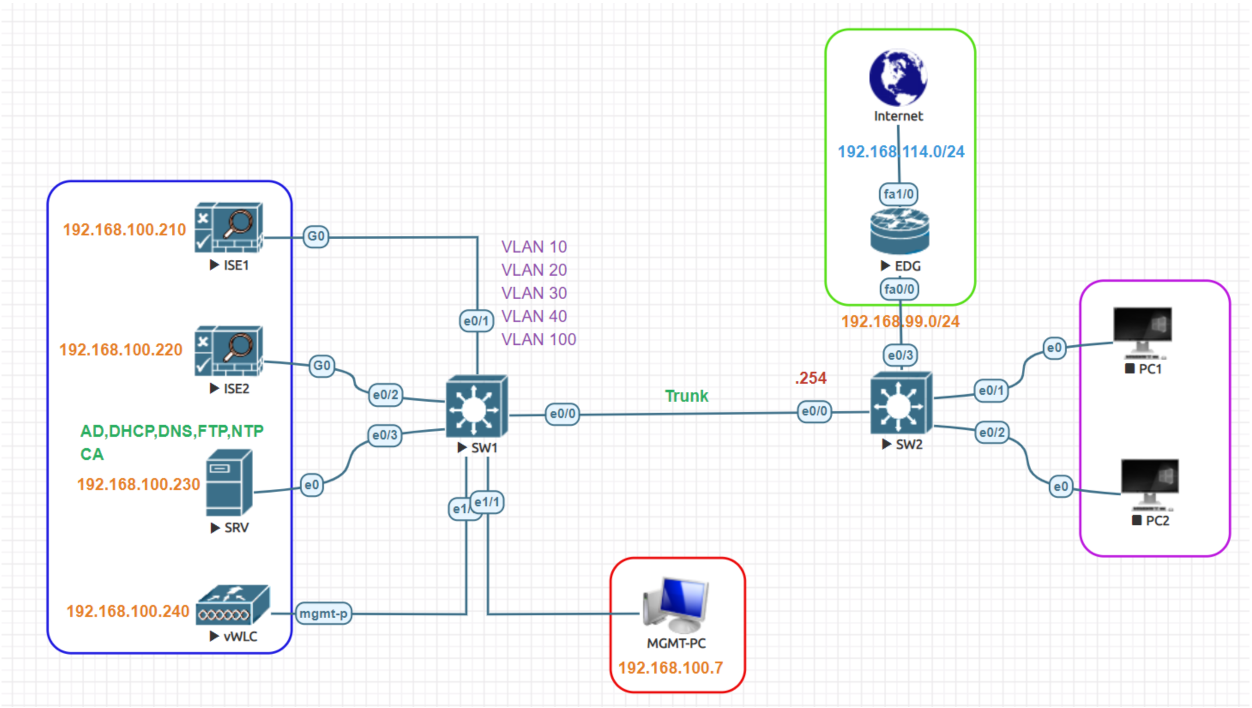
Downloadable ACL Lab:

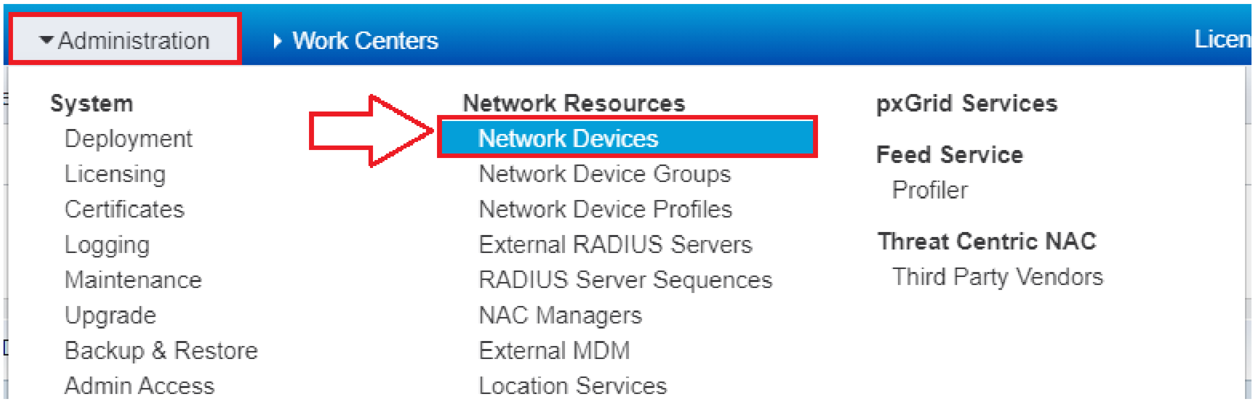


Cisco ISE Primary IP Address	192.168.100.210
Cisco ISE Secondary IP Address	192.168.100.220
AD, DNS and CA Server IP Address	192.168.100.230
Domain Name:	test.local
Test User/Group	E1/Employee
Test VLAN	VLAN 20
VLAN Subnet	192.168.20.0/24
VLAN 20 Gateway	192.168.20.1
Authenticator Switch	SW2
Authentication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

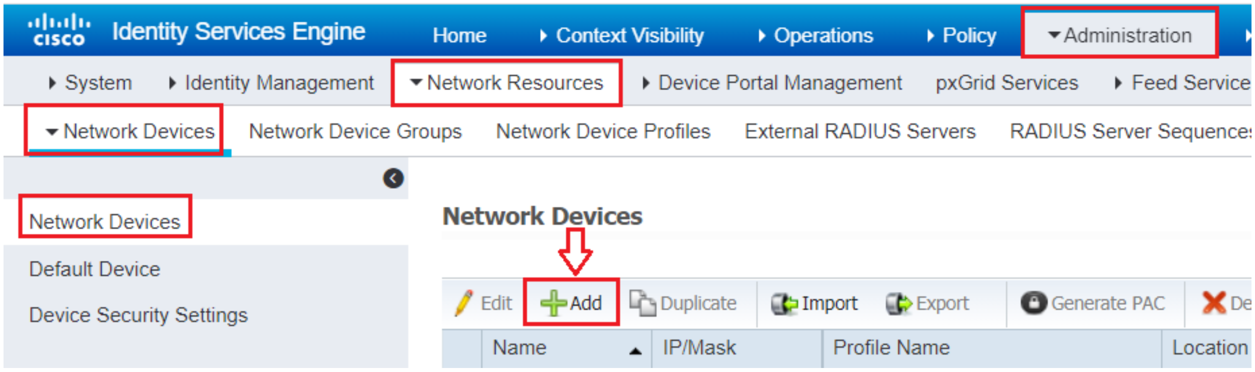
Dot1X Configuration
SW2(config)#aaa new-model
SW2(config)#dot1x system-auth-control
SW2(config)#radius server ISE1
SW2(config-radius-server)# address ipv4 192.168.100.210 auth-port 1812 acct-port 1813
SW2(config-radius-server)#key Test123
SW2(config-radius-server)#radius server ISE2
SW2(config-radius-server)# 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

Add Network Device:

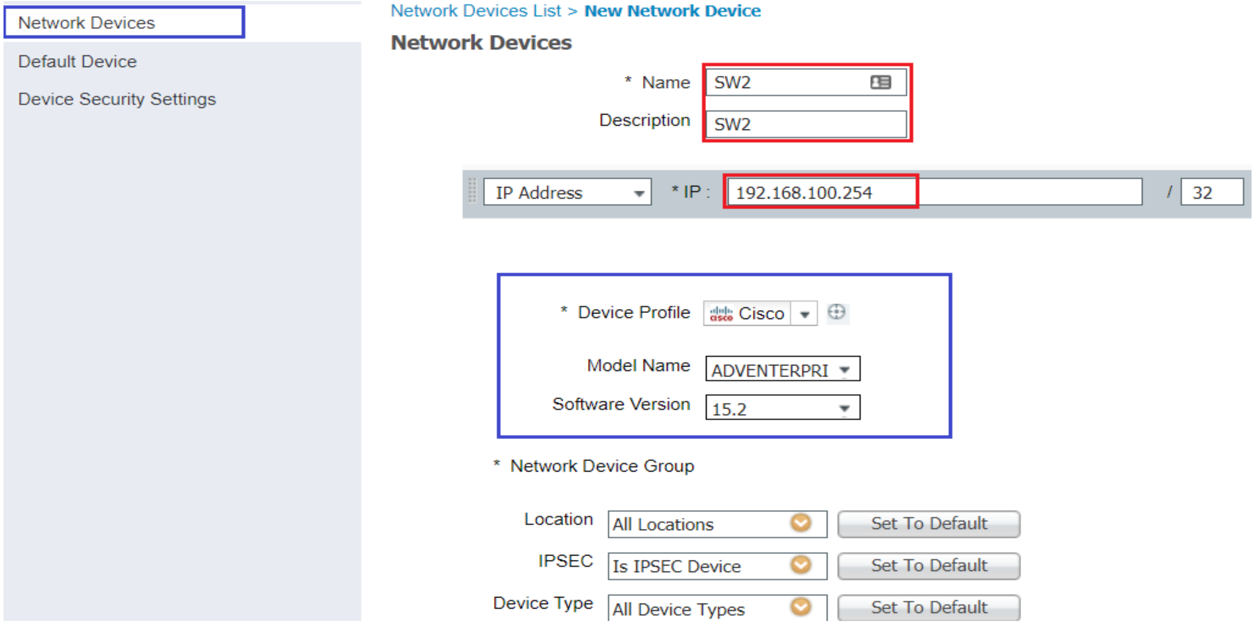
Go to Administration > Network Resources > Network Devices to add the Device (SW2).



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.

