2FA with Google Authenticator

Two factor authentication (2FA) enables increased security when authenticating user sessions. TekRADIUS supports many different ways to support 2FA. You can implement 2FA with Google Authenticator for local user profiles created in TekRADIUS.

2FA with Active Directory Accounts using Concatenated-Password Attribute

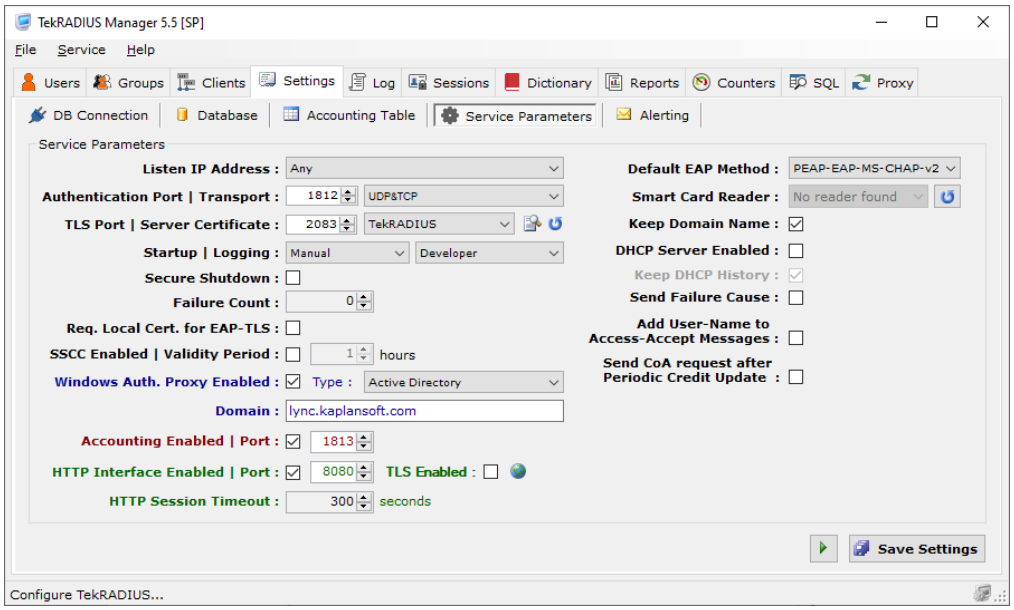
Concatenated-Password attribute allows you to specify a regular expression pattern to split received User-Password in an authentication request. TekRADIUS will update User-Password to value captured with regular expression capture group named **password**. You can get other part using capture group named **auxstr**. TekRADIUS will use updated User-Password in primary authentication method specified for the user. You can pass "auxstr" value in `%auxstr%` variable as a parameter to an executable specified with External-Executable. This is useful when you need to implement two factor authentication with an access server which does not support RADIUS challenges. Usage of this attribute requires a commercial license. Here is a sample;

```
Concatenated-Password = (?<auxstr>[^,]+),(?<password>.+)
```

Regular expression pattern must contain **password** and **auxstr** named capture groups. This regular expression splits received passwords concatenated with a comma in User-Password attribute and sets User-Password to second part of the original User-Password value. Captured first part value assigned to `%auxstr%` variable.

Concatenated-Password is a string type attribute and can exist only as a check attribute in User or Group profiles.

In this sample configuration, user will be authenticated against active directory and then received OTP will be validate with Google-Authenticator.

