Introduction

This document explains how to configure the Wireless LAN controller (WLC) for Extensible Authentication Protocol (EAP) authentication with the use of an external 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.
- Microsoft Windows 7 Native Supplicant with Intel 6300-N Driver Version 14.3.
- 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

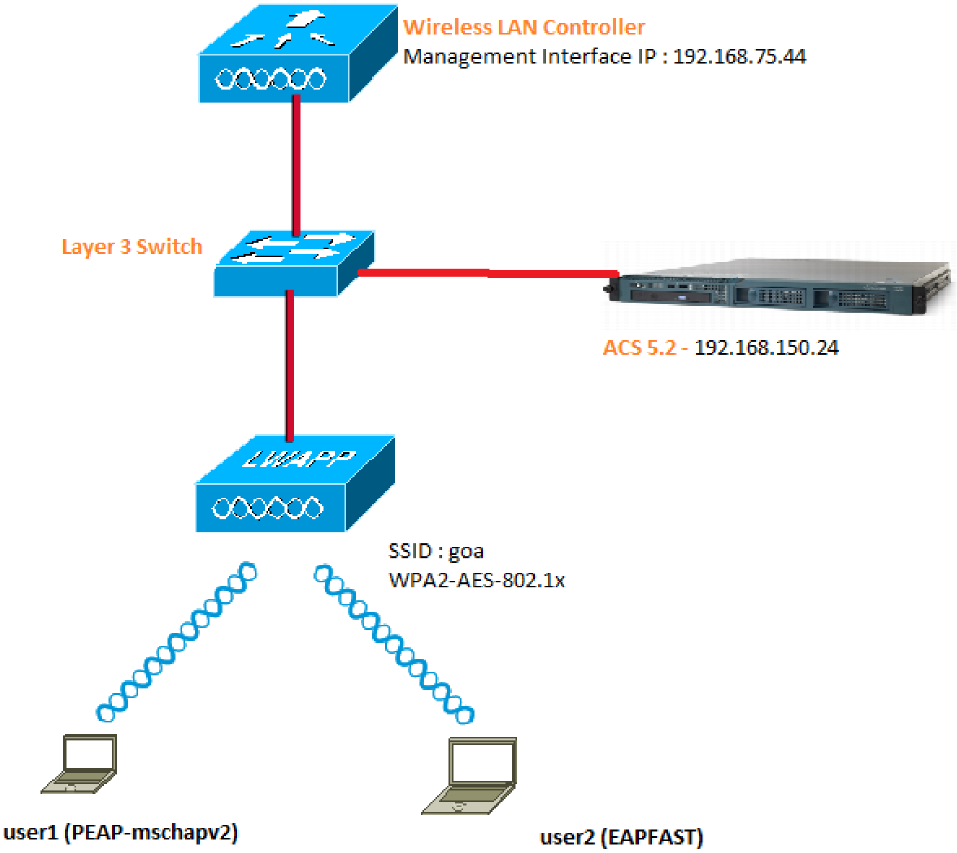
Refer to Cisco Technical Tips Conventions for more information on document conventions.

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:



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.
- VLAN 253 is used throughout this configuration. Both users connect to the same SSID "goa". However user1 is configured to authenticate using peap-mschapv2 and user2 using EAP-FAST.
- Users will be assigned in vlan 253.

VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.1
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. WLC Configuration
3. Wireless Client Utility Configuration

RADIUS Server Configuration

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.

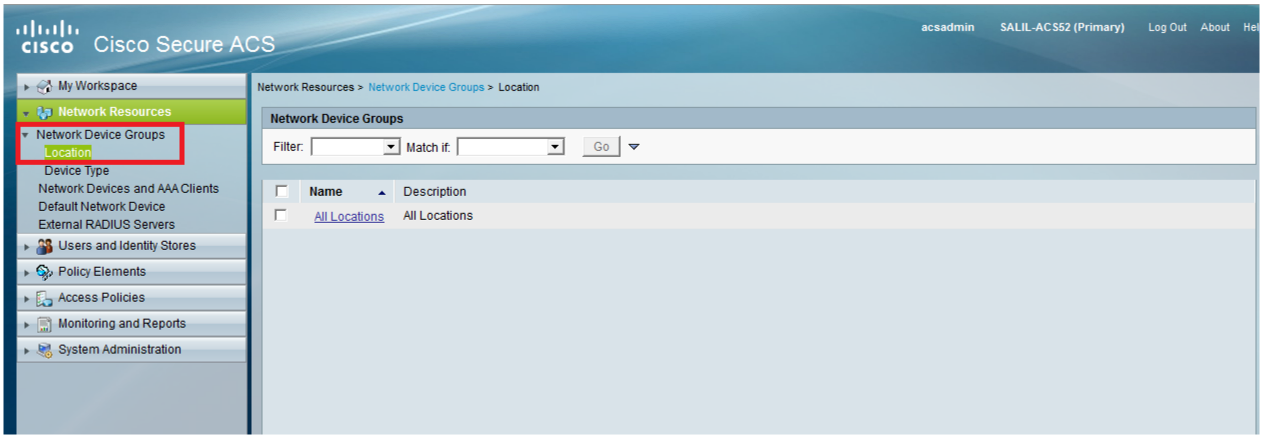
a) Configuring Network Resources.

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

This procedure explains how to add the WLC as a AAA client on the RADIUS server so that the WLC can pass the user credentials 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)

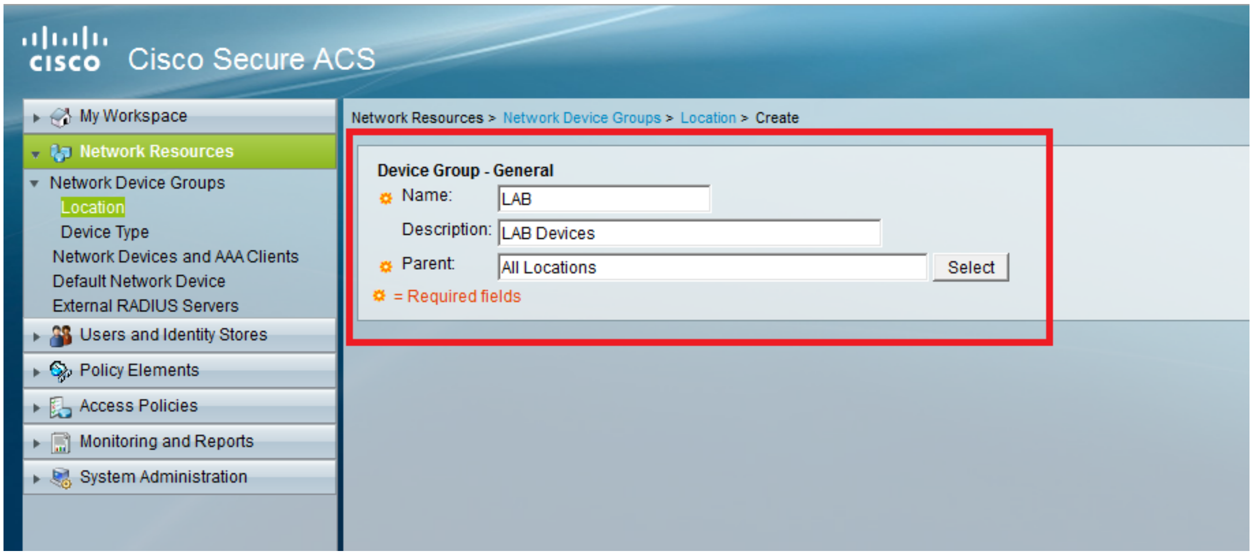


Network Resources > Network Device Groups > Location

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

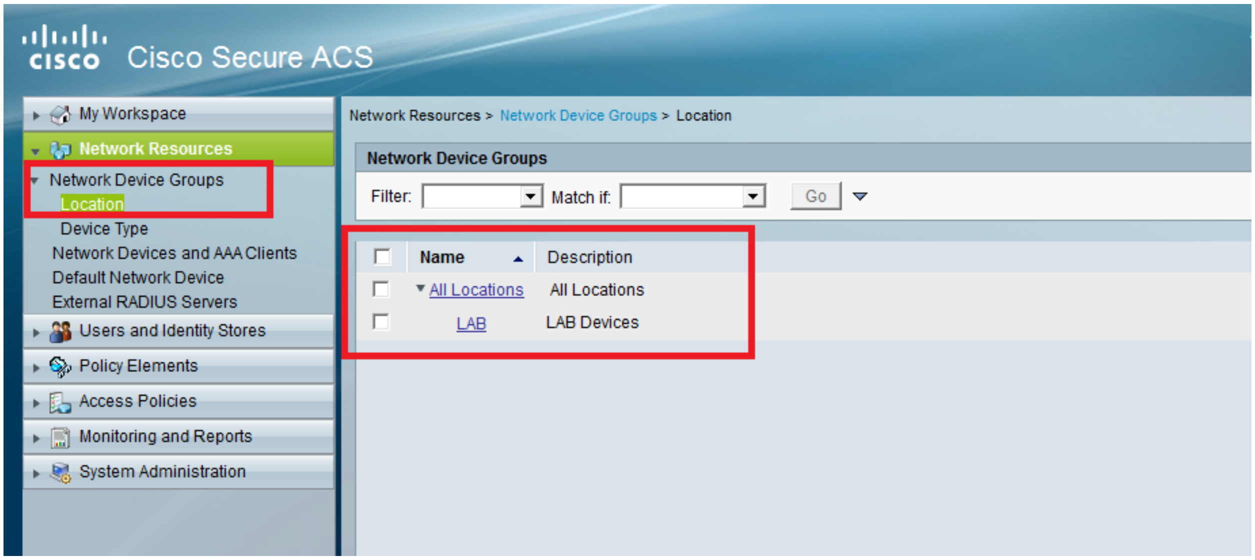
Name: LAB

Description: LAB Devices

Parent: All Locations

= Required fields

5. It should look like :

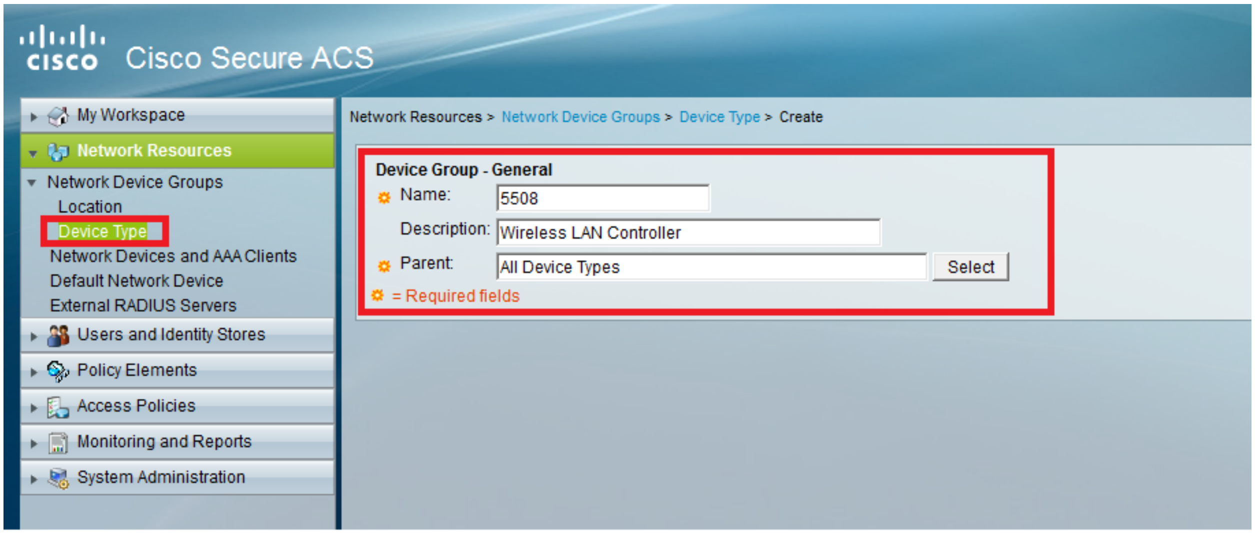


Network Resources > Network Device Groups > Location

Network Device Groups

□	Name	Description
□	All Locations	All Locations
□	LAB	LAB Devices

6. Now, Click Device Type -> Create



Network Resources > Network Device Groups > Device Type > Create

Device Group - General

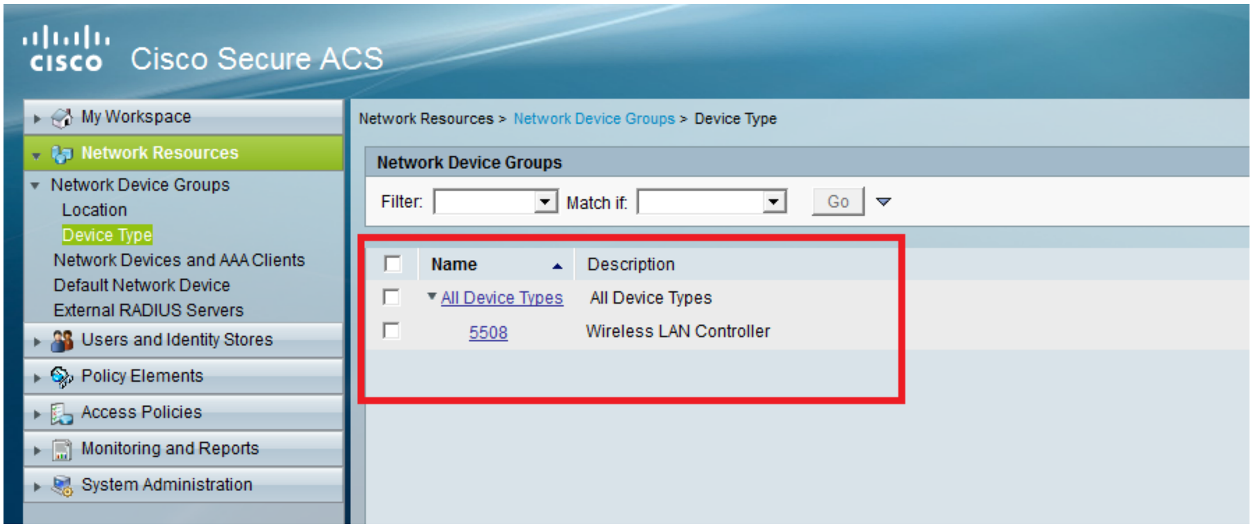
Name: 5508

Description: Wireless LAN Controller

Parent: All Device Types

= Required fields

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

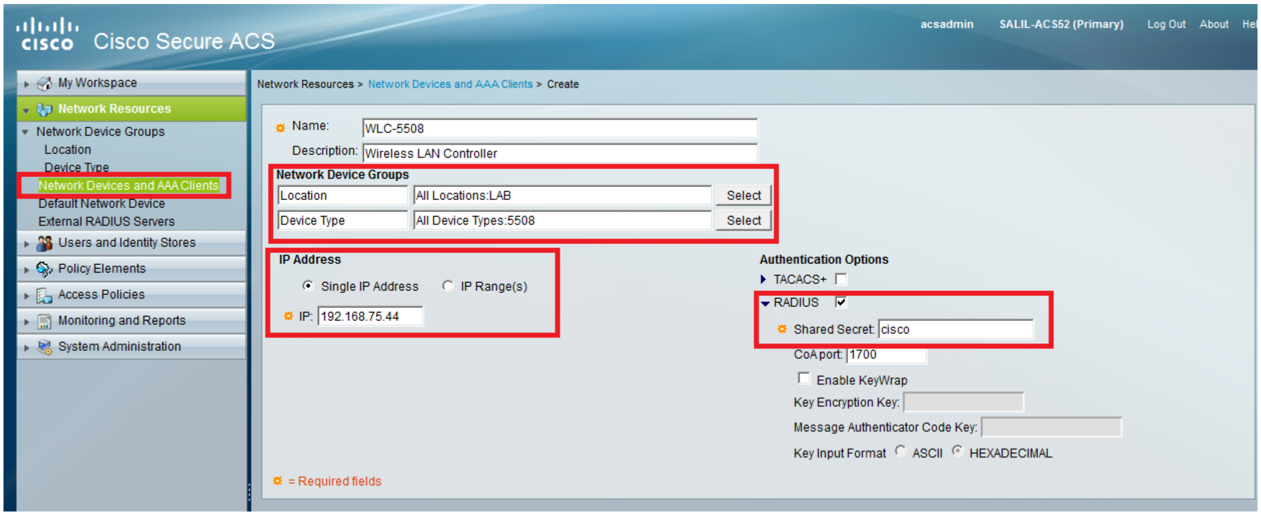


Network Resources > Network Device Groups > Device Type

Network Device Groups

□	Name ▲	Description
□	▾ All Device Types	All Device Types
□	5508	Wireless LAN Controller

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: WLC-5508
Description: Wireless LAN Controller

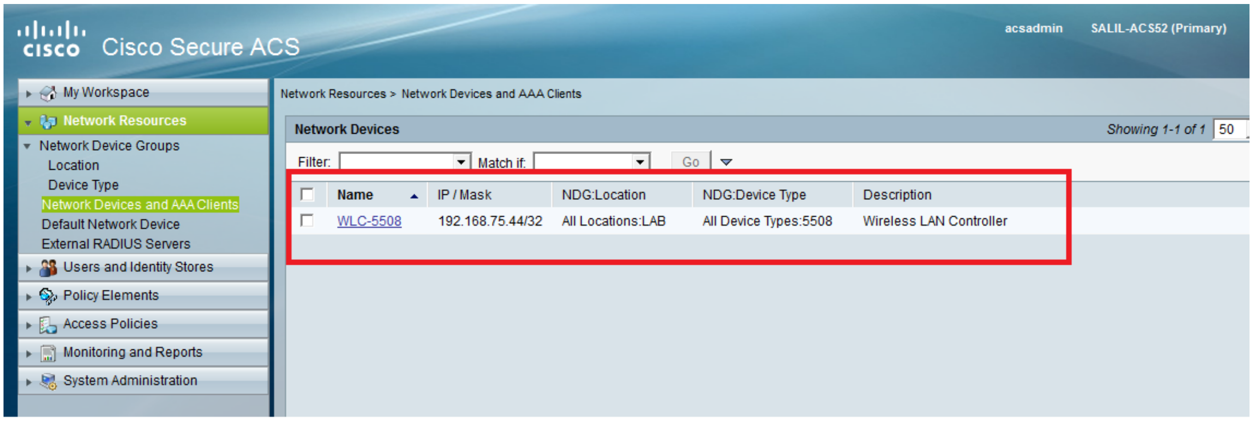
Network Device Groups
Location: All Locations:LAB
Device Type: All Device Types:5508

IP Address
● Single IP Address ○ IP Range(s)
IP: 192.168.75.44

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

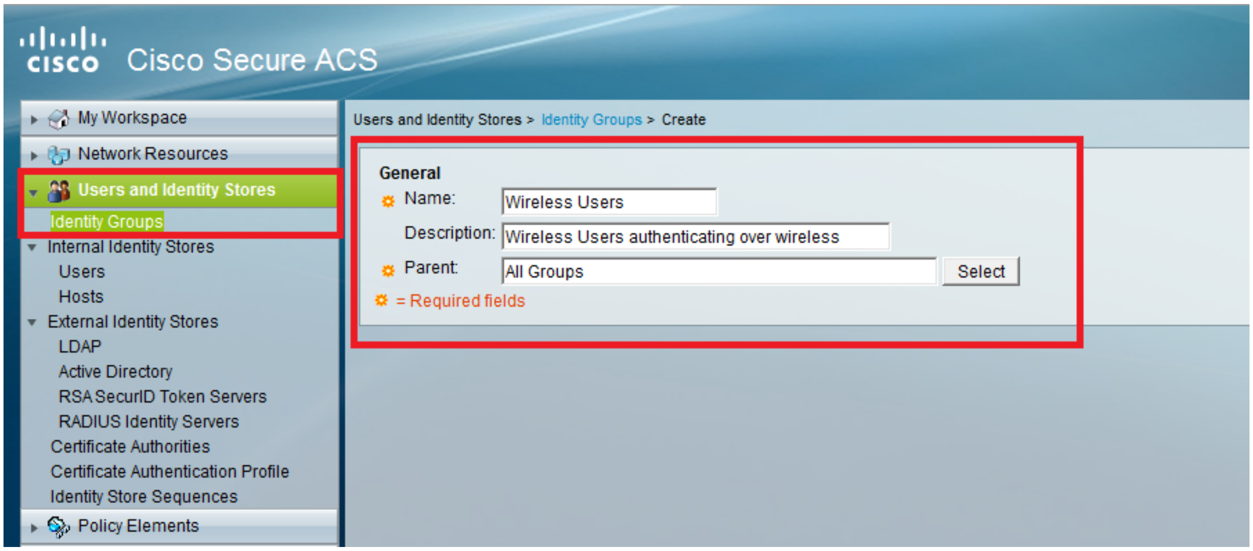
Network Devices — Showing 1-1 of 1 50

□	Name ▲	IP / Mask	NDG:Location	NDG:Device Type	Description
□	WLC-5508	192.168.75.44/32	All Locations:LAB	All Device Types:5508	Wireless LAN Controller

b) Configuring Users.

