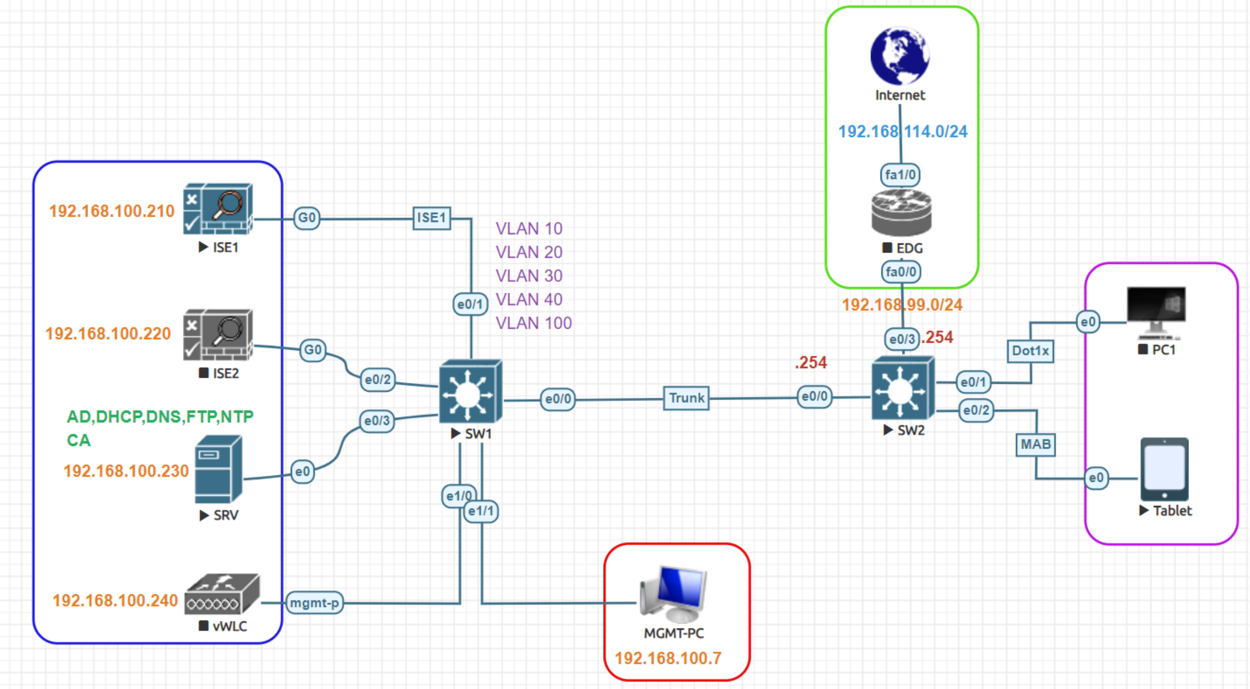
Profile Lab:

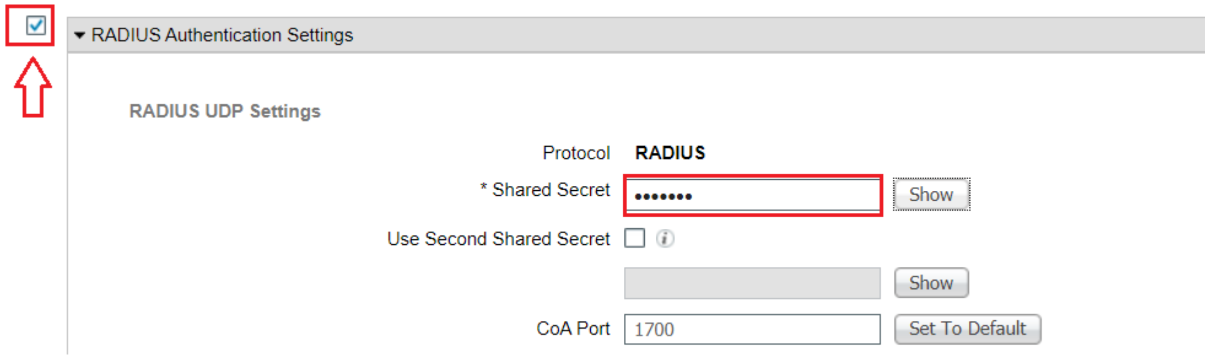


Cisco ISE Primary IP Address	192.168.100.210
Cisco ISE Secondary IP Address	192.168.100.220
AD, DNS and CA Server IP Address	192.168.100.230
Domain Name:	test.local
Test User/Group	E1/Employee
Test VLAN	VLAN 20
VLAN Subnet	192.168.20.0/24
VLAN 20 Gateway	192.168.20.1
Authenticator Switch	SW2
Authentication Switch MGMT IP	192.168.100.254
SW2 Dot1x Interface	Ethernet 0/1
SW2 MAB Interface	Ethernet 0/2
Profile Device	PC1
Profile Device	Tablet

