Introduction

This document describes how to configure a Lightweight Access Point as a 802.1x supplicant to authenticate against a RADIUS Server such as ACS 5.2.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Have basic knowledge of the WLC and Lightweight Access Points (LAPs).
- Have functional knowledge of the AAA server.
- Have thorough knowledge of wireless networks and wireless security issues.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5508 WLC that runs firmware release 7.0.220.0.
- Cisco 3502 Series LAP.
- Cisco Secure Access Control Server (ACS) that runs version 5.2.
- Cisco 3560 series switch.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

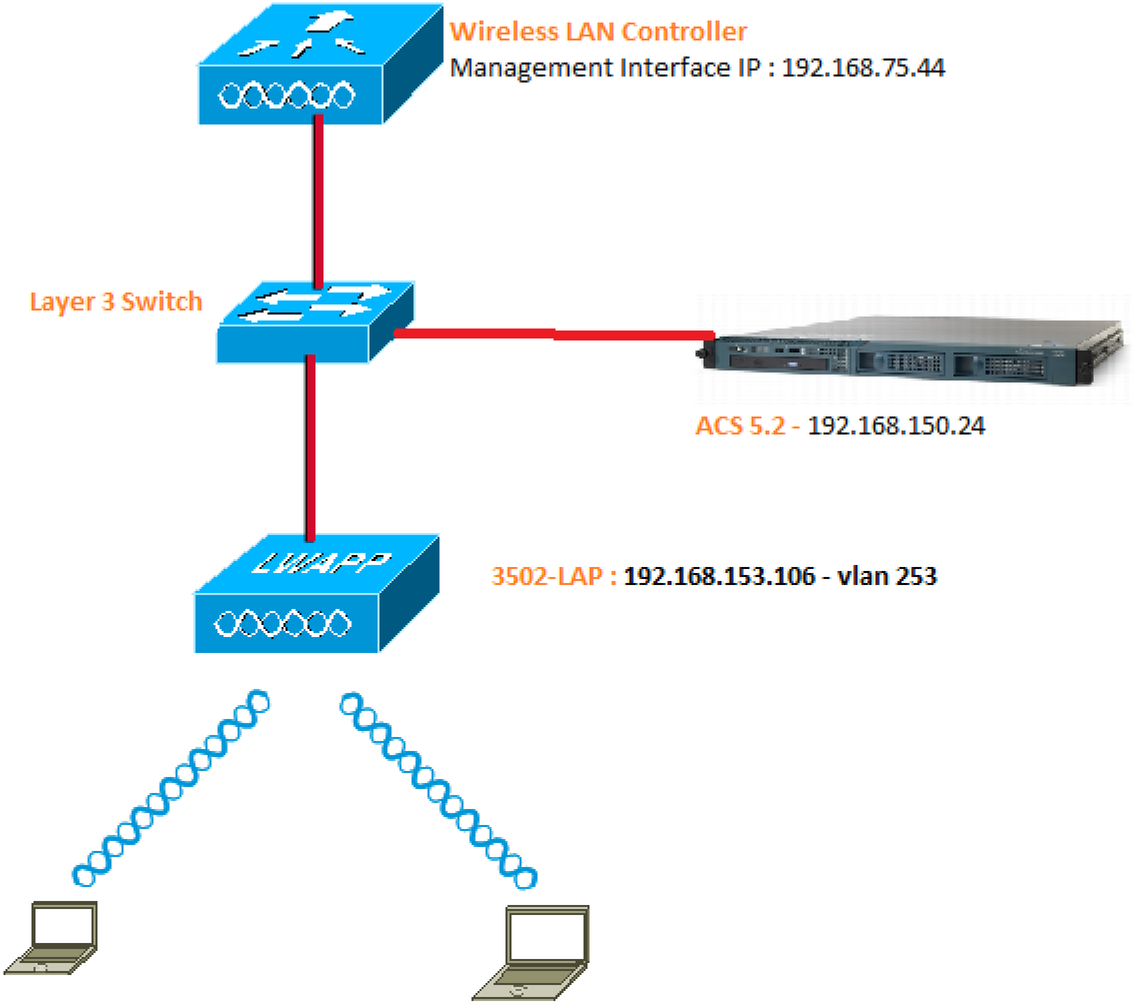
LAPs have factory installed X.509 certificates, signed by a private key, that are burned into the device at the time of manufacture. LAPs use this certificate to authenticate with the WLC at the join process. This method describes another way to authenticate LAPs. With WLC software, you can configure the 802.1x authentication between a Cisco Aironet access point and a Cisco switch. The access point acts as the 802.1x supplicant and is authenticated by the switch against a RADIUS Server (ACS) that uses EAP-FAST with anonymous PAC provisioning. Once it is configured for 802.1x authentication, the switch does not allow any traffic other than 802.1x traffic to pass through the port until the device connected to the port authenticates successfully. An access point can be authenticated either before it joins a WLC or after it has joined a WLC, in which case you configure 802.1x on the switch after the LAP joins the WLC.

Configure

In this section, you are presented with the information to configure the features described in this document.

Network Diagram

This document uses this network setup:


Wireless LAN Controller
Management Interface IP : 192.168.75.44
Layer 3 Switch
ACS 5.2 - 192.168.150.24
LWAPP
3502-LAP : 192.168.153.106 - vlan 253

These are the configuration details of the components used in this diagram:

- The IP address of the ACS (RADIUS) server is 192.168.150.24.
- The Management and AP-manager Interface address of the WLC is 192.168.75.44.
- The DHCP servers address 192.168.150.25.
- LAP is placed in VLAN 253.

VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.10
VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

Assumptions:

Switches are configured for all Layer 3 vlans.
DHCP server is assigned a DHCP scope.
Layer 3 connectivity exists between all devices in the network.
Lightweight AP is already joined to the WLC.
Each vlan has /24 mask.
ACS 5.2 has a Self Signed Certificate installed.

Configuration Steps

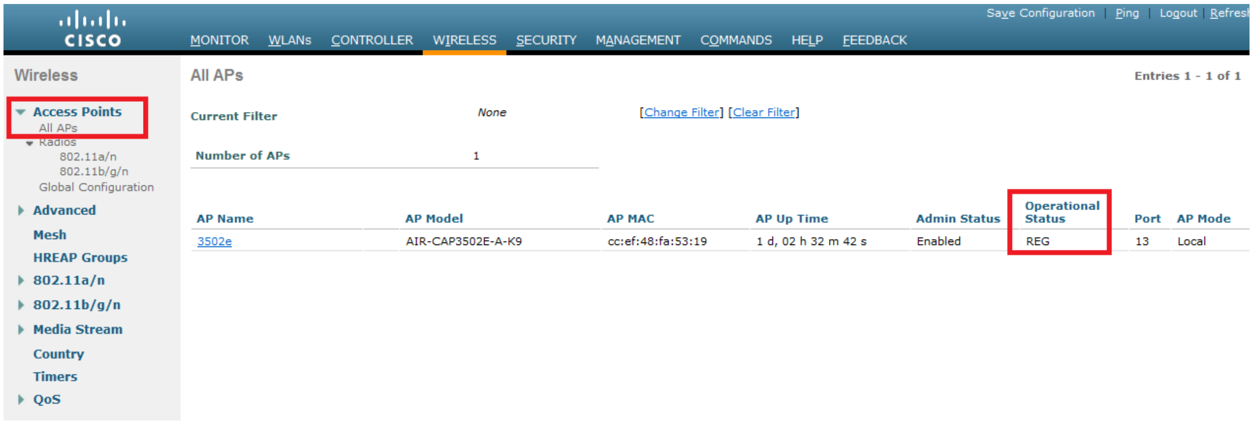
This configuration is separated into three categories:

1. RADIUS Server Configuration
2. LAP configuration.
3. Switch configuration.

LAP configuration

Assumptions:
LAP is already registered to the WLC using either option 43, DNS or statically configured WLC management Interface IP.

1. Verify LAP registration on the WLC.
   Wireless → Access points → All APs.


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
802.11a/n
802.11b/g/n
Global Configuration
Advanced
Mesh
HREAP Groups
802.11a/n
802.11b/g/n
Media Stream
Country
Timers
QoS
[Change Filter] [Clear Filter]

