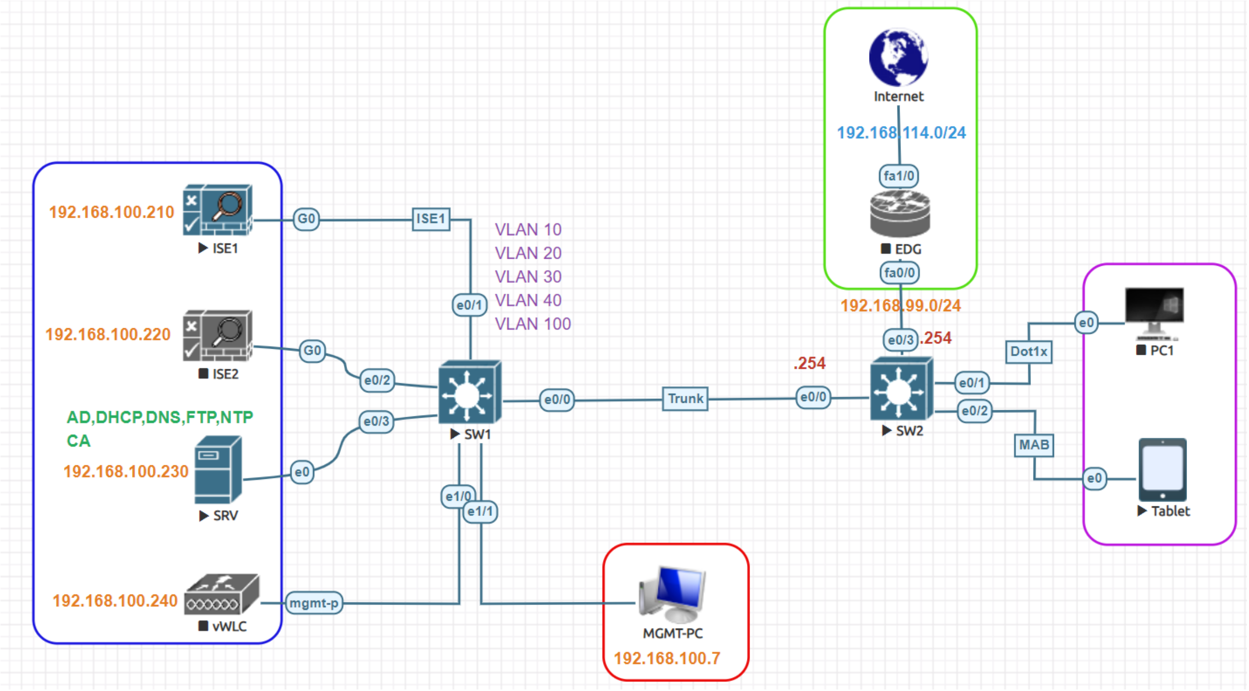
MAB LAB:

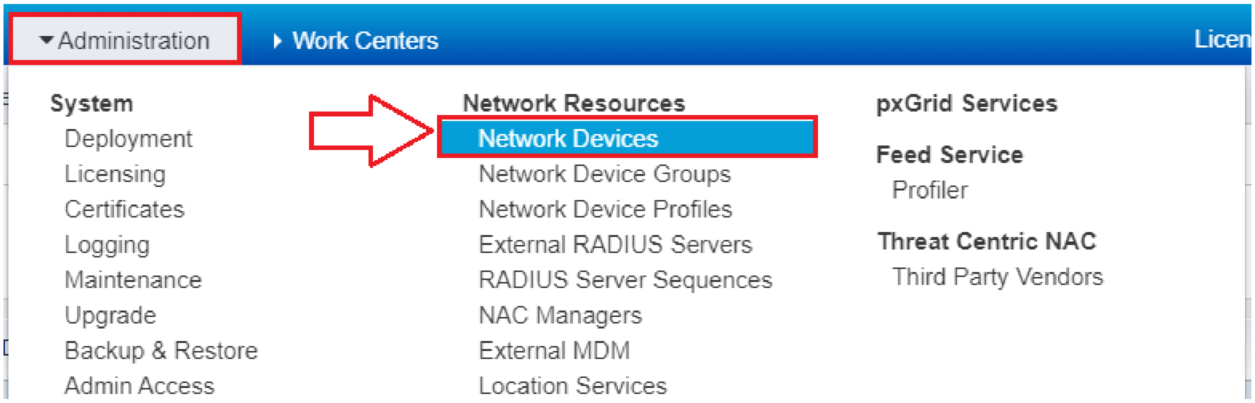


Cisco ISE Primary IP Address	192.168.100.210
Cisco ISE Secondary IP Address	192.168.100.220
AD, DNS and CA Server IP Address	192.168.100.230
Domain Name	test.local
Test User/Group	N/A
Test VLAN	VLAN 20
VLAN Subnet	192.168.20.0/24
VLAN 20 Gateway	192.168.20.1
Authenticator Switch	SW2
Authentication Switch MGMT IP	192.168.100.254
SW2 MAB Interface	Ethernet 0/2
MAB Endpoint	Android 9.1
MAB Endpoint MAC Address	50:01:00:07:00:00

