Configuration example with FreeRadius 802.1X authentication server

This is an example of `RADIUS` server supporting the `802.1X` authentication methods:

- `FreeRadius V3.0.19` (Ubuntu Linux)

FreeRadius server: reactivate or inactivate 802.1X authentication methods In the `FreeRadius` server, the authentication method can be inactivated or reactivated in the files below:

file name	CHAP	PAP	MSCHAP	MD5	GTC	TLS	TTLS	PEAPV0	MSCHAPV2	FAST
`/opt/etc/raddb/mods-enabled/chap`	yes	-	-	-	-	-	-	-	-	-
`/opt/etc/raddb/mods-enabled/pap`	-	yes	-	-	-	-	-	-	-	-
`/opt/etc/raddb/mods-enabled/mschap`	-	-	yes	-	-	-	-	-	-	-
`/opt/etc/raddb/mods-enabled/eap`	-	-	-	yes	yes	yes	yes	yes	yes	yes

FreeRadius server: location example of trusted and server certificate

`freeradius/alpine-innes/certificate_files/ca.pem`: trusted certificate (auto-signed) `freeradius/alpine-innes/certificate_files/server.pem`: `RADIUS` server's certificate

Check that `FreeRadius` server has valid intermediate certificates (ca.pem) and server certificate (server.pem):

- .p12 to .pem

```
openssl pkcs12 -in client.p12 -out client.pem
```

- .pem certificate edition

```
openssl x509 -in client.pem -text
openssl x509 -in server.pem -text
openssl x509 -in ca.pem -text
```

If not valid, regenerate again the certificate with a valid date. Store carefully the `ca.pem` trusted certificate which should be needed to configure the `Qeedji` device.

FreeRadius server: location for configuration file example to declare the switchs supporting the 802.1X security

`../freeradius/alpine-innes/config-files/clients.conf`

In the `clients.conf` file, declare a client for each switches supporting `802.1X` security running in the secured network.

```
client <name> {
    ipaddr = <LAN switch1 IP address>
    secret = <freetext_secret_number>
}

client <name> {
    ipaddr = <WLAN switch2 IP address>
    secret = <freetext_secret_number>
}
```

extract of `clients.conf` file example

```
# switch TP-Link
client TPLink-1500G {
    ipaddr = 192.168.1.129
    secret = password
}

# AP TP-Link
client TPLink-EAP225 {
    ipaddr = 192.168.1.220
    secret = password
}
```

FreeRadius server: location for configuration file example to declare the devices which has to be authenticate in the 802.1X secured network `../freeradius/alpine-innes/config-files/authorize`

In the `authorize` file, declare a client for each device having to work in the secured network.

```
# <device_name_comment>
<device_LAN_MAC_address_number> Cleartext-Password := "
<device_LAN_MAC_address_in_lower_case_without_dash>"
        Reply-Message = "Hello, %{User-Name}"
```

IMPORTANT: Whatever whether your Gekkota OS device is working with LAN or WLAN interface, enter in this file the LAN MAC address shown in the WebUI or shown on the test card or stuck at the back of the device `<device_LAN_MAC_address_in_lower_case_without_dash>` (MAC stamped with a star when the testcard is activated on the Gekkota OS device).

extract of `authorize` file example

```
# sma300 wifi
001ce6021e45    Cleartext-Password := "001ce6021e45"
        Reply-Message = "Hello, %{User-Name}"

# sma300 wifi 2
001ce6023bdc    Cleartext-Password := "001ce6023bdc"
        Reply-Message = "Hello, %{User-Name}"

# sma300
001ce6020f59    Cleartext-Password := "001ce6020f59"
        Reply-Message = "Hello, %{User-Name}"

# dmb400
001ce60222e8    Cleartext-Password := "001ce60222e8"
```

```
        Reply-Message = "Hello, %{User-Name}"

# dmb400-00003 wifi
001ce602440b    Cleartext-Password := "001ce602440b"
        Reply-Message = "Hello, %{User-Name}"

# dme204
00142d407975    Cleartext-Password := "00142d407975"
        Session-timeout = 3600,
        Reply-Message = "Hello, %{User-Name}"
```

FreeRadius toolbox: client certificate generation with the trusted certificate for the device

The `FreeRadius` toolbox offers the possibility to generate, with the appropriate trusted certificated, the required client certificates for the devices. They have to be generated the one after the other. The `FreeRadius` toolbox prevent to generate twice a `client.p12` certificate for a given device. So rename it, and do think to store carefully the generated `.p12` certificate for your device.

Edit the source file `client.cnf` and enter the input_password and output password required when needing to load the `.p12` certificate in the `Qeedji` Gekkota OS device. `\\192.168.2.0\innes\freeradius-server-3.0.19\raddb\certs\client.cnf`

Copy the `freeradius/alpine-innes/certificate_files/ca.pem` to `\\192.168.2.0\innes\freeradius-server-3.0.19\raddb\certs\client.cnf`

```
input_password      = <p12_certificate_private_password>
output_password     = <p12_certificate_private_password>
countryName     = FR
stateOrProvinceName = <your_state>
localityName        = <your_city>
organizationName    = <your_organization>
emailAddress        = <your_email_address>
commonName      = <device_LAN_MAC_address_in_lower_case_without_dash>
```

Extract of `client.cnf` file example

```
[ req ]
prompt          = no
distinguished_name  = client
default_bits        = 2048
input_password      = whatever
output_password     = whatever

[client]
countryName     = FR
stateOrProvinceName = France
localityName        = Paris
organizationName    = Qeedji
emailAddress        = john.smith@qeedji.tech
commonName      = 001ce602440b
```

Launch the `client.p12` certificate generation for your device with the command

```
make client.pem
```

Trouble shooting options

- In case authentication issue, check that:
  - your serveur RADIUS is running properly with, the appropriate IP address value declared in the switch,
  - the serveur RADIUS trust certificate has a validity date which has not expired. The clients certificate with with trust certificate have also a validity date which has not expired,
  - the authentication methods used on the devices are properly supported by the server,
  - the devices MAC are properly declared on the server with the right MAC address,
  - 802.1X switches are properly declared on the server with the right IP address.

Others examples of RADIUS servers

RADIUS authentication server equipment examples
FreeRADIUS [2]
Cisco Aironet 1200 AP (local RADIUS server)
hostapd
Periodik Labs Elektron
Lucent NavisRadius
Interlink RAD-Series
Radiator
Meetinghouse Aegis
Funk Steel-Belted
Funk Odyssey
Microsoft IAS

[2] RADIUS authentication server used for qualification

Some identification method names supported by your RADIUS authentication server may be not supported by the Gekkota OS device or reciprocally. For further information, contact support@qeedji.tech