All APs

Entries 1 - 1 of 1

Current Filter: None

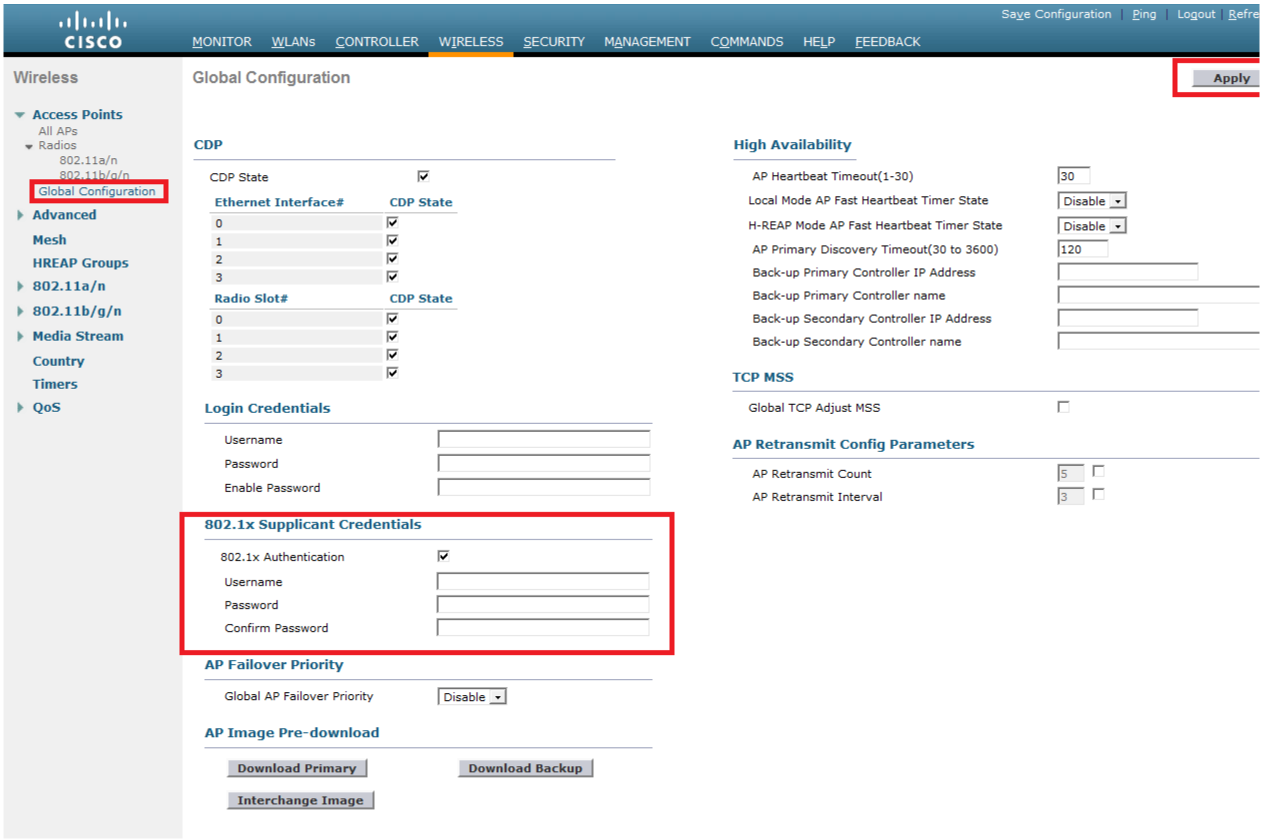
Number of APs: 1

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode
3502e	AIR-CAP3502E-A-K9	cc:ef:48:fa:53:19	1 d, 02 h 32 m 42 s	Enabled	REG	13	Local

2. Configure 802.1x credentials for the LAP. You can configure the username/password in two ways :
   - Globally for all LAPs

- Individually for all LAPs.

a) For an already joined LAP, you can set the credentials globally so every LAP which joins the WLC will inherit those credentials.



Global Configuration

CDP

CDP State ☑

Ethernet Interface#	CDP State
0	☑
1	☑
2	☑
3	☑

Radio Slot#	CDP State
0	☑
1	☑
2	☑
3	☑

Login Credentials

Username
Password
Enable Password

802.1x Supplicant Credentials

802.1x Authentication ☑
Username
Password
Confirm Password

AP Failover Priority

Global AP Failover Priority: Disable

AP Image Pre-download

High Availability

AP Heartbeat Timeout(1-30): 30
Local Mode AP Fast Heartbeat Timer State: Disable
H-REAP Mode AP Fast Heartbeat Timer State: Disable
AP Primary Discovery Timeout(30 to 3600): 120
Back-up Primary Controller IP Address
Back-up Primary Controller name
Back-up Secondary Controller IP Address
Back-up Secondary Controller name

TCP MSS

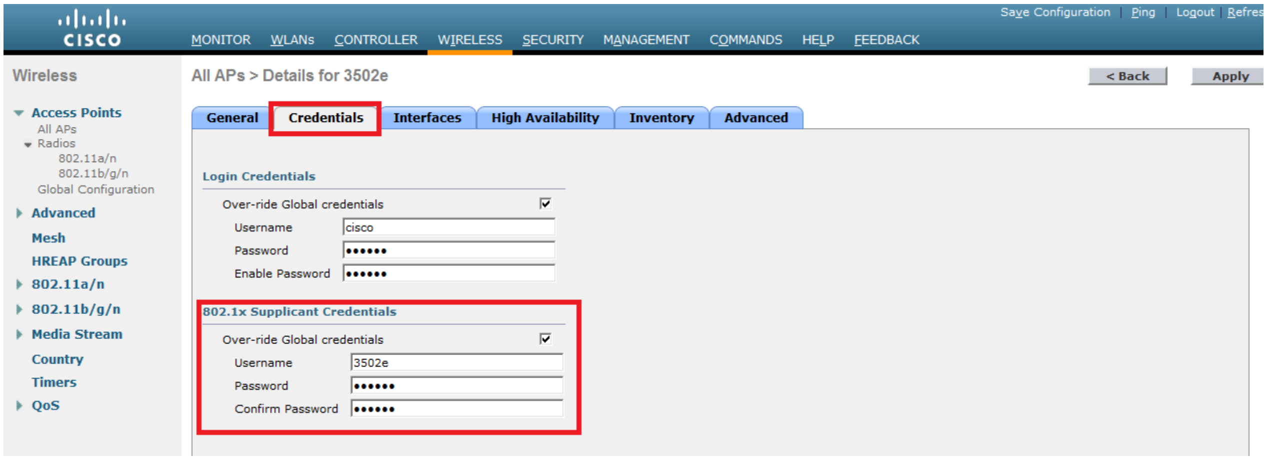
Global TCP Adjust MSS □

AP Retransmit Config Parameters

AP Retransmit Count: 5 □
AP Retransmit Interval: 3 □

b) Configure 802.1 x profiles per AP. In our example, we are going to configure credentials per AP.

Click on Wireless → All APs → Select the concerned AP. Add the username and password under 802.1x Supplicant Credentials.



All APs > Details for 3502e

Login Credentials

Over-ride Global credentials ☑

Username: cisco

Password: ••••••

Enable Password: ••••••

802.1x Supplicant Credentials

Over-ride Global credentials ☑

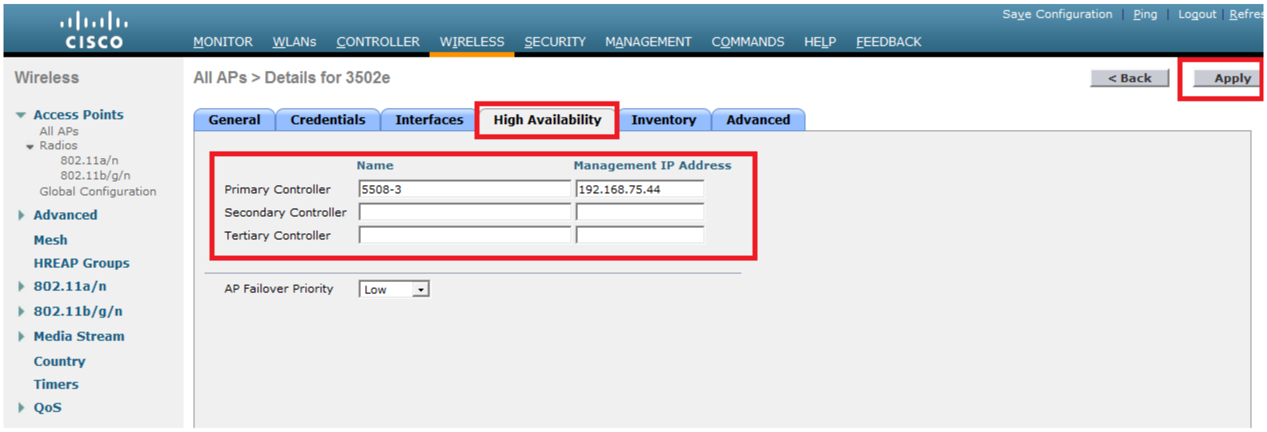
Username: 3502e

Password: ••••••

Confirm Password: ••••••

Note: Login-Credentials are used to Telnet,SSH or console to the AP.

3. Make sure you have configured the High Availability section. Hit Apply.



All APs > Details for 3502e

	Name	Management IP Address
Primary Controller	5508-3	192.168.75.44
Secondary Controller		
Tertiary Controller		

AP Failover Priority: Low

Note: Once saved, these credentials are retained across WLC and AP reboots. They change only when the LAP joins a new WLC. The LAP assumes the username and password that were configured on the new WLC.

If the access point has not joined a WLC yet, you must console into the LAP to set the credentials and use this CLI command in the enable mode:

```
LAP#lwapp ap dot1x username <username> password <password>
```

OR

```
LAP#capwap ap dot1x username <username> password <password>
```

Note: This command is available only for access points that run the recovery image.

Default username and password for LAP: cisco/Cisco

Switch Configuration

The switch acts as an authenticator for the LAP and authenticates the LAP against a RADIUS server. If the switch does not have the compliant software, upgrade the switch. On the switch CLI, enter these commands to enable the 802.1x authentication on a switch port:

```
switch#configure terminal
switch(config)#dot1x system-auth-control
switch(config)#aaa new-model
```

!--- Enables 802.1x on the Switch.

```
switch(config)#aaa authentication dot1x default group radius
switch(config)#radius server host 192.168.150.24 key cisco
```

!--- configures the radius server with shared secret and enables switch to send 802.1x information to Radius server for authentication.

```
switch(config)#ip radius source-interface vlan 253
```

!--- We are sourcing radius packets from vlan 253 with NAS IP: 192.168.153.10

```
switch(config)interface gigabitEthernet 0/11
switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253
switch(config-if)mls qos trust dscp
switch(config-if)spanning-tree portfast
```

!--- gig0/11 is the port number on which the access point is connected.

```
switch(config-if)dot1x pae authenticator
```

!--- configures dot1x authentication

```
switch(config-if)dot1x port-control auto
```

!--- With this command switch initiates the 802.1x authentication.

Note: If you have other APs on the same switch and you do not want them to use 802.1x you can either leave the port un-configured for 802.1x or issue the following command.

```
switch(config-if)authentication port-control force-authorized
```

RADIUS Server Configuration

LAP is authenticated with EAP-FAST. Make sure that the RADIUS server you use supports this EAP method if you are not using Cisco ACS 5.2.

Configuration on Radius server is divided into 4 steps.

a) Configuring Network Resources.
b) Configuring Users.
c) Defining Policy Elements.
d) Applying Access Policies.

ACS 5.x is a policy-based access control system. i.e ACS 5.x uses a rule-based policy model instead of the group-based model used in the 4.x versions.

The ACS 5.x rule-based policy model provides more powerful and flexible access control compared to the older group-based approach.