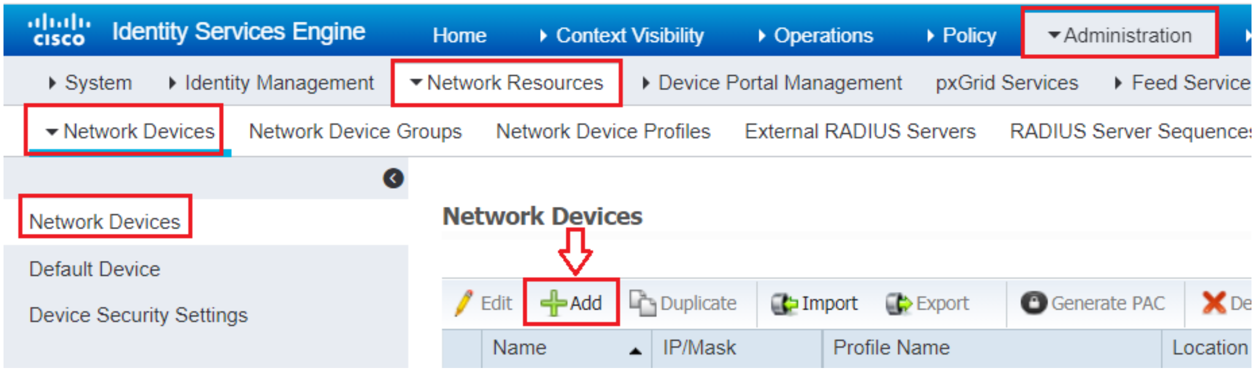
MAB Configuration
SW2(config)#aaa new-model
SW2(config)#dot1x system-auth-control
SW2(config)#radius server ISE1
SW2(config-radius-server)# address ipv4 192.168.100.210 auth-port 1812 acct-port 1813
SW2(config-radius-server)#key Test123
SW2(config-radius-server)#radius server ISE2
SW2(config-radius-server)# address ipv4 192.168.100.220 auth-port 1812 acct-port 1813
SW2(config-radius-server)#key Test123
SW2(config-radius-server)#radius-server attribute 6 on-for-login-auth
SW2(config)#radius-server attribute 8 include-in-access-req
SW2(config)#radius-server attribute 25 access-request include
SW2(config)#radius-server vsa send accounting
SW2(config)#radius-server vsa send authentication
SW2(config)#radius-server dead-criteria time 30 tries 3
SW2(config)#radius-server timeout 2
SW2(config)#aaa group server radius ISE-GROUP
SW2(config-sg-radius)#server name ISE1
SW2(config-sg-radius)#server name ISE2
SW2(config-sg-radius)#ip radius source-interface Vlan100
SW2(config-sg-radius)#aaa authentication dot1x default group ISE-GROUP
SW2(config)#aaa authorization network default group ISE-GROUP
SW2(config)#aaa accounting update periodic 5
SW2(config)#aaa accounting dot1x default start-stop group ISE-GROUP
SW2(config)#aaa server radius dynamic-author
SW2(config-locsvr-da-radius)#client 192.168.100.210 server-key Test123
SW2(config-locsvr-da-radius)#client 192.168.100.220 server-key Test123
SW2(config-locsvr-da-radius)#snmp-server community Test123 RO
SW2(config)#interface Ethernet0/2
SW2(config-if)#description Android Tablet
SW2(config-if)#switchport access vlan 20
SW2(config-if)#switchport mode access
SW2(config-if)#authentication host-mode multi-auth
SW2(config-if)#authentication open
SW2(config-if)#authentication port-control auto
SW2(config-if)#mab
SW2(config-if)#dot1x pae authenticator
SW2(config-if)#dot1x timeout tx-period 10
SW2(config-if)#spanning-tree portfast edge
SW2(config-if)#authentication event fail action next-method
SW2(config-if)#authentication order dot1x mab

Add Network Device:

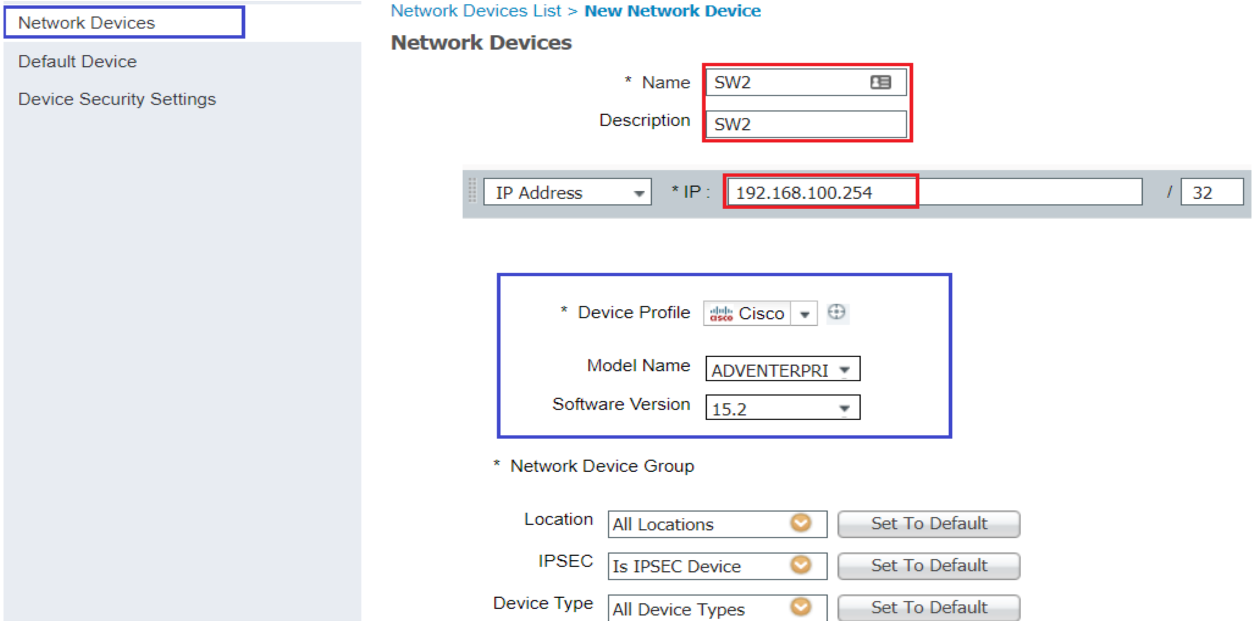
Go to Administration > Network Resources > Network Devices to add the Device (SW2).



Click on Add button to add Network Device like Router and Switch.