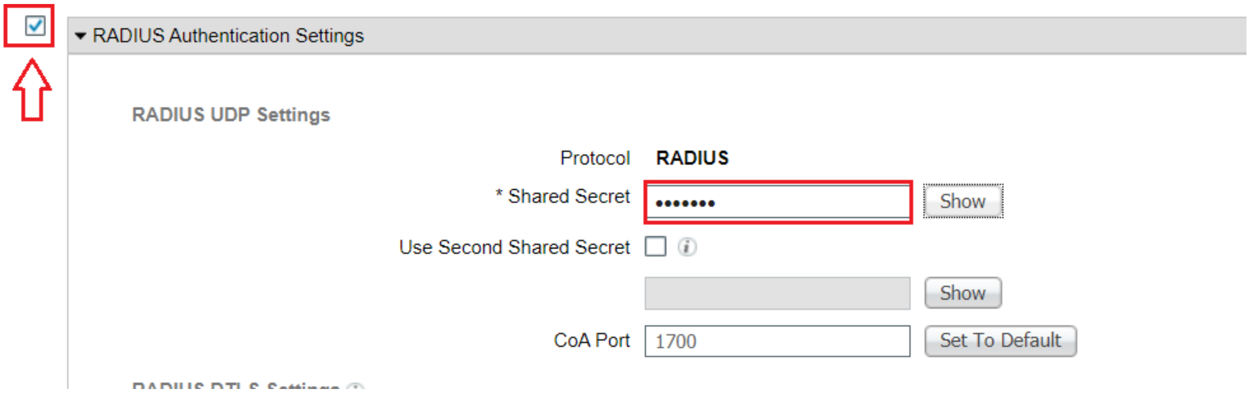


* Name	SW2
Description	SW2
IP Address	* IP : 192.168.100.254 / 32
* Device Profile	Cisco
Model Name	ADVENTERPRI
Software Version	15.2

* Network Device Group

Location	All Locations	Set To Default
IPSEC	Is IPSEC Device	Set To Default
Device Type	All Device Types	Set To Default

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



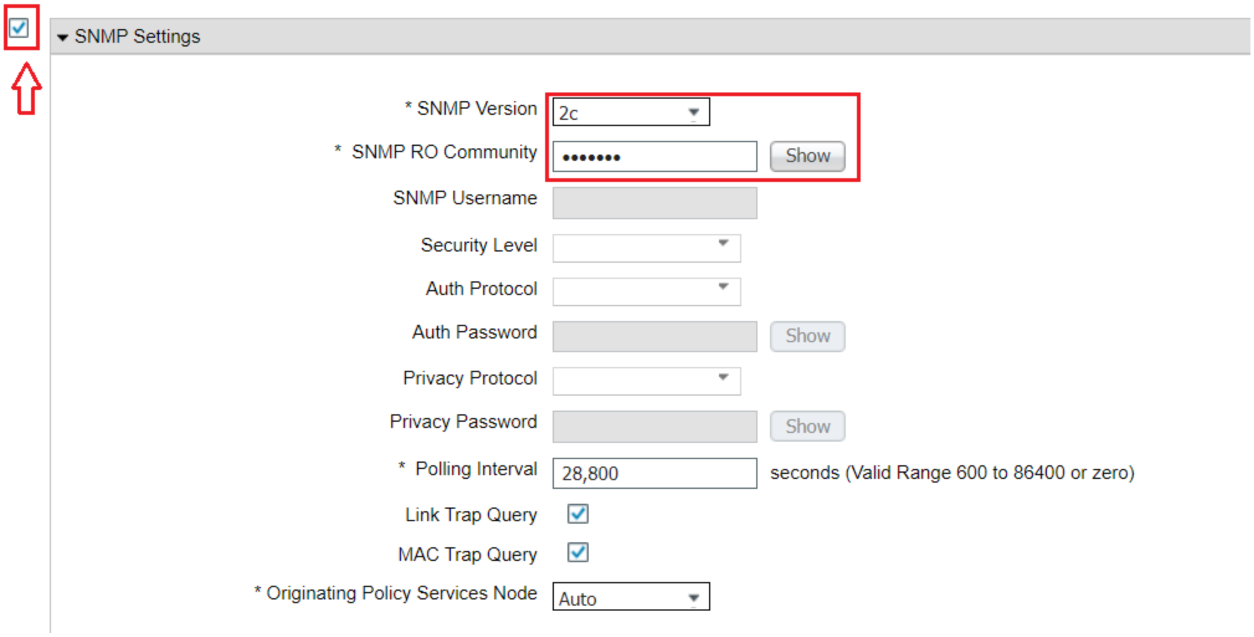
☑ ▾ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol	RADIUS
* Shared Secret	••••••• Show
Use Second Shared Secret	□
	Show
CoA Port	1700 Set To Default

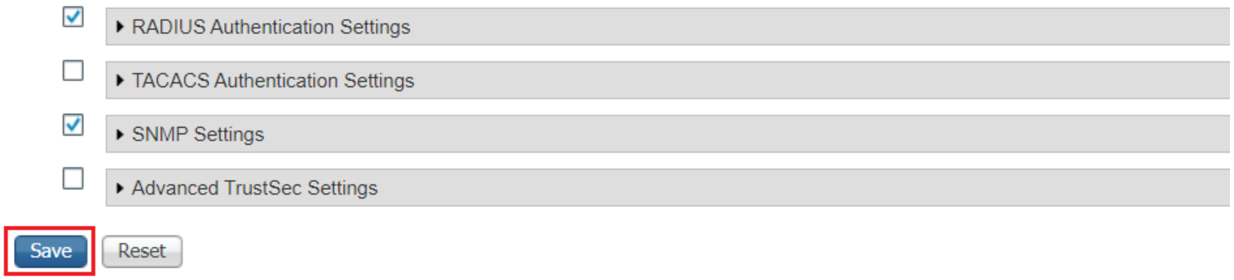
RADIUS DTLS Settings

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

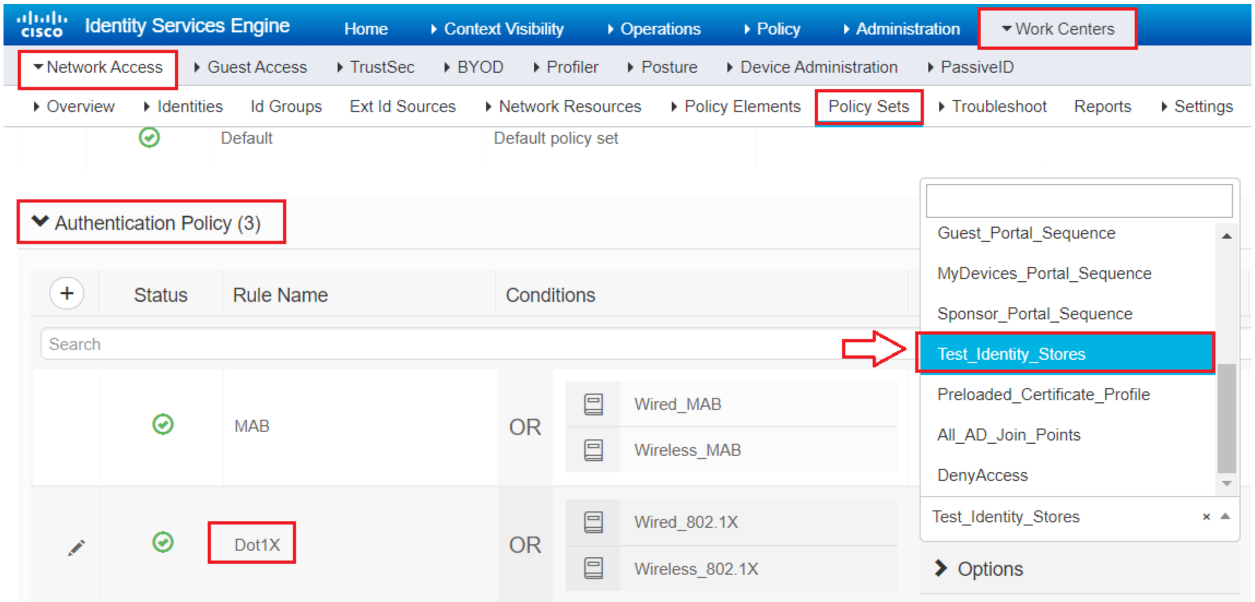
☑ ▸ SNMP Settings

□ ▸ Advanced TrustSec Settings

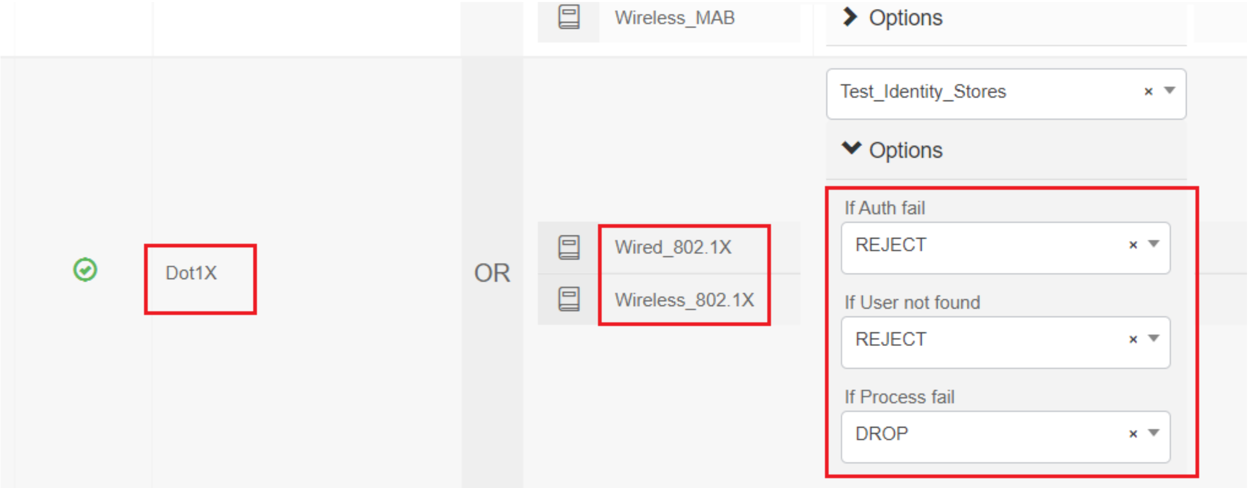
Save Reset

802.1x Authentication Polices:

For network access policies, choose Work Centers > Network Access > Policy Sets. Change the default Identity store to Test_Identity_Stores which we created earlier.



