

Setting up a RADIUS Server

Goal: To set up a LANforge wireless access point with a local RADIUS server.

-
1. The LANforge **auto-install --do_radius** option will setup FreeRADIUS on the LANforge system with two example EAP methods, EAP-TLS and EAP-TTLS
 2. The config files for FreeRADIUS are located in **/etc/raddb**
 - A. **/etc/raddb/certs** contains the files necessary for **EAP-TLS**
 - B. The LANforge auto-install copies the necessary files into **/home/lanforge** for use by LANforge wireless clients.

- C. For **EAP-TLS**, use client.p12 as the client's Private Key and ca.pem as the client's CA Cert File. The Private Key password is lanforge

sta205 (ct523-3n-f20) Configure Settings

Port Status Information

Current: LINK-UP GRO Associated

Driver Info: Port Type: WIFI-STA Parent: wiphy2 [wiphy2...](#)

Port Configurables

Standard Configuration **Advanced Configuration** Misc Configuration Corruptions Custom WiFi

Advanced WiFi Settings

Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

Key Management:	WPA-EAP	HESSID:	00:00:00:00:00:00
Pairwise Ciphers:	DEFAULT	Realm:	
Group Ciphers:	DEFAULT	Client Cert:	
WPA PSK:		IMSI:	
EAP Methods:	EAP-TLS	Milenage:	
EAP Identity:		Domain:	
EAP Anon Identity:		Consortium:	
EAP Password:		Phase-1:	
EAP Pin:		Phase-2:	
Private Key:	/home/lanforge/client.p12	PK Password:	lanforge
CA Cert File:	/home/lanforge/ca.pem	PAC File:	
Network Auth:		ieee80211w:	Disabled (0)

☒ Advanced/802.1x ☐ Enable 802.11u ☐ HotSpot 2.0 ☐ Enable PKC

Print Display Probe Display Scan Sync Apply OK Cancel

- D. /etc/raddb/users contains the user and password for **EAP-TLS**

- E. The example **EAP-TTLS** user is testuser with password testpasswd. Additional entries can be added to the users file, then restart FreeRADIUS with systemctl restart radiusd.service

Port Status Information

Current: LINK-UP GRO Authorized

Driver Info: Port Type: WIFI-STA Parent: wiphy2 [wiphy2...](#)

Port Configurables

Standard Configuration **Advanced Configuration** Misc Configuration Corruptions Custom WiFi

Advanced WiFi Settings

Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

Key Management: **WPA-EAP** HESSID: 00:00:00:00:00:00

Pairwise Ciphers: DEFAULT Realm:

Group Ciphers: DEFAULT Client Cert:

WPA PSK: IMSI:

EAP Methods: **EAP-TTLS** Milenage:

EAP Identity: **testuser** Domain:

EAP Anon Identity: Consortium:

EAP Password: **testpasswd** Phase-1:

EAP Pin: Phase-2:

Private Key: PK Password:

CA Cert File: PAC File:

Network Auth: IEEE80211w: Disabled (0)

☒ Advanced/802.1x ☐ Enable 802.11u ☐ HotSpot 2.0 ☐ Enable PKC

Print Display Probe Display Scan Sync Apply OK Cancel

3. An alternative to FreeRADIUS is to use the hostapd RADIUS server.

- A. Stop the FreeRADIUS service with systemctl stop radiusd.service

- B. Modify the interface to use for the hostapd process and select the RADIUS checkbox.

The screenshot shows the 'eth1 (ct521-1ac-f20) Configure Settings' window. The 'Services' section on the left has the 'RADIUS' checkbox checked and highlighted with a red box. Other sections include 'General Interface Settings', 'Port Rates', 'Advert Rates', and 'Offload'.

- C. Create a hostapd_<port-name>.conf file in the /home/lanforge/wifi directory with the following info.

```
root@ct521-1ac-f20:/home/lanforge/wifi
File Edit View Search Terminal Help
[root@ct521-1ac-f20 wifi]# cat hostapd_eth1.conf
interface=eth1
driver=wired
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
dump_file=/home/lanforge/wifi/hostapd_eth1.dump
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0
ieee8021x=1
eapol_key_index_workaround=0
eap_server=1
eap_user_file=/etc/hostapd.eap_user
server_id=lf0301.lanforge.com
eap_sim_db=unix:/tmp/hlr_auc_gw.sock
radius_server_auth_port=1812
radius_server_clients=/etc/hostapd.radius_clients

ca_cert=/etc/raddb/certs/ca.pem
server_cert=/etc/raddb/certs/server.pem
private_key=/etc/raddb/certs/server.key
private_key_passwd=lanforge

[root@ct521-1ac-f20 wifi]#
```