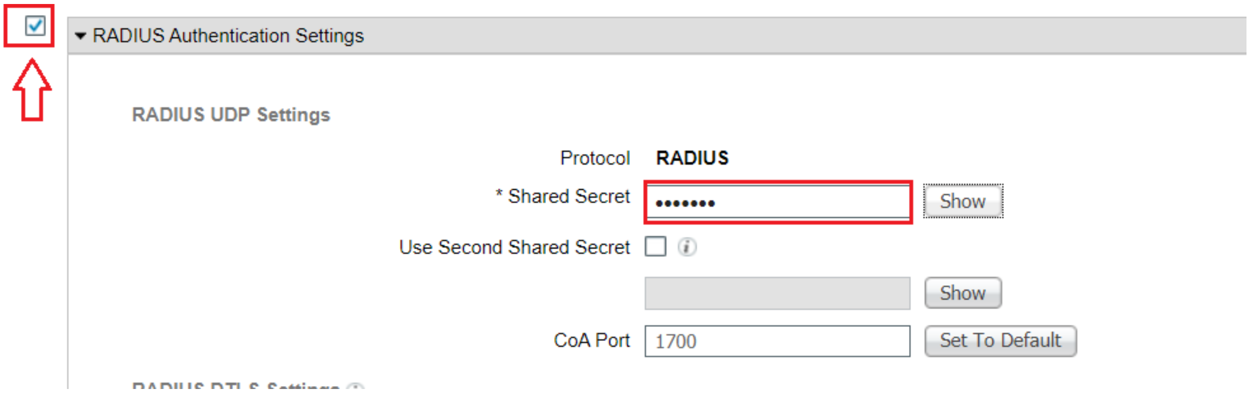


Configure **Name** of device, **IP address** configured. Scroll down to set Authentication settings.



* Name	SW2
Description	SW2
IP Address	* IP : 192.168.100.254 / 32
* Device Profile	Cisco
Model Name	ADVENTERPRI
Software Version	15.2
* Network Device Group	
Location	All Locations
IPSEC	Is IPSEC Device
Device Type	All Device Types

Scroll down to set Authentication settings. Set Password configured as Server key on Switch device “Test123” and save settings.



☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

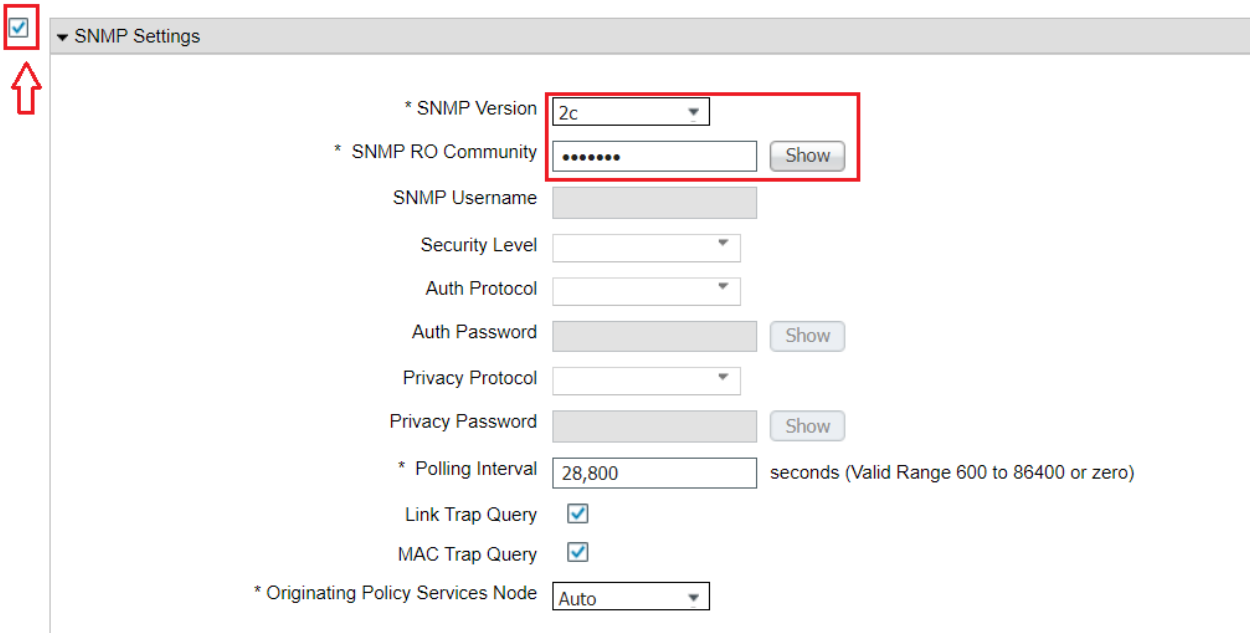
* Shared Secret ••••••• Show

Use Second Shared Secret □

Show

CoA Port 1700 Set To Default

Scroll down to check SNMP Settings and set SNMP RO Community string settings, Click Submit.



☑ SNMP Settings

* SNMP Version 2c

* SNMP RO Community ••••••• Show

SNMP Username

Security Level

Auth Protocol

Auth Password Show

Privacy Protocol

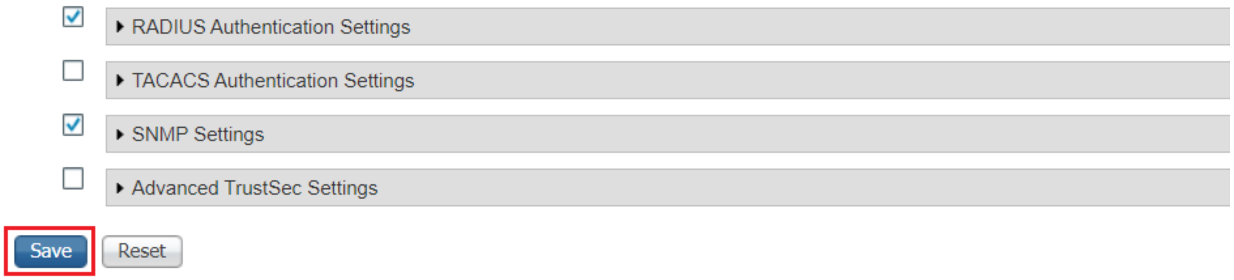
Privacy Password Show

* Polling Interval 28,800 seconds (Valid Range 600 to 86400 or zero)