If the authentication fail the user will be Rejected, if user not found the user will be rejected, while if the process of Dot1x fail the user will be dropped.



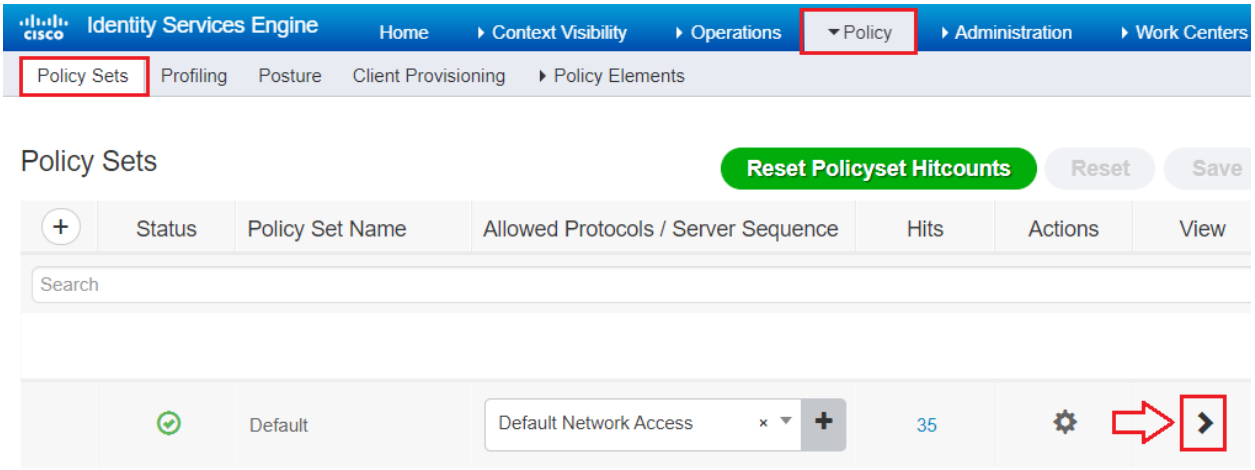
If Auth fail: REJECT

If User not found: REJECT

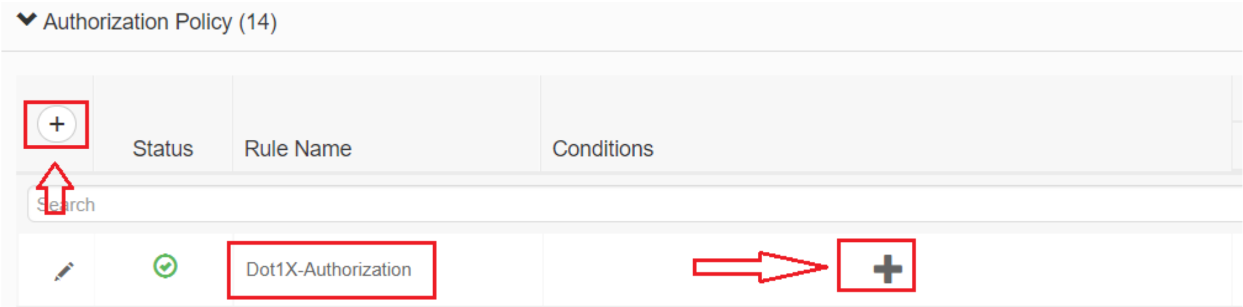
If Process fail: DROP

802.1x Authorization Polices:

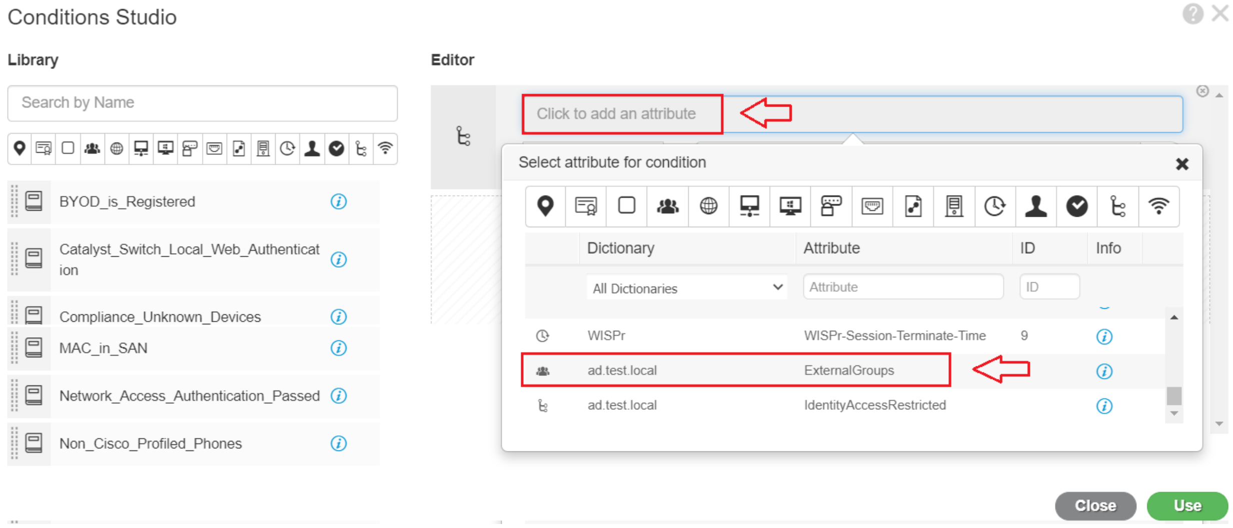
Navigate to Policy>Policy Sets > click on Arrow Icon >



Navigate to Authorization Policy section click on round circle Plus icon to add new Authorization Policy, name the authorization policy in this case Dot1x-Authorization. In Conditions click on Plus icon to set the conditions for authorization policy.

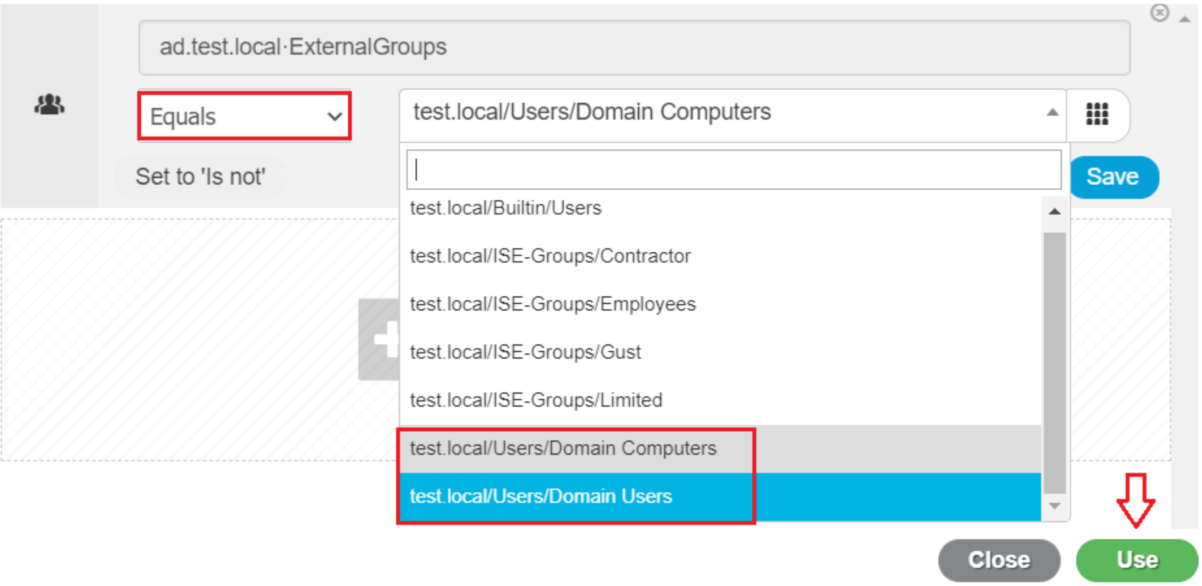


In Conditions Studio > Editor click to add an attribute choose ad.test.local


Conditions Studio
Library
Search by Name
BYOD_is_Registered
Catalyst_Switch_Local_Web_Authentication
Compliance_Unknown_Devices
MAC_in_SAN
Network_Access_Authentication_Passed
Non_Cisco_Profiled_Phones
Editor
Click to add an attribute
Select attribute for condition
All Dictionaries
Attribute
ID
Close
Use

Dictionary	Attribute	ID	Info
WISPr	WISPr-Session-Terminate-Time	9	ⓘ
ad.test.local	ExternalGroups		ⓘ
ad.test.local	IdentityAccessRestricted		ⓘ

