Authentication through Azure Active Directory

This document describes how to set up TekRADIUS using external application Authenticator.exe to communicate with an OAuth2 *(Azure Active Directory)* identity provider backend allowing users to connect to a RADIUS authenticated network without needing on premise systems.

Microsoft Azure Active Directory supports Resource Owner Password Credentials Grant[1]. The Password Grant[2] does not require user interaction with a web browser which is impossible during RADIUS authentication.

For 802.1X and WPA Enterprise authentication, you must use EAP-TTLS/PAP dor other scenarios you must use PAP authentication method. MFA enabled accounts are not supported in Azure Active Directory.

Microsoft Azure AD (Office 365) Configuration

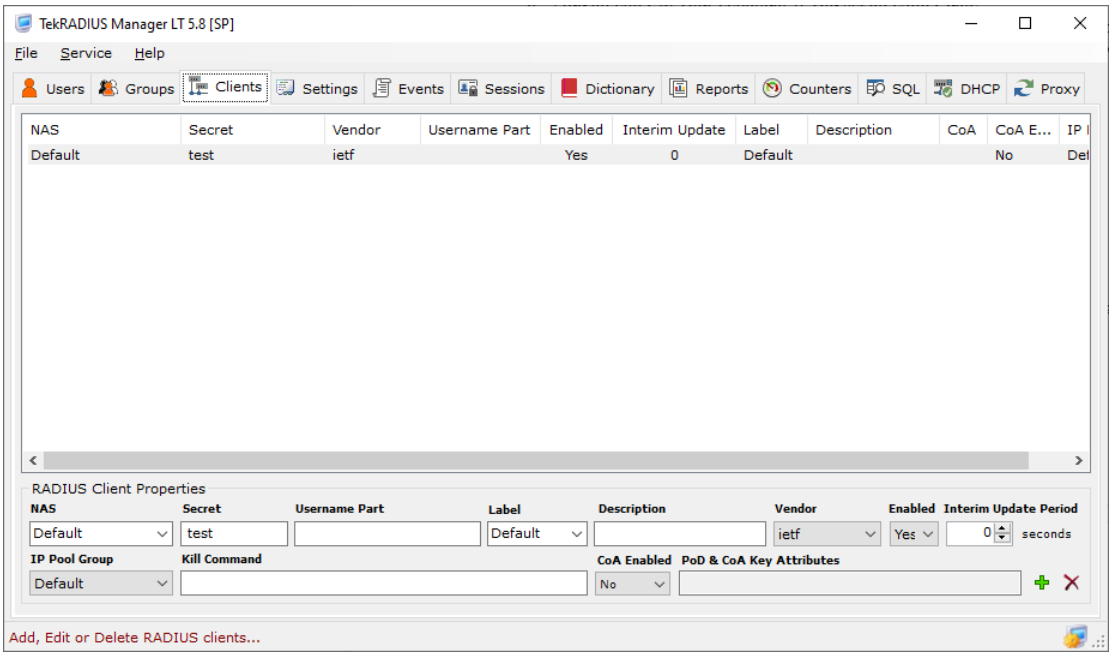
1. Log into your Microsoft Azure account as an administrator *(Microsoft Azure Portal)*
2. 

Go to “App registrations” and select “New registration”
3. Enter following and then click on “New Registration”
    a. **Name:** TekRADIUS-OAUTH2
    b. **Supported account types:** My organization only *(Single tenant)*
    c. **Redirect URI:** Leave it blank
4. Make a note of the “Client ID” for later use.
5. For your new application, go to “Certificates & secrets” and click “New client secret”
    a. You should enter the server name of your RADIUS server.
    b. Add an entry to your cellandar if you set an expiry date.
6. Make a note of the newly created “Client secret”. Client secret values cannot be viewed, except for immediately after creation. Be sure to save the secret when created before leaving the page.
7. Go to “API permissions”
    a. click on “Add a permission”
        i. go to the “Microsoft APIs” tab
        ii. select 'Microsoft Graph'
        iii. select “Application permissions”
        iv. check Directory.Read.All
        v. click on “Add permissions”
    b. User.Read should be an already present “Delegated” permission type
    c. Click on the “Grant admin consent” button *(An email notification will be sent)*

