

Configurar RADIUS y WLC (802.1X)

Configurar RADIUS on Linux

1. Instalar freeRADIUS
 - a. Sudo apt-get install freeradius
2. Verificar versión
 - a. Freeradius -v
3. Crear usuarios
 - a. nano /etc/freeradius/users
 - b. usuario Cleartext := "Password"

```
# Educational purposes, they may be deleted from the deployed
# configuration without impacting the operation of the server.
#
oscar Cleartext-Password := "123456"
luis Cleartext-Password := "luis123"
cris Cleartext-Password := "cris123"
victor Cleartext-Password := "victor123"
#
# Deny access for a specific user. Note that this entry MUST
```

4. Configurar cliente WLC
 - a. Nano /etc/freeradius/client.conf
 - b. Client "Nombre_Cliente {
ipaddr = IPADDR
secret = SecretPass
shortname = WLC_NAME
nastype = Tipo_de_Dis
}

```
#}
client WLC_INS {
    ipaddr = 172.16.0.5
    secret = 123456
    shortname = WLC_INS
    nastype = cisco
}
```

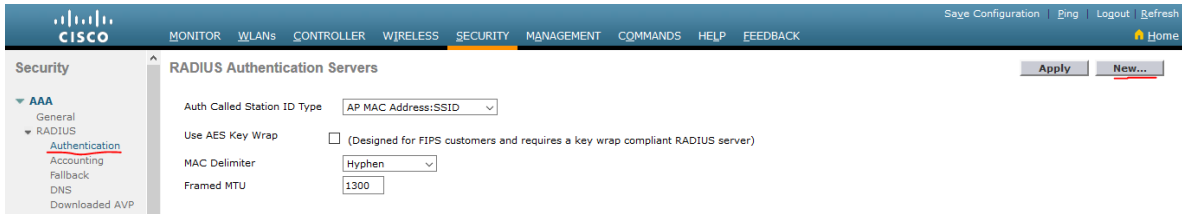
5. Reestablecer servicios
 - a. Service freeradius restart
6. Test de usuarios

- a. radtest usuario Password localhost 1812 testing123

```
root@ubuntu:~# radtest oscar 123456 127.0.0.1 testing123
Usage: radtest [OPTIONS] user passwd radius-server[:port] nas-port-number secret [ppphint] [nasname]
  -d RADIUS_DIR      Set radius directory
  -t <type>          Set authentication method
                    type can be pap, chap, mschap, or eap-md5
  -P protocol        Select udp (default) or tcp
  -x                 Enable debug output
  -4                 Use IPv4 for the NAS address (default)
  -6                 Use IPv6 for the NAS address
root@ubuntu:~# radtest cris cris123 localhost 1812 testing123
Sent Access-Request Id 26 from 0.0.0.0:53572 to 127.0.0.1:1812 length 74
  User-Name = "cris"
  User-Password = "cris123"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Cleartext-Password = "cris123"
Received Access-Accept Id 26 from 127.0.0.1:1812 to 0.0.0.0:0 length 20
```