In Editor > Equals > test.local/users/Domain Computers also, create new same policy for test.local/users/Domain Users



ad.test.local·ExternalGroups

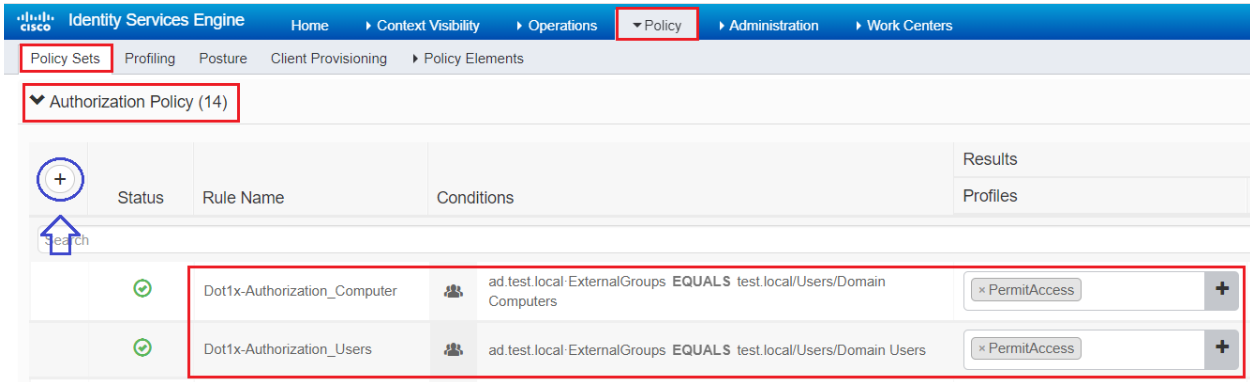
Equals

test.local/Users/Domain Computers

Set to 'Is not'

- test.local/Builtin/Users
- test.local/ISE-Groups/Contractor
- test.local/ISE-Groups/Employees
- test.local/ISE-Groups/Gust
- test.local/ISE-Groups/Limited
- test.local/Users/Domain Computers
- test.local/Users/Domain Users

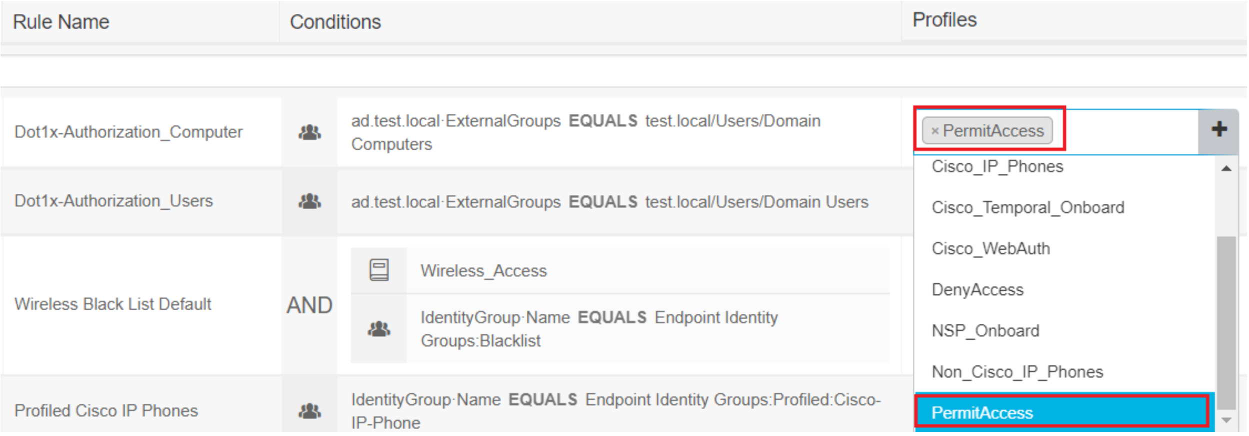
Finally, two Authorization Polices are created for Dot1x Authorization.



Authorization Policy (14)

Status	Rule Name	Conditions	Results Profiles
✓	Dot1x-Authorization_Computer	ad.test.local·ExternalGroups **EQUALS** test.local/Users/Domain Computers	× PermitAccess
✓	Dot1x-Authorization_Users	ad.test.local·ExternalGroups **EQUALS** test.local/Users/Domain Users	× PermitAccess

In Profile choose PermitAccess from dropdown and click Save.

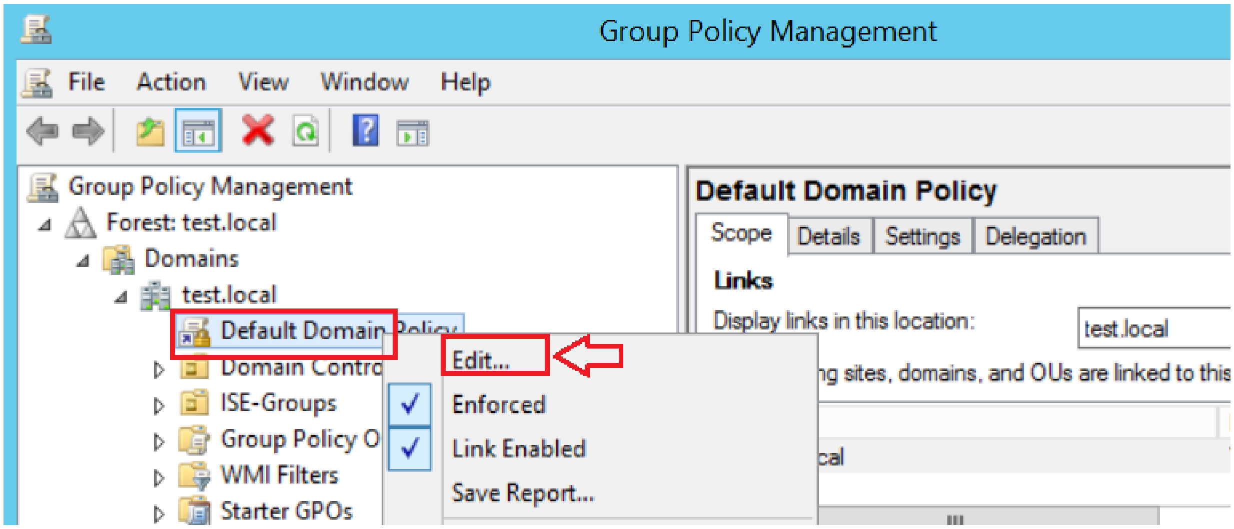


Rule Name	Conditions	Profiles
Dot1x-Authorization_Computer	ad.test.local·ExternalGroups **EQUALS** test.local/Users/Domain Computers	× PermitAccess
Dot1x-Authorization_Users	ad.test.local·ExternalGroups **EQUALS** test.local/Users/Domain Users	
Wireless Black List Default	AND Wireless_Access IdentityGroup·Name **EQUALS** Endpoint Identity Groups:Blacklist	
Profiled Cisco IP Phones	IdentityGroup·Name **EQUALS** Endpoint Identity Groups:Profiled:Cisco-IP-Phone	

- Cisco_IP_Phones
- Cisco_Temporal_Onboard
- Cisco_WebAuth
- DenyAccess
- NSP_Onboard
- Non_Cisco_IP_Phones
- PermitAccess

Dot1x Client Group Policy Creation:

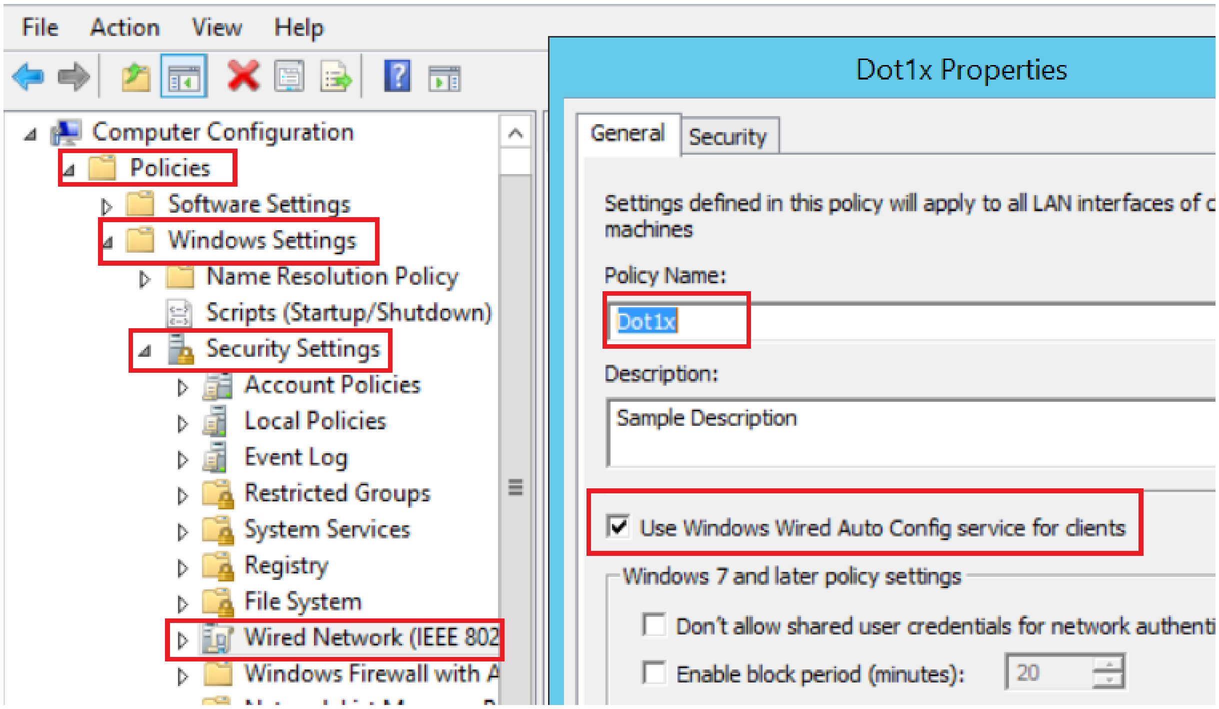
Let’s create group policy to push down dot1x settings to clients. Open Group Policy Management. Highlight the domain and right-click on Default Domain Policy and click Edit.



Display links in this location: test.local

ng sites, domains, and OUs are linked to this

Navigate to Computer Configuration>Windows Settings>Security Settings>Wired Network and right-click on it. Choose Create a New Wired Network Policy. This will open the New Wired Network Policy Properties box. Name your policy whatever you'd like it to be and make sure the Use Windows Wired Auto Config service for clients box is checked.



