# FreeRADIUS with LDAP

FreeRADIUS is often deployed with an LDAP directory used as the identity store.

This means that the password is retrieved from the directory as an attribute and then verified by FreeRADIUS. It is important that you know which obfuscation mechanism is being used in your LDAP directory as not all EAP authentication protocols are compatible with all obfuscation types. DeployingRADIUS, Alan DeKok's site, has a handy compatibility matrix that lists authentication systems and their authentication protocol compatibility.

To use LDAP directories with passthrough authentication (such as SASL) with FreeRADIUS, please see the FreeRADIUS + OpenLDAP with SASL topic. This may be your only option if the compatibility matrix shows that the obfuscation type is incompatible with the EAP-TTLS inner authentication type.

To use Active Directory as an LDAP directory, please see the Using Active Directory topic.

## Step-by-step guide

### 1. Modify FreeRADIUS LDAP support

1. Install the `freeradius-ldap` module, if you haven't already.
2. Configure the `ldap` module (in `/etc/raddb/mods-available` on RedHat/CentOS or `/etc/freeradius/mods-available` on Debian /Ubuntu) as per the standard configuration with the server name(s), port(s), and whether TLS is required.

   > We recommend you use TLS.

3. Configure the `identity` and `password` options for a user that will have browse and attribute retrieval rights on the LDAP directory.

   > We recommend using a user that is as unprivileged as possible and not used for anything else.

4. Below the `base_dn`, from which all searches start, you will find the `update` section, which returns attributes from LDAP.
5. This may include the `userPassword` LDAP attribute, which FreeRADIUS will use to authenticate. If the password attribute in your LDAP directory has a different name, change that here.
6. Scroll to the `user` section. You may wish to modify the `base_dn`, `filter`, and `scope` settings there to match what your LDAP directory requires to return a single user object. FreeRADIUS will set an `Ldap-UserDN` attribute that will be used for binding as a user if the search is successful.

   > You may wish to test your LDAP search with tools such as `ldapsearch` to test your DN and your filters. See http://wiki.freeradius.org/modules/Rlm_ldap for more information.

7. Save the file.

### 3. Modify FreeRADIUS EAP support, if necessary

It is rare that network access servers still use PAP. Instead, they use a variety of EAP types, which can wrap PAP to provide better security for user credentials. The default is EAP-MD5.

Depending on the compatibility matrix, you may need to adjust the `default_eap_type` for the `ttls` EAP type to something different.

The default settings in the `eap` module in FreeRADIUS set PAP as the password mechanism for EAP-GTC, so no changes are required. What is required though is setting the default type for EAP conversations:

1. To set the default EAP type in tunneled EAP conversations, such as EAP-TTLS, scroll to the `ttls` section, then set its `default_eap_type` to either `gtc` or `md5`.

   > PEAP support also includes a `default_eap_type` setting. This setting should not be modified.