In the older group-based model, a group defines policy because it contains and ties together three types of information:

- Identity information—This information can be based on membership in AD or LDAP groups or a static assignment for internal ACS users.
- Other restrictions or conditions—Time restrictions, device restrictions, and so on.
- Permissions—VLANs or Cisco IOS privilege levels.

The ACS 5.x policy model is based on rules of the form:
If condition then result
For example, we use the information described for the group-based model:
If identity-condition, restriction-condition then authorization-profile.

So this gives us flexibility to limit under what conditions the user is allowed to access the network and at the same time what authorization level is allowed when specific conditions are met.

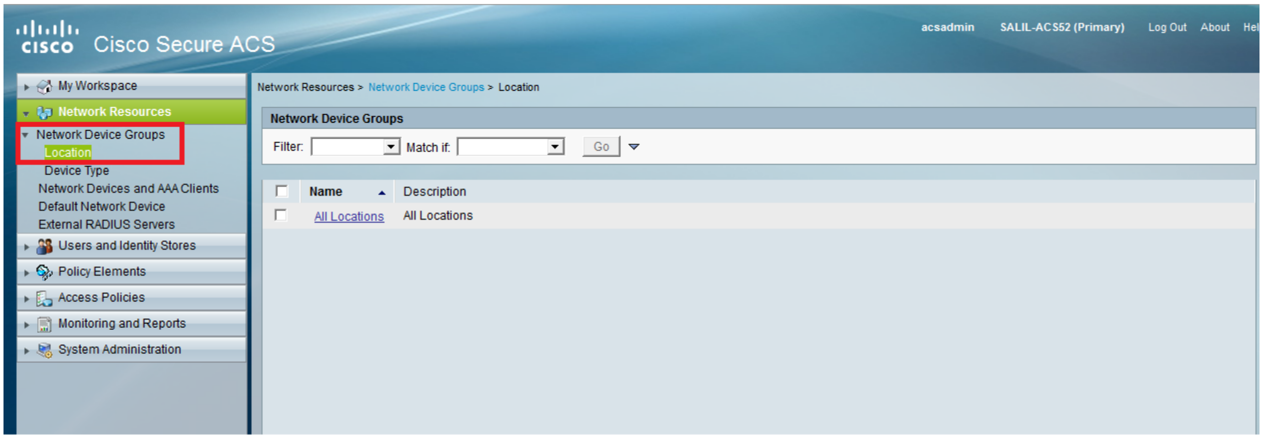
a) Configuring Network Resources.

In this section, we configure the AAA Client for the Switch on the RADIUS Server.

This procedure explains how to add the Switch as a AAA client on the RADIUS server so that the Switch can pass the user credentials of the LAP to the RADIUS server.

Complete these steps:

1. From the ACS GUI, click Network Resources.
2. Then Click Network Device Groups.
3. Click Location → Create (at the bottom)