Settings defined in this policy will apply to all LAN interfaces of c machines

Policy Name: Dot1x

Description: Sample Description

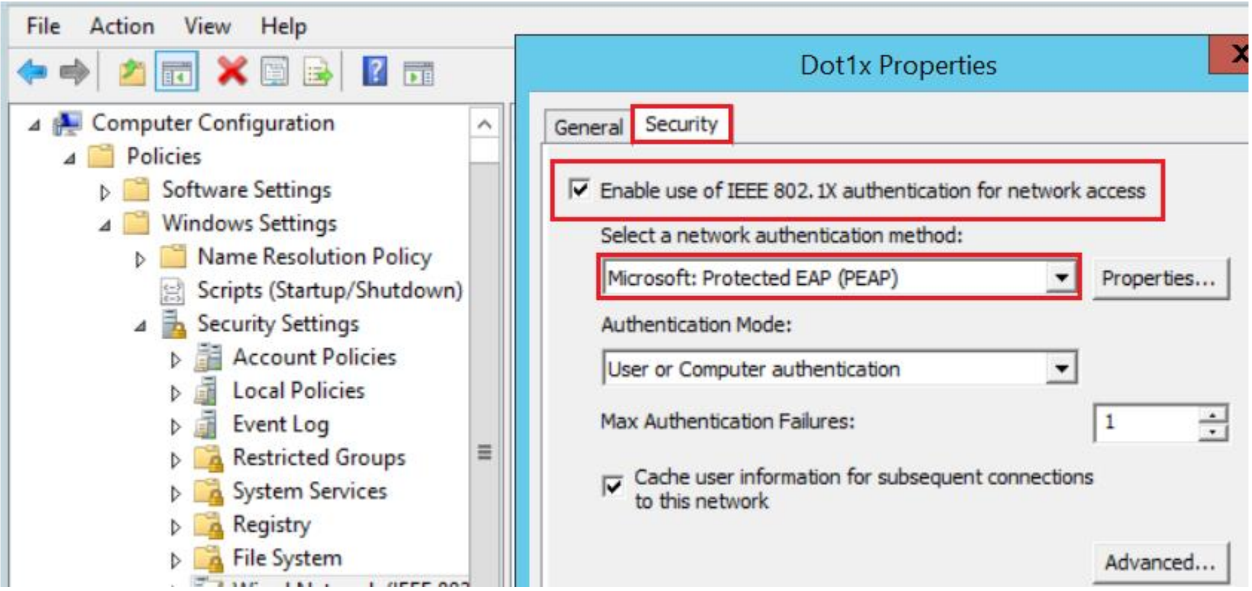
☑ Use Windows Wired Auto Config service for clients

Windows 7 and later policy settings

☐ Don’t allow shared user credentials for network authenti

☐ Enable block period (minutes): 20

On the Security tab, ensure that the Enable use of IEEE 802.1X authentication for network access box is checked and from the Select a network authentication method drop-down, choose Microsoft: Protected EAP (PEAP). Click on the Properties button to the right of it.



☑ Enable use of IEEE 802. 1X authentication for network access

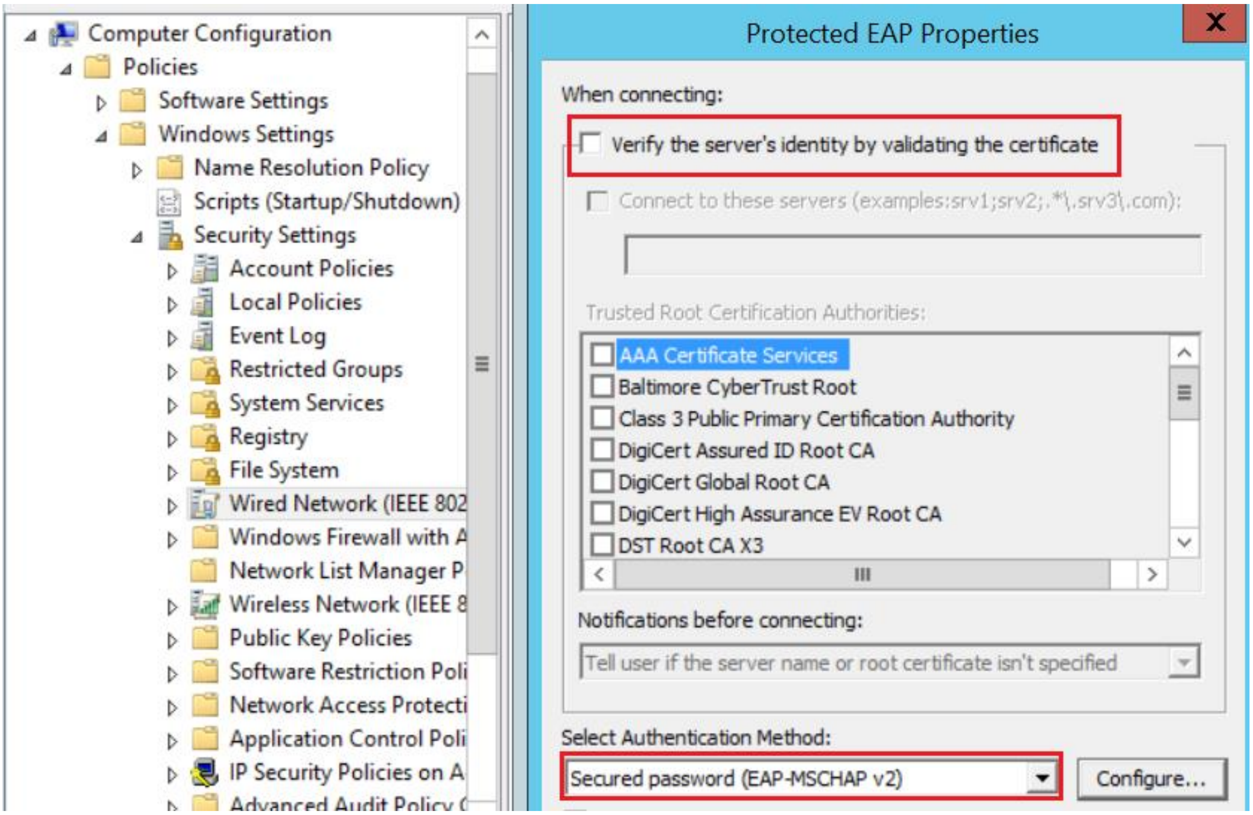
Select a network authentication method:
Microsoft: Protected EAP (PEAP)

Authentication Mode:
User or Computer authentication

Max Authentication Failures: 1

☑ Cache user information for subsequent connections to this network

In the Properties box that pops up, uncheck the boxes next to Verify the server's identity by validating the certificate. Under the Select Authentication Method drop-down, this is where we will select our inner method. Choose Secured password (EAP-MSCHAP v2) options.



When connecting:

☐ Verify the server's identity by validating the certificate

☐ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

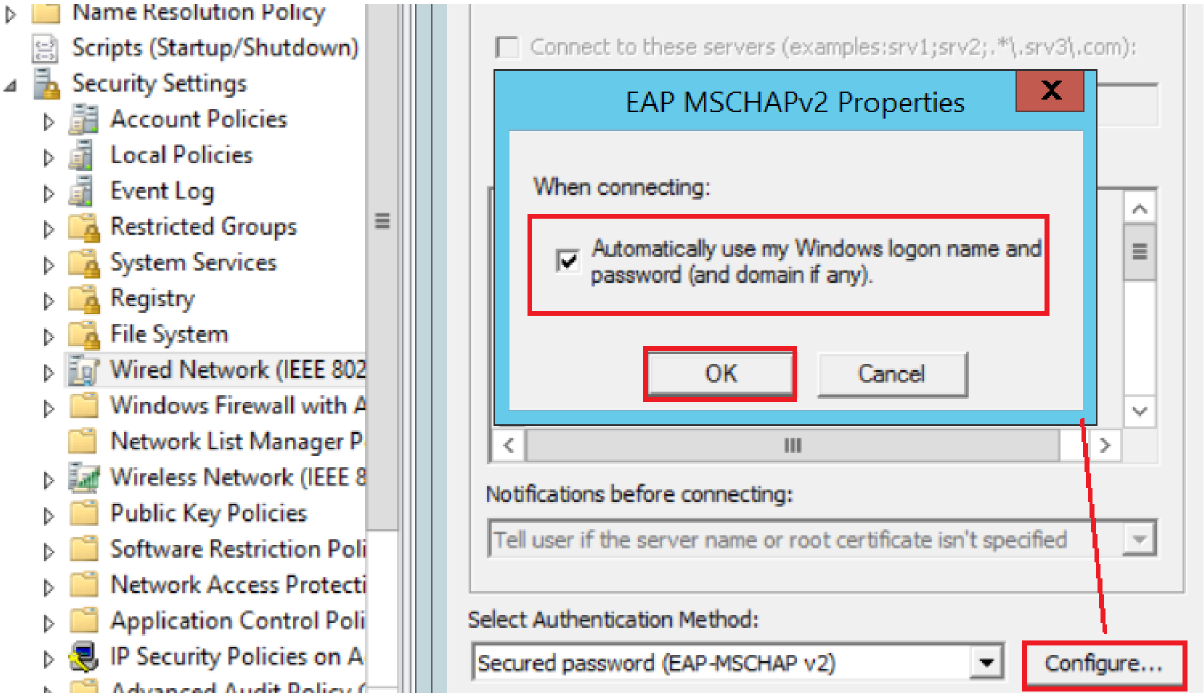
Trusted Root Certification Authorities:

☐ AAA Certificate Services
☐ Baltimore CyberTrust Root
☐ Class 3 Public Primary Certification Authority
☐ DigiCert Assured ID Root CA
☐ DigiCert Global Root CA
☐ DigiCert High Assurance EV Root CA
☐ DST Root CA X3

Notifications before connecting:
Tell user if the server name or root certificate isn't specified

Select Authentication Method:
Secured password (EAP-MSCHAP v2)

Click on the Configure... box next to it. EAP MSCHAPv2 box should pop up. Check the boxes and click OK to save your settings. Do the same for the rest of the boxes you have open.