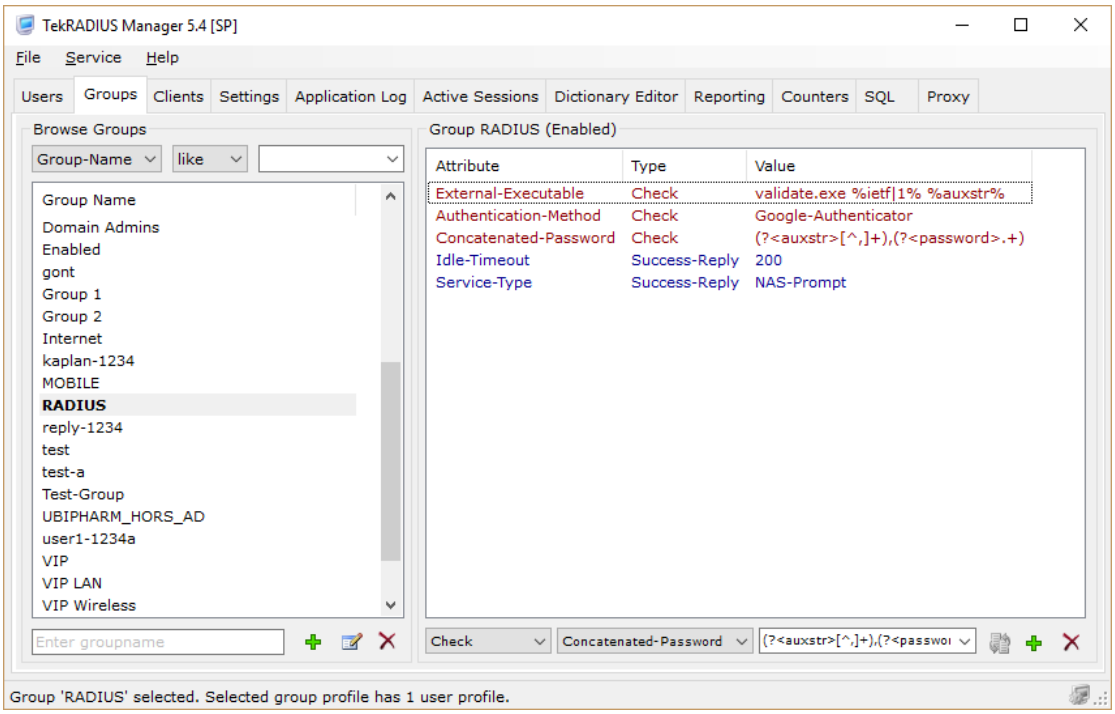


TekRADIUS Settings

We will use an Active Directory account named radius.user. This users' primary group name is RADIUS.

You need to enable Windows Auth. Proxy and set its type to Active directory in TekRADIUS Manager / Settings / Service Parameters. TekRADIUS Manager will automatically set domain name when you set Windows Auth. Proxy type. You also need to enable HTTP interface of TekRADIUS for users which will enable them to initialize their Google-Authenticator application in their mobile devices. Each user must be logged into TekRADIUS HTTP interface with their Active Directory account information and initialize their Google-Authenticator application.

Create a group profile for Active Directory RADIUS group in TekRADIUS,



Group Profile

Primary authentication method will be set to Google-Authenticator by adding Authentication-Method = Google-Authenticator as a check attribute to the group profile. User must be enter his/her password in following format;

```
Active Directory account password,Google-Authenticator OTP
```

User will enter Active Directory account password concatenated with Google-Authenticator OTP. You will also need an external utility to validate active directory account called validate.exe. This can be downloaded from https://www.kaplansoft.com/TekRADIUS/release/Validate.zip. Validate.exe, validates Active Directory user name and password in the command line and returns 0 as return code when validation is successful.

This is TekRADIUS log in developer mode for a successful authentication attempt;

```
26.08.2018 13:36:47.190 - RadAuth req. from : 192.168.88.3:54802 [UDP]

Size              : 120 / 120
Identifier        : 8
Attributes        :

 NAS-Port = 37
 User-Name = radius.user
 NAS-IP-Address = 192.168.88.3
 NAS-Identifier = 78-8A-20-BF-EA-B2
 Calling-Station-Id = 00-0E-C6-D3-F2-45
 Called-Station-Id = 78-8A-20-BF-EA-B1
 Framed-MTU = 1500

26.08.2018 13:36:47.206 - Authentication query; for user 'radius.user'; SELECT Attribute, Val from
Users with (NOLOCK) where UserName = 'radius.user' and Attribute <> 'ietf|1' and AttrType = 0

26.08.2018 13:36:47.300 - GoogleAuthenticator Authentication commencing for user 'radius.user'

26.08.2018 13:36:47.300 - External executable: validate.exe, Parameters: radius.user Xxx123!

26.08.2018 13:36:51.106 - External executable exit code: 0

26.08.2018 13:36:51.106 - Check items control for user 'radius.user' - Start (RADIUS)
[GoogleAuthenticator].

26.08.2018 13:36:51.184 - Check items control for user 'radius.user' - Stop (RADIUS).

26.08.2018 13:36:51.184 - Google Authenticator authentication successful for user 'radius.user'

26.08.2018 13:36:51.184 - Fetching Success-Reply items for user 'radius.user' - Start.

26.08.2018 13:36:51.200 - Fetching Success-Reply items for user 'radius.user' - Stop.

26.08.2018 13:36:51.200 - Generating Reply Packet - Start.

26.08.2018 13:36:51.262 - Generating Reply Packet - Stop.
```

Concatenated-Password attribute is supported with the latest version of TekRADIUS and you can use this attribute in scenarios where PAP authentication is method is used.