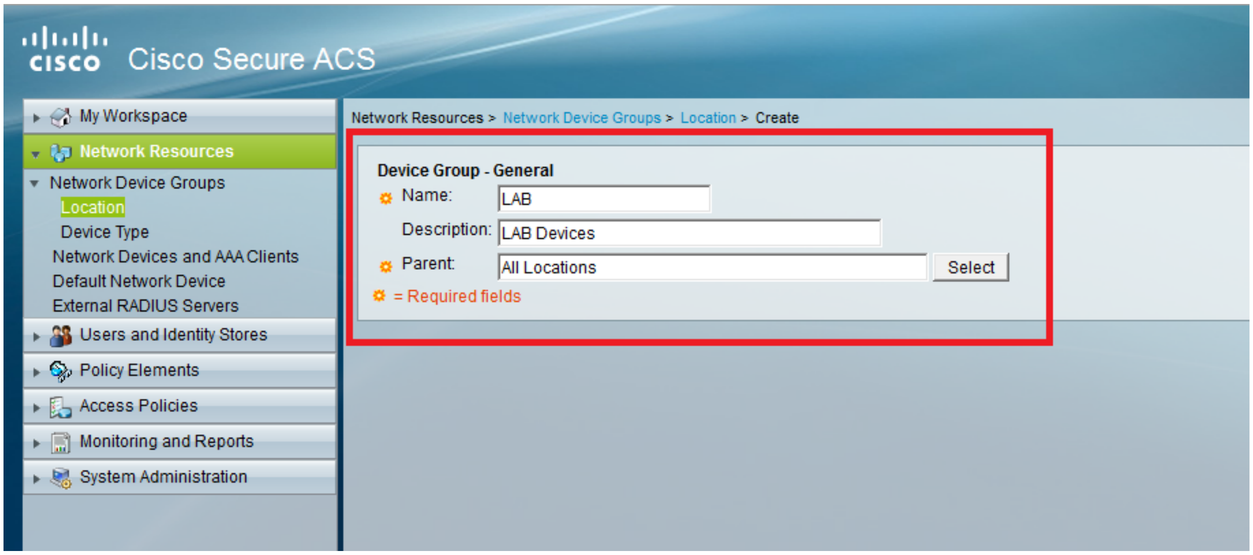


Network Resources > Network Device Groups > Location

Network Device Groups

Name	Description
All Locations	All Locations

4. Add the required fields and Click submit.



Network Resources > Network Device Groups > Location > Create

Device Group - General

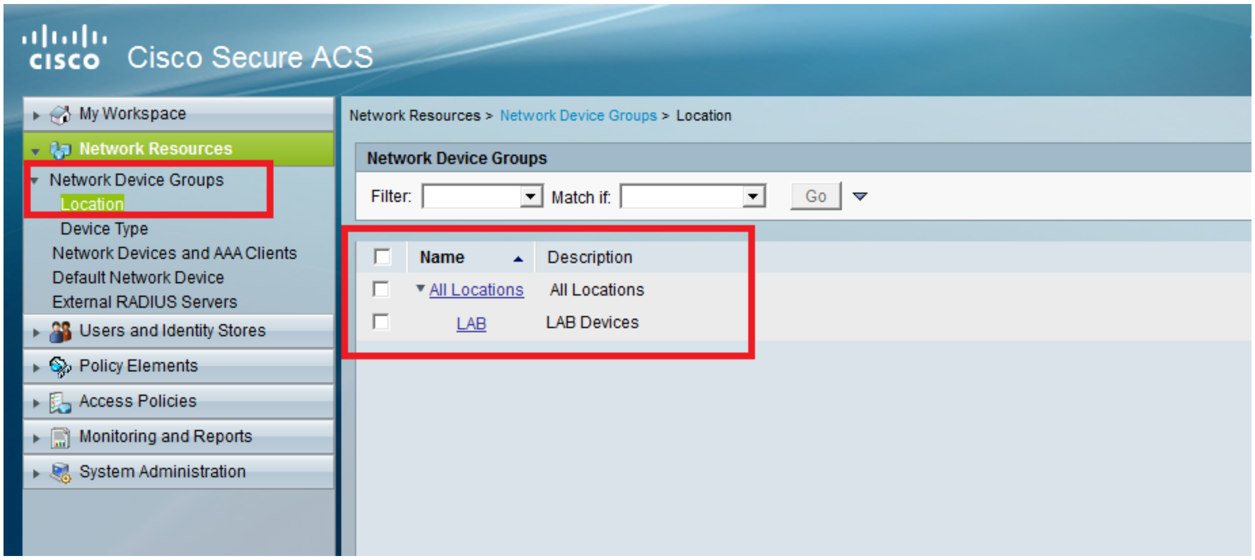
Name: LAB

Description: LAB Devices

Parent: All Locations

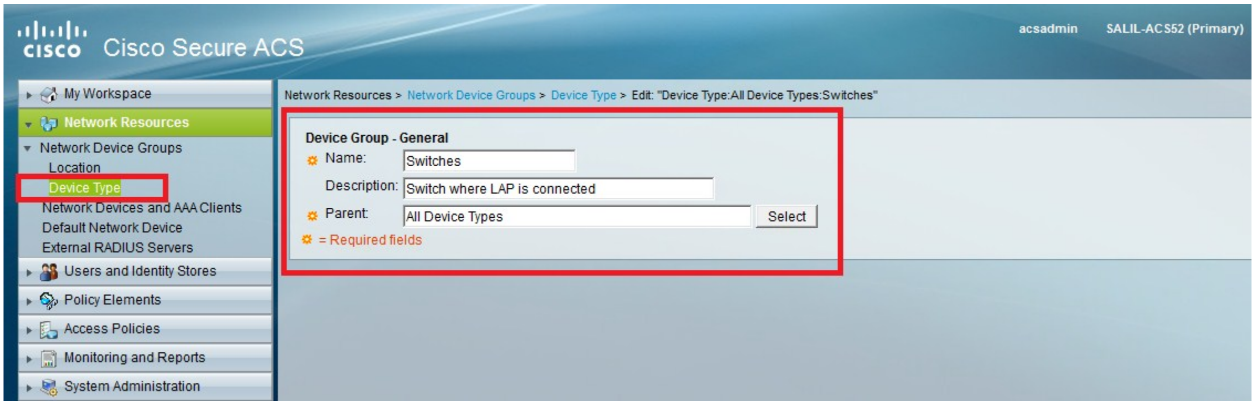
= Required fields

5. It should look like :



	Name	Description
□	All Locations	All Locations
□	LAB	LAB Devices

6. Now, Click Device Type -> Create



Device Group - General

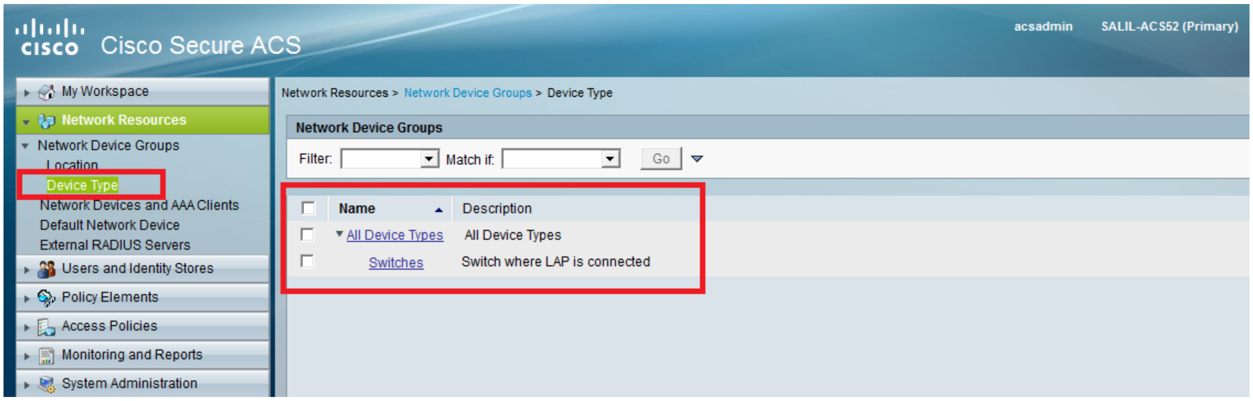
Name: Switches

Description: Switch where LAP is connected

Parent: All Device Types

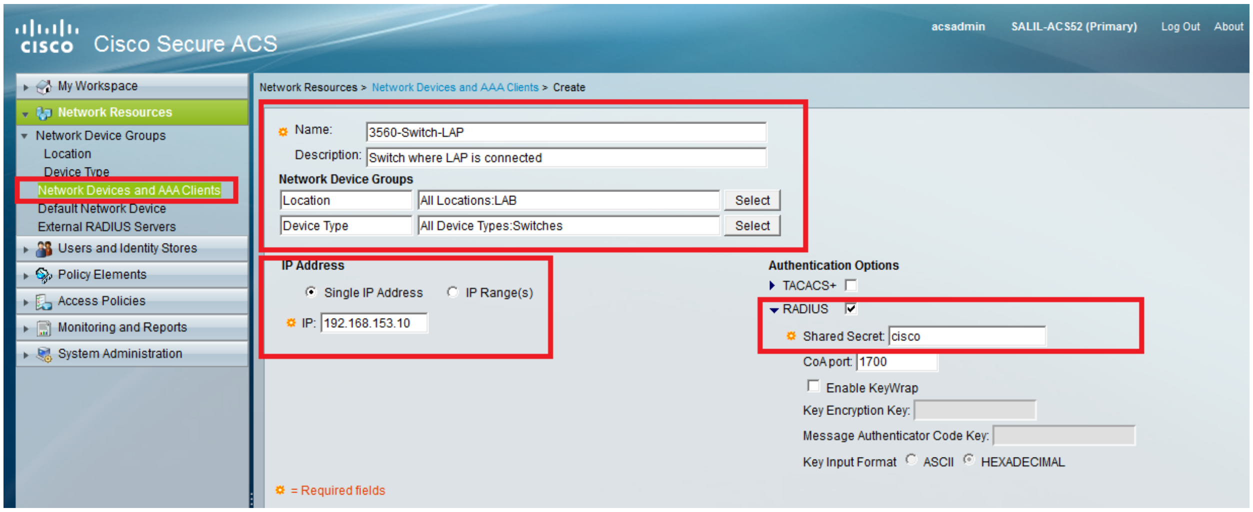
= Required fields

7. Click Submit. Once completed it should look like :



	Name	Description
□	All Device Types	All Device Types
□	Switches	Switch where LAP is connected

8. Next, Network Resources > Network Devices and AAA Clients.
9. Click Create and fill in the details as below.



Network Resources > Network Devices and AAA Clients > Create

Name: 3560-Switch-LAP

Description: Switch where LAP is connected

Network Device Groups

Location	All Locations:LAB	Select
Device Type	All Device Types:Switches	Select

IP Address

● Single IP Address ○ IP Range(s)

IP: 192.168.153.10

Authentication Options

TACACS+ □

RADIUS ☑

Shared Secret: cisco

CoA port: 1700

□ Enable KeyWrap

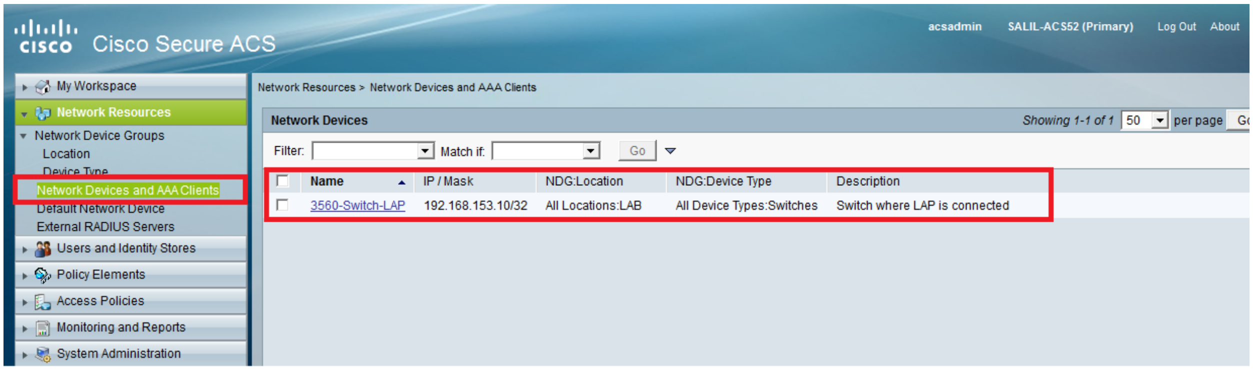
Key Encryption Key:

Message Authenticator Code Key:

Key Input Format ○ ASCII ● HEXADECIMAL

= Required fields

10. Click Submit. Page should look like below.



Network Resources > Network Devices and AAA Clients

Network Devices — Showing 1-1 of 1 — 50 per page

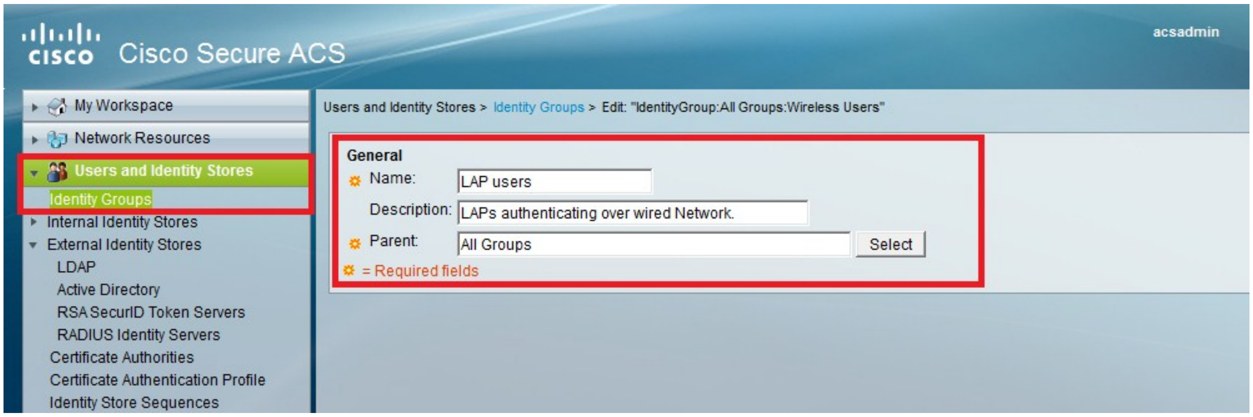
Filter: Match if: Go

□	Name	IP / Mask	NDG:Location	NDG:Device Type	Description
□	3560-Switch-LAP	192.168.153.10/32	All Locations:LAB	All Device Types:Switches	Switch where LAP is connected

b) Configuring Users.

In this section, we will create user on ACS as what we configured previously. We will assign user to a group called “LAP users”.

Click Users and Identity Stores →Identity Groups → Create



Users and Identity Stores > Identity Groups > Edit: "IdentityGroup:All Groups:Wireless Users"

General

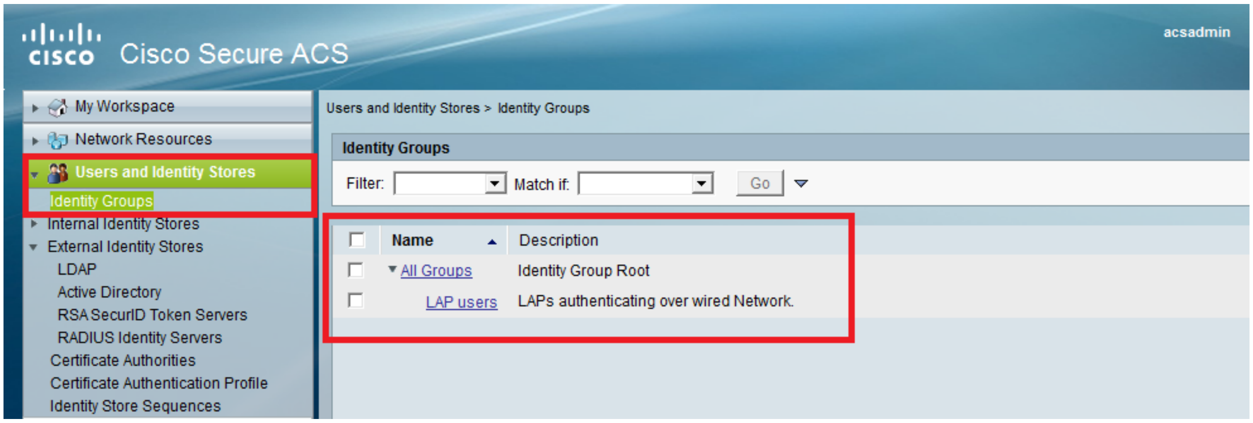
Name: LAP users

Description: LAPs authenticating over wired Network.