- Name Resolution Policy
- Scripts (Startup/Shutdown)
- Security Settings
  - Account Policies
  - Local Policies
  - Event Log
  - Restricted Groups
  - System Services
  - Registry
  - File System
  - Wired Network (IEEE 802
  - Windows Firewall with A
  - Network List Manager P
  - Wireless Network (IEEE 8
  - Public Key Policies
  - Software Restriction Poli
  - Network Access Protecti
  - Application Control Poli
  - IP Security Policies on A
  - Advanced Audit Policy C

□ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

EAP MSCHAPv2 Properties

When connecting:

☑ Automatically use my Windows logon name and password (and domain if any).

OK | Cancel

Notifications before connecting:

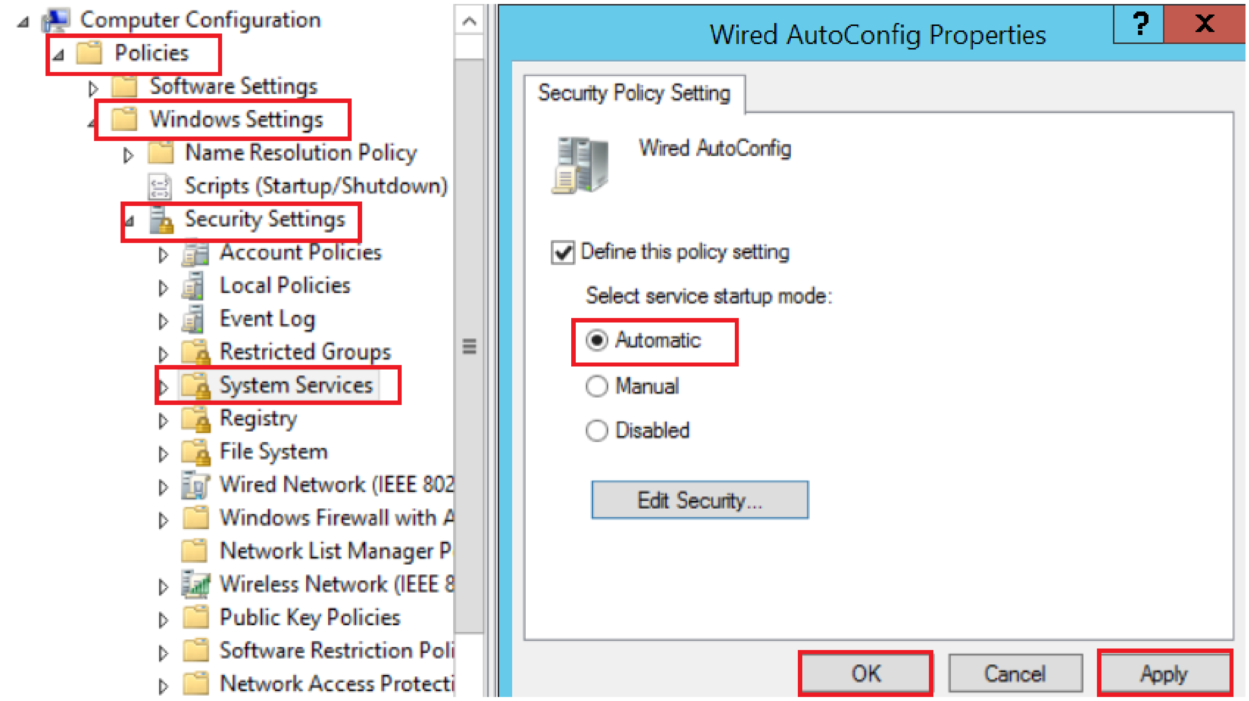
Tell user if the server name or root certificate isn't specified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

Configure...

Wired Autoconfig service is not enabled by default on Windows machines. In order to get the dot1x wired settings to work, this should be enabled so let's create a group policy. Navigate to Computer Configuration>Policies>Windows Settings>Security Settings>System Settings>Wired Autoconfig. Check box for Define this policy setting and choose the radio button for Automatic.



- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802
        - Windows Firewall with A
        - Network List Manager P
        - Wireless Network (IEEE 8
        - Public Key Policies
        - Software Restriction Poli
        - Network Access Protecti

Wired AutoConfig Properties

Security Policy Setting

Wired AutoConfig

☑ Define this policy setting

Select service startup mode:

● Automatic

○ Manual

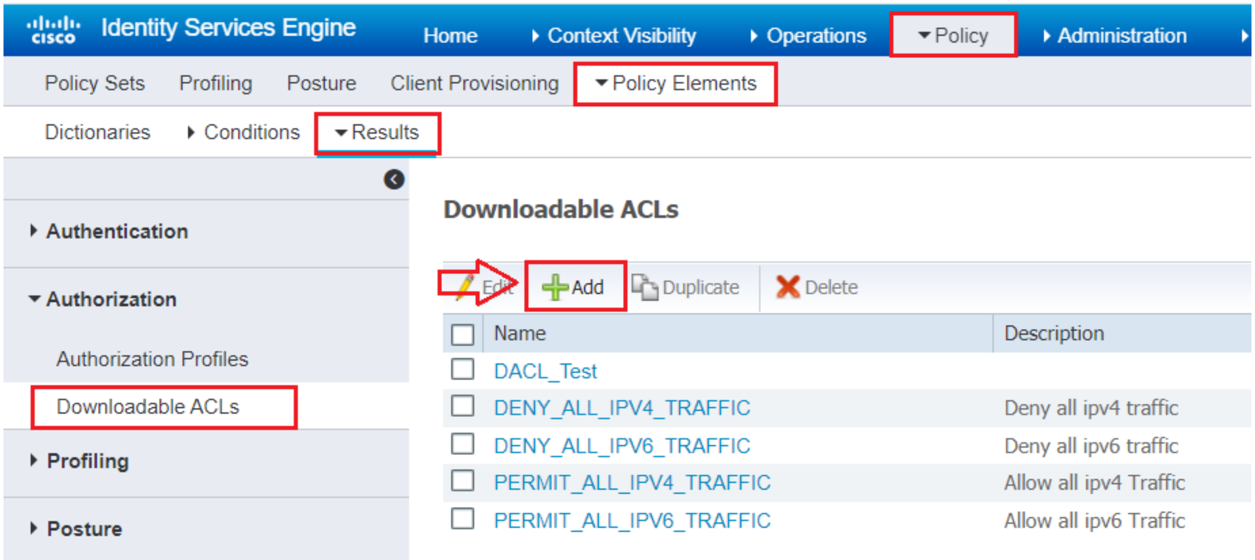
○ Disabled

Edit Security...

OK | Cancel | Apply

Configuring Downloadable ACL:

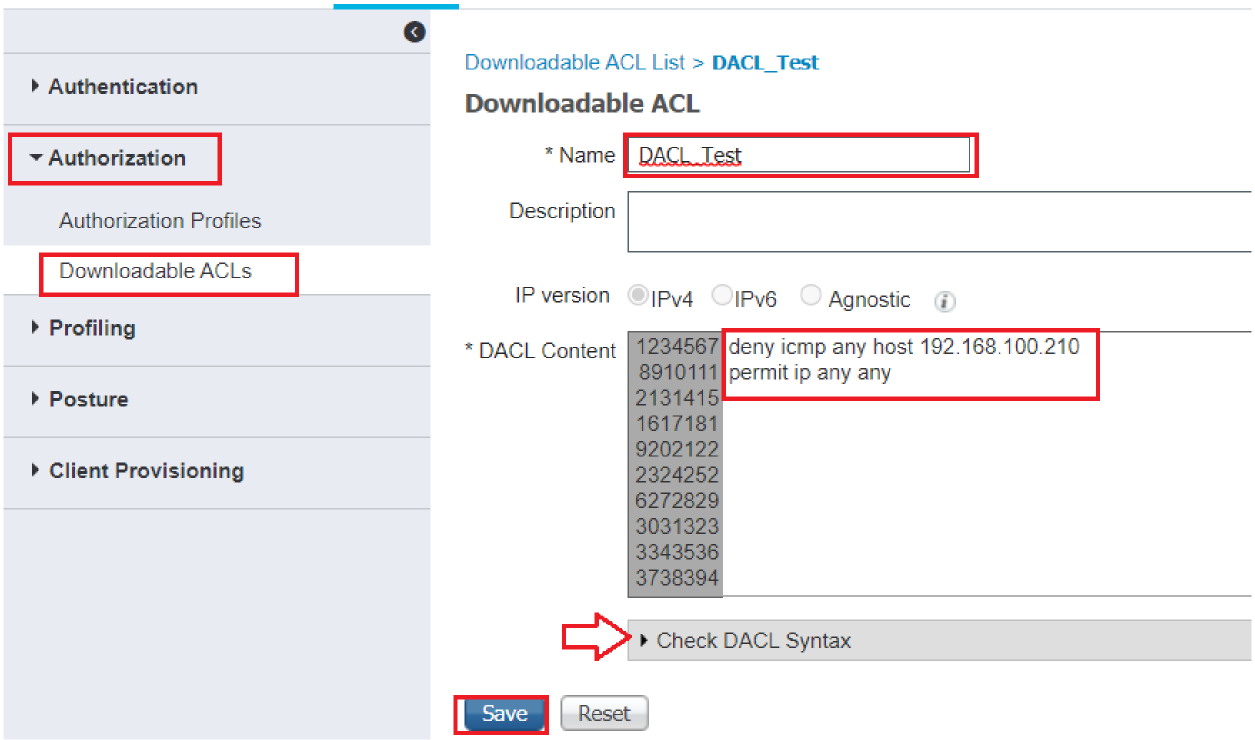
Navigate to Policy> Policy Elements> Results> Authorization> Downloadable ACLs click Add