In this section, we will create local users on ACS. i.e user1 and user2. Both users are assigned in group called “Wireless Users”.

1. Click Users and Identity Stores →Identity Groups → Create



Users and Identity Stores > Identity Groups > Create

General

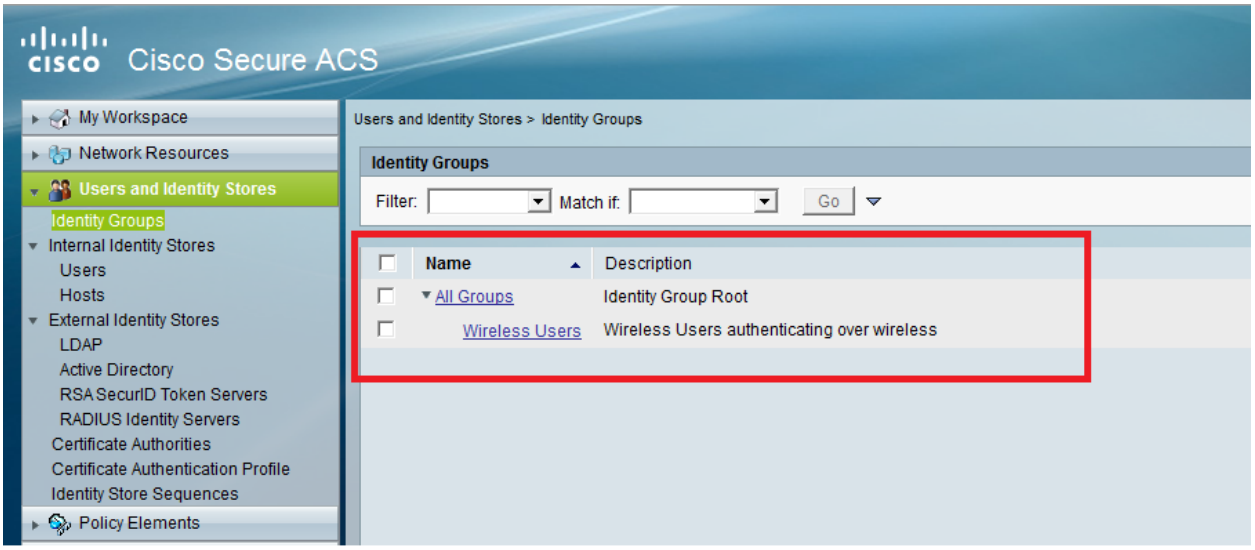
Name: Wireless Users

Description: Wireless Users authenticating over wireless

Parent: All Groups

= Required fields

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

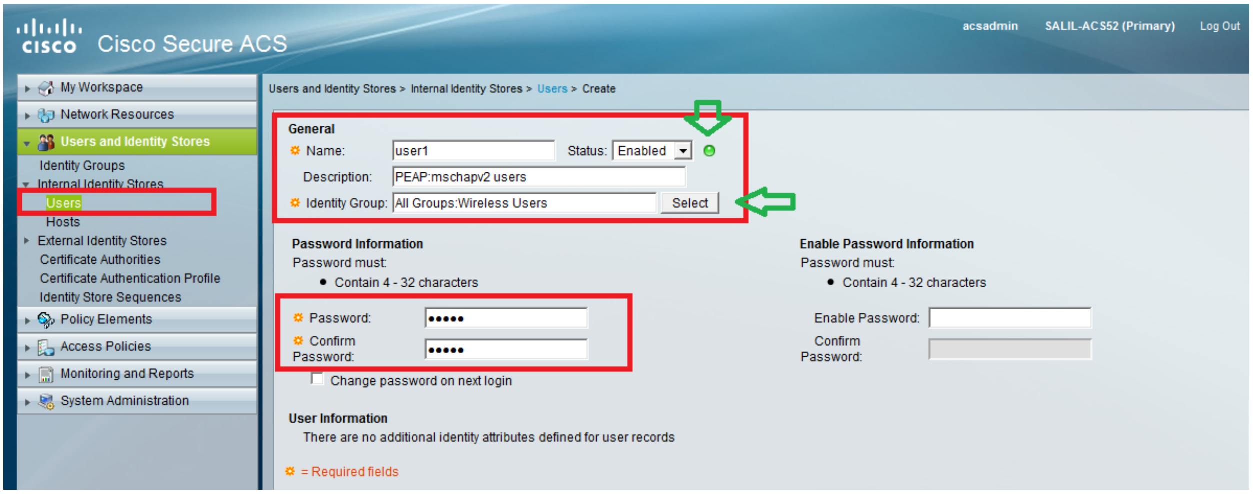


Users and Identity Stores > Identity Groups

Identity Groups

☐	Name	Description
☐	All Groups	Identity Group Root
☐	Wireless Users	Wireless Users authenticating over wireless

3. Next step is to create users user1 and user2 and assign it to group “Wireless Users”.
4. Click Users and Identity Stores →Identity Groups → Users → Create



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

General

Name: user1 Status: Enabled

Description: PEAP:mschapv2 users

Identity Group: All Groups:Wireless 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:

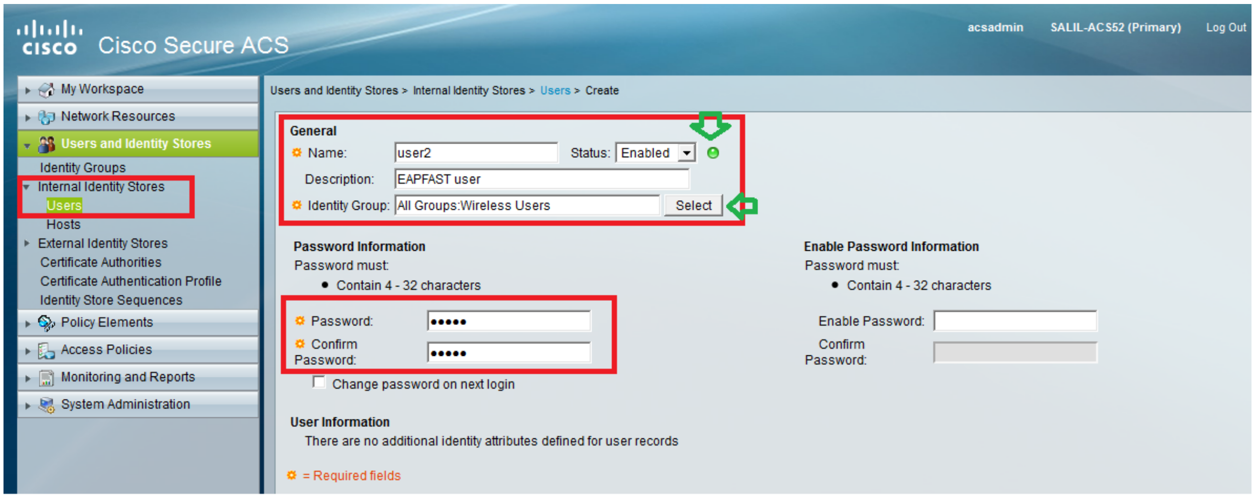
Confirm Password:

User Information

There are no additional identity attributes defined for user records

= Required fields

5. Similarly Create user2.



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

General

Name: user2 Status: Enabled

Description: EAPFAST user

Identity Group: All Groups:Wireless 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:

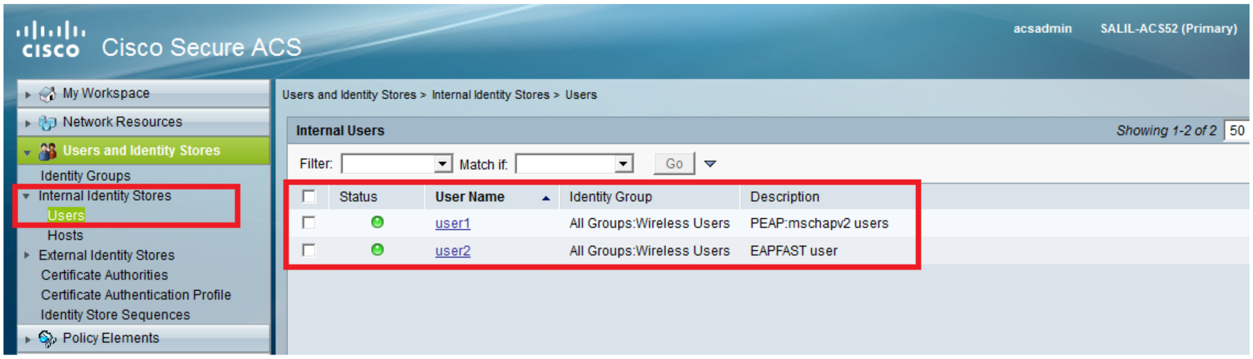
Confirm Password:

User Information

There are no additional identity attributes defined for user records

= Required fields

6. Finally, the page should look like :



Users and Identity Stores > Internal Identity Stores > Users

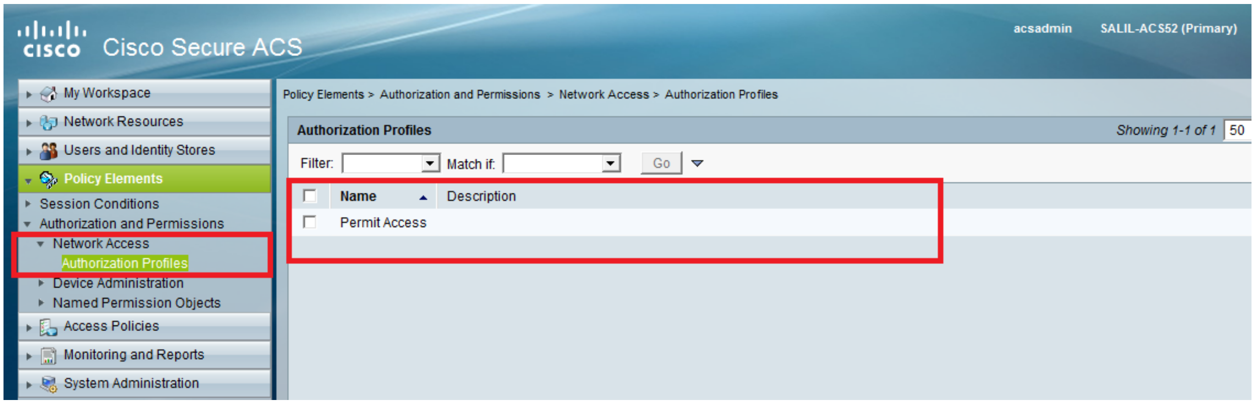
Internal Users

Showing 1-2 of 2 50

□	Status	User Name	Identity Group	Description
□	●	user1	All Groups:Wireless Users	PEAP:mschapv2 users
□	●	user2	All Groups:Wireless Users	EAPFAST user

c) Defining Policy Elements.

Verify Permit Access is set.



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles

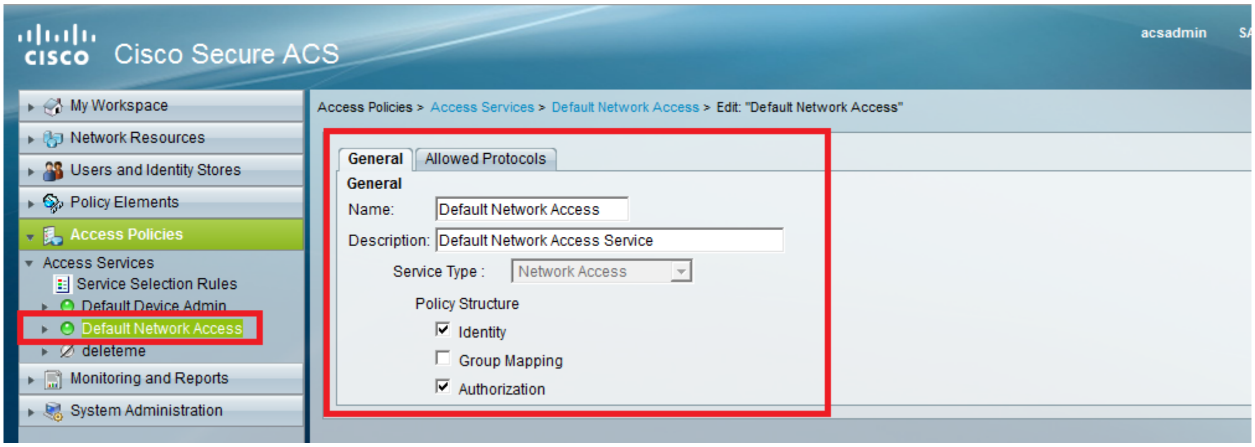
Authorization Profiles — Showing 1-1 of 1 — 50

	Name	Description
□	Permit Access	

d) Applying Access Policies

In this section we will select which Authentication methods are to be used and how the rules are to be configured. We will create rules based of above steps.

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



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

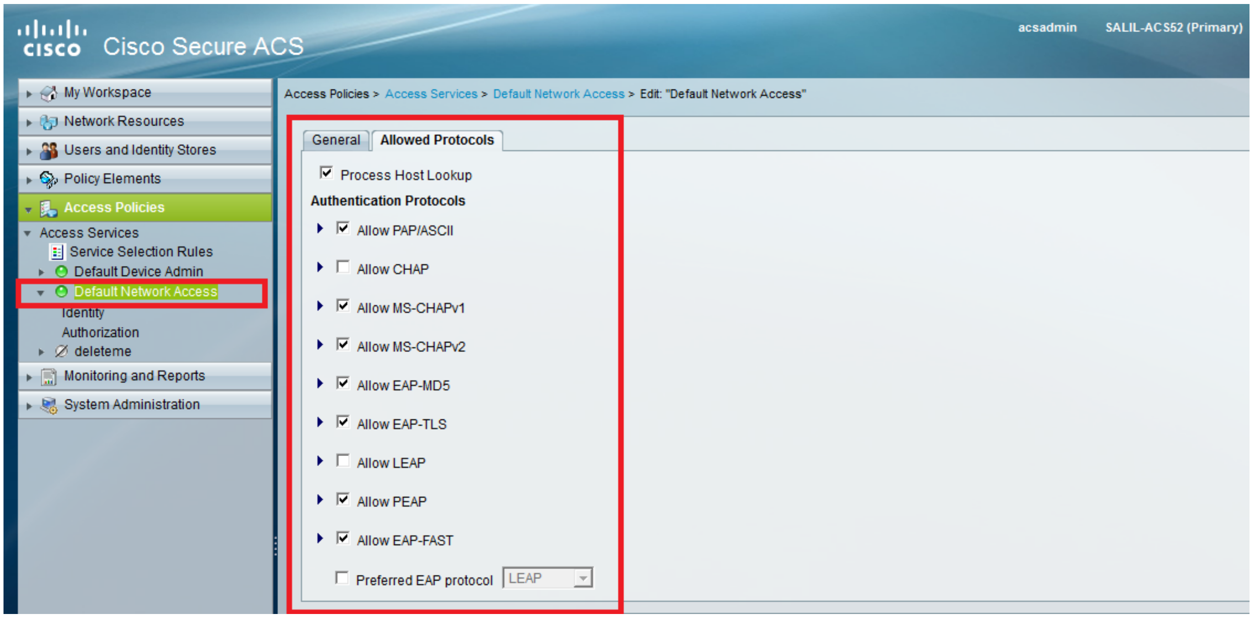
Policy Structure

☑ Identity

□ Group Mapping

☑ Authorization

2. You can Select which EAP method you would like wireless Clients to Authenticate. In our example, we will use PEAP- MSCHAP-V2 and EAP-FAST.