Link Trap Query ☑

MAC Trap Query ☑

* Originating Policy Services Node Auto



☑ RADIUS Authentication Settings

□ TACACS Authentication Settings

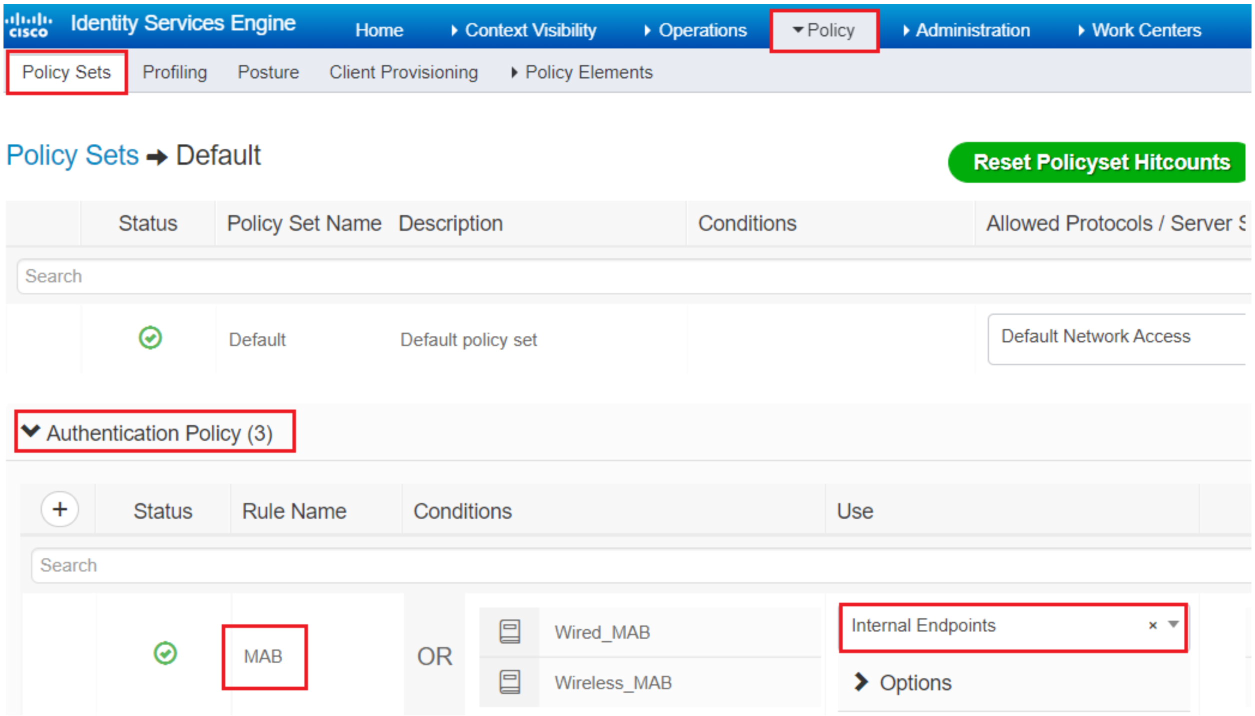
☑ SNMP Settings

□ Advanced TrustSec Settings

Save Reset

MAB Authentication Polices:

choose Work Centers > Network Access > Policy Sets>Authentication Policy. Use the default MAB Authentication Policy which check Internal endpoints MAC address.



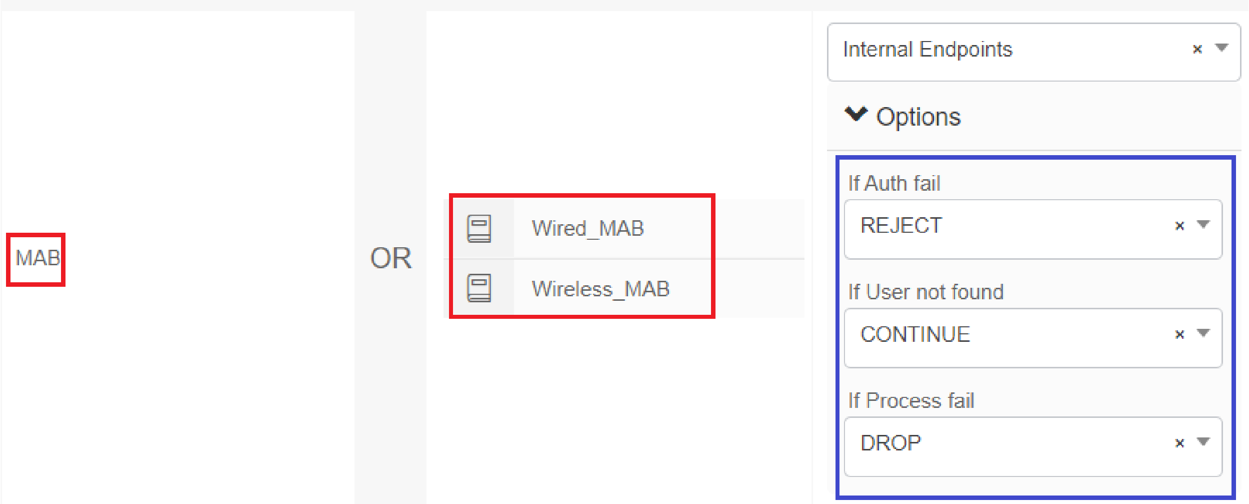
Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S
✓	Default	Default policy set		Default Network Access

Authentication Policy (3)

Status	Rule Name	Conditions	Use
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints Options

If the authentication fail the Device will be Rejected, if user not found the user will be rejected, while if the process fail the Device will be dropped.