2FA with Local User Profiles Using Access-Challenge

You can deploy 2FA with local user profiles and Google Authenticator. Windows Authentication Proxy must be disabled in this scenario. You need to create to user groups first;

2FA-GA. This group contains attributes used in the second phase of the authentication session. In this example you need to have only following attribute as a check attributed added to 2FA-GA group;

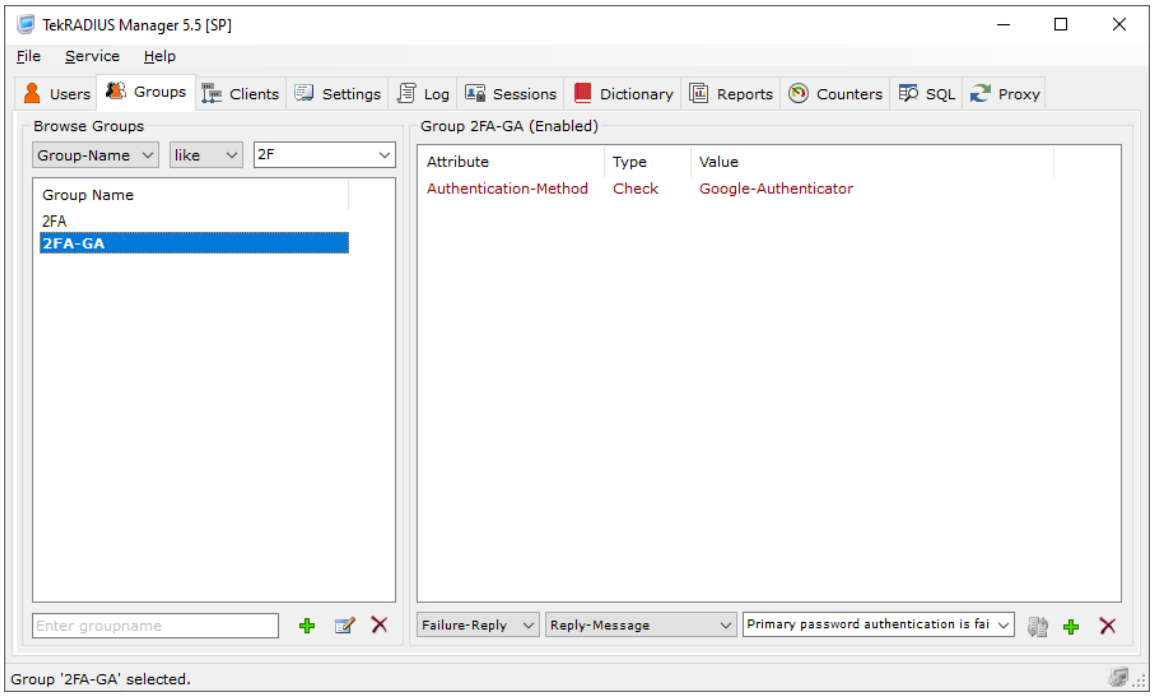
- Authentication-Method = Google-Authenticator.

2FA Group. This group contains primary authentication method attributes. In this example PAP authentication is configured. Following attributes are added to 2FA group as check attributes;