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

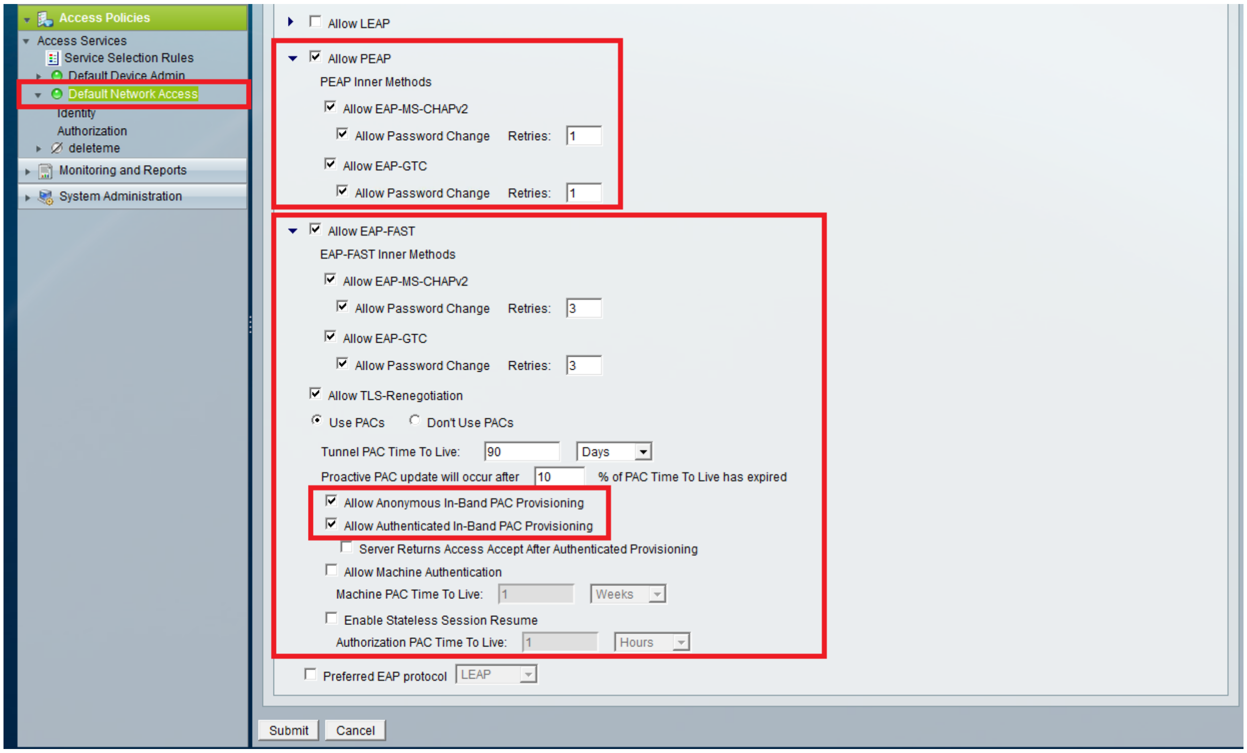
☑ Allow EAP-TLS

□ 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

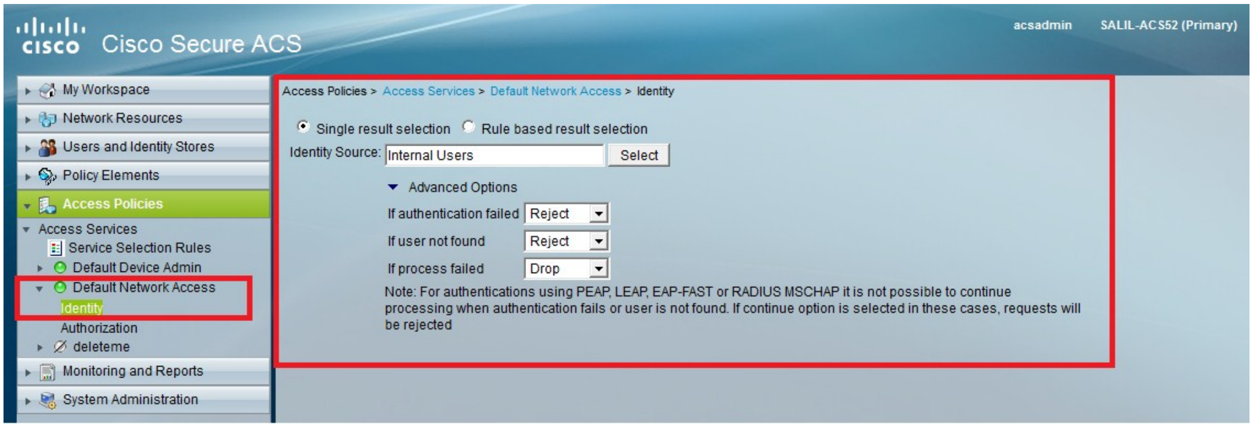
Machine PAC Time To Live: 1 Weeks

□ 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

Advanced Options

If authentication failed: Reject

If user not found: Reject

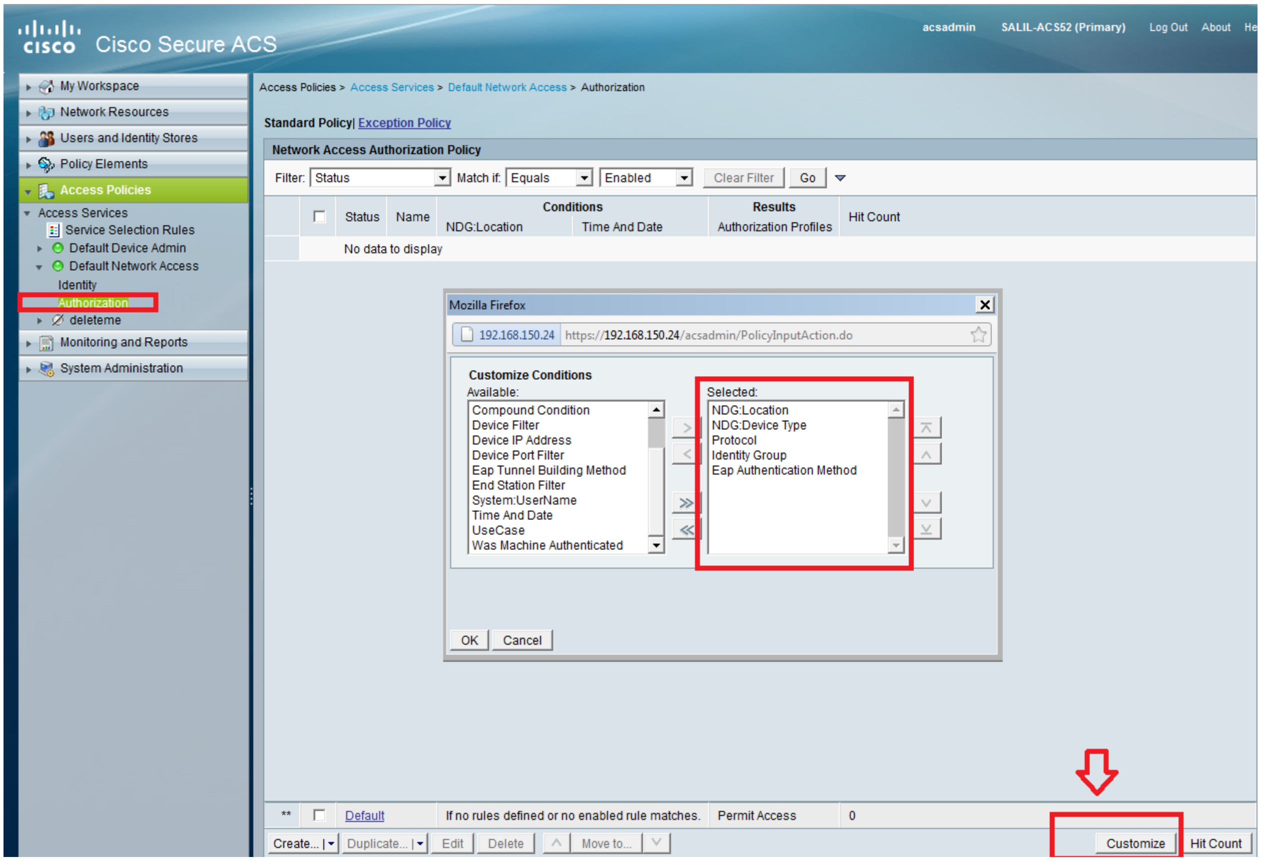
If process failed: Drop

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

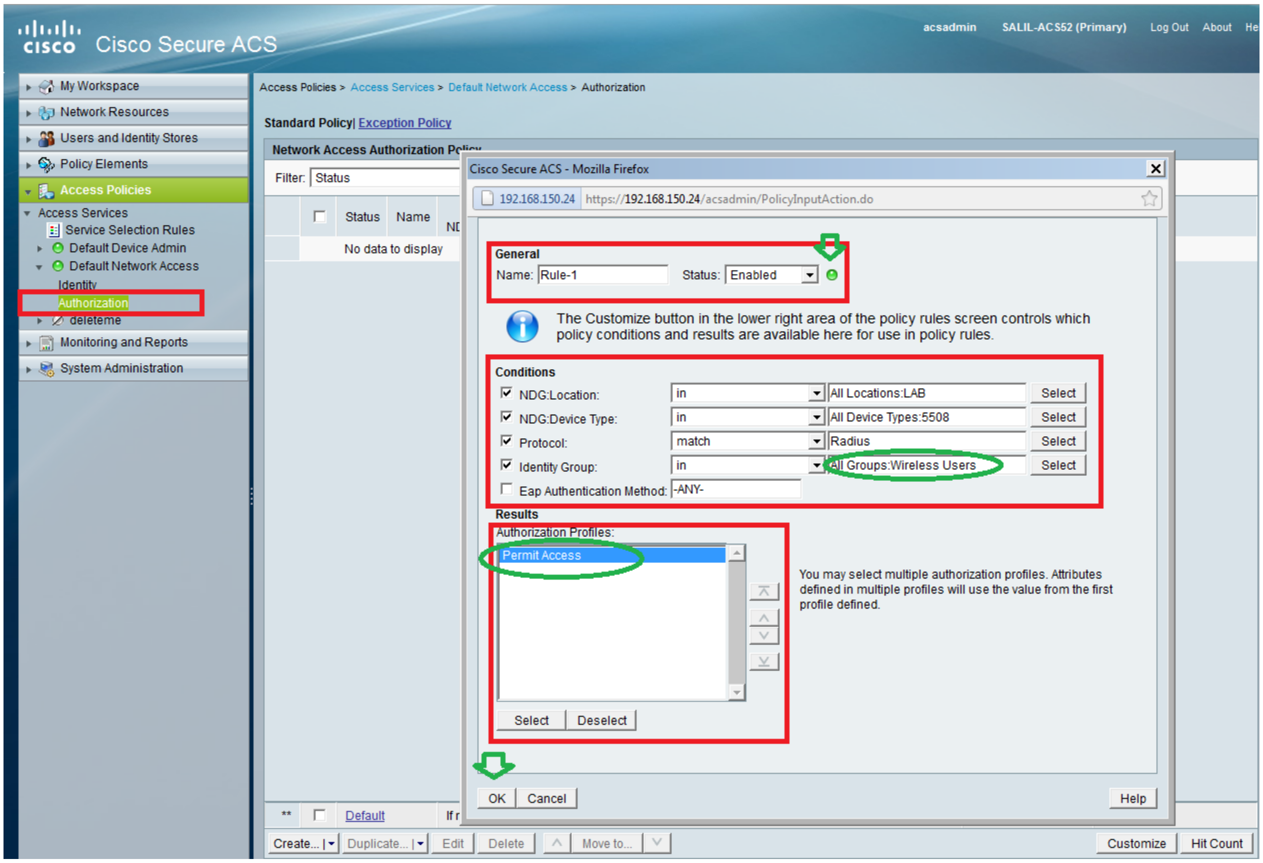
192.168.150.24 https://192.168.150.24/acsadmin/PolicyInputAction.do

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

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



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:5508	Select
☑ Protocol:	match	Radius	Select
☑ Identity Group:	in	All Groups:Wireless Users	Select
□ Eap Authentication Method:	-ANY-		

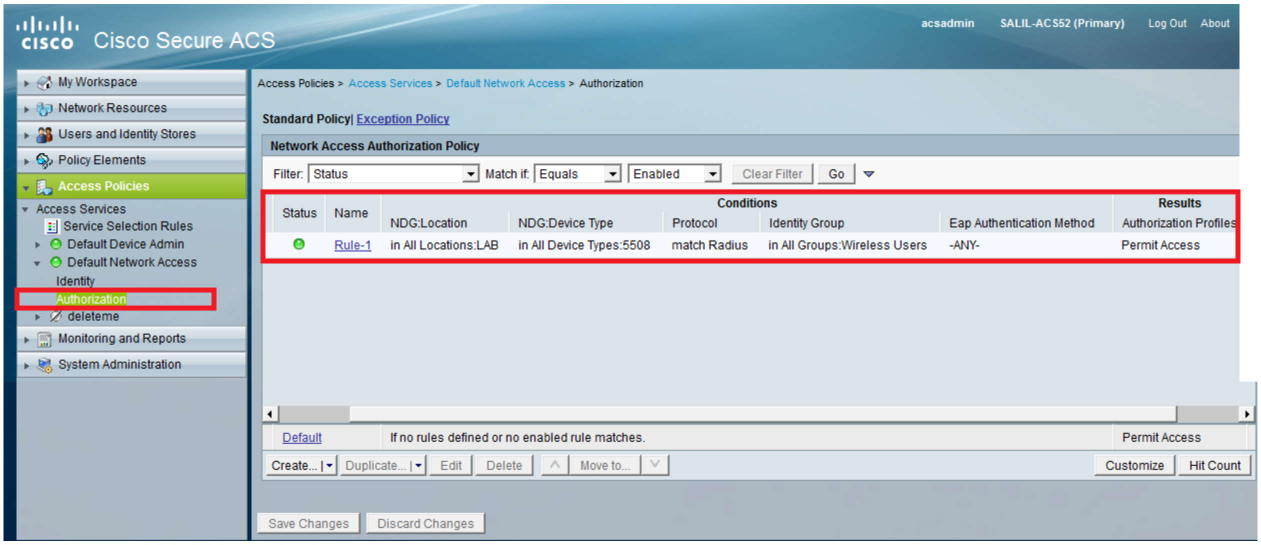
Results

Authorization Profiles:

Permit Access

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

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".



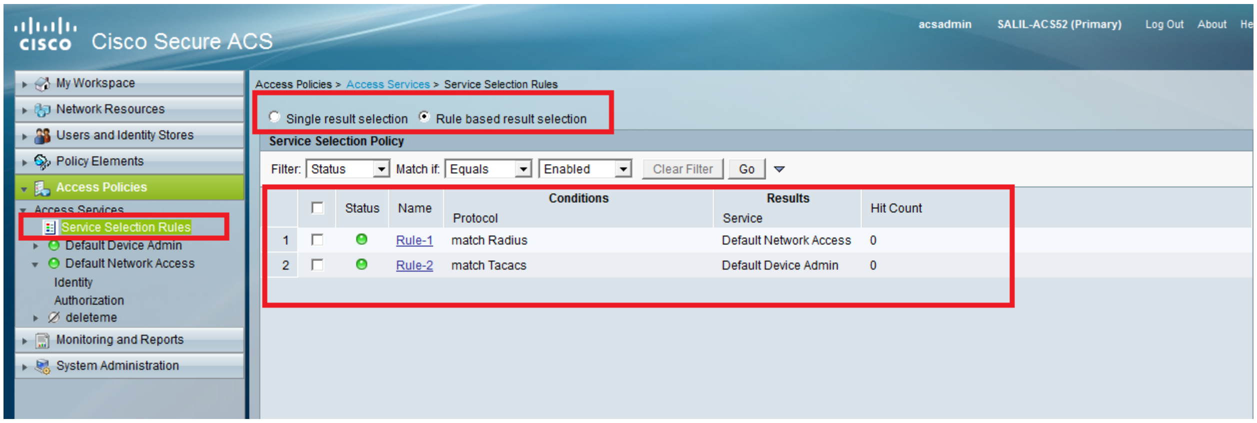
Network Access Authorization Policy

Filter: Status Match if: Equals Enabled

		Conditions					Results
Status	Name	NDG:Location	NDG:Device Type	Protocol	Identity Group	Eap Authentication Method	Authorization Profiles
●	Rule-1	in All Locations:LAB	in All Device Types:5508	match Radius	in All Groups:Wireless Users	-ANY-	Permit Access

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.



○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Enabled

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

WLC Configuration

This configuration requires these steps:

- Configure the WLC with the Details of the Authentication Server
- Configure the Dynamic Interfaces (VLANs)
- Configure the WLANs (SSID)

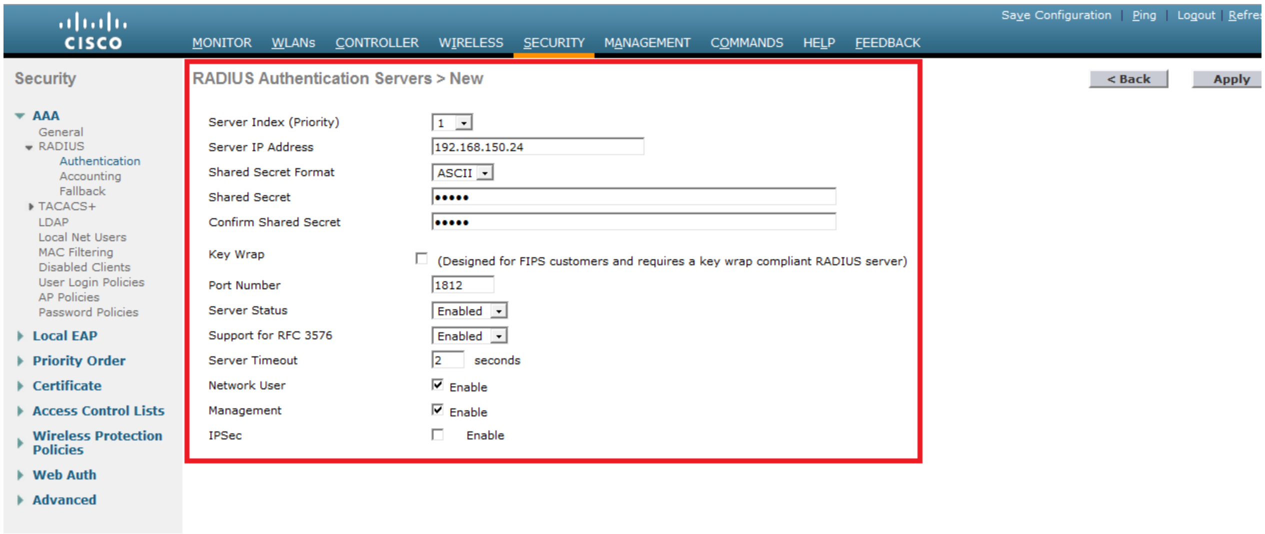
Configure the WLC with the Details of the Authentication Server

It is necessary to configure the WLC so it can communicate with the RADIUS server to authenticate the clients, and also for any other transactions.

Complete these steps:

From the controller GUI, click Security.

1. Enter the IP address of the RADIUS server and the Shared Secret key used between the RADIUS server and the WLC.
   This Shared Secret key should be the same as the one configured in the RADIUS server.



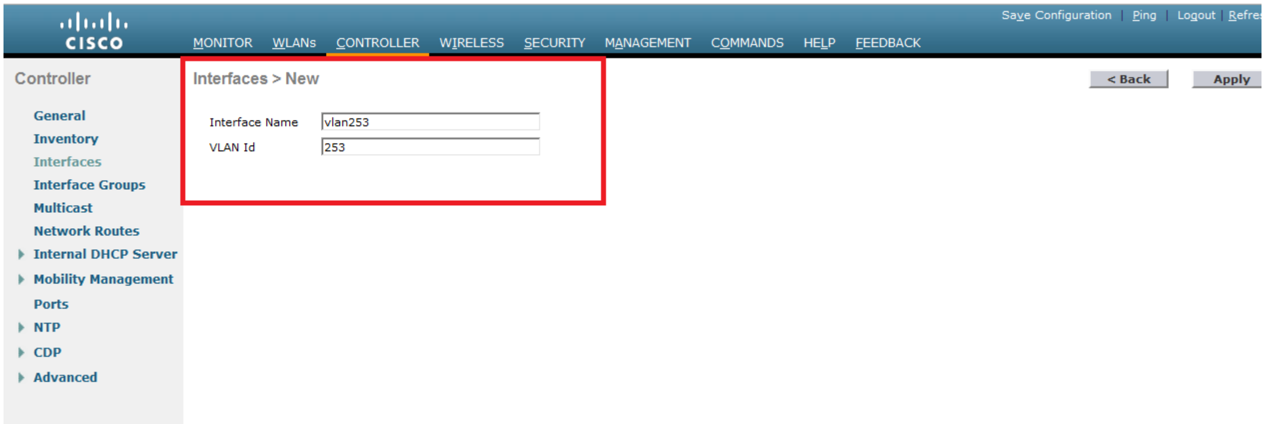
RADIUS Authentication Servers > New

Server Index (Priority)	1
Server IP Address	192.168.150.24
Shared Secret Format	ASCII
Shared Secret	•••••
Confirm Shared Secret	•••••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	☑ Enable
Management	☑ Enable
IPSec	□ Enable

Configure the Dynamic Interfaces (VLANs)

This procedure explains how to configure dynamic interfaces on the WLC.