MAB

OR Wired_MAB, Wireless_MAB

Internal Endpoints

Options

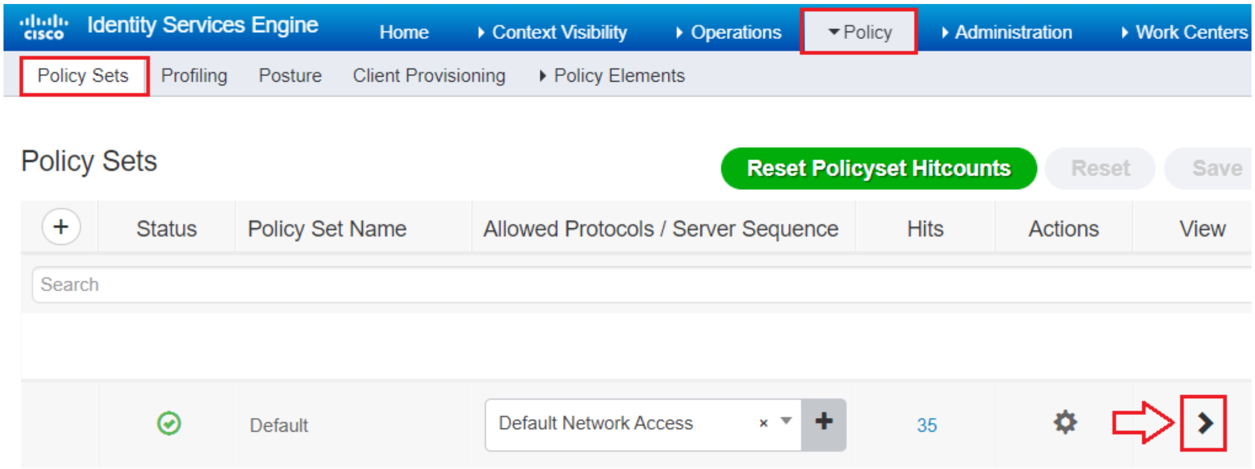
If Auth fail: REJECT

If User not found: CONTINUE

If Process fail: DROP

MAB Authorization Polices:

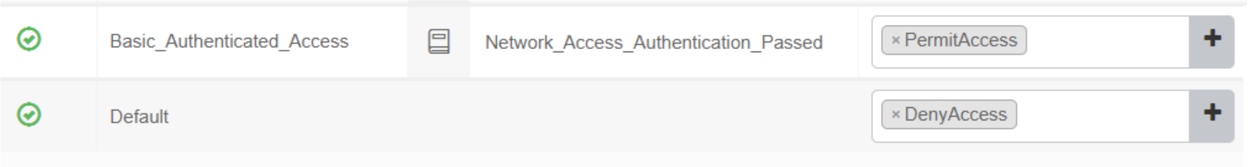
Navigate to Policy>Policy Sets > click on Arrow Icon >



Policy Sets

+	Status	Policy Set Name	Allowed Protocols / Server Sequence	Hits	Actions	View
	Search					
	✓	Default	Default Network Access	35	⚙	>

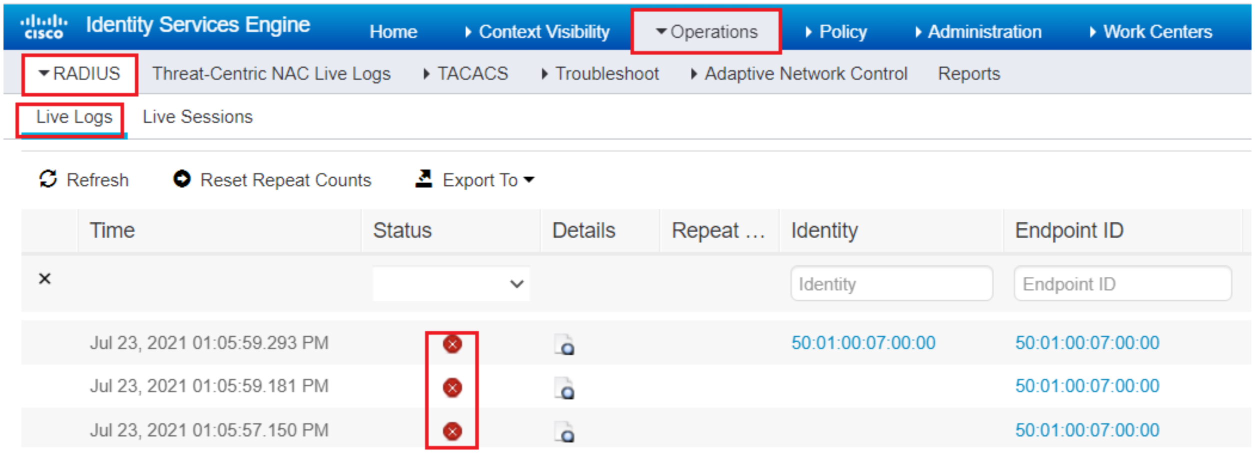
Navigate to Authorization Policy section, there is default and Basic_Authenticated_Access rules already it will use these default Authorization Policy to permit access.



✓	Basic_Authenticated_Access	▤	Network_Access_Authentication_Passed	× PermitAccess
✓	Default			× DenyAccess

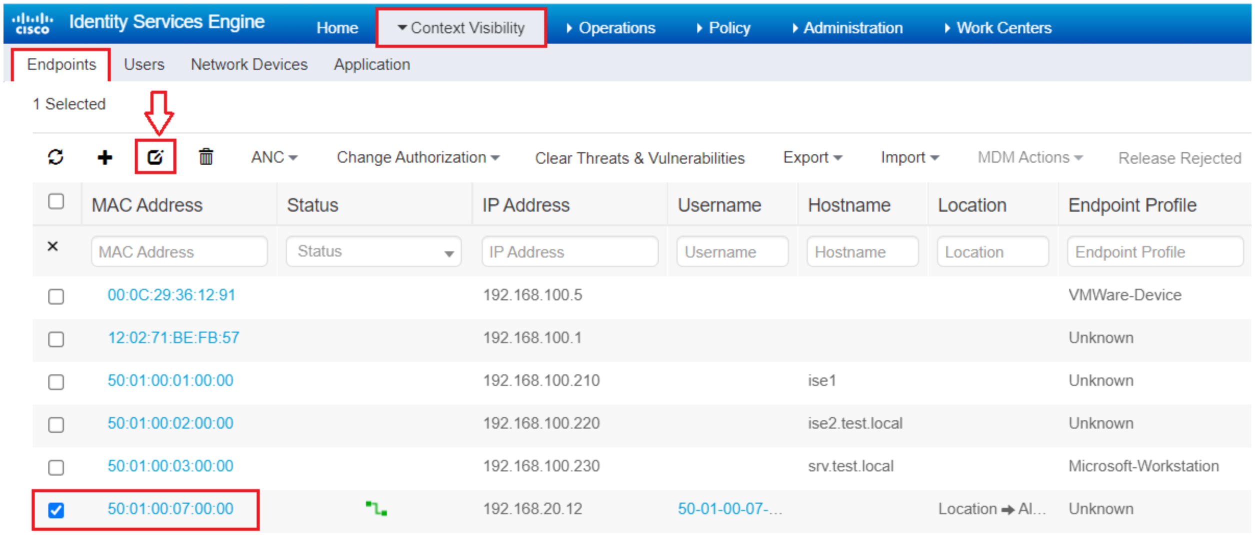
MAB Device Authentication:

Boot Android Device. Navigate to ISE Operations>RADIUS>Live Logs. You will notice that authentication is failed because Android MAC address is not found in Internal database.