D. Setup the desired EAP methods and passwords in the /etc/hostapd.eap_users file.

```
root@ct521-1ac-f20:/etc
File Edit View Search Terminal Help
[root@ct521-1ac-f20 etc]# cat hostapd.eap_user
"dot11r.user" PEAP
"dot11r.user" MSCHAPV2 "!!dot11r123" [2]

"dot11r.user@lanforge.com" PEAP
"dot11r.user@lanforge.com" MSCHAPV2 "!!dot11r123" [2]

"user-md5" MD5 "!!user-md5" [2]

"user-fast" MSCHAPV2 "!!fast123" [2]

"lanforge.peap" PEAP
"lanforge.peap" MSCHAPV2 "!!lanforge123" [2]

"lanforge.peap@lanforge.com" PEAP
"lanforge.peap@lanforge.com" MSCHAPV2 "!!lanforge123" [2]

"lanforge.tls" TLS

"lanforge.ttls" TLS,TTLS
"lanforge.ttls" MD5,TTLS-PAP,TTLS-CHAP,TTLS-MSCHAP,TTLS-MSCHAPV2 "!!ttls123" [2]

"lanforge.gtc" TTLS,PEAP
"lanforge.gtc" GTC "!!gtc123" [2]

"0"* AKA
"1"* SIM
* TTLS

"*@lanforge.com" TLS
"0"* SIM,TTLS,TLS,PEAP,AKA
"1"* SIM,TTLS,TLS,PEAP,AKA

"*@mytest.com" TLS
"0"* SIM,TTLS,TLS,PEAP,AKA
"1"* SIM,TTLS,TLS,PEAP,AKA

[root@ct521-1ac-f20 etc]#
```

E. If using **EAP-SIM** or **EAP-AKA**, verify entries in the /etc/hlr_auc_gw.milenage_db file, then start the HLR tool.

```
root@ct521-1ac-f20:/home/lanforge
File Edit View Search Terminal Help
[root@ct521-1ac-f20 lanforge]# pwd
/home/lanforge
[root@ct521-1ac-f20 lanforge]# . lanforge.profile
[root@ct521-1ac-f20 lanforge]# hlr_auc_gw -m /etc/hlr_auc_gw.milenage_db > /tmp/hlr_auc_fw.log &
[1] 27335
[root@ct521-1ac-f20 lanforge]# ps auxwww |grep hlr
root    27335  0.0  0.0 19676 2204 pts/0    S   09:15   0:00 hlr_auc_gw -m /etc/hlr_auc_gw.milenage_db
root    27338  0.0  0.0 112668 2304 pts/0    S+  09:15   0:00 grep --color=auto hlr
[root@ct521-1ac-f20 lanforge]#
```


F. Verify the hostapd process is running for the interface selected for the RADIUS server, here it is eth1.

```
root@ct521-1ac-f20:/home/lanforge
File Edit View Search Terminal Help
[root@ct521-1ac-f20 lanforge]# ps auxwww |grep hostapd_eth1
root      808    0.0   0.0 112668 2308 pts/0    S+   09:36   0:00 grep --color=auto hostapd_eth1
root     15628  0.0   0.0 56380 4816 ?        S<s  08:32   0:00 ./local/bin/hostapd -t -d -f /home/lanforge/
/wifi/hostapd_log_eth1.txt -B -P /home/lanforge/wifi/hostapd_eth1.pid wifi/hostapd_eth1.conf
[root@ct521-1ac-f20 lanforge]#
```

4. Whether you use FreeRADIUS or hostapd RADIUS, setup your AP with the RADIUS server's IP address and port.

A. If using a LANforge AP on the same system as the RADIUS server, then the AP will address the RADIUS server at localhost or 127.0.0.1 with port 1812.

The screenshot shows the 'vap1 (ct521-1ac-f20) Configure Settings' window. The 'Advanced Configuration' tab is selected. The 'Advanced WiFi Settings' section is expanded, and the 'RADIUS IP', 'RADIUS Port', and 'RADIUS Secret' fields are highlighted with a red box. The 'RADIUS IP' is set to '127.0.0.1', 'RADIUS Port' is '1812', and 'RADIUS Secret' is 'lanforge'. Other settings like 'Pairwise Ciphers', 'Group Ciphers', 'Ignore Probes', 'Ignore Auth-Assoc', 'Ignore Assoc', 'Ignore Re-Assoc', 'Corrupt GTK', 'HS20 Capabilities', 'HS20 Oper Class', 'HS20 WAN Metrics', 'IEEE80211w', 'Venue Group', 'Network Type', 'Network Auth', 'Use 80211d', 'Use 80211h', 'BSS-Load', 'Neighbor Reports', 'BSS Transition', 'Advanced/802.1x', 'Short-Preamble', 'HotSpot 2.0', 'Disable DGAF', 'Enable 802.11u', '802.11u Internet', '802.11u ASRA', '802.11u ESR', and '802.11u UESA' are also visible.

B. If using an external AP or WLAN Controller, then configure the device to address the RADIUS server on the network connected to a LANforge interface configured for RADIUS.