Parent: All Groups Select

= Required fields

1. Once you click submit the page should look like as :



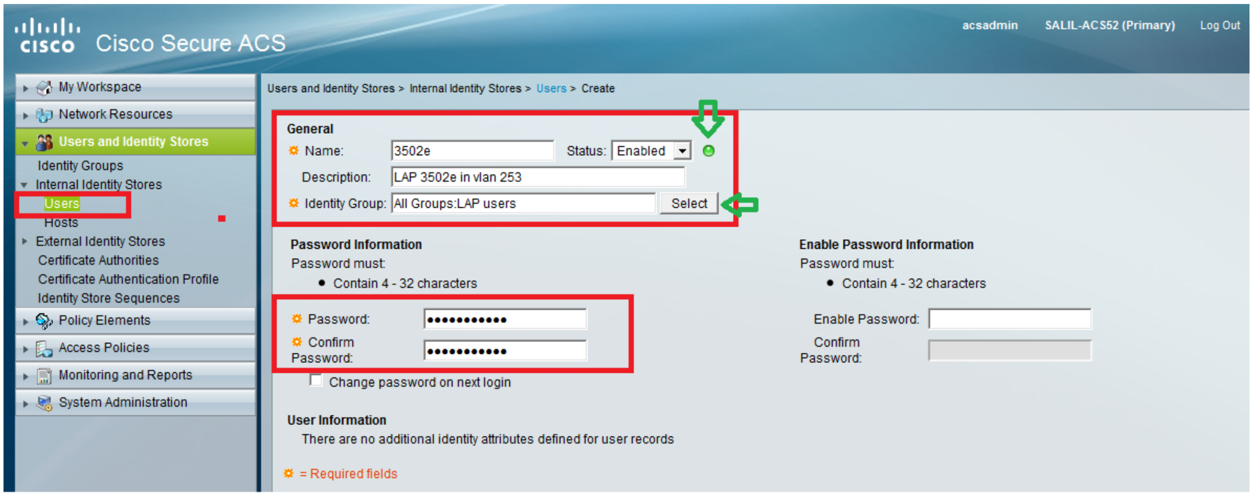
Users and Identity Stores > Identity Groups

Identity Groups

Filter: Match if:

□	Name	Description
□	All Groups	Identity Group Root
□	LAP users	LAPs authenticating over wired Network.

2. Next step is to create 3502e and assign it to group “LAP users”.
3. Click Users and Identity Stores →Identity Groups → Users → Create



Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: 3502e Status: Enabled

Description: LAP 3502e in vlan 253

Identity Group: All Groups:LAP users

Password Information

Password must:

- Contain 4 - 32 characters

Password: •••••••••••

Confirm Password: •••••••••••

□ Change password on next login

Enable Password Information

Password must:

- Contain 4 - 32 characters

Enable Password:

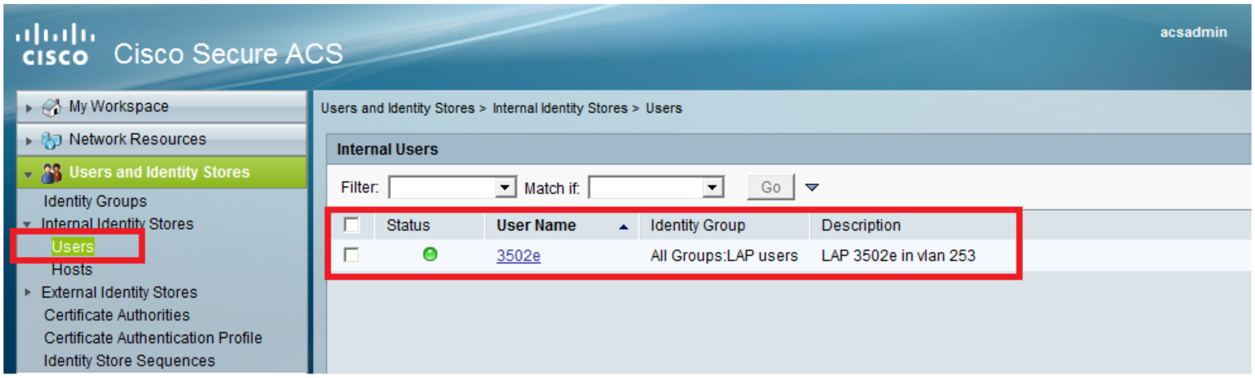
Confirm Password:

User Information

There are no additional identity attributes defined for user records

= Required fields

4. Finally, the page should look like :



Users and Identity Stores > Internal Identity Stores > Users

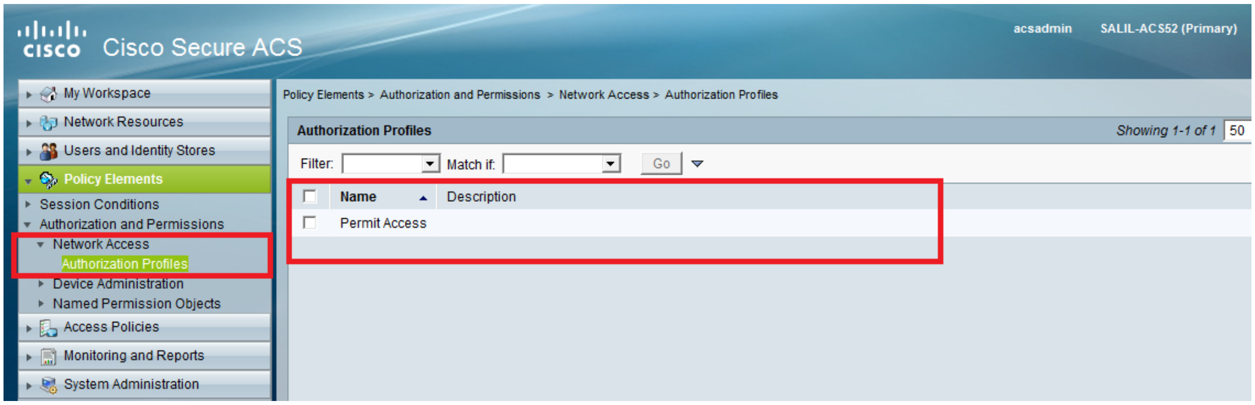
Internal Users

Filter: Match if:

□	Status	User Name	Identity Group	Description
□	●	3502e	All Groups:LAP users	LAP 3502e in vlan 253

c) Defining Policy Elements.

Verify Permit Access is set.

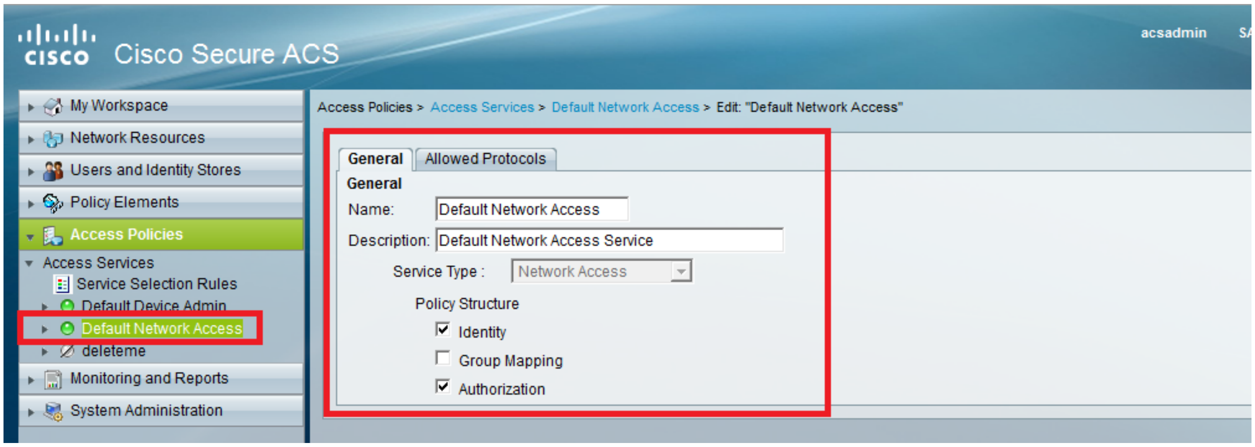


	Name	Description
□	Permit Access	

d) Applying Access Policies

In this section we will select EAP-FAST as the Authentication method used for LAPs to authenticate. We will then create rules based of above steps.

1. Access Policies→Access Services→Default Network Access→Edit: "Default Network Access"



General

Name: Default Network Access

Description: Default Network Access Service

Service Type : Network Access

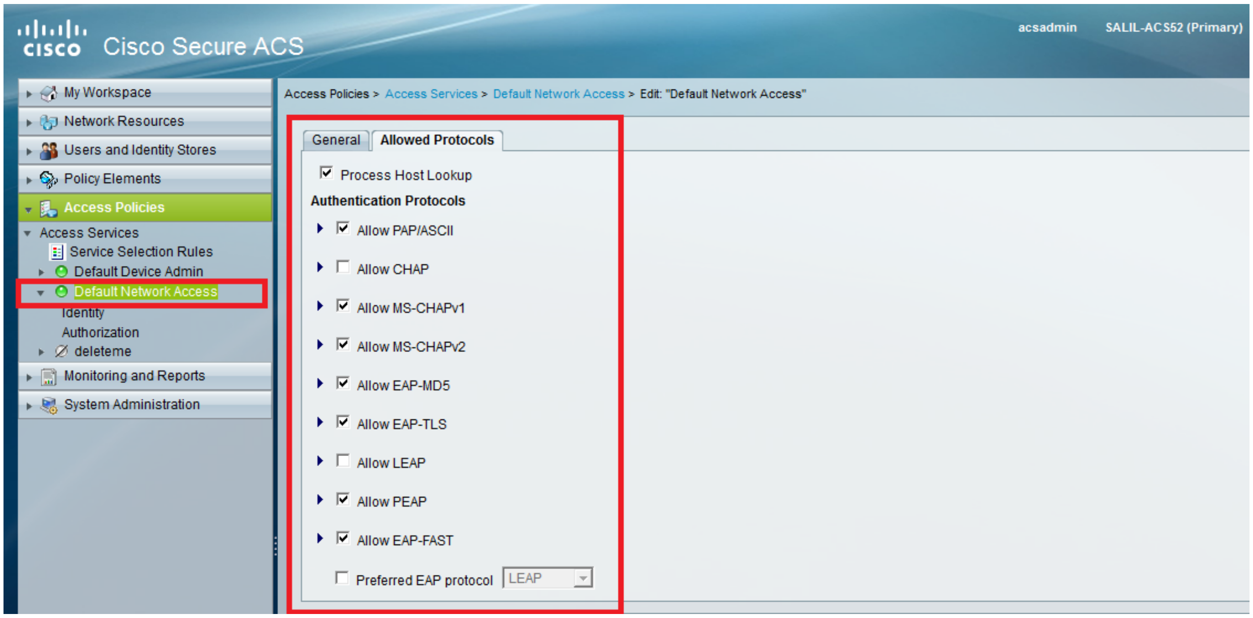
Policy Structure

☑ Identity

☐ Group Mapping

☑ Authorization

2. Make sure you have enabled EAP-FAST and anonymous in-Band PAC provisioning.



Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"

