Using the FreeRADIUS Users File

FreeRADIUS by default supports a flat file format as a local identity store. This flat file is stored as `/etc/raddb/users` (or `/etc/freeradius/users`).

The file consists of a series of configuration directives used by the `files` module to authorise and authenticate users.

The basic user entry looks like this:

```
username<tab>[Authorisation item], [Authorisation item], ...
<tab><tab>[Reply item], [Reply item], ...
```

The formatting of the stanza above is very important. There should be a <tab> in between the username and any authorisation items, and a line break followed by a <tab> before any reply items.

The minimum authorisation item next to the username would be a corresponding password entry. Usually this password is in clear text, indicated by the attribute `Cleartext-Password`. Reply items on the subsequent line are optional.

A sample user entry

```
moonshot        Cleartext-Password := "testing1234"
                        User-Name = 'moonshot'
```

For more information about configuration directives, see the FreeRADIUS man page for users(5).

For Moonshot, it is recommended that `files` lookups and authentications are limited to the `/etc/raddb/sites-available/inner-tunnel` (or `/etc/freeradius/sites-available/inner-tunnel`) file, as Moonshot uses EAP-TTLS and the real username is only exposed in the tunnel itself.

1. For initial testing

For the purposes of initial testing, you can use a simple local flat file, creating a user with username "testuser" and password "testing".

1. Open `/etc/raddb/users` (or `/etc/freeradius/users`) for editing and put the following at the top of the file:

```
testuser        Cleartext-Password := "testing"
                        Reply-Message = "Hello test user. You have authenticated!"
```

2. For small-scale deployments

For a small-scale deployment, such as a pilot project or an Authentication Policy Community, follow the above step for each of the users you wish to add, starting each user on a new line.

If you do not wish to use clear-text passwords for your users, you may wish to use attributes such as `MD5-Password`, `SMD5-Password`, `Crypt-Password`, `SHA-Password`, `SSHA-Password` or `NT-Password` (see FreeRADIUS Rlm_ldap for details) instead of `Cleartext-Password` to obfuscate passwords in the appropriate format. If necessary, use Base64 encoding to make the value storable in the flat file.

Protocol and password format compatibility

Be aware that not all password obfuscation mechanisms are compatible with all RADIUS protocol types. For more information, please see the DeployingRADIUS Protocol and Password Compatibility matrix for more information.