WiFi WPA Enterprise

Win 11

Windows 11 22H2 not connecting to WPA Enterprise

1. Open Registry Editor
2. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\RasMan\PPP\EAP\13`
3. Create `DWORD` key `TlsVersion` value `FC0`

`TlsVersion` coding (values cane be OR-ed):

1. 0000 1100 0000 = 0x0C0 TLS1.0
2. 0011 0000 0000 = 0x300 TLS1.1
3. 1100 0000 0000 = 0xC00 TLS1.2

Android 11+ Devices

NOTE: DRAFT!

Freeradius log:

```
eap_peap: TLS Alert read:fatal:unknown CA
```

Reason: The CA (Certification Authority) is not recognized by the client.

Cerficate used by Freeradius:

/etc/freeradius/3.0/mods-enabled/eap

```
    private_key_file = /etc/ssl/private/radius.int.example.com.key
    certificate_file = /etc/ssl/certs/radius.int.example.com.crt
```

Background:

- https://extremeportal.force.com/ExtrArticleDetail?an=000092023
- Certificate Compatibility

Hints:

Workaround for Android based phone:

- Download own CA from URL. Do not install it.
- Open `Settings` -> `Security` -> `Encryption & Credentials` -> `Install a`

`Certificate -> Wi-Fi Certificate`

- Try to connect to WPA Enterprise network
  - EAP Method: PEAP
  - Phase 2 authentication: MSCHAPV2
  - CA certificate: Install. After installation choose just installed certificate
  - Online certificate status: Do not verify

TODO

Android:

- “Domain” = CN from radius cert (=radius host name?)
- Possible to add alternate names to cert to use short domain

https://learn.microsoft.com/pl-pl/mem/intune/configuration/wi-fi-settings-android-enterprise

https://community.ui.com/questions/what-domain-for-android-when-setting-up-wpa2-enterprise-w-built-in-radius/4efa22a5-c909-465b-9755-a8507e34b08a#answer/3a14eb34-5ead-47ed-9472-910752c7ee50

https://community.ui.com/questions/UDM-Radius-WPA-Enterprise-Android-11/10e1ef71-a0e5-4b83-885d-80deccbdef25

```
I don't disagree, but bottom line is that 11 will never connect without a trusted CA root (and all intermediates in the chain, if there are any, above the certificate your RADIUS server is presenting) physically installed to the phone. Just how it is.
```

Starting with Android 11 QPR1, you must enter the domain for server certification validation in order to successfully connect.

https://extremeportal.force.com/ExtrArticleDetail?an=000092023

```
The RADIUS certificate used by the 802.1X wireless controller or access point must use either:

    A certificate signed by a trusted public Root certificate authority and configured to supply clients with the full certificate chain (root -> intermediate(s) -> server), OR
    In the case of self-signed or private CA, pre-load the root and any intermediate certificates on the device's trust store prior to connection.
```

Add both certs to client ? how to add intermediate ca ?

New CA are added to `User store` only. There is no option without root right to move it to `System store`

FreeRadius with mixed CAs

/etc/freeradius/3.0/mods-enabled/eap

Use `ca_path` or `ca_file` not both. Using `ca_path` requires run `c_rehash` on pointed dir to created

hashes do certs.

```
tls-config tls-common {
  private_key_password =
  private_key_file = ${certdir}/radius.int.example.com.key

  certificate_file = ${certdir}/radius.int.example.com.crt
  ca_path = ${cadir}

  auto_chain = yes
}
```

```
tls-config tls-common {
  private_key_password =
  private_key_file = ${certdir}/radius.int.example.com.key

  certificate_file = ${certdir}/radius-chain.crt
  auto_chain = no
}
```

apt-get install eapoltest

Consider one selfsigned CA: https://networkradius.com/doc/3.0.10/raddb/home.html