access_SW	172.16.101.3/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/> Core-SW	172.17.110.1/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/> WLC	10.16.242.20/32	Cisco	All Locations	All Device Types	