☑ Process Host Lookup

Authentication Protocols

☑ Allow PAP/ASCII

□ Allow CHAP

☑ Allow MS-CHAPv1

☑ Allow MS-CHAPv2

☑ Allow EAP-MD5

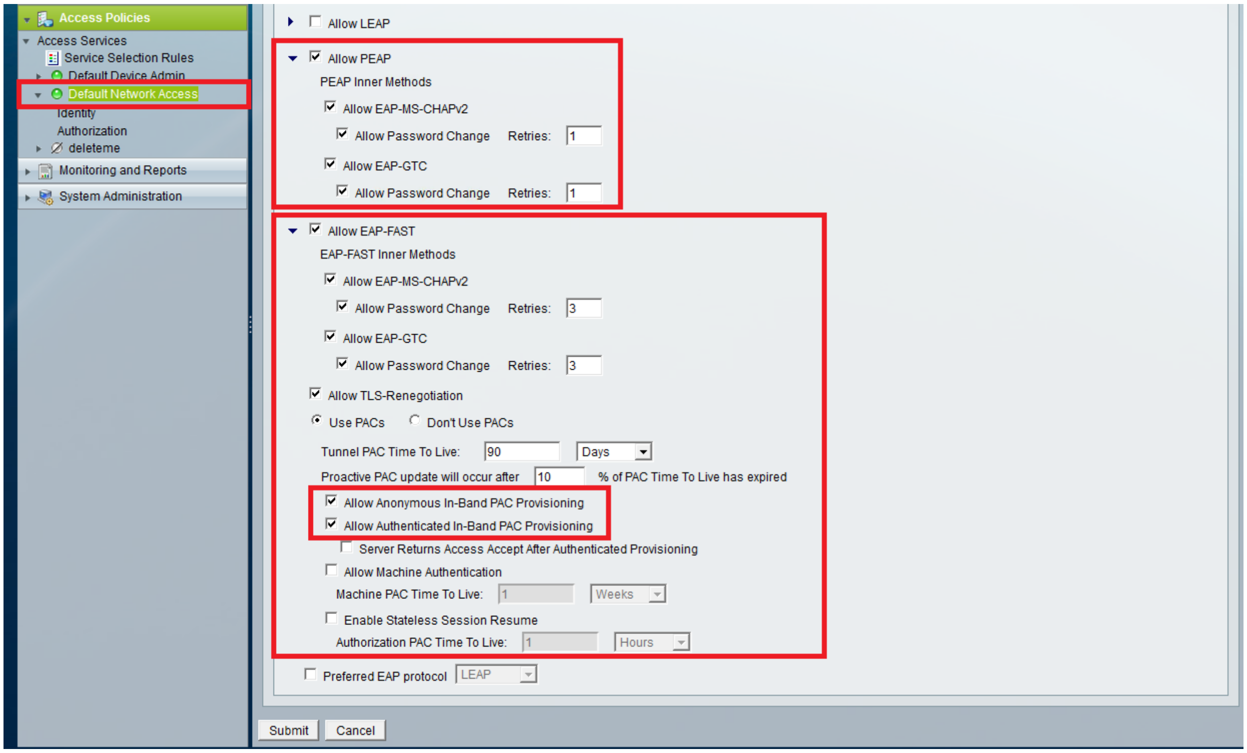
☑ Allow EAP-TLS

□ Allow LEAP

☑ Allow PEAP

☑ Allow EAP-FAST

□ Preferred EAP protocol LEAP



□ Allow LEAP

☑ Allow PEAP

PEAP Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries: 1

☑ Allow EAP-GTC

☑ Allow Password Change Retries: 1

☑ Allow EAP-FAST

EAP-FAST Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries: 3

☑ Allow EAP-GTC

☑ Allow Password Change Retries: 3

☑ Allow TLS-Renegotiation

● Use PACs ○ Don't Use PACs

Tunnel PAC Time To Live: 90 Days

Proactive PAC update will occur after 10 % of PAC Time To Live has expired

☑ Allow Anonymous In-Band PAC Provisioning

☑ Allow Authenticated In-Band PAC Provisioning

□ Server Returns Access Accept After Authenticated Provisioning

□ Allow Machine Authentication

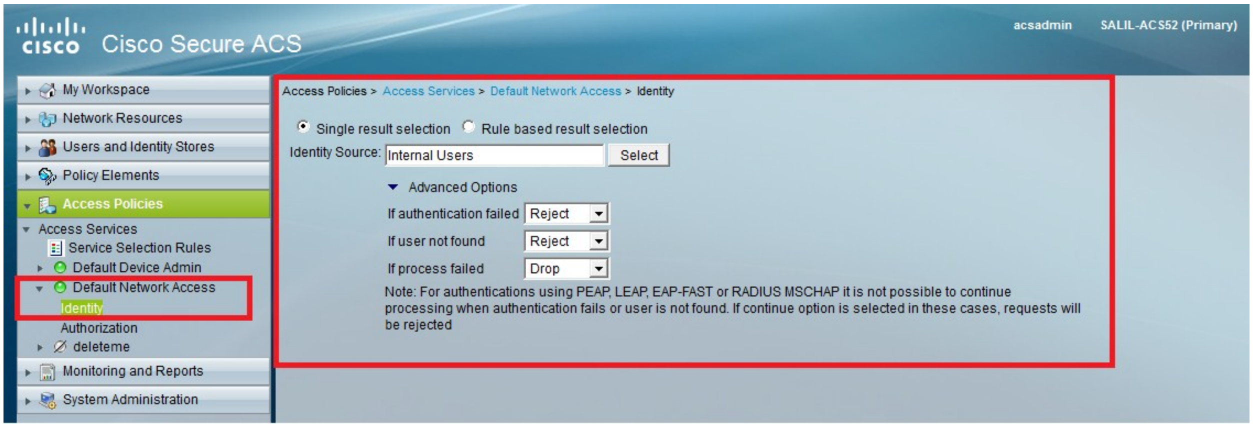
Machine PAC Time To Live: 1 Weeks

□ Enable Stateless Session Resume

Authorization PAC Time To Live: 1 Hours

□ Preferred EAP protocol LEAP

3. Click Submit.
4. Verify Identity group that you have selected. In our case we will use Internal Users which we created on ACS and then save changes.



Access Policies > Access Services > Default Network Access > Identity

● Single result selection ○ Rule based result selection

Identity Source: Internal Users Select

Advanced Options

If authentication failed: Reject

If user not found: Reject

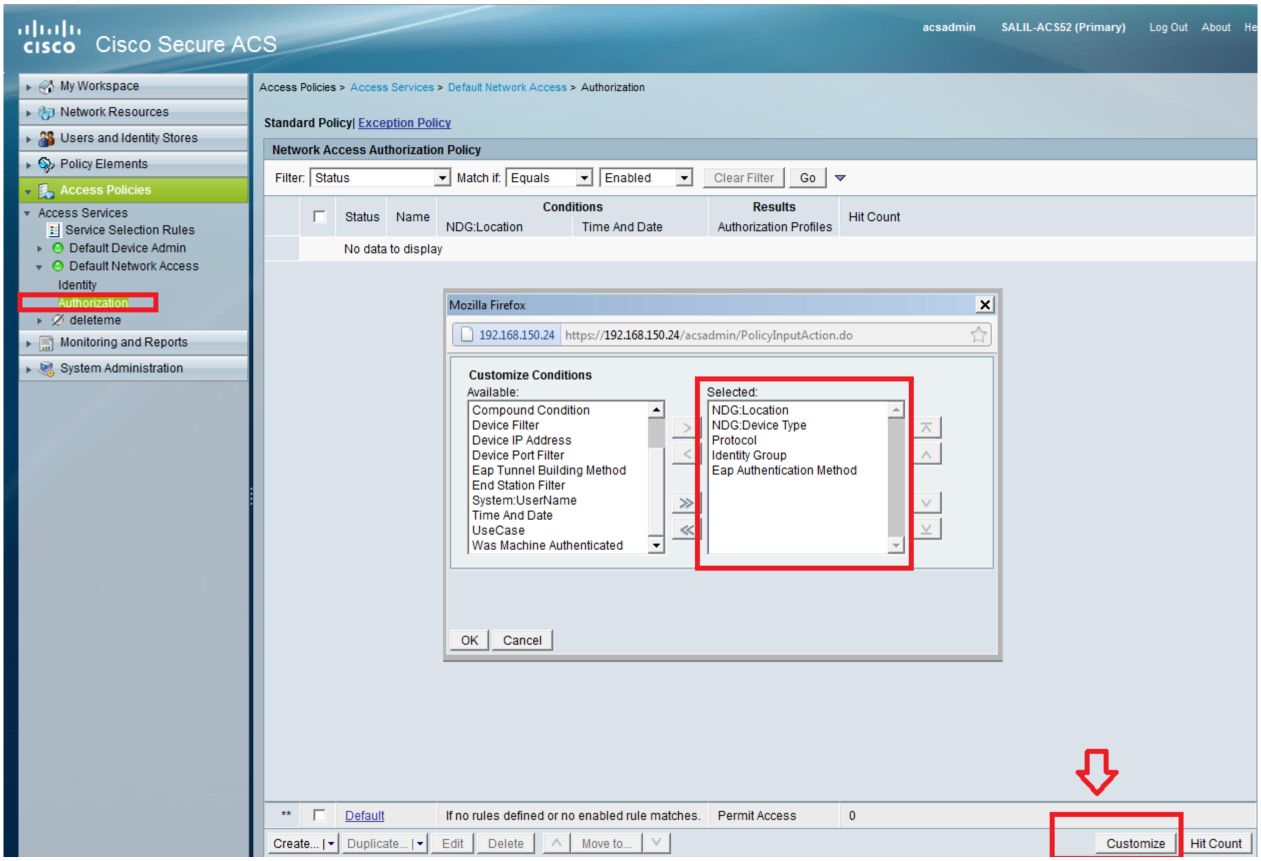
If process failed: Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected

5. Next verify the Authorization Profile under :

   Access Policies →Access Services →Default Network Access →Authorization.