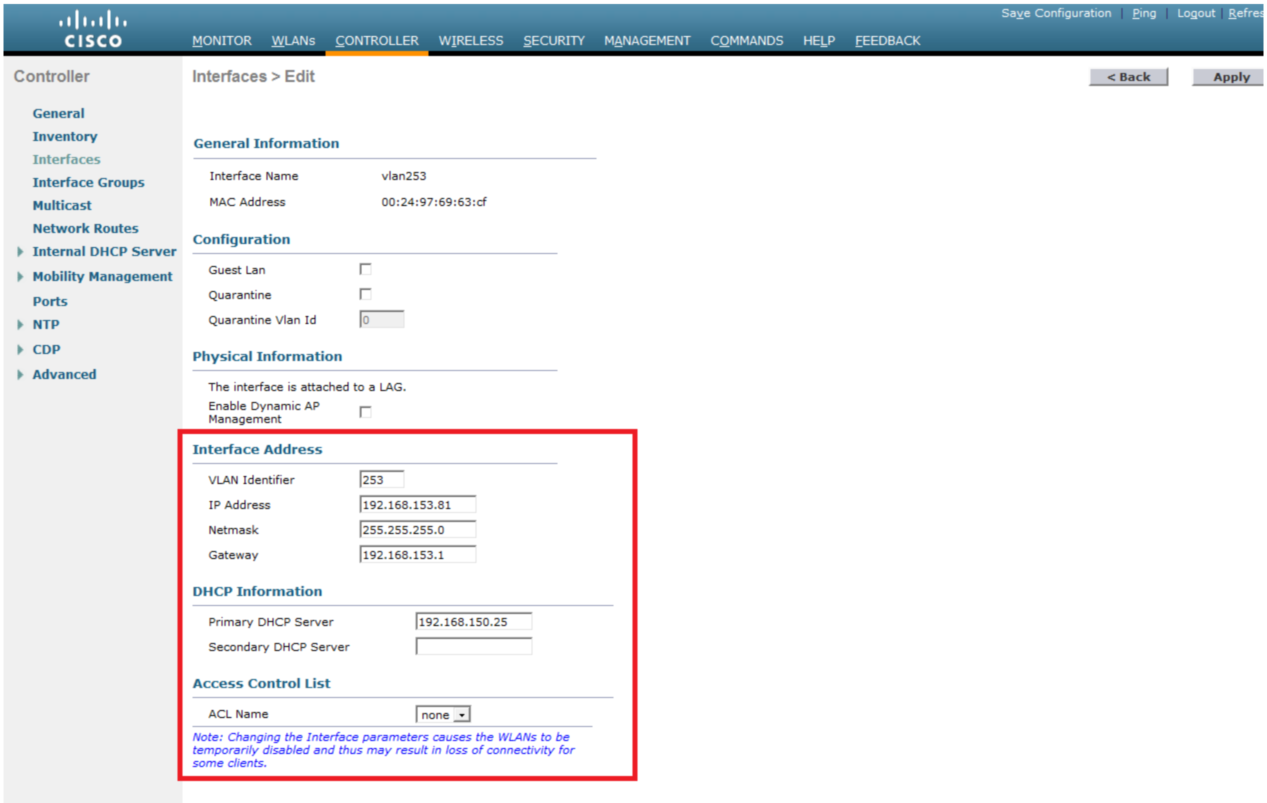
1) From the controller GUI, under the Controller > Interfaces window, the dynamic interface is configured.



Interfaces > New

Interface Name	vlan253
VLAN Id	253

2) Click Apply on this window.
3) This takes you to the Edit window of this dynamic interface (VLAN 253 here).
4) Enter the IP Address and default Gateway of this dynamic interface.



Interfaces > Edit

General Information

Interface Name	vlan253
MAC Address	00:24:97:69:63:cf

Configuration

Guest Lan	□
Quarantine	□
Quarantine Vlan Id	0

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management □

Interface Address

VLAN Identifier	253
IP Address	192.168.153.81
Netmask	255.255.255.0
Gateway	192.168.153.1

DHCP Information

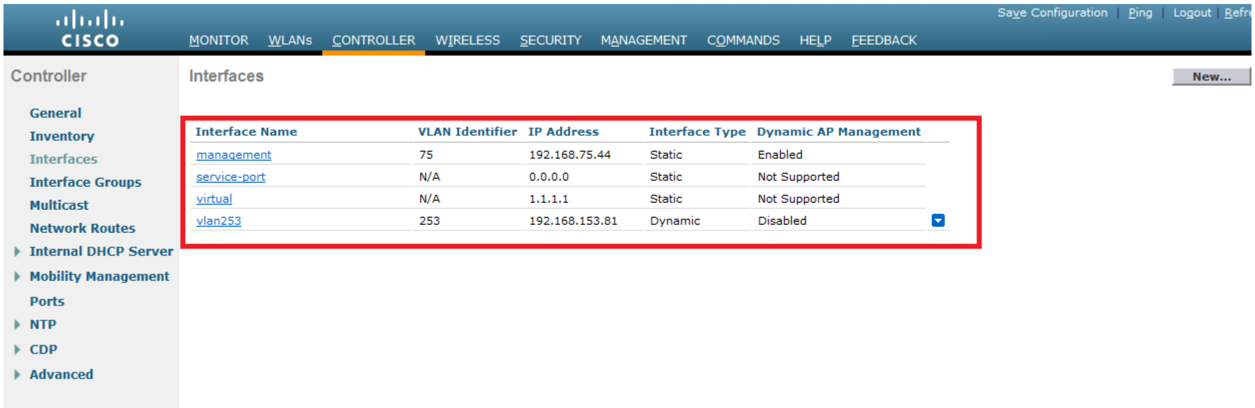
Primary DHCP Server	192.168.150.25
Secondary DHCP Server	

Access Control List

ACL Name	none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

5) Click Apply.
6) Interfaces configured should look like :



Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	75	192.168.75.44	Static	Enabled
service-port	N/A	0.0.0.0	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported
vlan253	253	192.168.153.81	Dynamic	Disabled

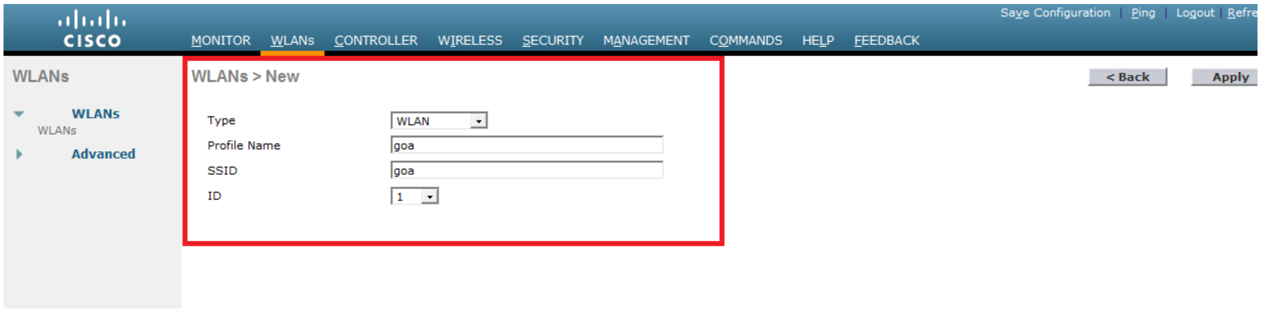
Configure the WLANs (SSID)

This procedure explains how to configure the WLANs in the WLC.
Complete these steps:

1. From the controller GUI, choose WLANs > Create New in order to create a new WLAN. The New WLANs window is displayed.

2. Enter the WLAN ID and WLAN SSID information.

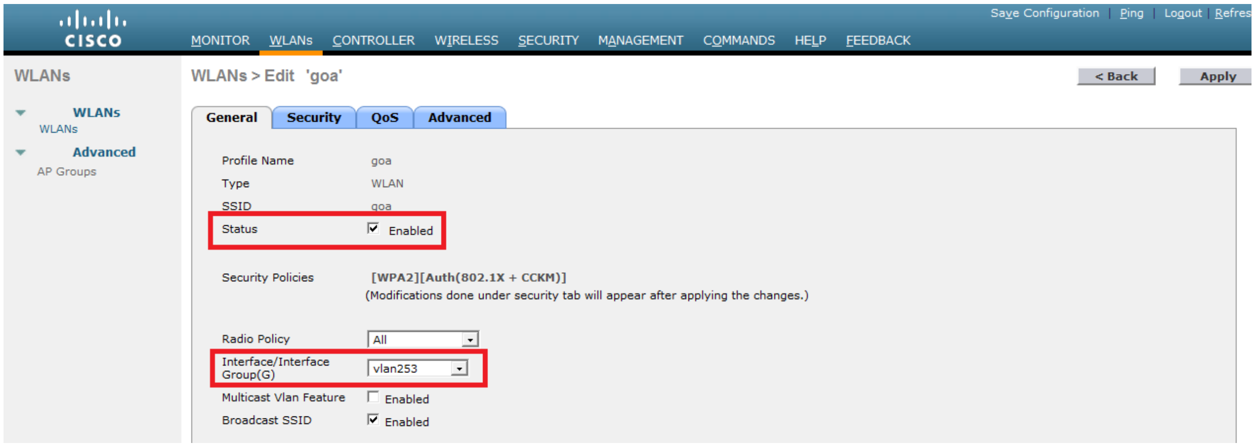
You can enter any name to be the WLAN SSID. This example uses “goa” as the WLAN SSID.


Save Configuration | Ping | Logout | Refre
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply

WLANs > New

Type: WLAN
Profile Name: goa
SSID: goa
ID: 1

3. Click Apply in order to go to the Edit window of the WLAN goa.

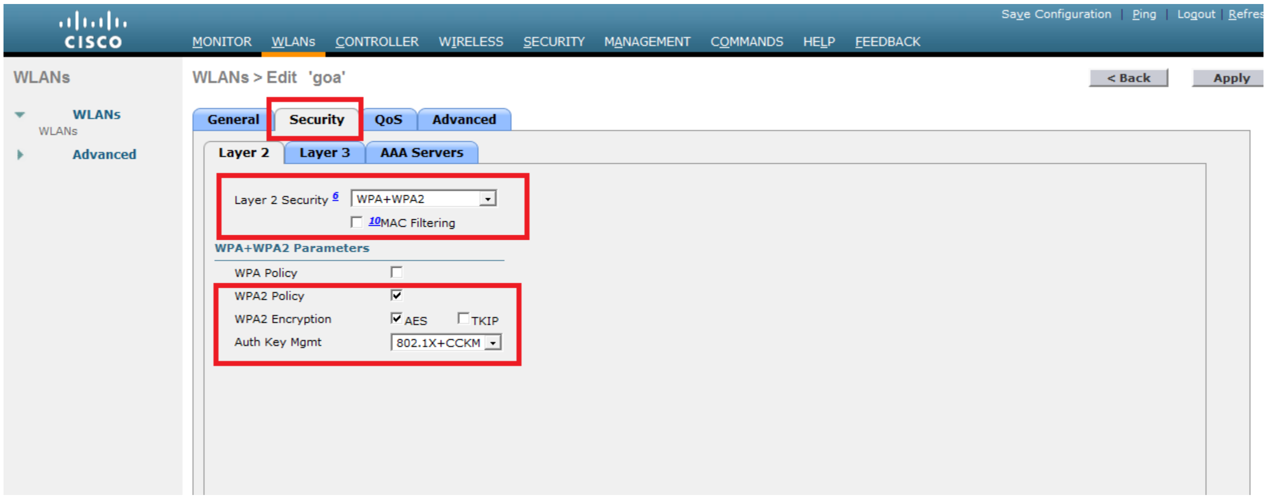

Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
AP Groups
< Back
Apply
General
Security
QoS
Advanced

WLANs > Edit 'goa'

Profile Name: goa
Type: WLAN
SSID: goa
Status: ☑ Enabled

Security Policies: [WPA2][Auth(802.1X + CCKM)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All
Interface/Interface Group(G): vlan253
Multicast Vlan Feature: □ Enabled
Broadcast SSID: ☑ Enabled

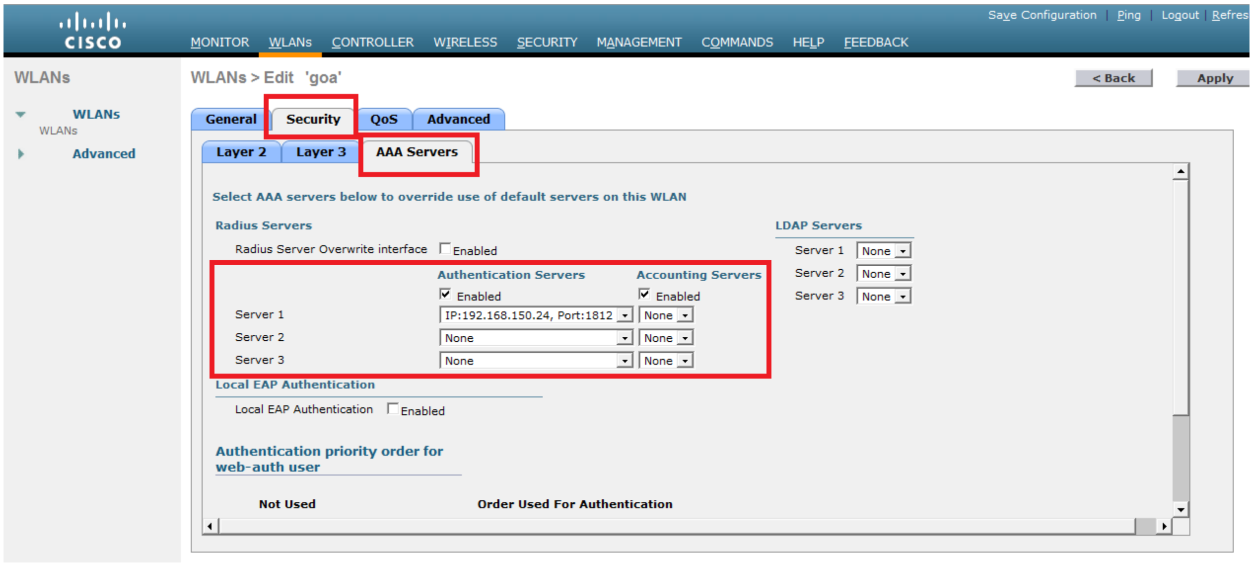

Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers

WLANs > Edit 'goa'

Layer 2 Security 6: WPA+WPA2
□ 10MAC Filtering

WPA+WPA2 Parameters

WPA Policy: □
WPA2 Policy: ☑
WPA2 Encryption: ☑ AES □ TKIP
Auth Key Mgmt: 802.1X+CCKM


Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers

WLANs > Edit 'goa'

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:192.168.150.24, Port:1812	None
Server 2	None	None
Server 3	None	None

LDAP Servers

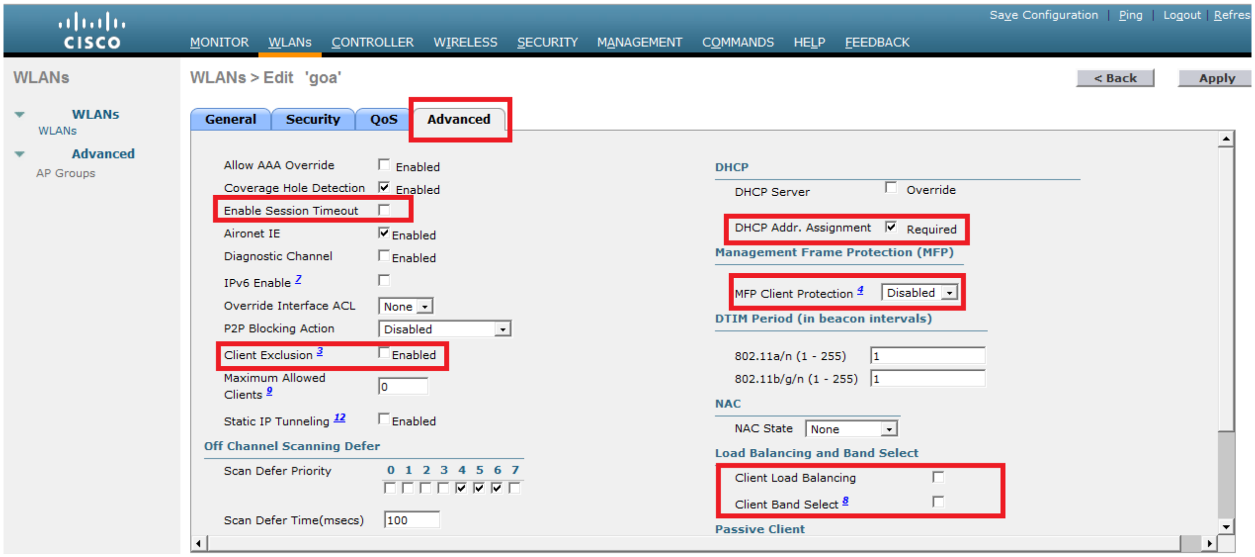
Server 1	None
Server 2	None
Server 3	None

Local EAP Authentication

Local EAP Authentication □ Enabled

Authentication priority order for web-auth user

Not Used | Order Used For Authentication


Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
AP Groups
< Back
Apply
General
Security
QoS
Advanced

WLANs > Edit 'goa'

Allow AAA Override	□ Enabled
Coverage Hole Detection	☑ Enabled
Enable Session Timeout	□
Aironet IE	☑ Enabled
Diagnostic Channel	□ Enabled
IPv6 Enable [7]	□
Override Interface ACL	None
P2P Blocking Action	Disabled
Client Exclusion [3]	□ Enabled
Maximum Allowed Clients [9]	0
Static IP Tunneling [12]	□ Enabled

Off Channel Scanning Defer

Scan Defer Priority	0	1	2	3	4	5	6	7
	□	□	□	□	☑	☑	☑	□

Scan Defer Time(msecs) 100

DHCP

DHCP Server	□ Override
DHCP Addr. Assignment	☑ Required

Management Frame Protection (MFP)