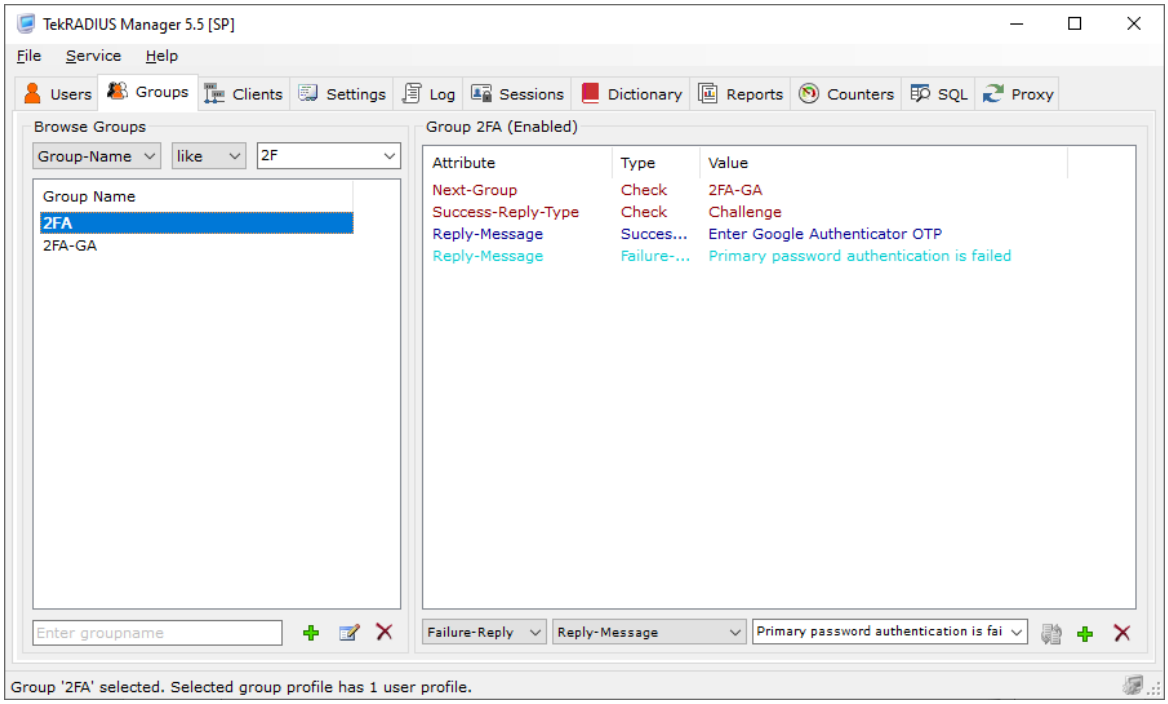
- Success-Reply-Type = Challenge (TekRADIUS will request Google Authenticator generated OTP if primary password authentication is successful)
- Next-Group = 2FA-GA (Attributes in this group will be used in the second phase of the authentication session)

You can optionally add Reply-Message attributes;

- Reply-Message (Success-Reply) = Enter Google Authenticator OTP
- Reply-Message (Failure-Reply) = Primary password authentication is failed