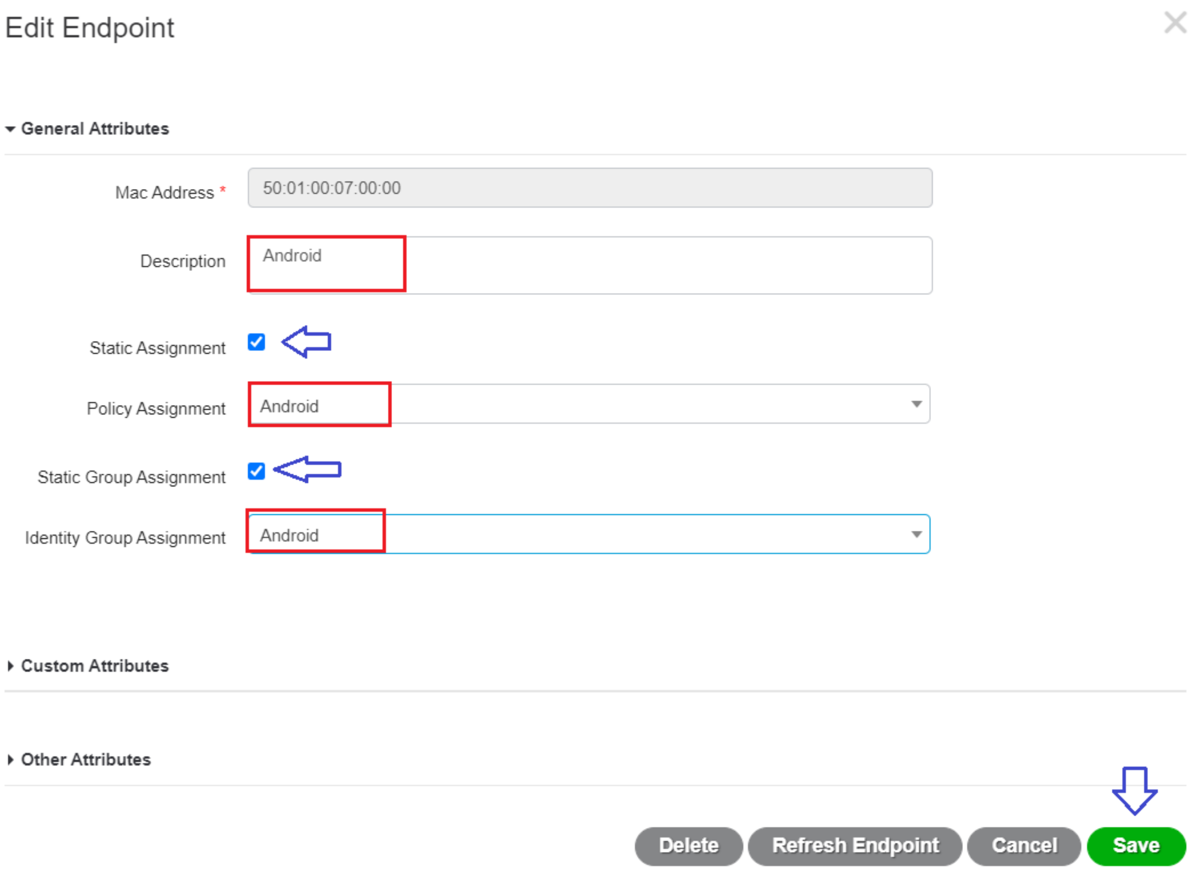
Time	Status	Details	Repeat ...	Identity	Endpoint ID
×				Identity	Endpoint ID
Jul 23, 2021 01:05:59.293 PM	☒	🔍		50:01:00:07:00:00	50:01:00:07:00:00
Jul 23, 2021 01:05:59.181 PM	☒	🔍			50:01:00:07:00:00
Jul 23, 2021 01:05:57.150 PM	☒	🔍			50:01:00:07:00:00

Navigate to ISE Context Visibility>Endpoints. Select Android rejected device, and click edit.



☐	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile
×	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile
☐	00:0C:29:36:12:91		192.168.100.5				VMWare-Device
☐	12:02:71:BE:FB:57		192.168.100.1				Unknown
☐	50:01:00:01:00:00		192.168.100.210		ise1		Unknown
☐	50:01:00:02:00:00		192.168.100.220		ise2.test.local		Unknown
☐	50:01:00:03:00:00		192.168.100.230		srv.test.local		Microsoft-Workstation
☑	50:01:00:07:00:00		192.168.20.12	50-01-00-07-...		Location ➔ Al...	Unknown

Description: Android, Static assignment: Android, Static group assignment: Android, Click Save