MFP Client Protection [4] Disabled

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)	1
802.11b/g/n (1 - 255)	1

NAC

NAC State None

Load Balancing and Band Select

Client Load Balancing	□
Client Band Select [8]	□

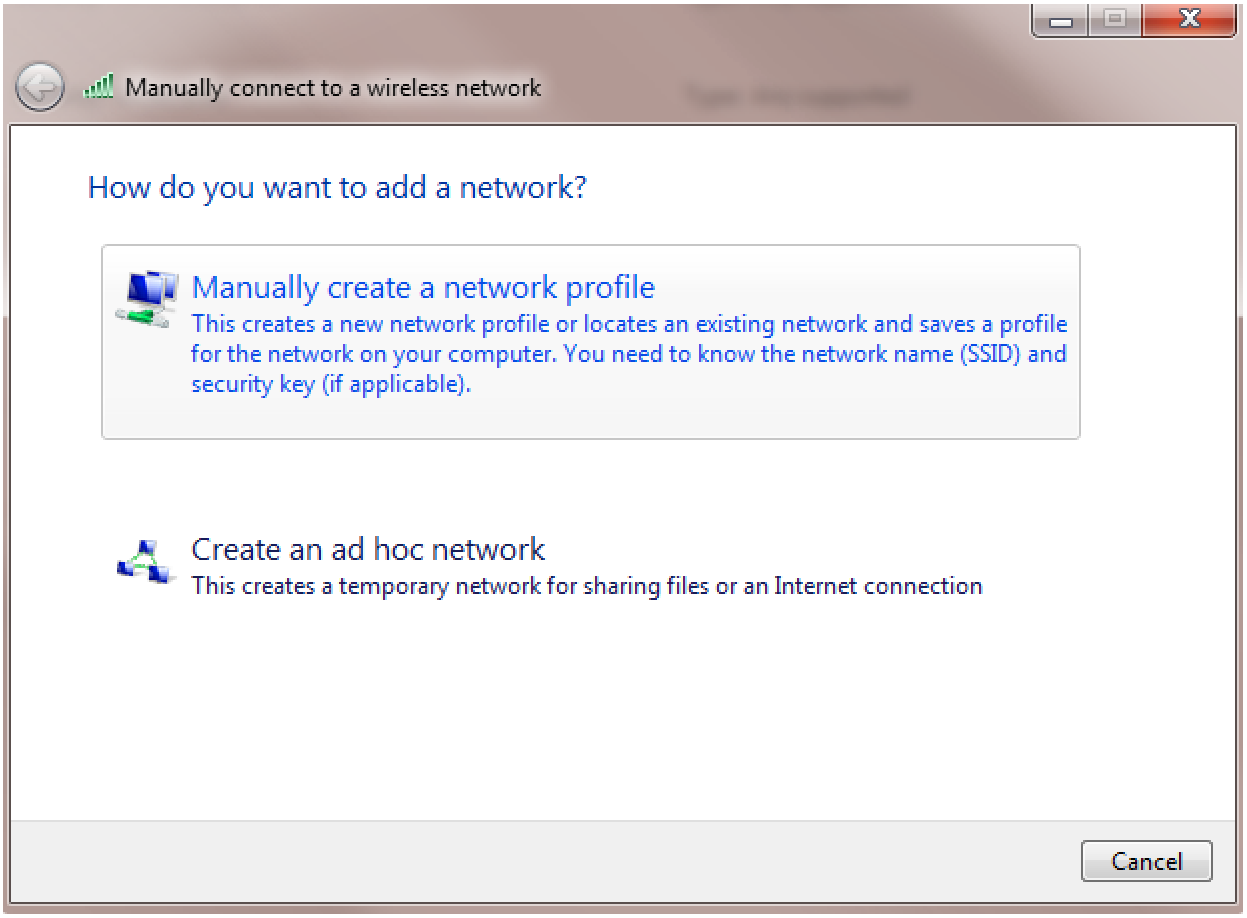
Passive Client

Wireless Client Utility Configuration – PEAP – mschapv2 (user1)

In our test client we are using Windows 7 Native supplicant with Intel 6300-N card running 14.3 driver version. It is recommended to test using latest drivers from Vendors.

Creating a Profile in WZC – Windows Zero Config:

1. Control Panel → Network and Internet → Manage Wireless Networks.
2. Add
3. Click manually create network Profile.

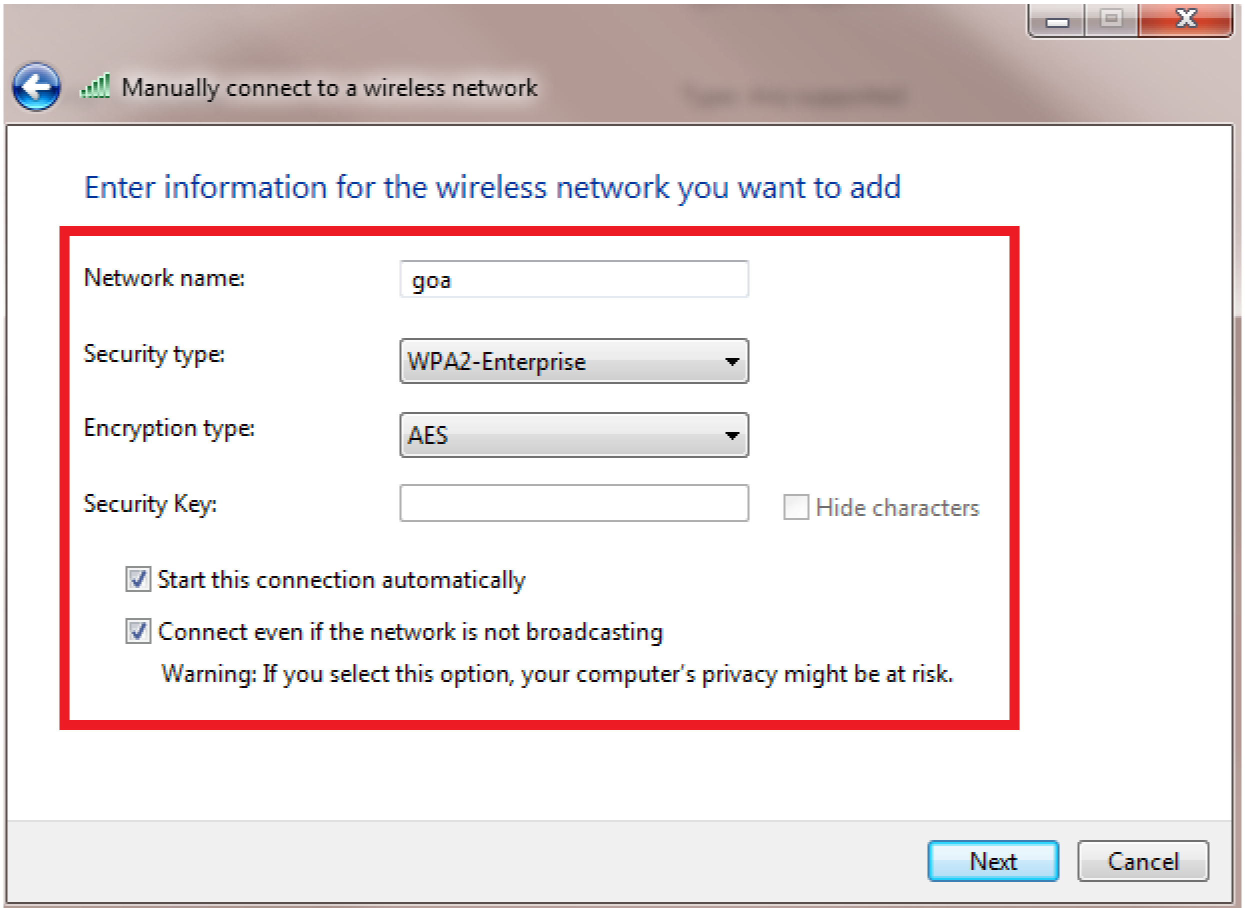


How do you want to add a network?

Manually create a network profile
This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).

Create an ad hoc network
This creates a temporary network for sharing files or an Internet connection

4. Add the details as configured on the WLC. SSID is case sensitive.
5. Click Next



Enter information for the wireless network you want to add

Network name: goa

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

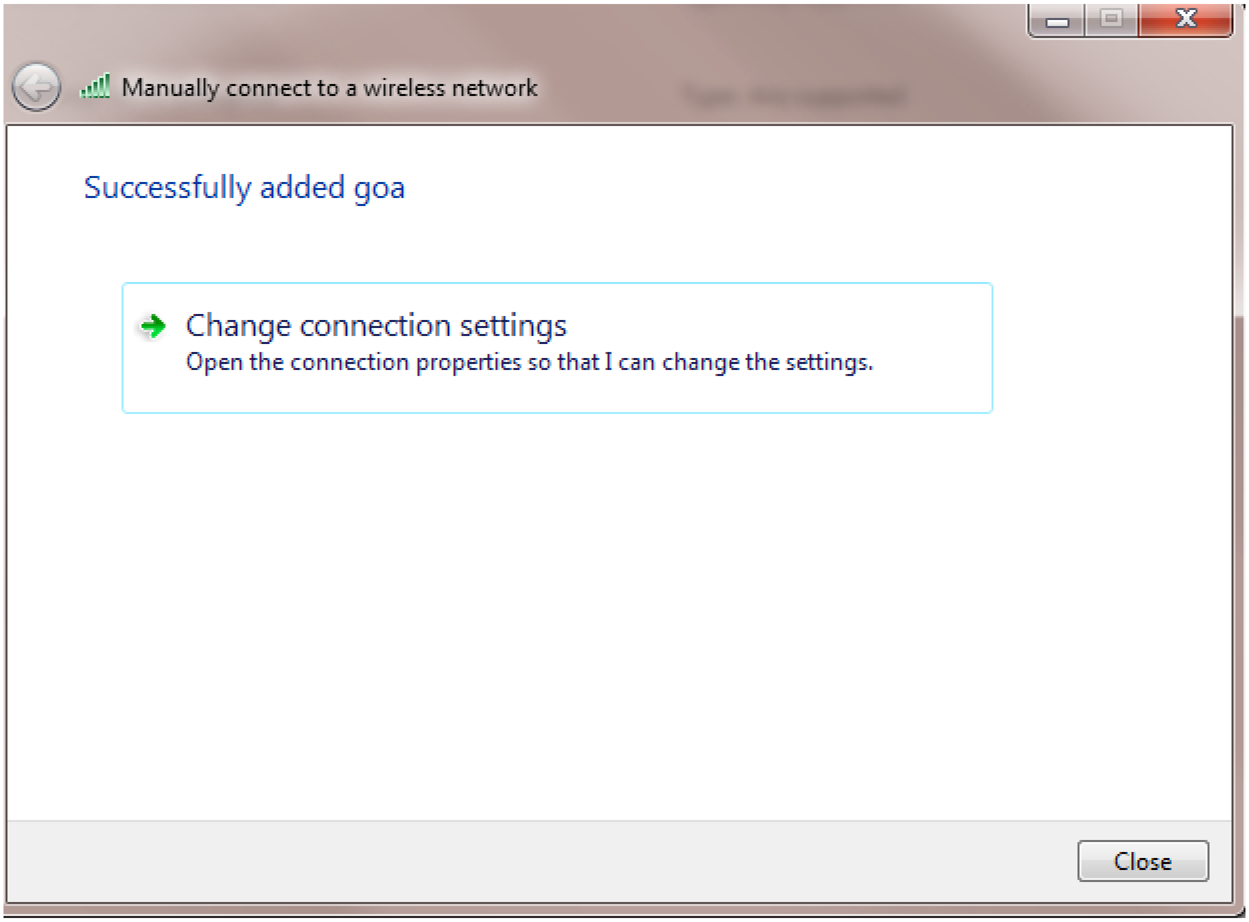
□ Hide characters

☑ Start this connection automatically

☑ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

6. Click Change Connection Settings to double check our settings.

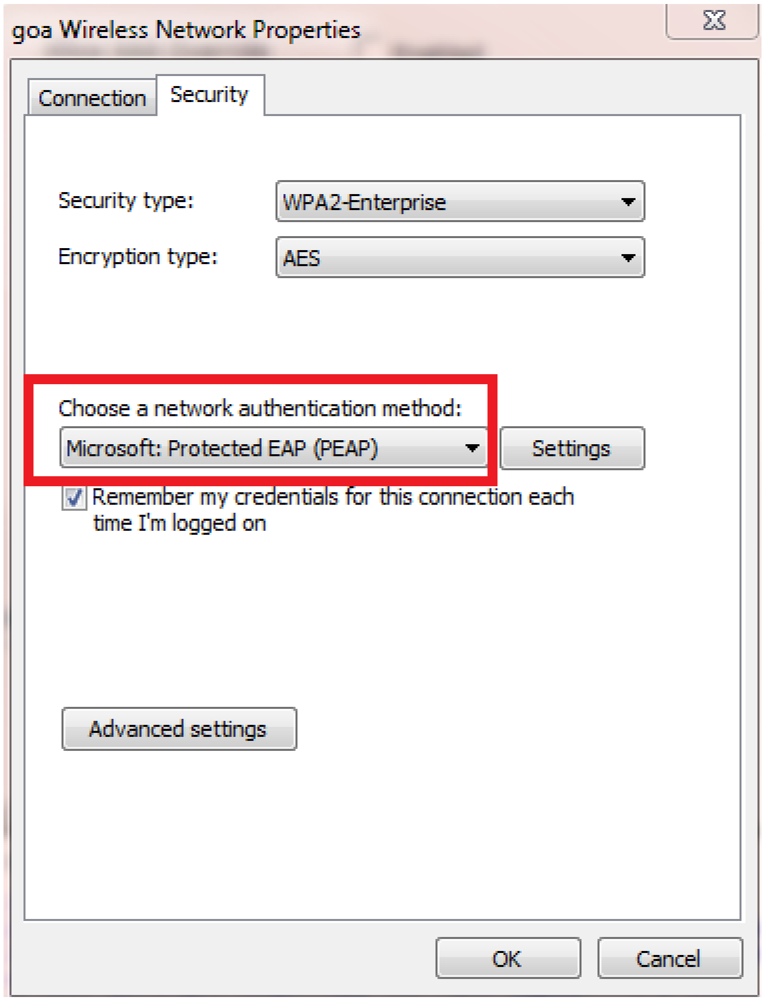


Successfully added goa

Change connection settings

Open the connection properties so that I can change the settings.

7. Make sure you have PEAP enabled.



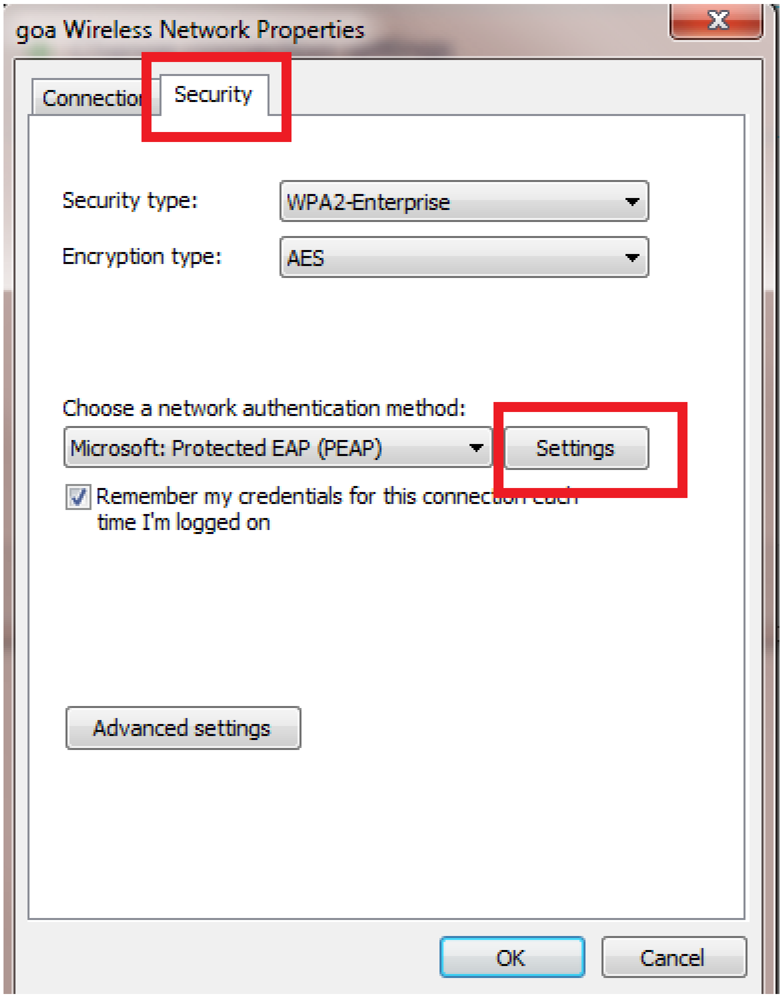
goa Wireless Network Properties

Security type: WPA2-Enterprise

Encryption type: AES

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

☑ Remember my credentials for this connection each time I'm logged on



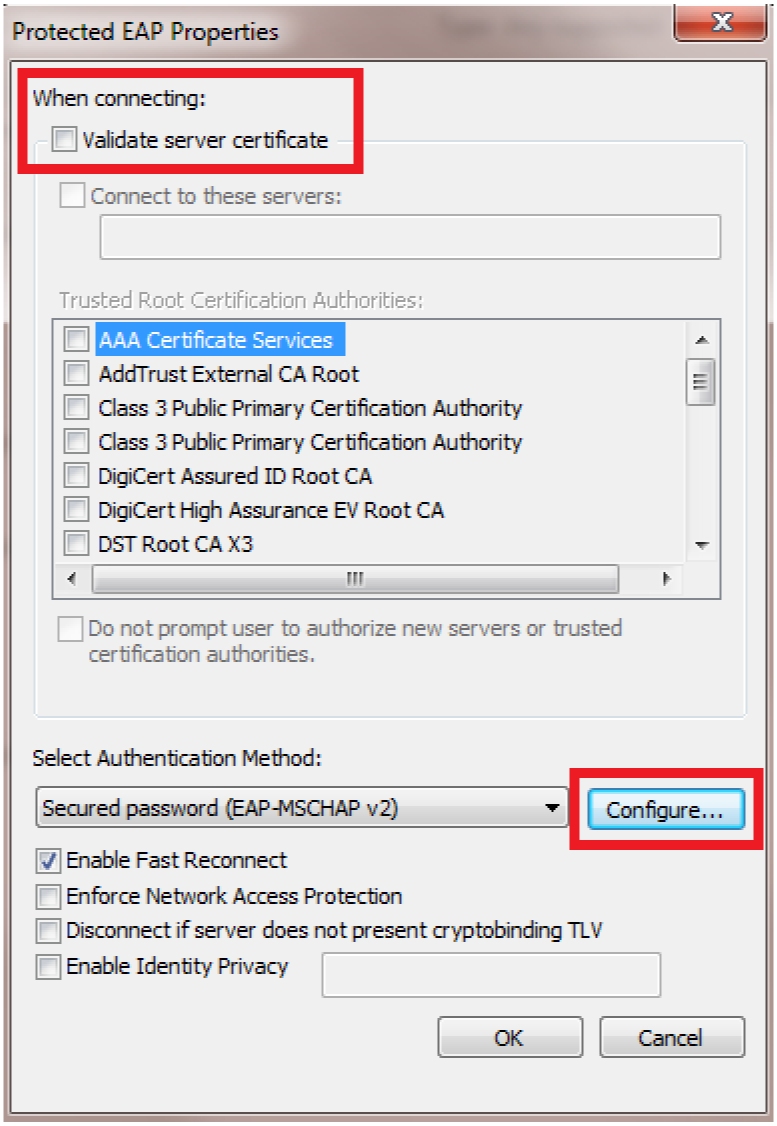
Security type: WPA2-Enterprise

Encryption type: AES

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

☑ Remember my credentials for this connection each time I'm logged on

8. In our example, we are not validating Server certificate. If you check this box and are not able to connect, try disabling the feature and test again.


Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

- □ AAA Certificate Services
- □ AddTrust External CA Root
- □ Class 3 Public Primary Certification Authority
- □ Class 3 Public Primary Certification Authority
- □ DigiCert Assured ID Root CA
- □ DigiCert High Assurance EV Root CA
- □ DST Root CA X3

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

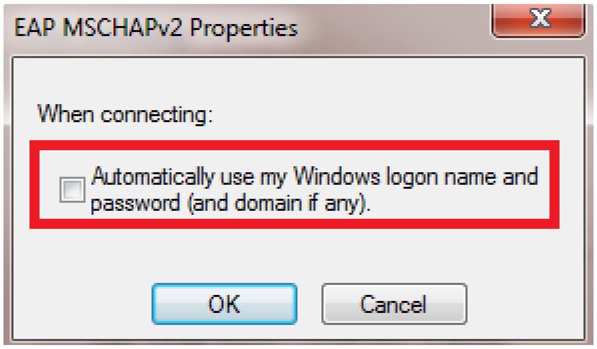
☑ Enable Fast Reconnect

□ Enforce Network Access Protection

□ Disconnect if server does not present cryptobinding TLV

□ Enable Identity Privacy

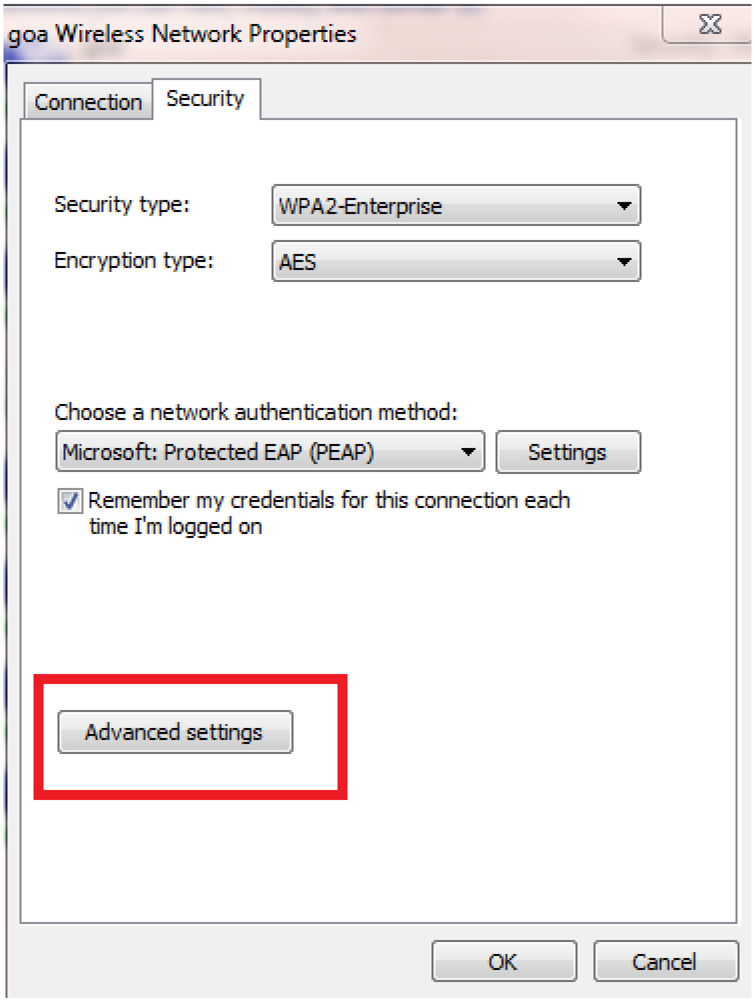
9. Optionally, you can use Windows credentials to login. However in our example we are not going to use that. Click OK.


EAP MSCHAPv2 Properties

When connecting:

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

10. Now Click Advanced settings to configure Username and Password.



goa Wireless Network Properties

Connection | Security

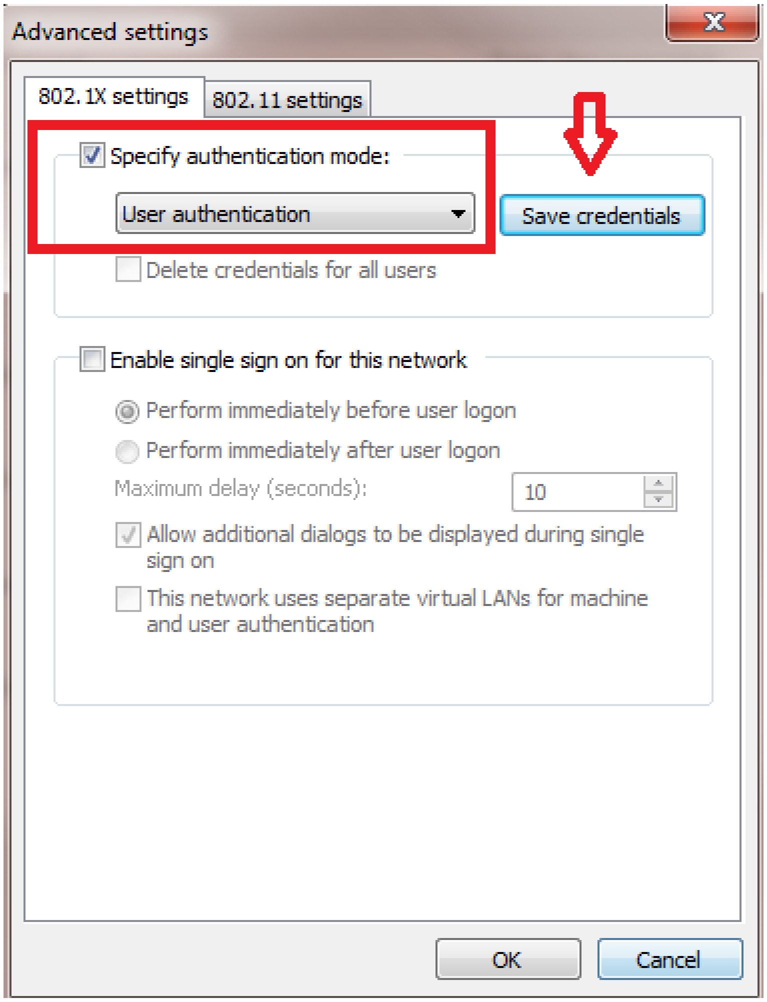
Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on



☑ Specify authentication mode:

User authentication

□ Delete credentials for all users

□ Enable single sign on for this network

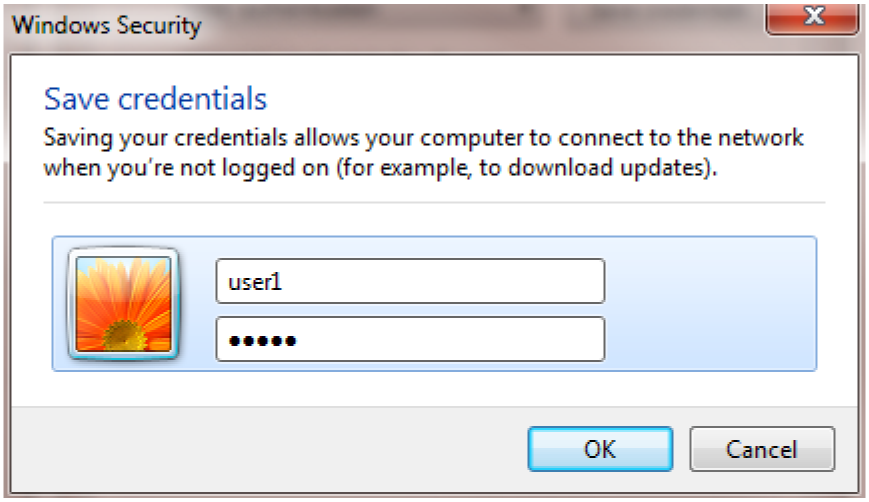
● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication



Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

user1

●●●●●

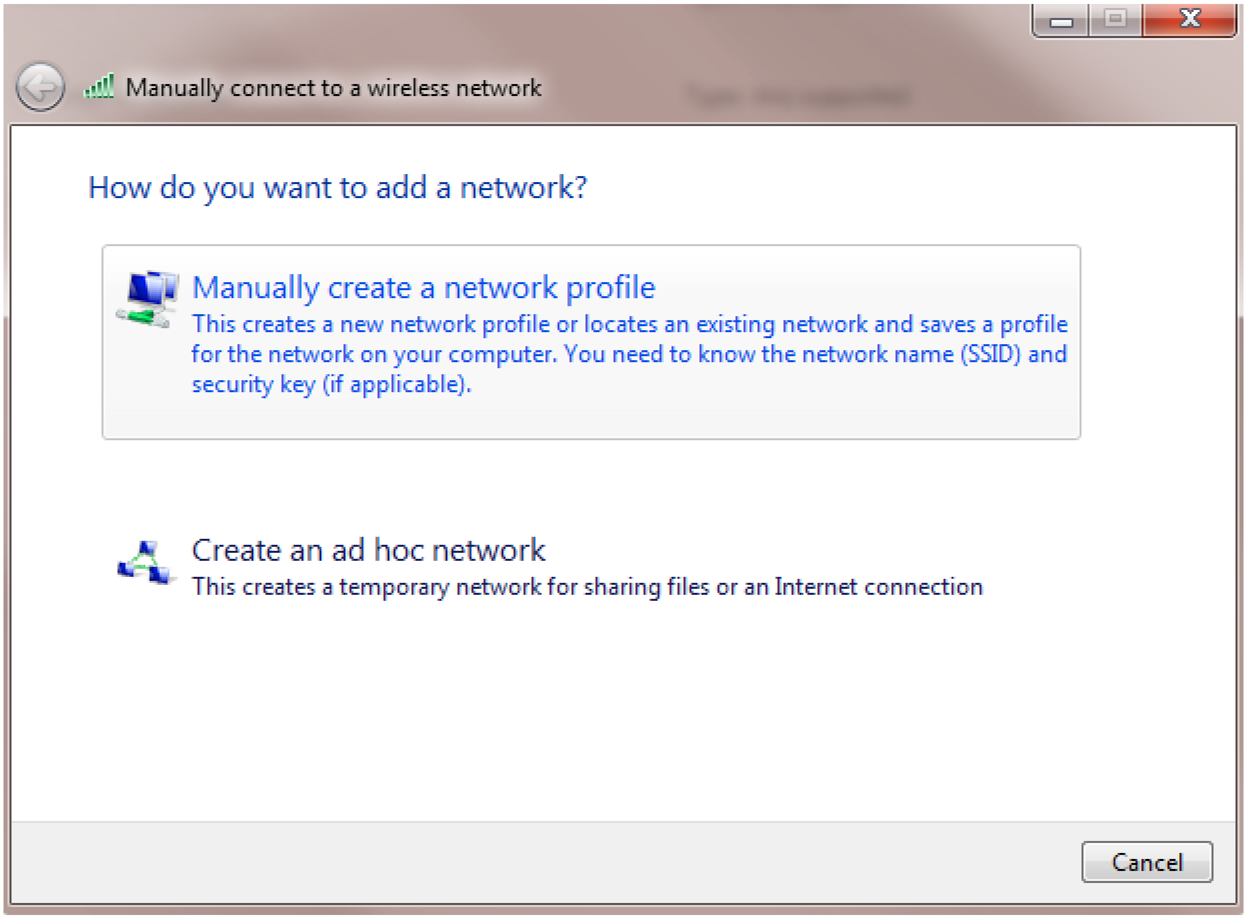
Your Client utility is ready to connect for user1.

Wireless Client Utility Configuration – EAPFAST (user2)

In our test client we are using Windows 7 Native supplicant with Intel 6300-N card running 14.3 driver version. It is recommended to test using latest drivers from Vendors.

Creating a Profile in WZC – Windows Zero Config:

1. Control Panel → Network and Internet → Manage Wireless Networks.
2. Add
3. Click manually create network Profile.



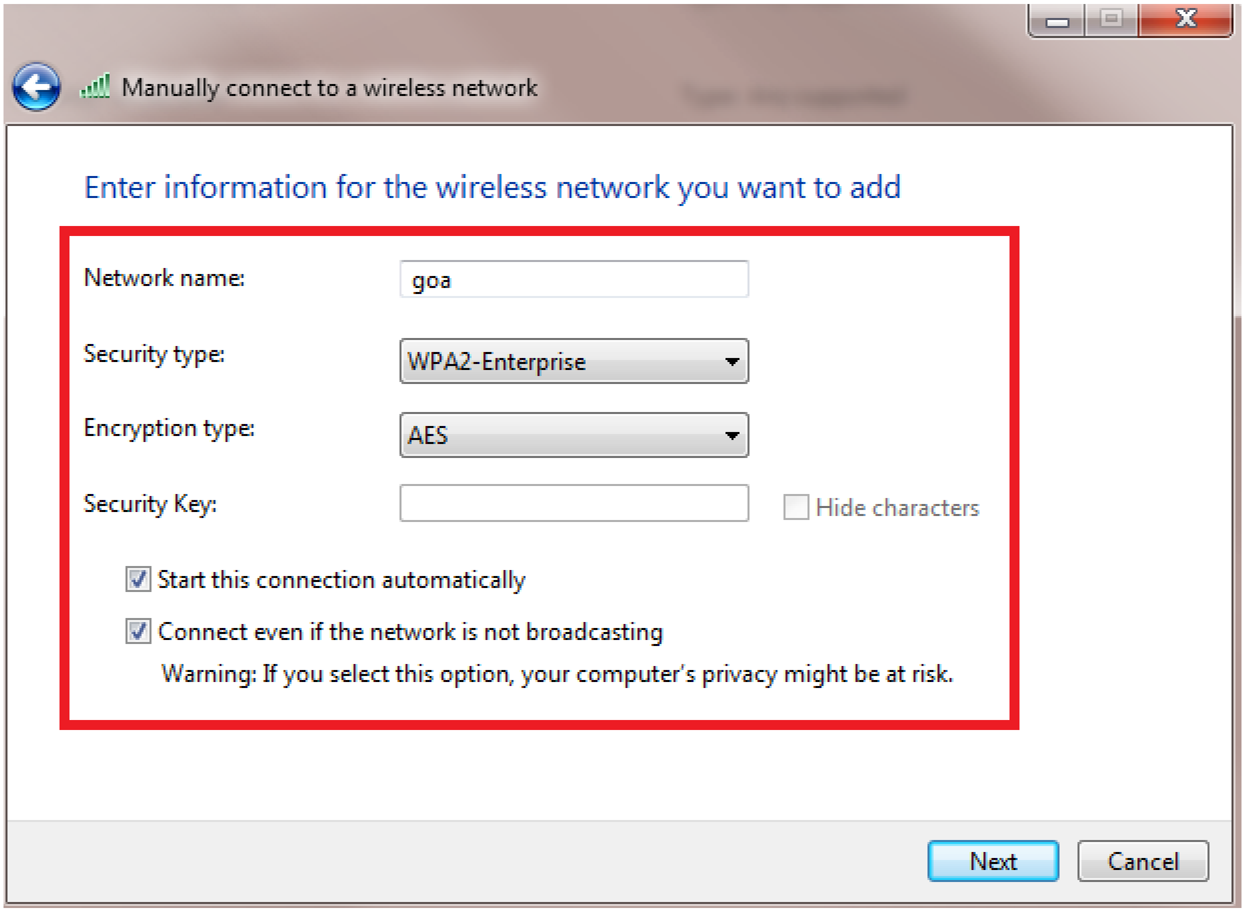
Manually connect to a wireless network

How do you want to add a network?

Manually create a network profile
This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).

Create an ad hoc network
This creates a temporary network for sharing files or an Internet connection

4. Add the details as configured on the WLC. SSID is case sensitive.
5. Click Next


Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: goa

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

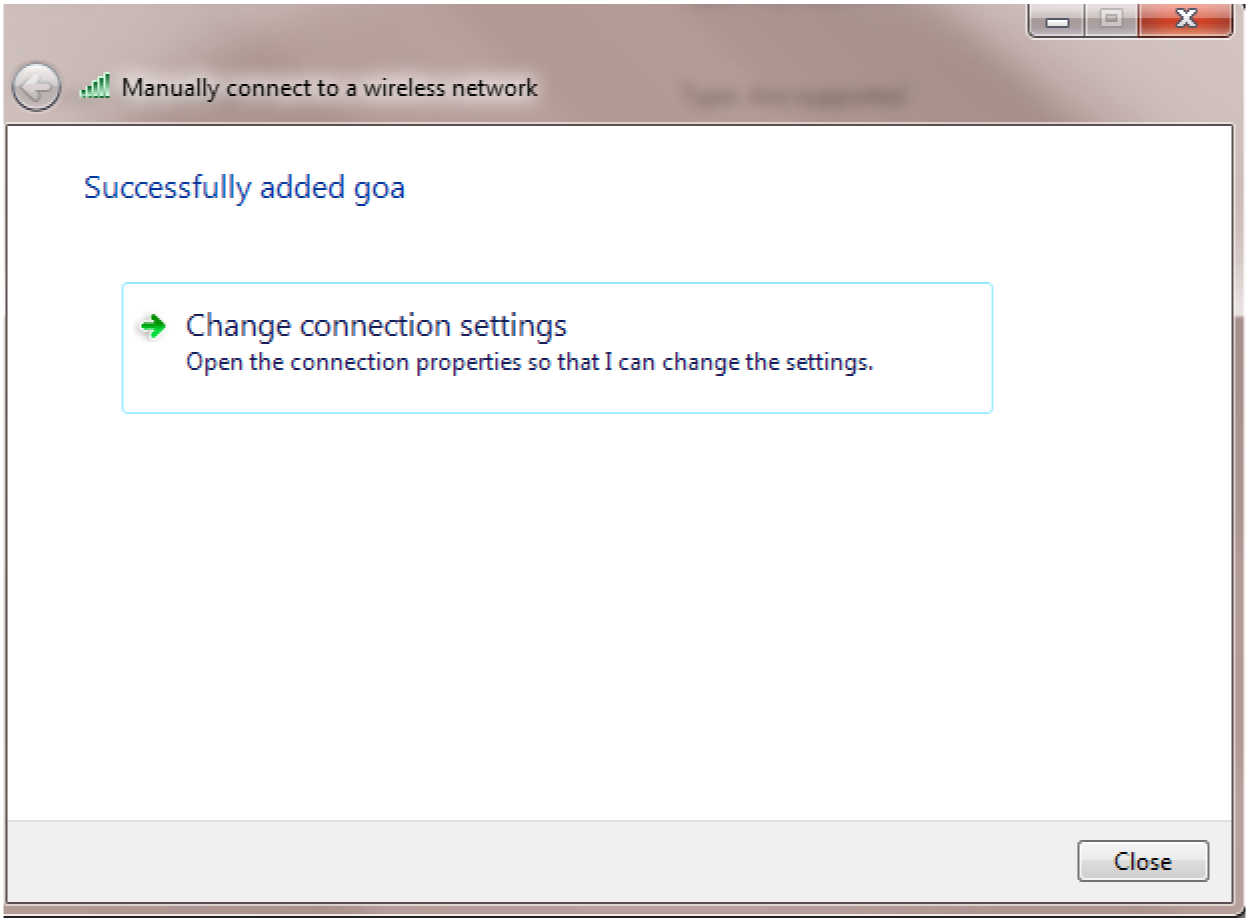
□ Hide characters

☑ Start this connection automatically

☑ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

6. Click Change Connection Settings to double check our settings.

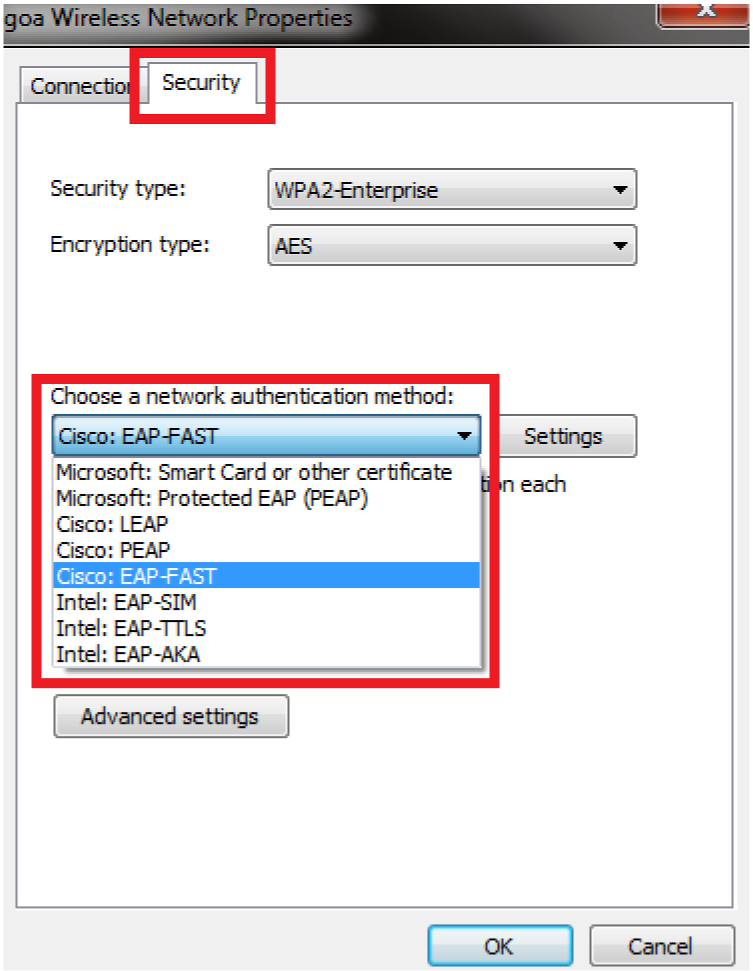


Manually connect to a wireless network

Successfully added goa

Change connection settings
Open the connection properties so that I can change the settings.