Dot1X 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 Ethernet0/1
SW2(config-if)#description win10 node
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 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

RADIUS Probe:

For RADIUS Probe, RADIUS Authentication Settings has to be enables Navigate to Administration > Network Resources > Network Devices to add the New Device.



☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

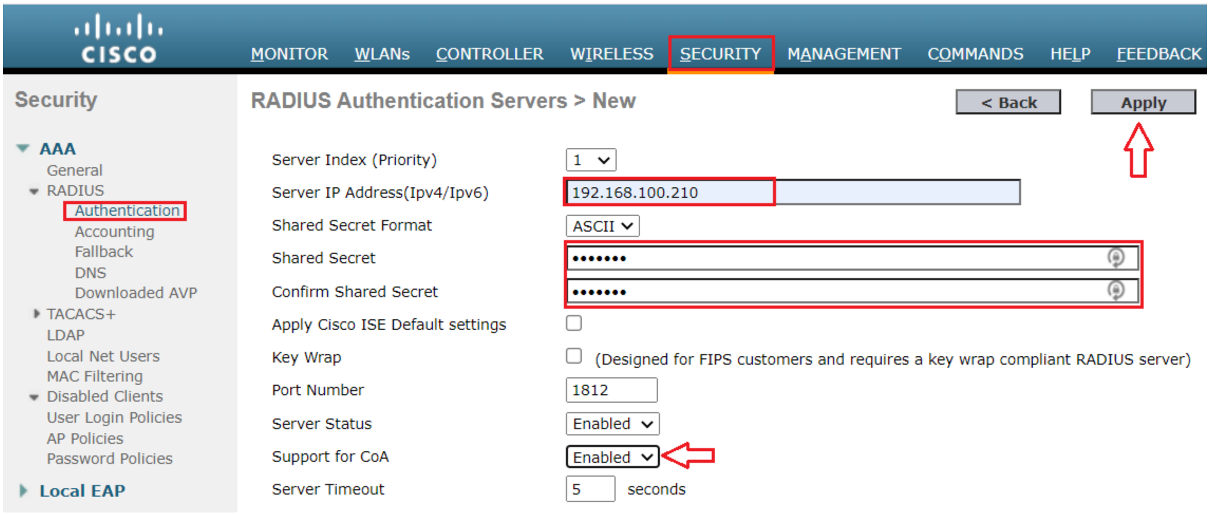
* Shared Secret ••••••• Show

Use Second Shared Secret □

Show

CoA Port 1700 Set To Default

From WLC GUI, click Security. From the menu on the left, click RADIUS > Authentication. The RADIUS Authentication servers page appears. To add a new RADIUS Server, click New.