[1] https://tools.ietf.org/html/rfc6749#section-4.3
[2] https://oauth.net/2/grant-types/password/

TekRADIUS Configuration

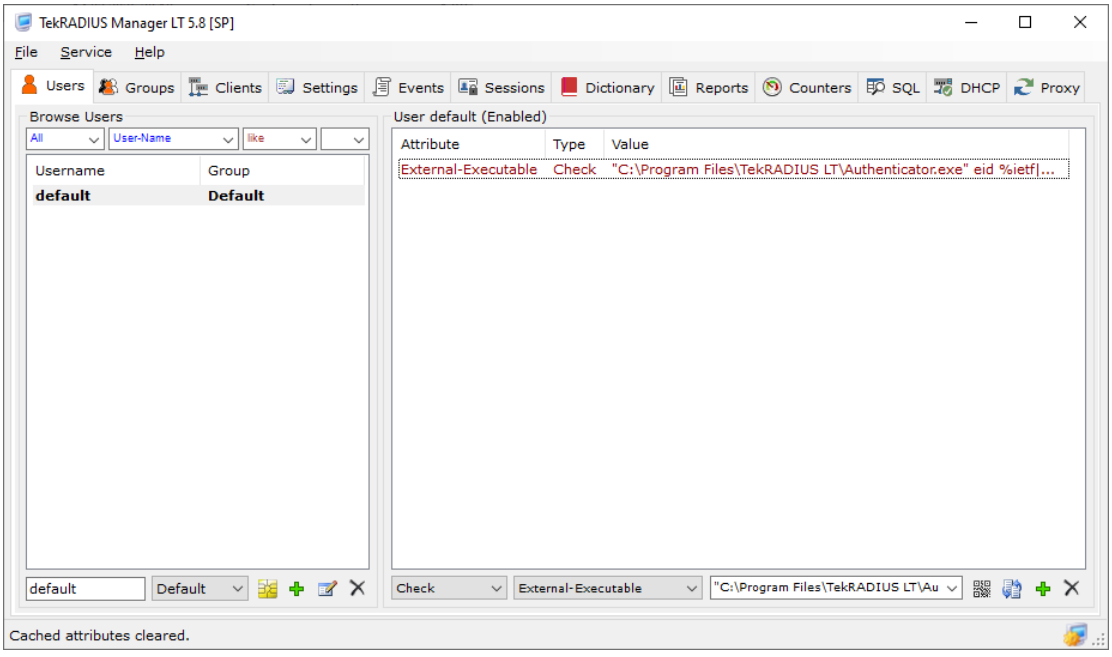
Create at least one client entry for your access device *(Acess controller, VPN server, Ethernet switch etc.)*



Download https://www.kaplansoft.com/TekRADIUS/release/Authenticator.zip extract Authenticator.exe and copy it to TekRADIUS applicaton directory *(C:\Program Files\TekRADIUS LT e.g.)* Add a user profile named default and add

```
External-Executable = "C:\Program Files\TekRADIUS LT\Authenticator.exe" eid %ietf|1% %ietf|2%
```

as a Check attribute.



Create a text file name Authenticator.ini with the following content based on the information you have noted while tenant creation in Azure Portal:

```
[example.com]
Tenant=123ea22d-72a4-775d-8e2e-7aa14a708062
ClientId=1d782735-64bf-47fb-b63f-95249dd049a9
ClientSecret=pAn8Q~ZajH268zdW07rLgRZfYSRQupsT_lhF1aax

[default]
Tenant=aaa
ClientId=bbb
ClientSecret=ccc
```

You can have a default tenant entry and individual tenant entires based on domain prefix in the usernames.

You can invoke Authenticator.exe though the command line for diagnostic purposes:

```
C:\Program Files\TekRADIUS LT>Authenticator eid test@example.com mypassword

Authentication successful.
```