   You can customize under what conditions you will allow user access to network and what authorization profile (attributes) you will pass once authenticated. This granularity is only available in ACS5.x . In our example we have selected Location,Device Type, protocol, identity Group, EAP Authentication Method.



Access Policies > Access Services > Default Network Access > Authorization

Standard Policy| Exception Policy

Network Access Authorization Policy

Filter: Status Match if: Equals Enabled

□	Status	Name	Conditions NDG:Location	 Time And Date	Results Authorization Profiles	Hit Count
		No data to display				
** □		Default	If no rules defined or no enabled rule matches.		Permit Access	0

Mozilla Firefox

192.168.150.24 https://192.168.150.24/acsadmin/PolicyInputAction.do

Customize Conditions

Available:

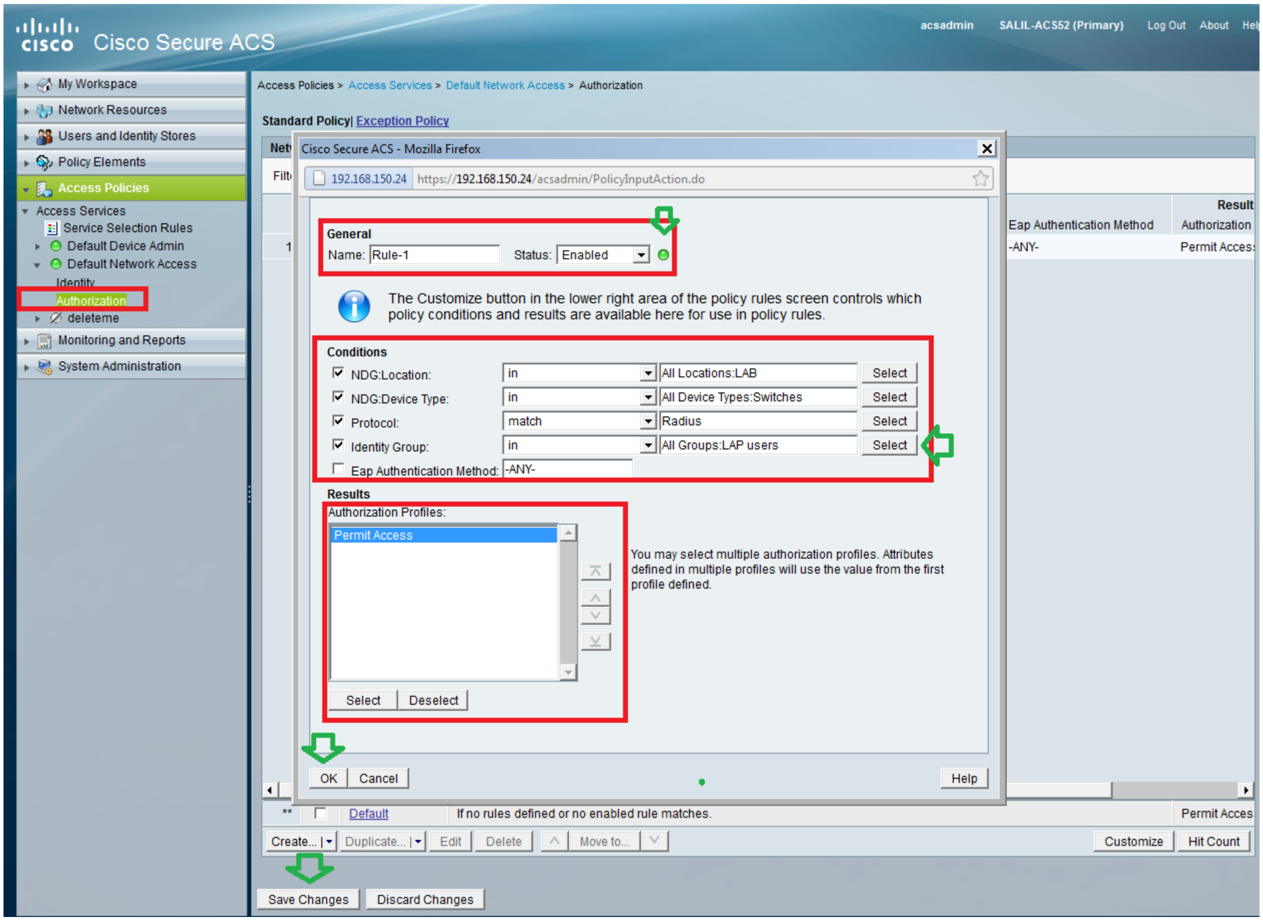
Compound Condition
Device Filter
Device IP Address
Device Port Filter
Eap Tunnel Building Method
End Station Filter
System:UserName
Time And Date
UseCase
Was Machine Authenticated

Selected:

NDG:Location
NDG:Device Type
Protocol
Identity Group
Eap Authentication Method

OK Cancel

6. Click OK in the window. Save Changes.
7. Next step is to create Rule. If no Rules are defined LAP is allowed access without any conditions.
8. Click Create → Rule -1. This Rule is for users in group "LAP users"



Access Policies > Access Services > Default Network Access > Authorization

Standard Policy| Exception Policy

Cisco Secure ACS - Mozilla Firefox

192.168.150.24 https://192.168.150.24/acsadmin/PolicyInputAction.do

General

Name: Rule-1 Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ NDG:Location:	in	All Locations:LAB	Select
☑ NDG:Device Type:	in	All Device Types:Switches	Select
☑ Protocol:	match	Radius	Select
☑ Identity Group:	in	All Groups:LAP users	Select
☐ Eap Authentication Method:	-ANY-		

Results

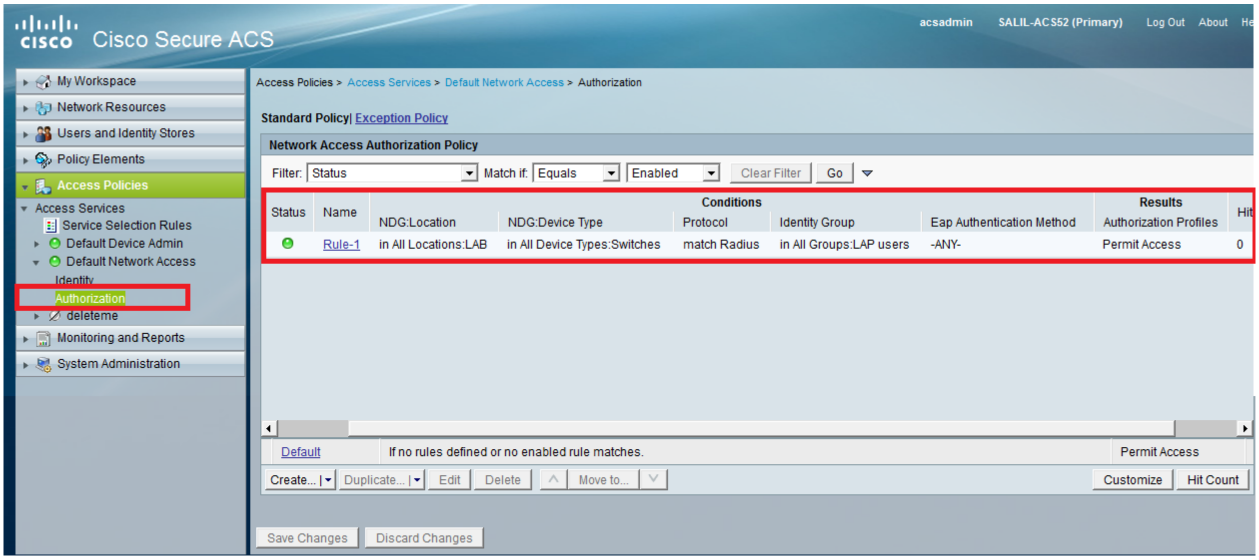
Authorization Profiles:

Permit Access

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

		Eap Authentication Method	Result Authorization
1		-ANY-	Permit Acces
**	☐ Default	If no rules defined or no enabled rule matches.	Permit Acces

9. Save changes. The page should look like as below. If you want users not matching the conditions to be denied then edit the default rule to say "deny access".