RADIUS Authentication Servers > New

Server Index (Priority) 1

Server IP Address(Ipv4/Ipv6) 192.168.100.210

Shared Secret Format ASCII

Shared Secret •••••••

Confirm Shared Secret •••••••

Apply Cisco ISE Default settings □

Key Wrap □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

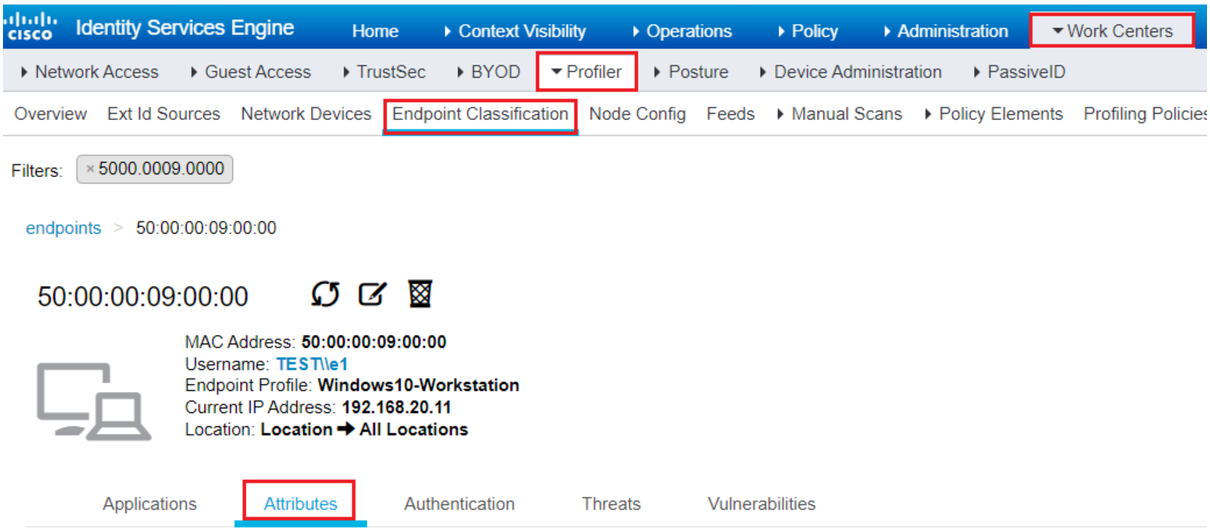
Port Number 1812

Server Status Enabled

Support for CoA Enabled

Server Timeout 5 seconds

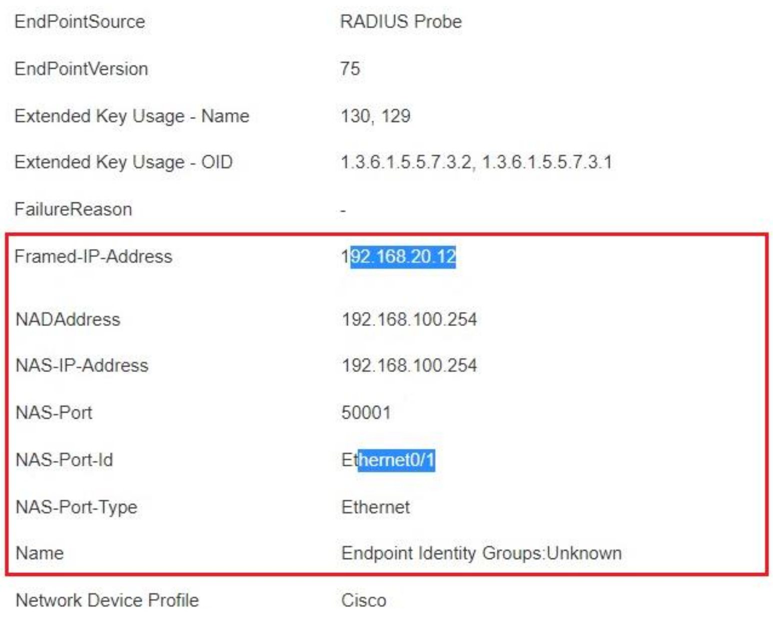
Looking at one of profiled hosts Work Centers>Profiler> Endpoint Classification> Endpoints, see the attributes that were collected:



Filters: × 5000.0009.0000

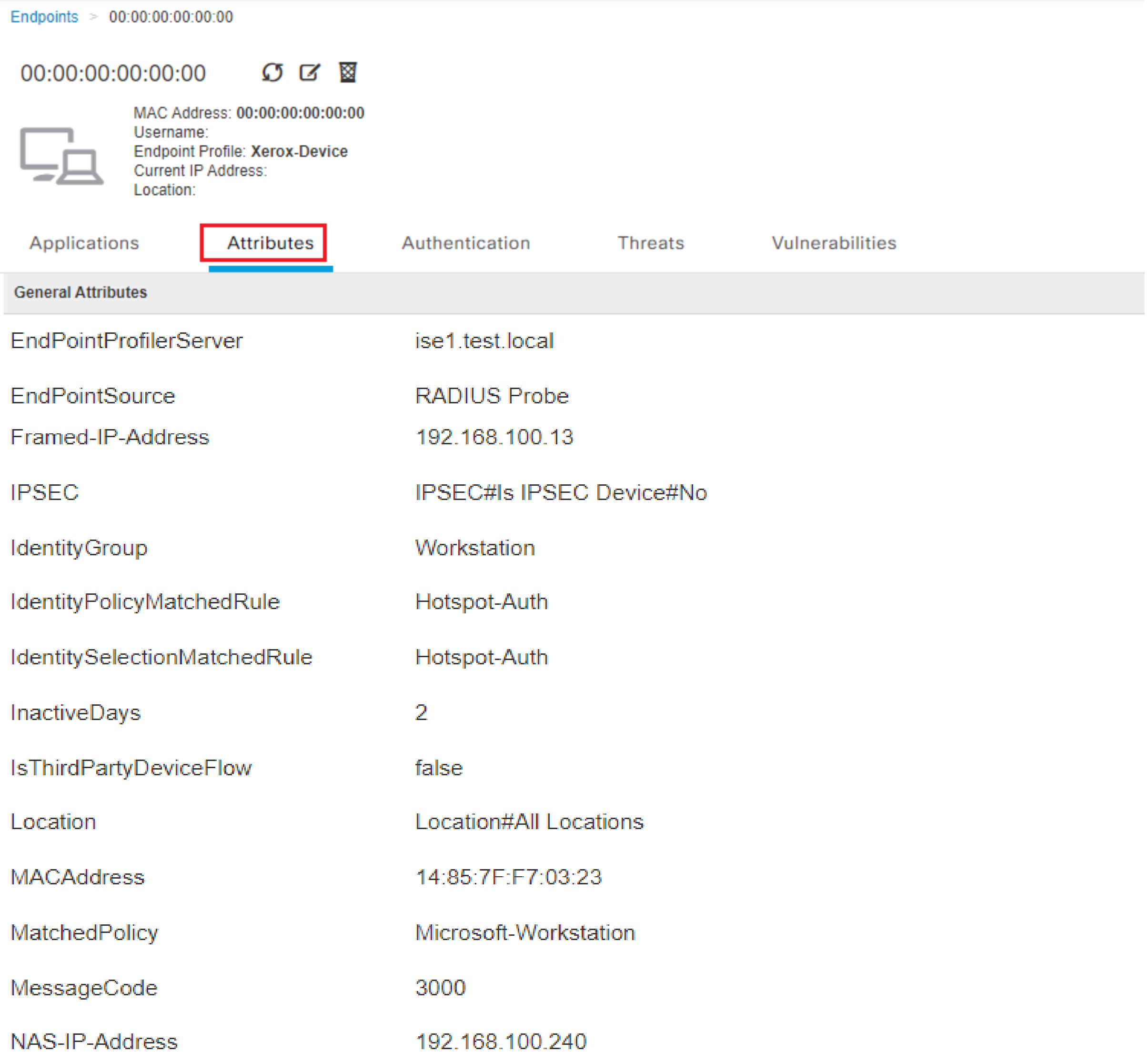
50:00:00:09:00:00

MAC Address: **50:00:00:09:00:00**
Username: **TEST\\e1**
Endpoint Profile: **Windows10-Workstation**
Current IP Address: **192.168.20.11**
Location: **Location ➔ All Locations**



EndPointSource	RADIUS Probe
EndPointVersion	75
Extended Key Usage - Name	130, 129
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1
FailureReason	-
Framed-IP-Address	192.168.20.12
NADAddress	192.168.100.254
NAS-IP-Address	192.168.100.254
NAS-Port	50001
NAS-Port-Id	Ethernet0/1
NAS-Port-Type	Ethernet
Name	Endpoint Identity Groups:Unknown
Network Device Profile	Cisco

Or Navigate to Context Visibility > Endpoints choose the endpoint to see the attributes.



Endpoints > 00:00:00:00:00:00

00:00:00:00:00:00

MAC Address: **00:00:00:00:00:00**
Username:
Endpoint Profile: **Xerox-Device**
Current IP Address:
Location:

General Attributes

EndPointProfilerServer	ise1.test.local
EndPointSource	RADIUS Probe
Framed-IP-Address	192.168.100.13
IPSEC	IPSEC#Is IPSEC Device#No
IdentityGroup	Workstation
IdentityPolicyMatchedRule	Hotspot-Auth
IdentitySelectionMatchedRule	Hotspot-Auth
InactiveDays	2
IsThirdPartyDeviceFlow	false
Location	Location#All Locations
MACAddress	14:85:7F:F7:03:23
MatchedPolicy	Microsoft-Workstation
MessageCode	3000
NAS-IP-Address	192.168.100.240