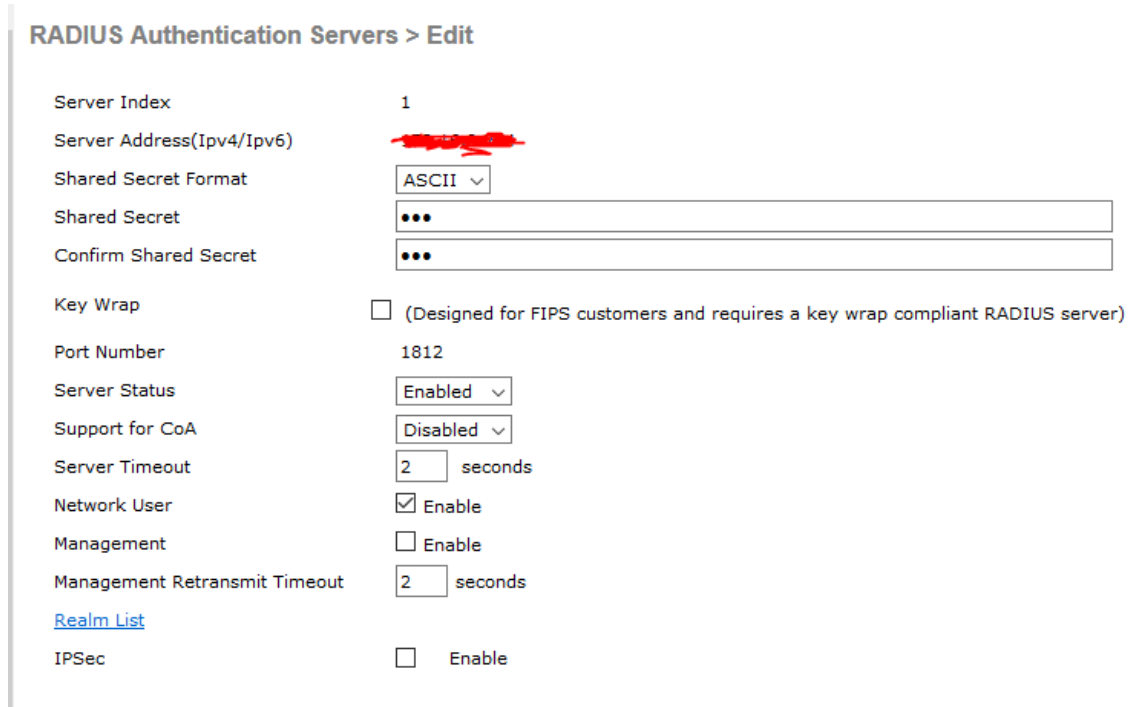
Configurar WLC

Acceder a la WLC > Security > RADIUS > Authentication > New...



Agregar siguiente información:

1. IP del Servidor
2. Secret (revisar paso 4 de instalación de RADIUS)



- 3.
4. Reestablecer servicios de servidor Radius (Revisar paso 5 de Instalación de RADIUS)
5. Seleccionar WLAN a la cual se configurará la autenticación



- a.
6. Security > Layer 2
 - a. WPA+WPA2
 - b. WAP Policy
 - c. WPA Encryption > AES

d. 802.1X

The screenshot shows the 'WLANs > Edit 'Test'' configuration page. The 'Security' tab is selected. Under the 'Layer 2' sub-tab, the 'Layer 2 Security' is set to 'WPA+WPA2'. The 'MAC Filtering' checkbox is unchecked. The 'WPA+WPA2 Parameters' section includes: 'WPA Policy' (checked), 'WPA Encryption' (checked) with 'AES' selected and 'TKIP' unselected, 'WPA2 Policy' (unchecked), and 'OSEN Policy' (unchecked). The 'Authentication Key Management' section includes: '802.1X' (checked) with 'Enable' selected, 'CCKM' (unchecked) with 'Enable' selected, 'PSK' (unchecked) with 'Enable' selected, and 'WPA gtk-randomize State' (unchecked) with 'Disable' selected.

e.

7. Security AAA Server

a. Seleccionar Servidor RADIUS

The screenshot shows the 'WLANs > Edit 'Test'' configuration page. The 'Security' tab is selected. Under the 'AAA Servers' sub-tab, the instruction reads: 'Select AAA servers below to override use of default servers on this WLAN'. The 'RADIUS Servers' section includes: 'RADIUS Server Overwrite interface' (unchecked) with 'Enabled' selected. Below this are three columns: 'Authentication Servers', 'Accounting Servers', and 'EAP Parameters'. The 'Authentication Servers' and 'Accounting Servers' columns each have a checked 'Enabled' checkbox. The 'EAP Parameters' column has an unchecked 'Enable' checkbox. A table lists six servers:

Server	Authentication Servers	Accounting Servers	EAP Parameters
Server 1	IP:172.16.0.254, Port:1812	None	Enable
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

b.

8. Apply

9. Probar autenticación de la SSID