Access Policies > Access Services > Default Network Access > Authorization

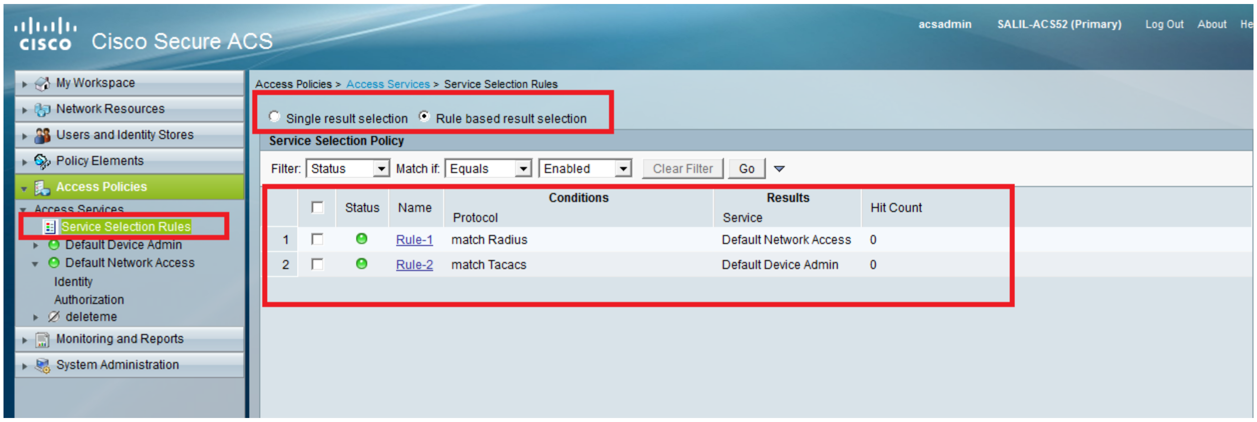
Standard Policy| Exception Policy

Network Access Authorization Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

Status	Name	Conditions					Results	Hit
		NDG:Location	NDG:Device Type	Protocol	Identity Group	Eap Authentication Method	Authorization Profiles	
●	Rule-1	in All Locations:LAB	in All Device Types:Switches	match Radius	in All Groups:LAP users	-ANY-	Permit Access	0
	Default	If no rules defined or no enabled rule matches.					Permit Access	

10. Last step is to do define Service Selection Rules. Use this page to configure a simple or rule-based policy to determine which service to apply to incoming requests. We will have the following rule based in our example.



Access Policies > Access Services > Service Selection Rules

○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

	☐	Status	Name	Conditions	Results	Hit Count
				Protocol	Service	
1	☐	●	Rule-1	match Radius	Default Network Access	0
2	☐	●	Rule-2	match Tacacs	Default Device Admin	0

Verification

Once 802.1x is enabled on the switch port, all the traffic except the 802.1x traffic is blocked through the port. The LAP, which is already registered to the WLC, gets disassociated. Only after a successful 802.1x authentication is other traffic allowed to pass through. Successful registration of the LAP to the WLC after the 802.1x is enabled on the switch indicates that the LAP authentication is successful.

AP console:

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
192.168.75.44:5247
```

!--- AP disconnects upon adding dot1x information in the gig0/11

```
*Jan 29 09:10:30.104: %WIDS-5-DISABLED: IDS Signature is removed and disabled.
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
administratively down
*Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset
Translating "CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25)

*Jan 29 09:10:36.203:  status of voice_diag_test from WLC is false
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0
authenticated [EAP-FAST]
*Jan 29 09:11:08.947: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0
assigned DHCP address 192.168.153.106, mask 255.255.255.0, hostname 3502e
```

!---Authentication is successful and AP gets an IP.

```
Translating "CISCO-CAPWAP-CONTROLLER.Wlab"...domain server (192.168.150.25)
*Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip:
192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.000: %CAPWAP-5-CHANGED: CAPWAP changed state to
*Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully
peer_ip: 192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.578: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44
*Jan 29 09:11:37.578: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN
*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
 wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller 5508-3
```

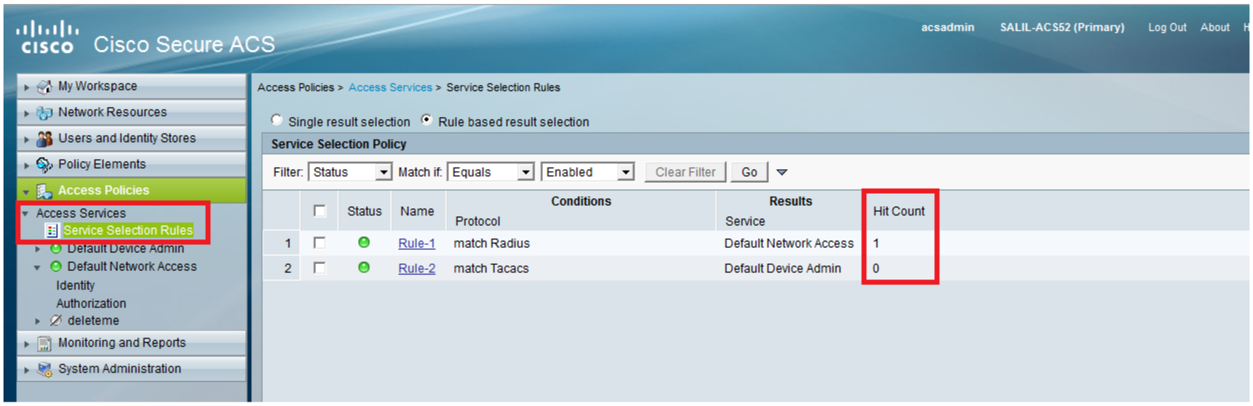
```
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake. Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS keys are plumbed successfully.

*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled
```

!---AP joins the 5508-3 WLC .

ACS Logs:

1) View the Hit counts:

If you are checking logs within 15 minutes of authentication, make sure you refresh the HIT count. On the same page, at the bottom you have a tab for “Hit Count”.



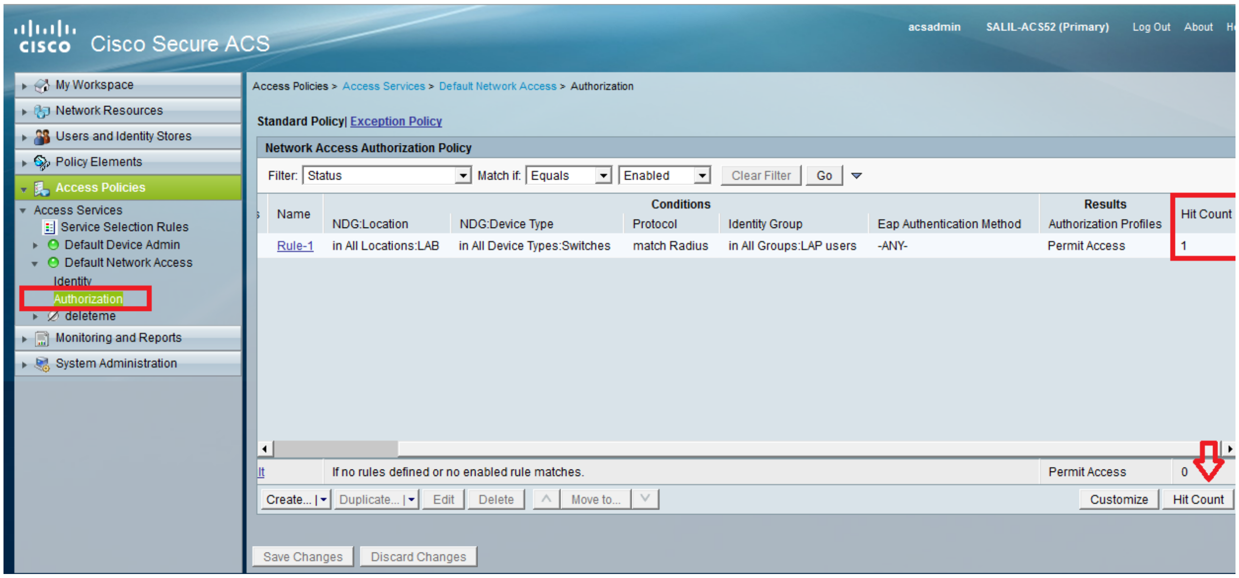
Access Policies > Access Services > Service Selection Rules

○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

	□	Status	Name	Conditions Protocol	Results Service	Hit Count
1	□	●	Rule-1	match Radius	Default Network Access	1
2	□	●	Rule-2	match Tacacs	Default Device Admin	0



Access Policies > Access Services > Default Network Access > Authorization

Standard Policy| Exception Policy

Network Access Authorization Policy

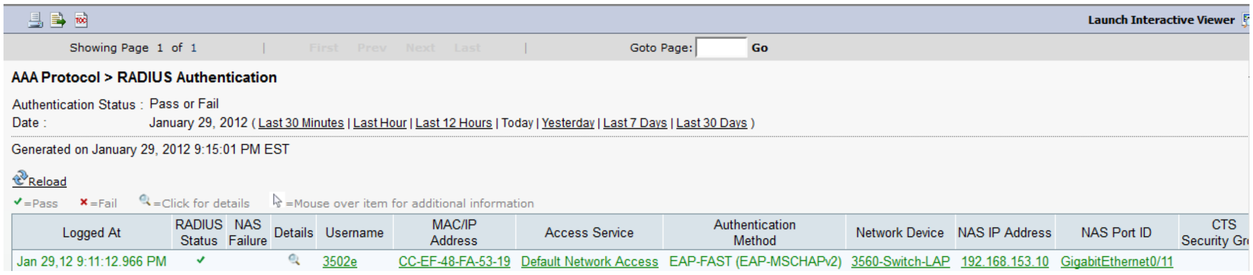
Filter: Status Match if: Equals Enabled Clear Filter Go

Name	Conditions					Results	Hit Count
	NDG:Location	NDG:Device Type	Protocol	Identity Group	Eap Authentication Method	Authorization Profiles	
Rule-1	in All Locations:LAB	in All Device Types:Switches	match Radius	in All Groups:LAP users	-ANY-	Permit Access	1

If no rules defined or no enabled rule matches. Permit Access 0

Create... | Duplicate... | Edit | Delete | Move to... | Customize | Hit Count
Save Changes | Discard Changes

2) Monitoring and Reports → New pop up window appears → Authentications –Radius – Today. You can also Click details to verify which Service selection rule was applied.


Launch Interactive Viewer
Showing Page 1 of 1 | First Prev Next Last | Goto Page: Go
Reload
✓=Pass ✗=Fail 🔍=Click for details =Mouse over item for additional information

AAA Protocol > RADIUS Authentication

Authentication Status : Pass or Fail
Date : January 29, 2012 (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on January 29, 2012 9:15:01 PM EST

Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Gr
Jan 29,12 9:11:12.966 PM	✓		🔍	3502e	CC-EF-48-FA-53-19	Default Network Access	EAP-FAST (EAP-MSCHAPv2)	3560-Switch-LAP	192.168.153.10	GigabitEthernet0/11	