7. Make sure you have EAP-FAST enabled.
   Note: By default WZC does not have EAP-FAST as authentication method. You have to download utility from third party vendor. In our case since it is Intel card, we have Intel proset installed on the system.



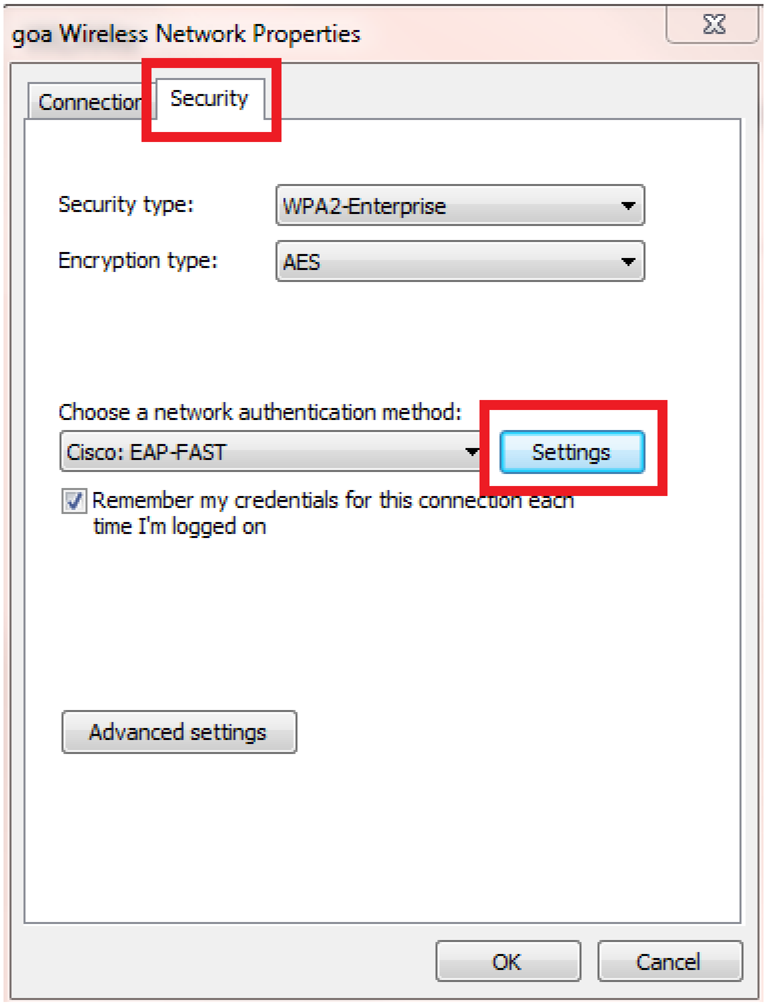
goa Wireless Network Properties

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Cisco: EAP-FAST



goa Wireless Network Properties

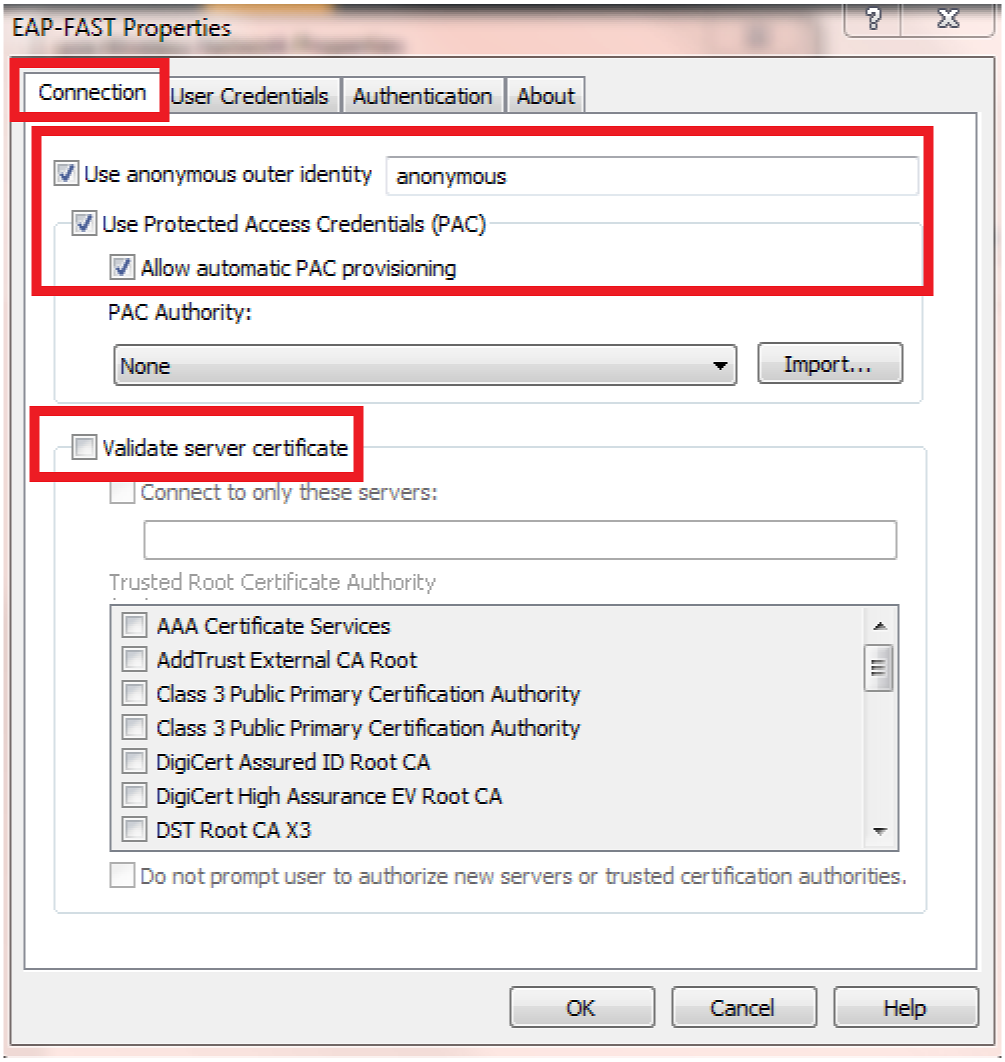
Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method: Cisco: EAP-FAST

☑ Remember my credentials for this connection each time I'm logged on

8. Enable “Allow automatic PAC provisioning” and make sure “validate Server certificate is unchecked.



☑ Use anonymous outer identity anonymous

☑ Use Protected Access Credentials (PAC)

☑ Allow automatic PAC provisioning

PAC Authority:

None

□ Validate server certificate

□ Connect to only these servers:

Trusted Root Certificate Authority

□ AAA Certificate Services

□ AddTrust External CA Root

□ Class 3 Public Primary Certification Authority

□ Class 3 Public Primary Certification Authority

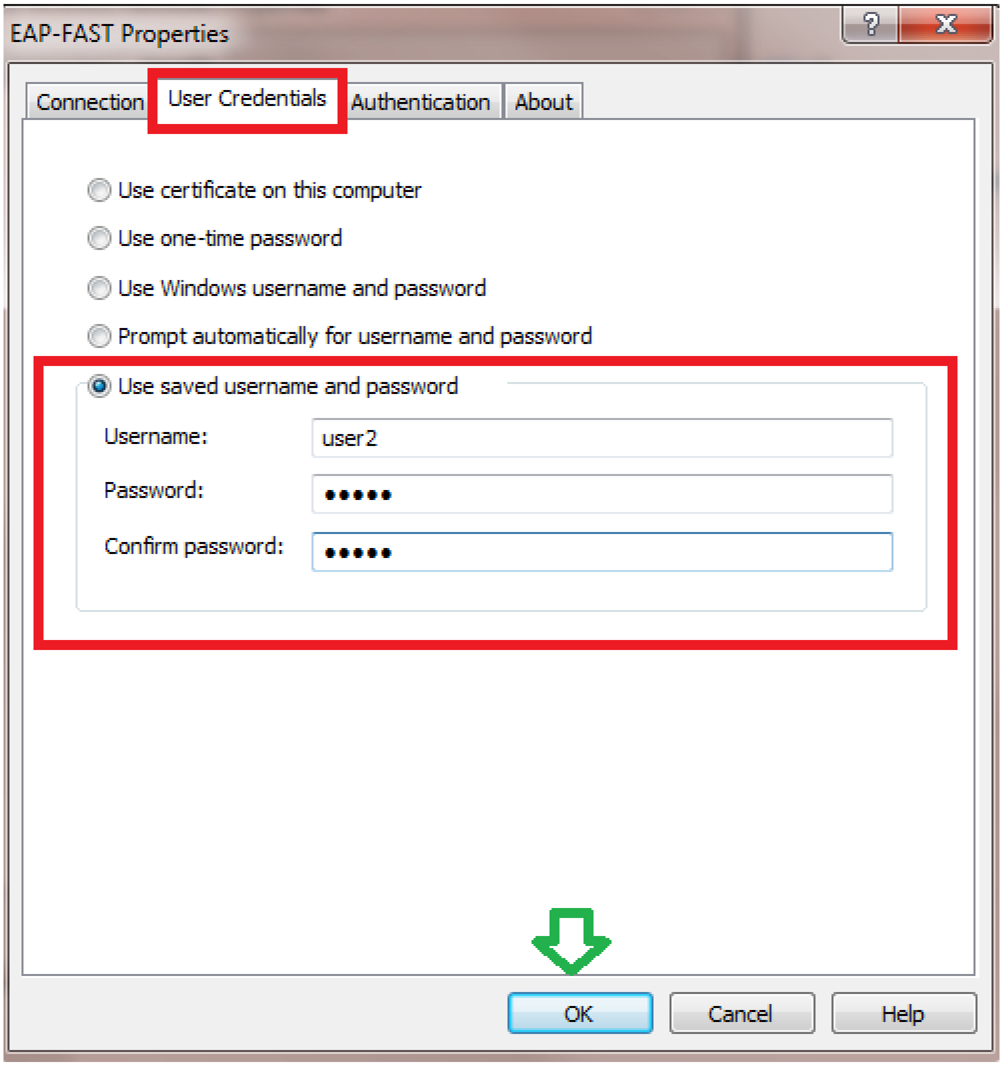
□ DigiCert Assured ID Root CA

□ DigiCert High Assurance EV Root CA

□ DST Root CA X3

□ Do not prompt user to authorize new servers or trusted certification authorities.

9. Next, Click User credentials. Enter the credentials of user2. Optionally, you can use Windows credentials to log. However in our example we are not going to use that.



EAP-FAST Properties

○ Use certificate on this computer

○ Use one-time password

○ Use Windows username and password

○ Prompt automatically for username and password

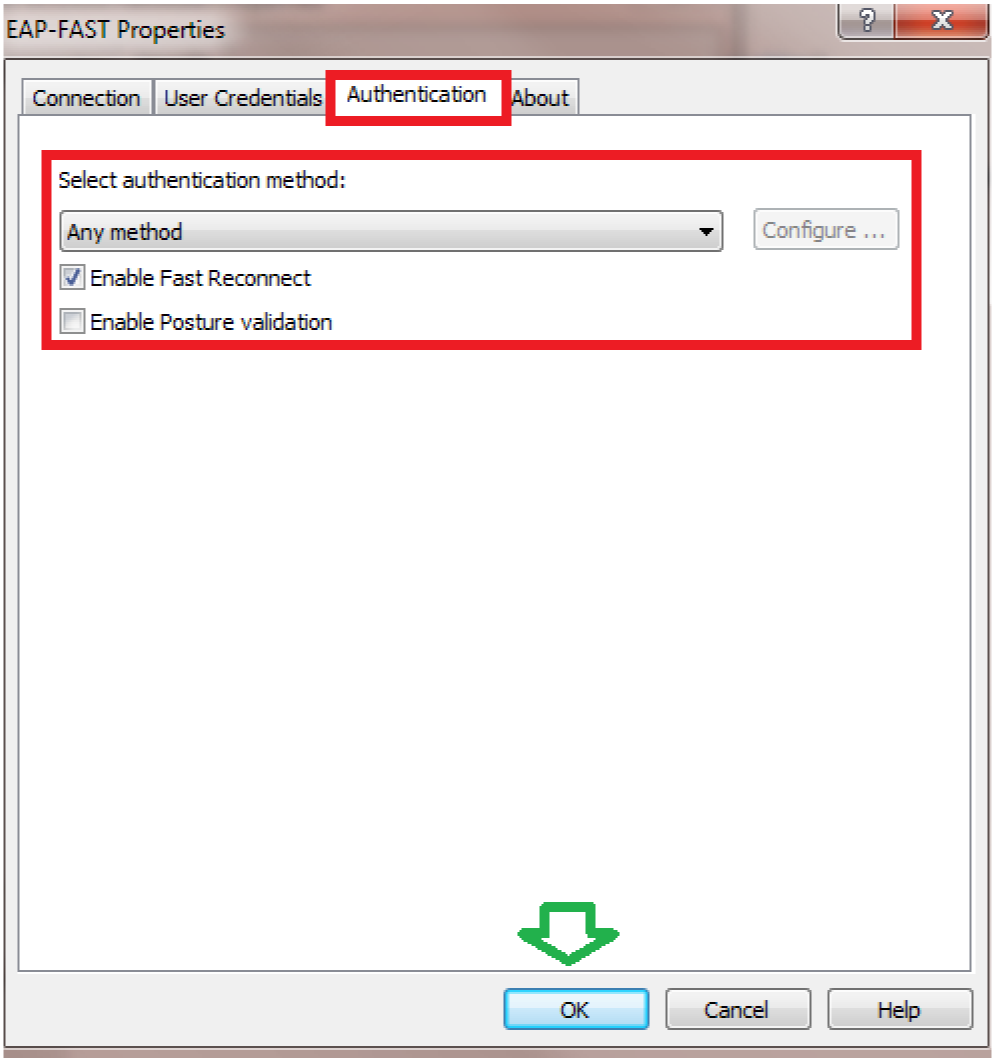
● Use saved username and password

Username: user2

Password: •••••

Confirm password: •••••

10. Click OK to complete the steps.



Select authentication method:

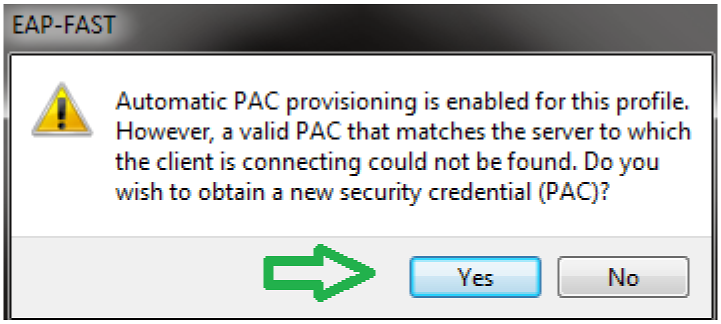
Any method

☑ Enable Fast Reconnect

☐ Enable Posture validation

Your Client utility is ready to connect for user2.

Note: When user2 is trying to authenticate, radius server is going to send a PAC. Accept the PAC to complete the authentication.

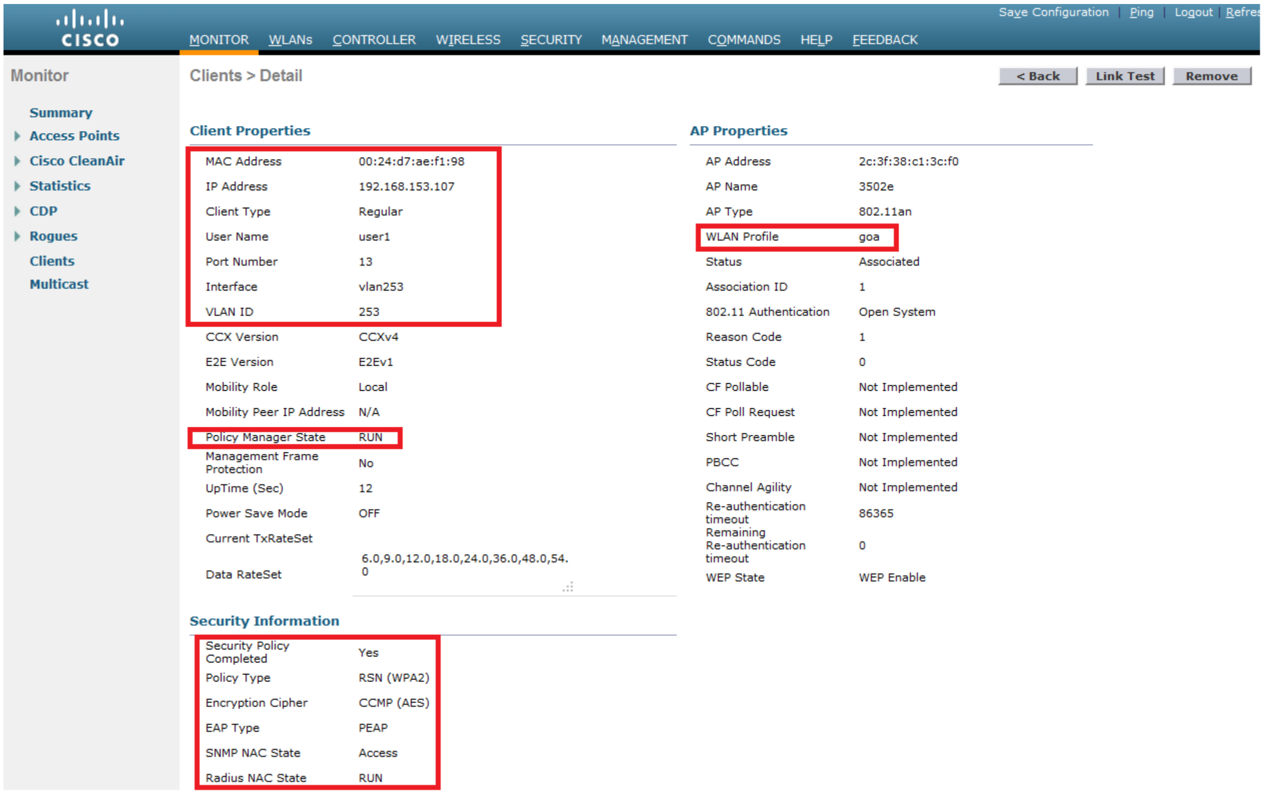


Automatic PAC provisioning is enabled for this profile. However, a valid PAC that matches the server to which the client is connecting could not be found. Do you wish to obtain a new security credential (PAC)?