Edit Endpoint

General Attributes

Mac Address * 50:01:00:07:00:00

Description Android

Static Assignment ☑

Policy Assignment Android

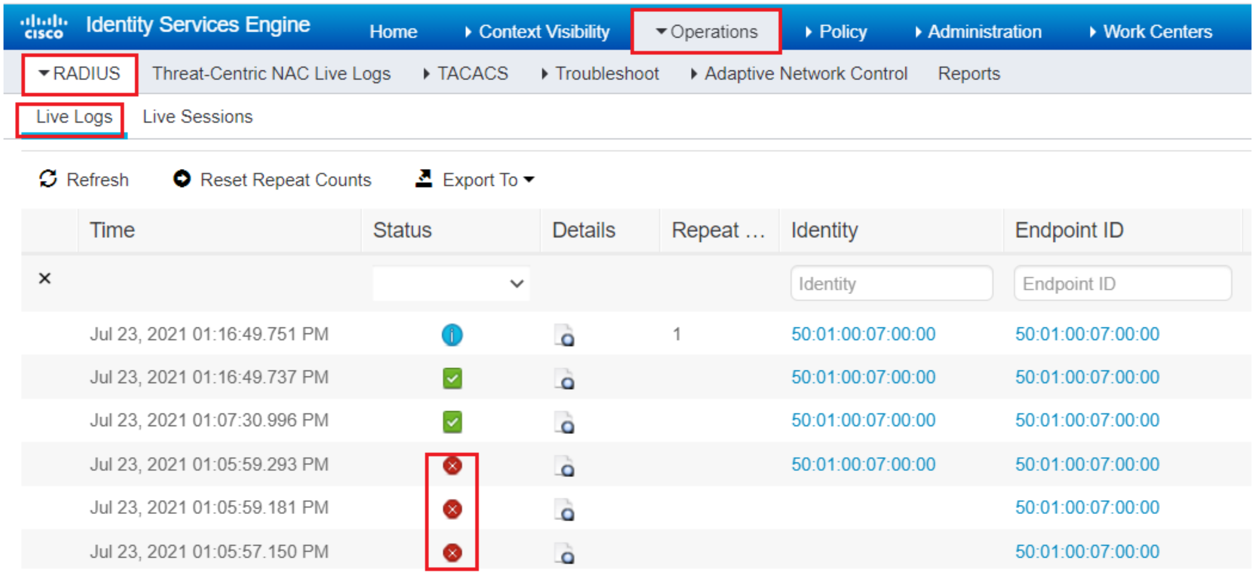
Static Group Assignment ☑

Identity Group Assignment Android

Custom Attributes

Other Attributes

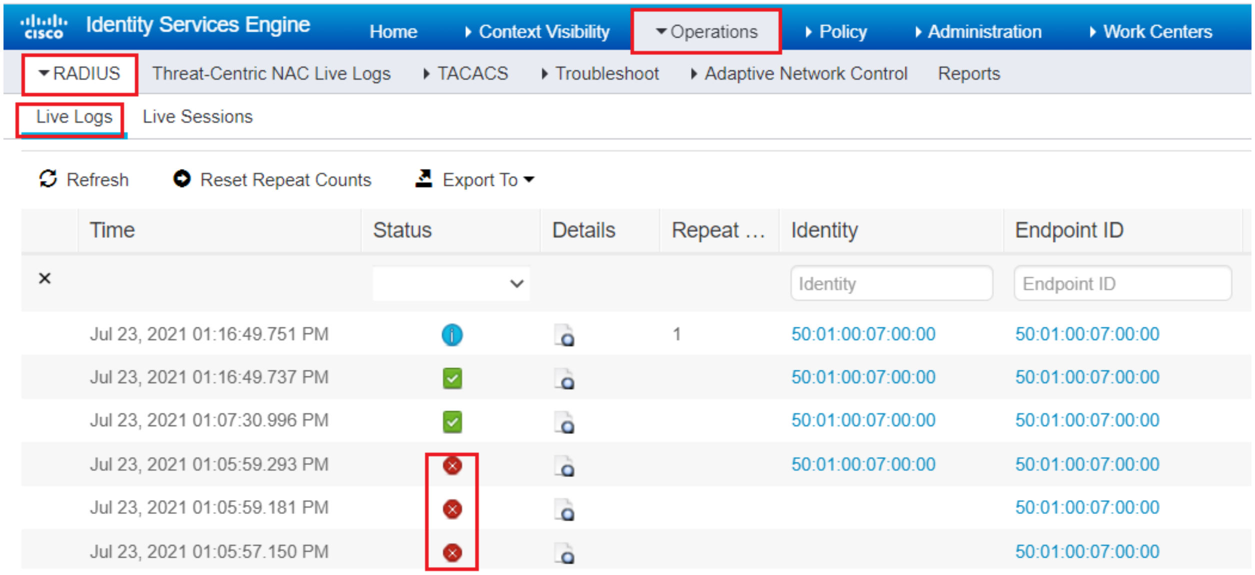
Navigate to ISE management Operations>Live Logs again. Now you will see that Android device is authenticated because this time the MAC address is now in Internal Endpoint database.



Time	Status	Details	Repeat …	Identity	Endpoint ID
Jul 23, 2021 01:16:49.751 PM	ℹ		1	50:01:00:07:00:00	50:01:00:07:00:00
Jul 23, 2021 01:16:49.737 PM	✓			50:01:00:07:00:00	50:01:00:07:00:00
Jul 23, 2021 01:07:30.996 PM	✓			50:01:00:07:00:00	50:01:00:07:00:00
Jul 23, 2021 01:05:59.293 PM	✗			50:01:00:07:00:00	50:01:00:07:00:00
Jul 23, 2021 01:05:59.181 PM	✗				50:01:00:07:00:00
Jul 23, 2021 01:05:57.150 PM	✗				50:01:00:07:00:00

Verification:

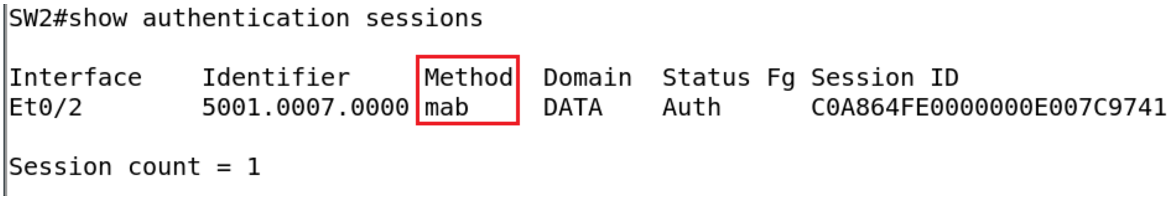
Navigate to Operations > RADIUS Livelog.