Downloadable ACLs

☐	Name	Description
☐	DACL_Test	
☐	DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic
☐	DENY_ALL_IPV6_TRAFFIC	Deny all ipv6 traffic
☐	PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic
☐	PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic

Create a DACL with Name DACL_Test. Create the DACL deny ICMP to ISE 192.168.100.210 and permit ip any any Click Save



Downloadable ACL List > DACL_Test

Downloadable ACL

* Name: DACL_Test

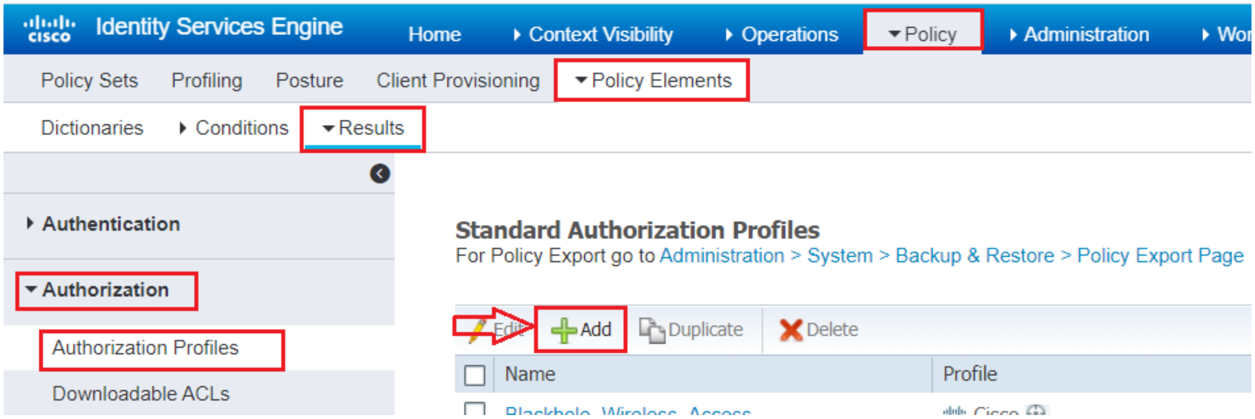
Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content

```
deny icmp any host 192.168.100.210
permit ip any any
```

Now add this DACL to a new Authorization Profile. Policy> Policy Elements> Results> Authorization> Authorization Profiles Click Add

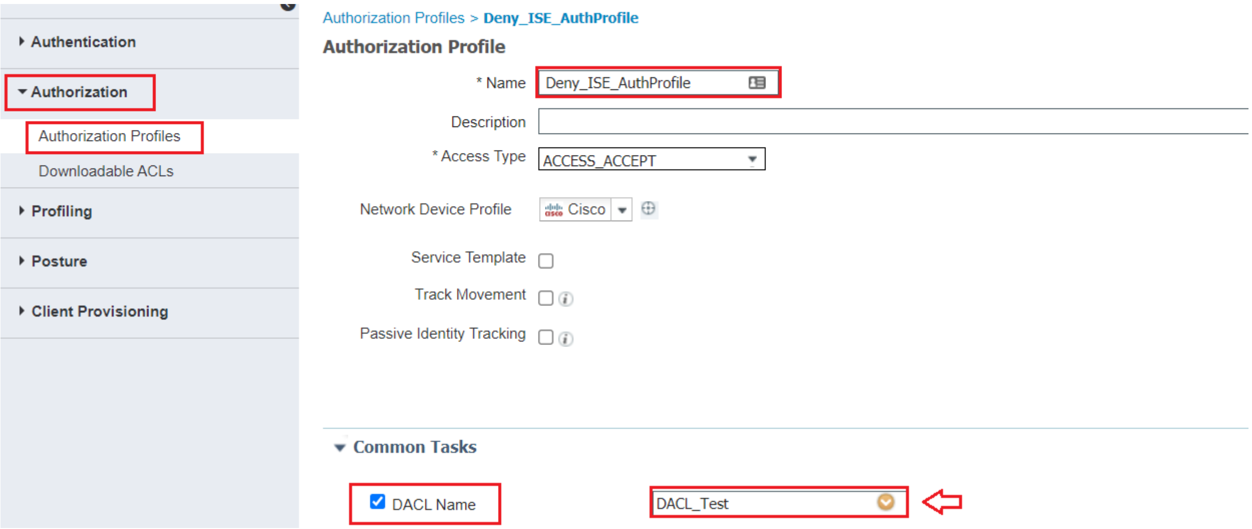


Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

	Name	Profile
□	Blackhole_Wireless_Access	Cisco

Name Authorization profile in this case Deny_ISE_AuthProfile. Select DACL Name from the drop-down list select the DACL previously configured called DACL_Test. Click Save.



Authorization Profile

* Name: Deny_ISE_AuthProfile

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

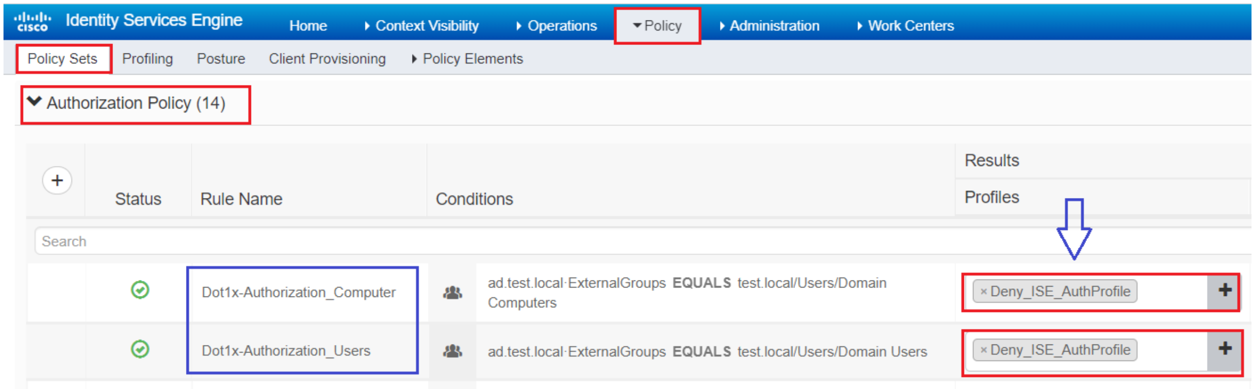
Track Movement □

Passive Identity Tracking □

Common Tasks

☑ DACL Name: DACL_Test

Go to Policy>Policy Sets navigate to Authorization Policy section. Under Profiles of Dot1x rules from drop-down list choose previously configured Authorization Profiles Deny_ISE_AuthProfile.



Authorization Policy (14)

Status	Rule Name	Conditions	Results Profiles
✓	Dot1x-Authorization_Computer	ad.test.local·ExternalGroups **EQUALS** test.local/Users/Domain Computers	Deny_ISE_AuthProfile
✓	Dot1x-Authorization_Users	ad.test.local·ExternalGroups **EQUALS** test.local/Users/Domain Users	Deny_ISE_AuthProfile

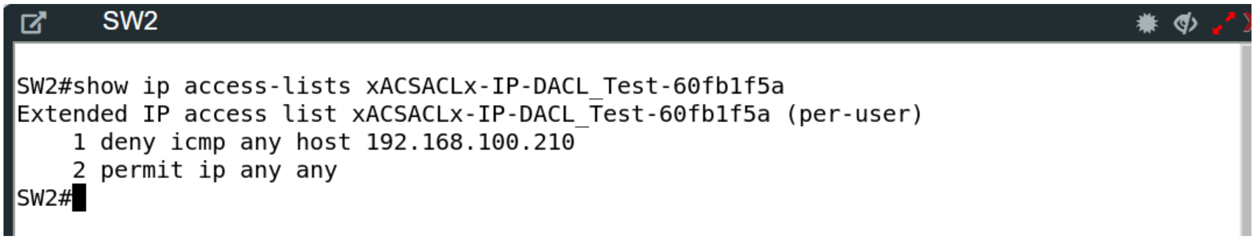
Verification:

SW2# debug radius authentication

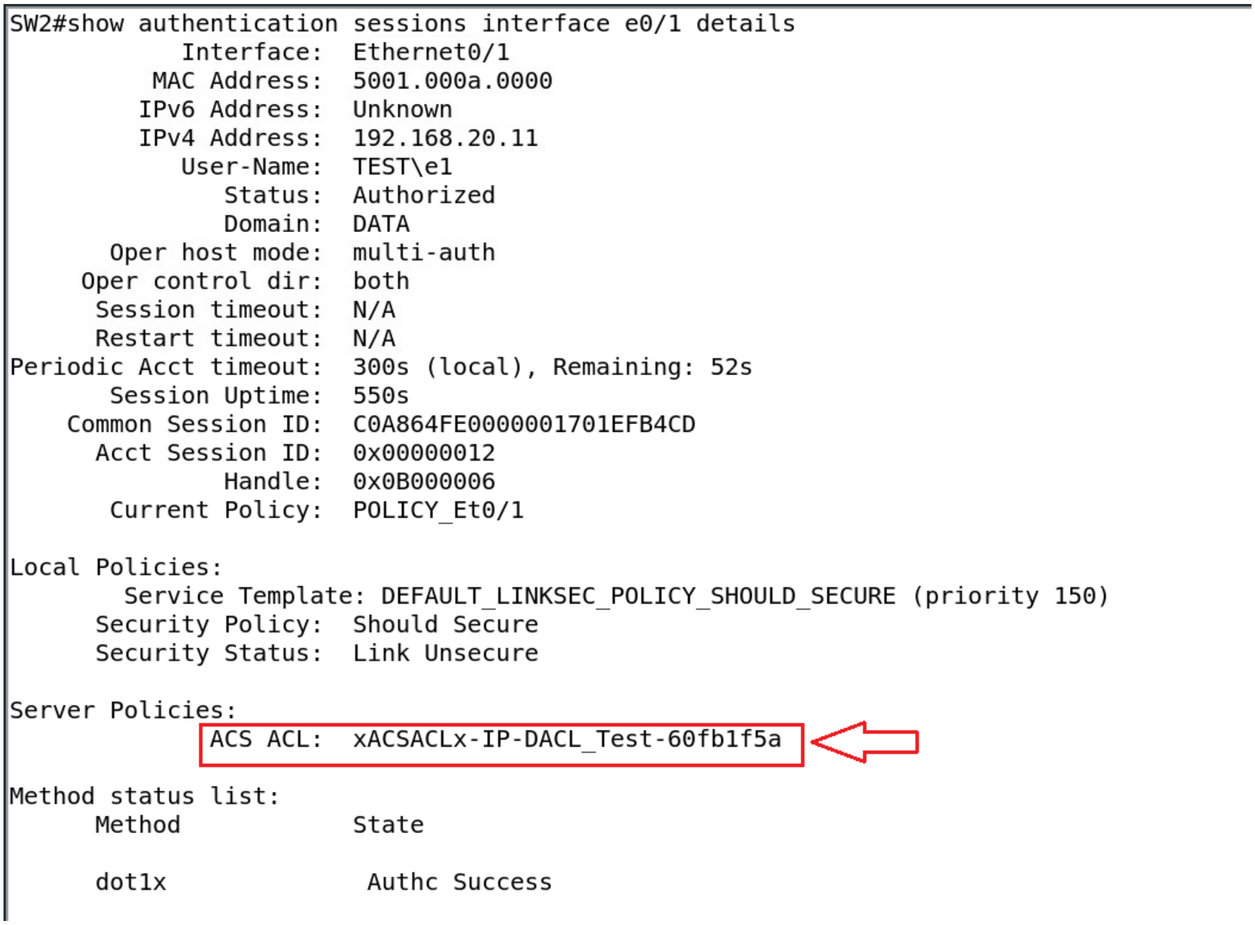
SW2# show authentication sessions interface ethernet 0/1

SW2# show authentication sessions interface ethernet 0/1 details

SW2# show ip interface ethernet0/1

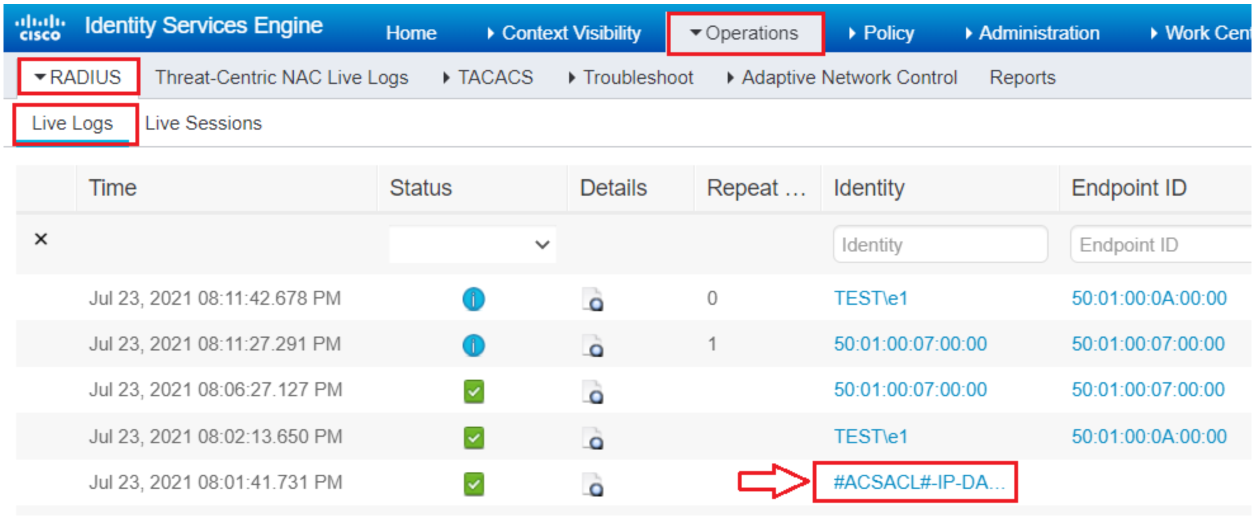


```
SW2#show ip access-lists xACSACLx-IP-DACL_Test-60fb1f5a
Extended IP access list xACSACLx-IP-DACL_Test-60fb1f5a (per-user)
    1 deny icmp any host 192.168.100.210
    2 permit ip any any
SW2#
```

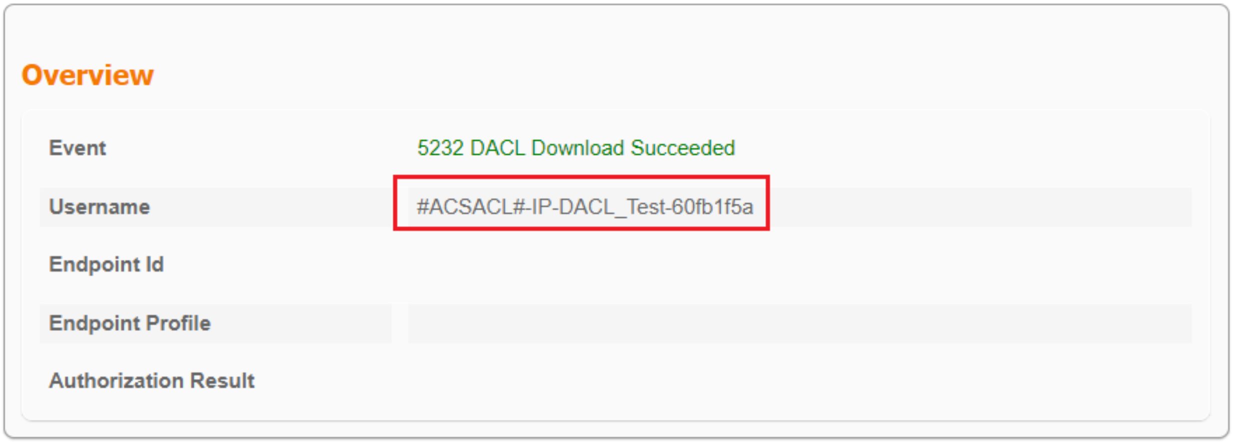


```
SW2#show authentication sessions interface e0/1 details
            Interface:  Ethernet0/1
          MAC Address:  5001.000a.0000
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.20.11
            User-Name:  TEST\e1
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  300s (local), Remaining: 52s
       Session Uptime:  550s
    Common Session ID:  C0A864FE0000001701EFB4CD
      Acct Session ID:  0x00000012
               Handle:  0x0B000006
       Current Policy:  POLICY_Et0/1

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

Server Policies:
              ACS ACL:  xACSACLx-IP-DACL_Test-60fb1f5a

Method status list:
      Method            State

      dot1x              Authc Success
```

Navigate to Operations > RADIUS> Live logs.

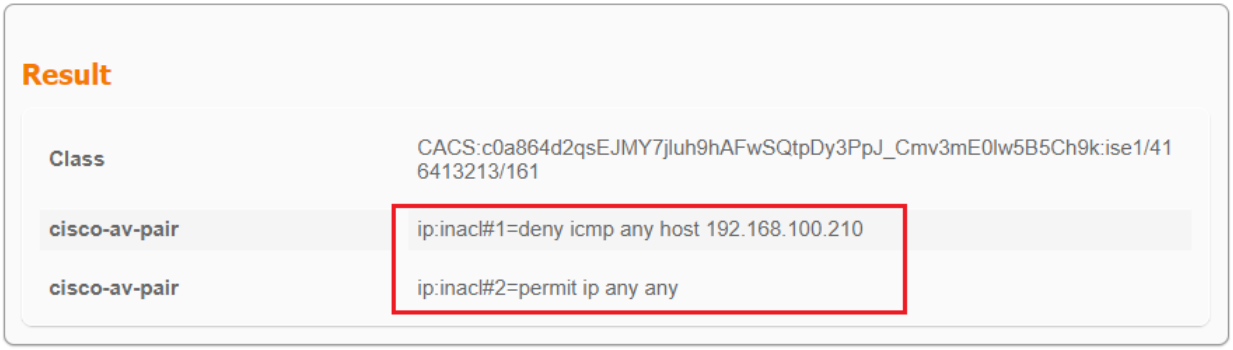


	Time	Status	Details	Repeat ...	Identity	Endpoint ID
×					Identity	Endpoint ID
	Jul 23, 2021 08:11:42.678 PM	ⓘ		0	TEST\e1	50:01:00:0A:00:00
	Jul 23, 2021 08:11:27.291 PM	ⓘ		1	50:01:00:07:00:00	50:01:00:07:00:00
	Jul 23, 2021 08:06:27.127 PM	✓			50:01:00:07:00:00	50:01:00:07:00:00
	Jul 23, 2021 08:02:13.650 PM	✓			TEST\e1	50:01:00:0A:00:00
	Jul 23, 2021 08:01:41.731 PM	✓			#ACSACL#-IP-DA...	



Overview

Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-DACL_Test-60fb1f5a
Endpoint Id	
Endpoint Profile	
Authorization Result	



Result

Class	CACS:c0a864d2qsEJMY7jluh9hAFwSQtpDy3PpJ_Cmv3mE0lw5B5Ch9k:ise1/416413213/161
cisco-av-pair	ip:inacl#1=deny icmp any host 192.168.100.210
cisco-av-pair	ip:inacl#2=permit ip any any