Verification

Verify- user1-(peap-mschapv2)

WLC GUI : Monitor → Clients → Select the MAC address.



Clients > Detail

Client Properties

MAC Address	00:24:d7:ae:f1:98
IP Address	192.168.153.107
Client Type	Regular
User Name	user1
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	12
Power Save Mode	OFF
Current TxRateSet	
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0

AP Properties

AP Address	2c:3f:38:c1:3c:f0
AP Name	3502e
AP Type	802.11an
WLAN Profile	goa
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86365
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RUN

WLC Radius Stats:

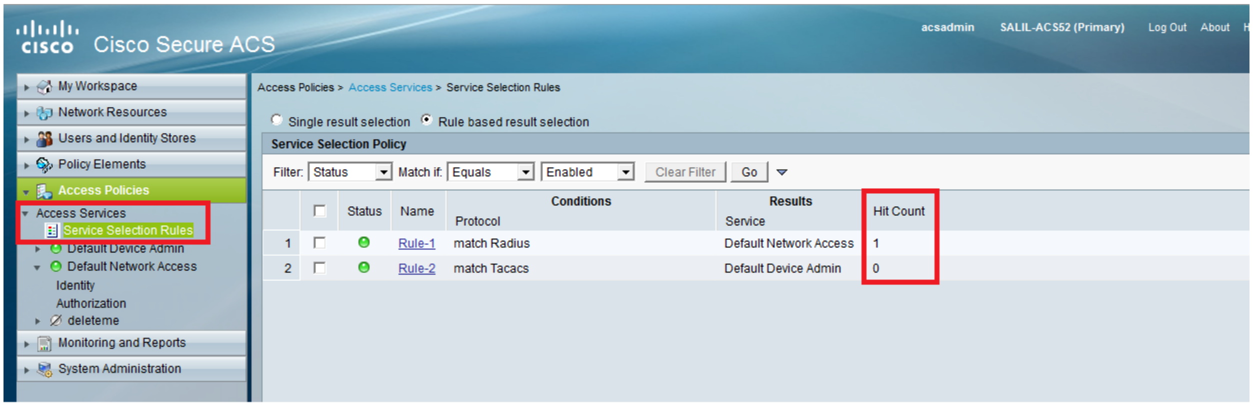
```
(Cisco Controller) >show radius auth statistics
Authentication Servers:

Server Index.................................... 1
Server Address.................................. 192.168.150.24
Msg Round Trip Time............................. 1 (msec)
First Requests.................................. 8
Retry Requests.................................. 0
Accept Responses................................ 1
Reject Responses................................ 0
Challenge Responses............................. 7
Malformed Msgs.................................. 0
```

```
Bad Authenticator Msgs.......................... 0
Pending Requests................................ 0
Timeout Requests................................ 0
Unknowntype Msgs................................ 0
Other Drops..................................... 0
```

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”.



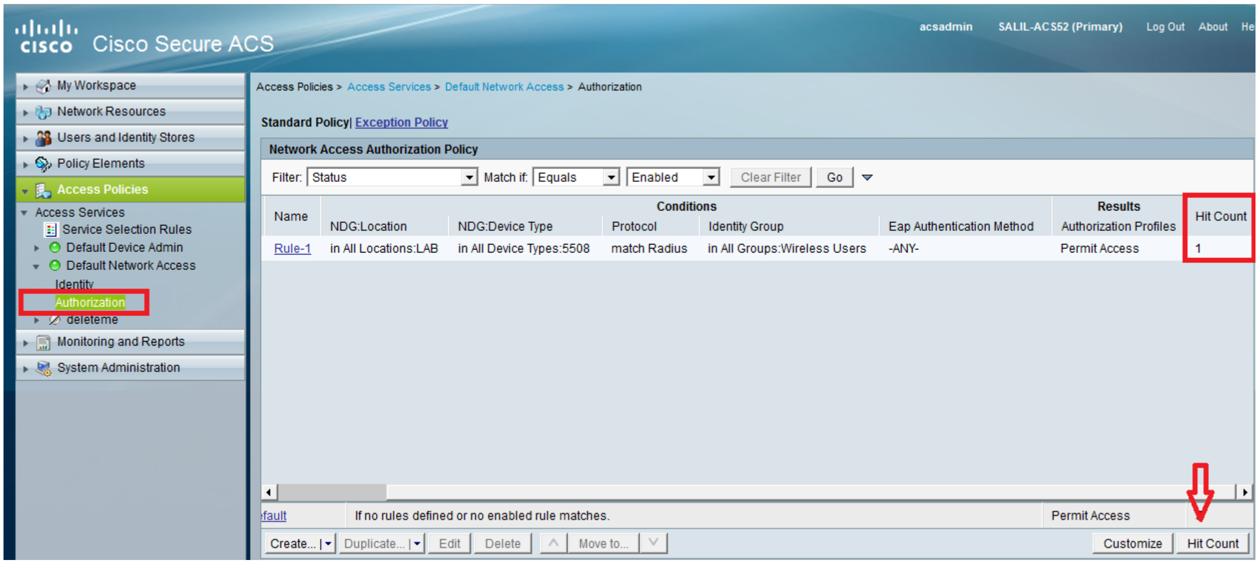
Access Policies > Access Services > Service Selection Rules

○ 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

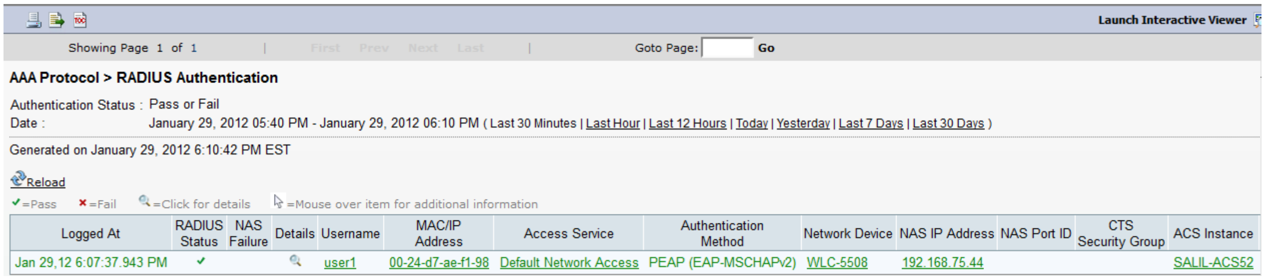
Network Access Authorization Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

Name	Conditions NDG:Location	NDG:Device Type	Protocol	Identity Group	Eap Authentication Method	Results Authorization Profiles	Hit Count
Rule-1	in All Locations:LAB	in All Device Types:5508	match Radius	in All Groups:Wireless Users	-ANY-	Permit Access	1

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

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

AAA Protocol > RADIUS Authentication

Authentication Status : Pass or Fail
Date : January 29, 2012 05:40 PM - January 29, 2012 06:10 PM (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

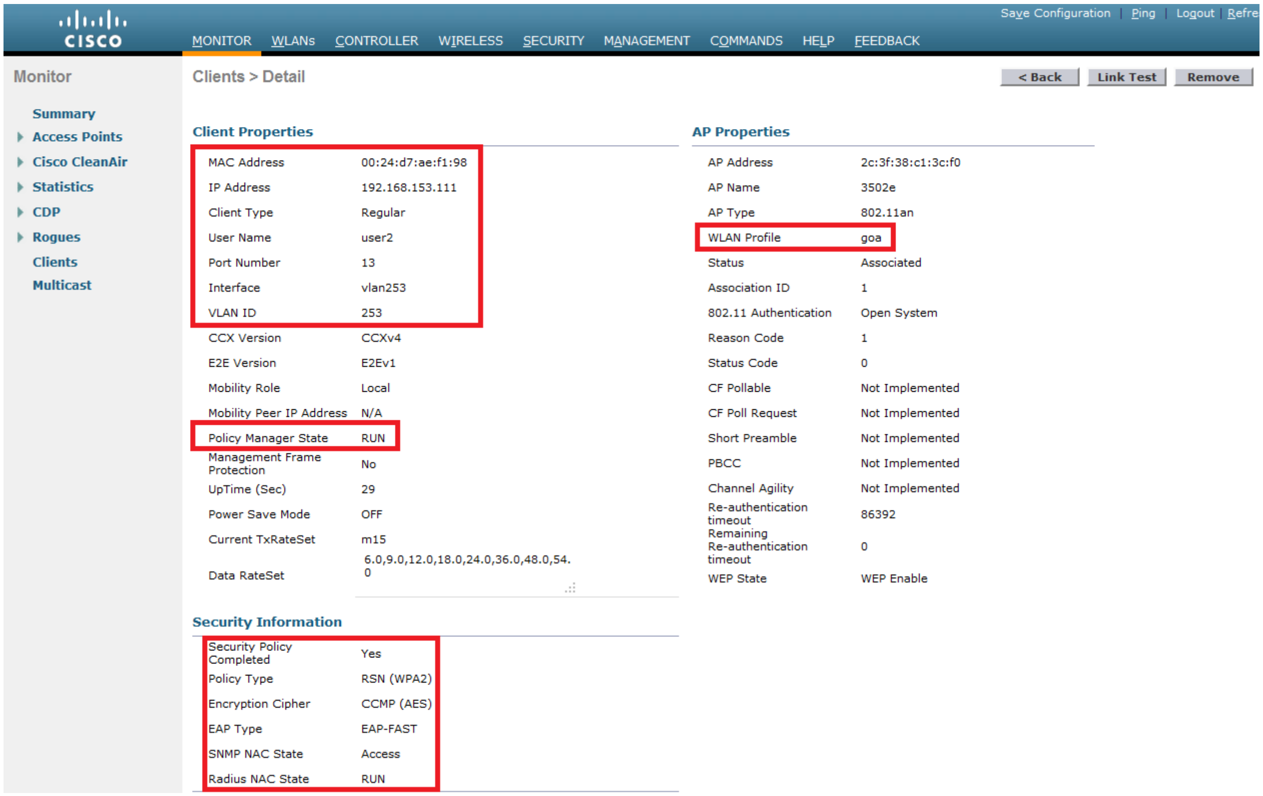
Generated on January 29, 2012 6:10:42 PM EST

Reload
✓=Pass ✗=Fail =Click for details =Mouse over item for additional information

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 Group	ACS Instance
Jan 29,12 6:07:37.943 PM	✓		🔍	user1	00-24-d7-ae-f1-98	Default Network Access	PEAP (EAP-MSCHAPv2)	WLC-5508	192.168.75.44			SALIL-ACS52

Verify- user2 (eapfast)

WLC GUI : Monitor → Clients → Select the MAC address.



CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refre
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Multicast
< Back
Link Test
Remove

Clients > Detail

Client Properties

MAC Address	00:24:d7:ae:f1:98
IP Address	192.168.153.111
Client Type	Regular
User Name	user2
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	29
Power Save Mode	OFF
Current TxRateSet	m15
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0

AP Properties

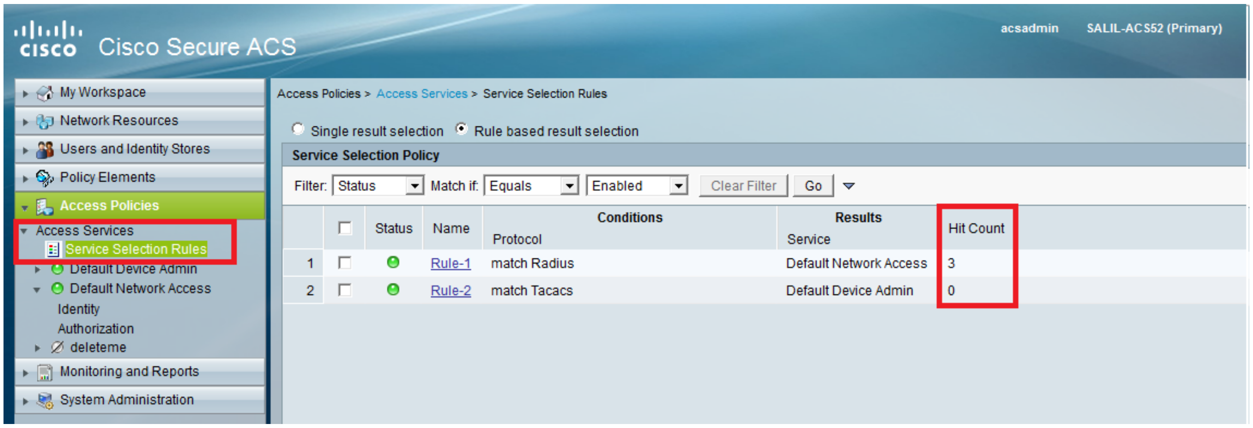
AP Address	2c:3f:38:c1:3c:f0
AP Name	3502e
AP Type	802.11an
WLAN Profile	goa
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86392
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

ACS Logs:

3) 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".



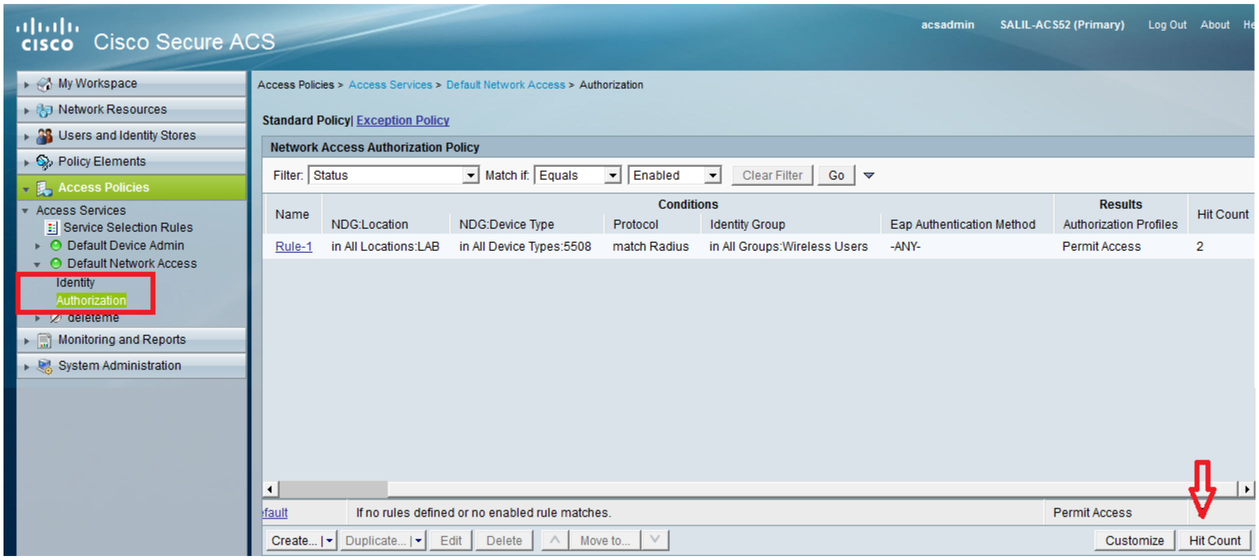
Access Policies > Access Services > Service Selection Rules

○ 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	3
2	☐	●	Rule-2	match Tacacs	Default Device Admin	0



Access Policies > Access Services > Default Network Access > Authorization

Standard Policy| Exception Policy

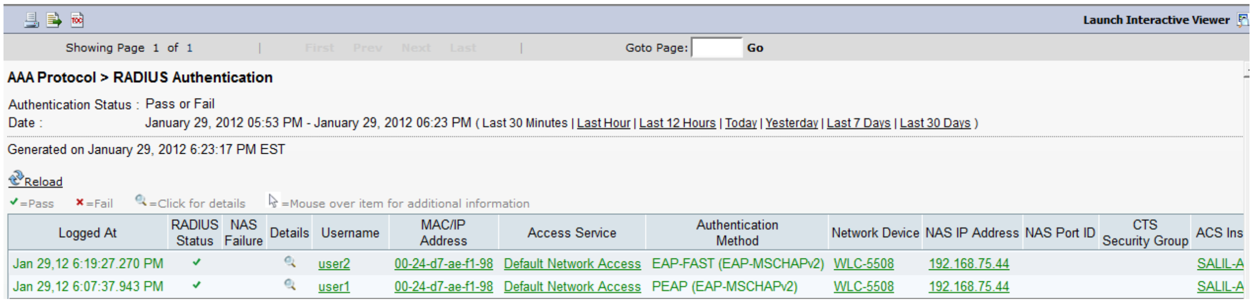
Network Access Authorization Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

Name	Conditions NDG:Location	NDG:Device Type	Protocol	Identity Group	Eap Authentication Method	Results Authorization Profiles	Hit Count
Rule-1	in All Locations:LAB	in All Device Types:5508	match Radius	in All Groups:Wireless Users	-ANY-	Permit Access	2

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

4) 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 05:53 PM - January 29, 2012 06:23 PM (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on January 29, 2012 6:23:17 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 Group	ACS Ins
Jan 29,12 6:19:27.270 PM	✓		🔍	user2	00-24-d7-ae-f1-98	Default Network Access	EAP-FAST (EAP-MSCHAPv2)	WLC-5508	192.168.75.44			SALIL-A
Jan 29,12 6:07:37.943 PM	✓		🔍	user1	00-24-d7-ae-f1-98	Default Network Access	PEAP (EAP-MSCHAPv2)	WLC-5508	192.168.75.44			SALIL-A

Troubleshooting:

1) If you run into issues run the following commands on WLC :

debug client <mac add of the client>
debug aaa all enable
show client detail <mac addr>. Verify the policy manager state.
show radius auth statistics. Verify the failure reason.

debug disable-all . To turn off debugs.
clear stats radius auth all. This command is used to clear radius statistics on the WLC.

2) Verify the logs in the ACS and see the failure reason.