Time	Status	Details	Repeat …	Identity	Endpoint ID
Jul 23, 2021 01:16:49.751 PM	ℹ		1	50:01:00:07:00:00	50:01:00:07:00:00
Jul 23, 2021 01:16:49.737 PM	✓			50:01:00:07:00:00	50:01:00:07:00:00
Jul 23, 2021 01:07:30.996 PM	✓			50:01:00:07:00:00	50:01:00:07:00:00
Jul 23, 2021 01:05:59.293 PM	✗			50:01:00:07:00:00	50:01:00:07:00:00
Jul 23, 2021 01:05:59.181 PM	✗				50:01:00:07:00:00
Jul 23, 2021 01:05:57.150 PM	✗				50:01:00:07:00:00

Verification Commands on Cisco Switch

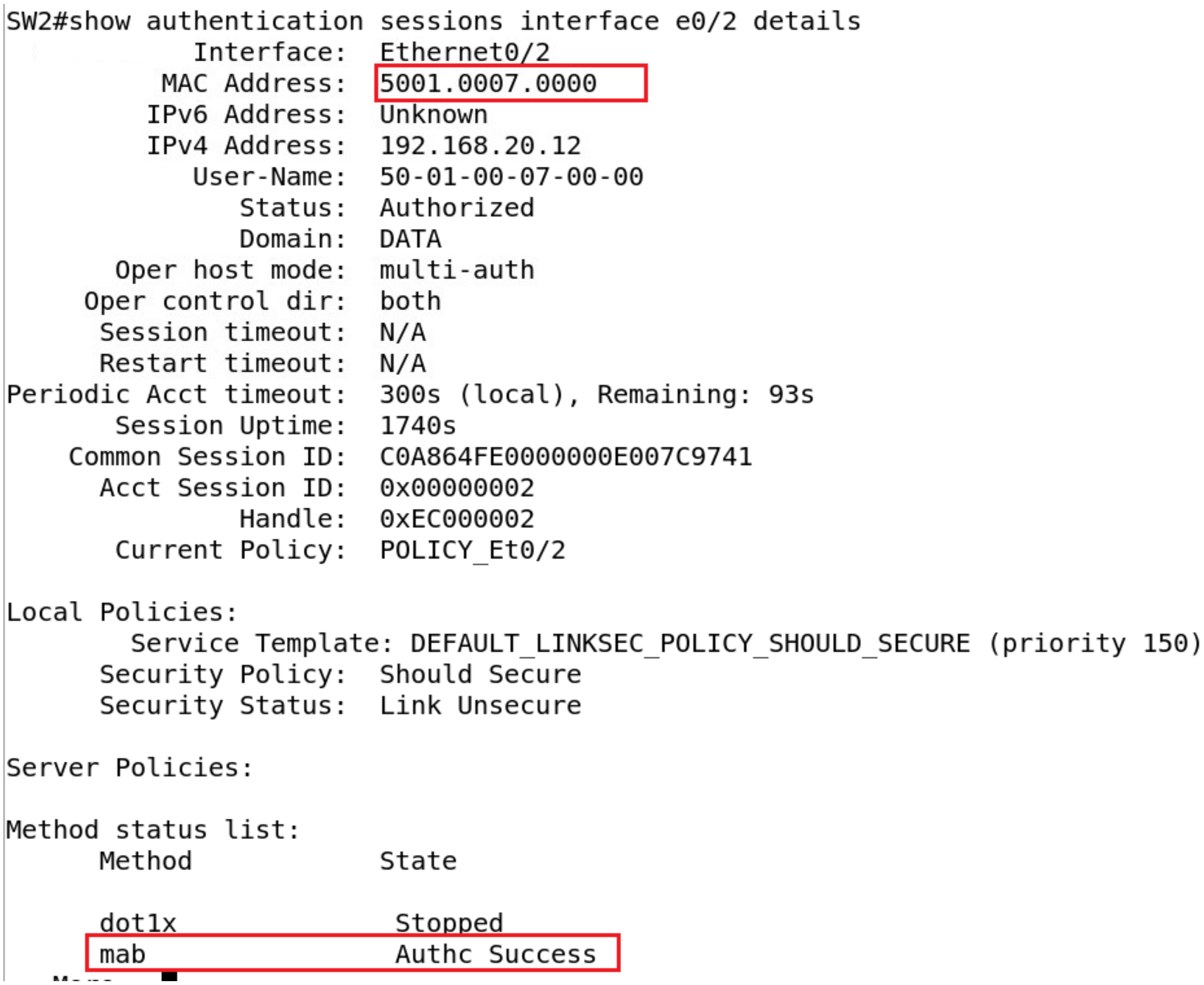
SW2# show mab all
SW2# debug radius authentication
SW2# Show authentication sessions
SW2# Show authentication sessions interface ethernet 0/2
SW2# Show authentication sessions interface ethernet 0/2 details



```
SW2#show authentication sessions

Interface    Identifier     Method  Domain  Status Fg Session ID
Et0/2        5001.0007.0000 mab     DATA    Auth      C0A864FE0000000E007C9741

Session count = 1
```



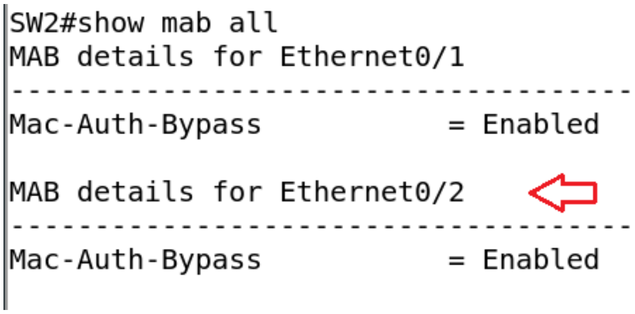
```
SW2#show authentication sessions interface e0/2 details
            Interface:  Ethernet0/2
          MAC Address:  5001.0007.0000
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.20.12
            User-Name:  50-01-00-07-00-00
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  300s (local), Remaining: 93s
       Session Uptime:  1740s
    Common Session ID:  C0A864FE0000000E007C9741
      Acct Session ID:  0x00000002
               Handle:  0xEC000002
       Current Policy:  POLICY_Et0/2

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure
      Security Status:  Link Unsecure

Server Policies:

Method status list:
      Method            State

      dot1x              Stopped
      mab                Authc Success
```



```
SW2#show mab all
MAB details for Ethernet0/1
-------------------------------------
Mac-Auth-Bypass           = Enabled

MAB details for Ethernet0/2
-------------------------------------
Mac-Auth-Bypass           = Enabled
```