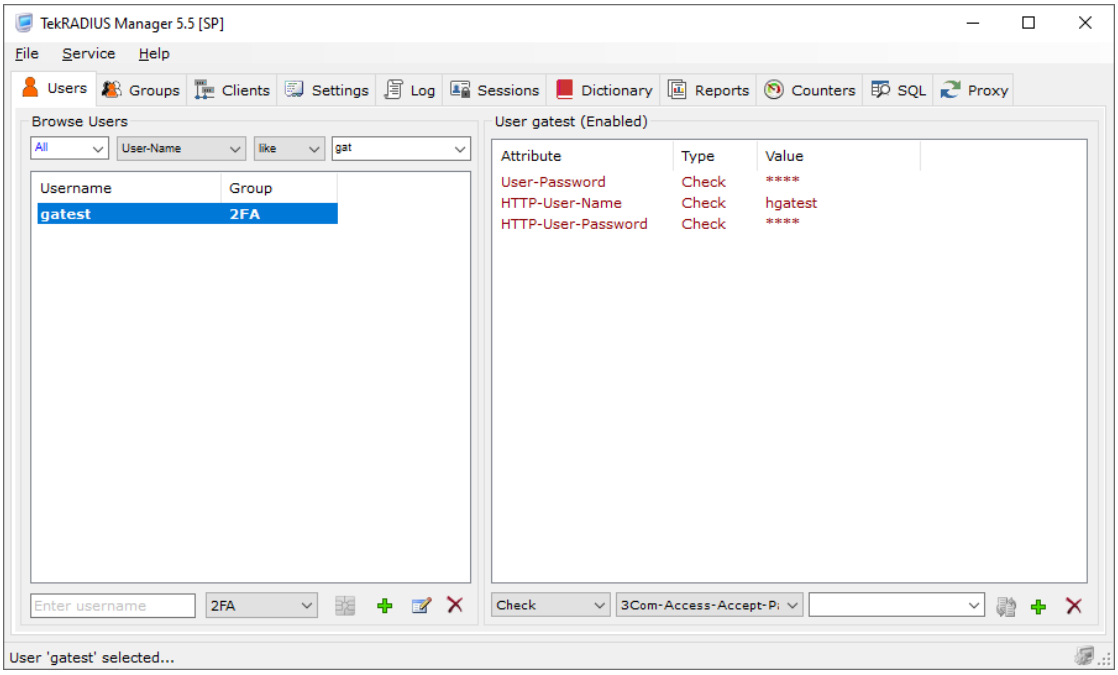
2FA-GA group Profile



2FA group Profile

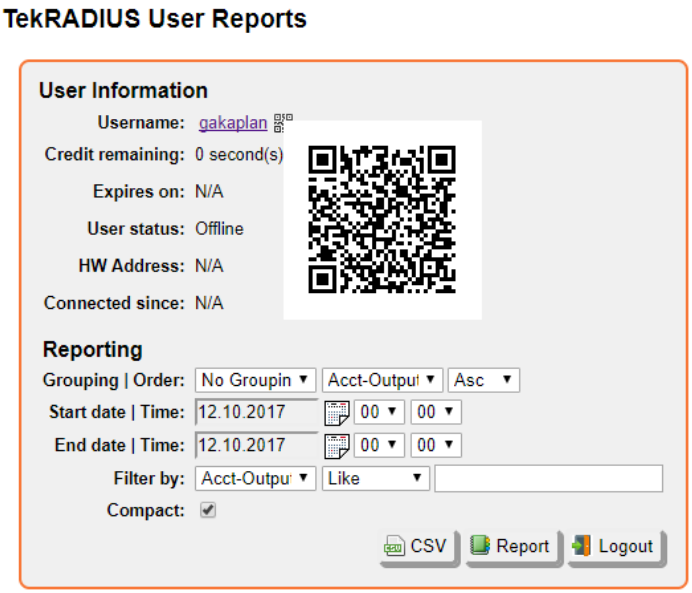
You need to create a user profile with following check attributes;

- User-Password = <This is the password to be used in the first phase of the authentication>
- HTTP-User-Name = <Username for HTTP interface login>
- HTTP-User-Password = <Password for HTTP interface login>



2FA-GA group Profile

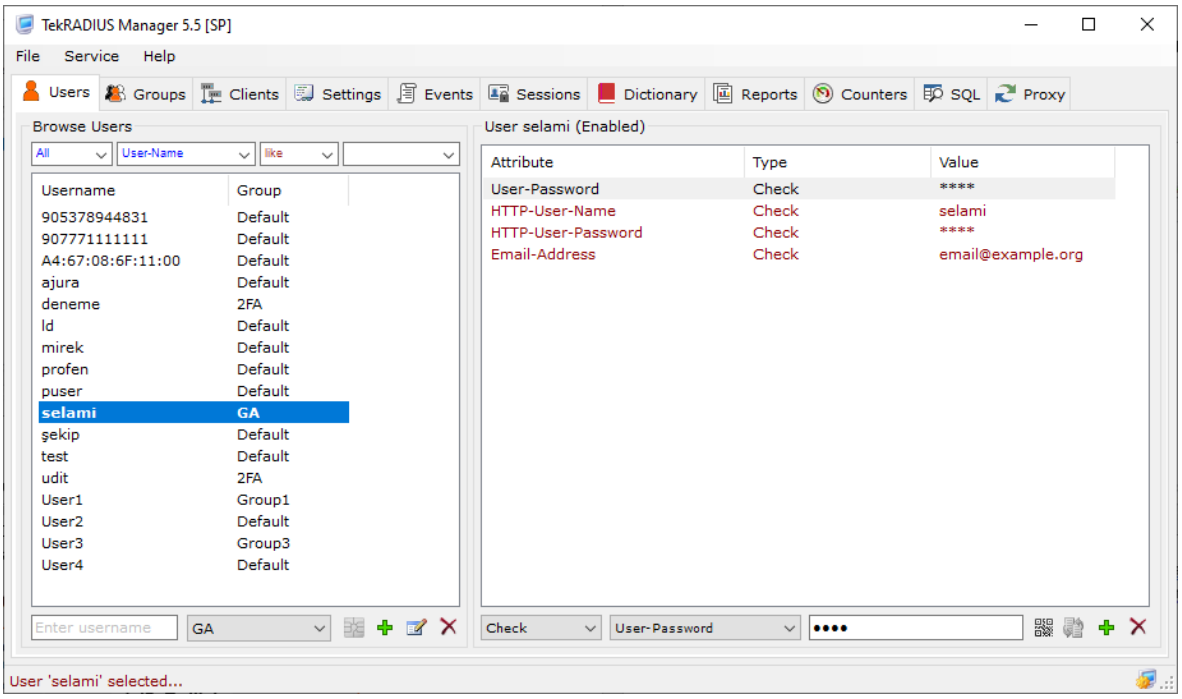
You must initialize Google Authenticator prior to make an authentication attempt. Connect to TekRADIUS HTTP interface with HTTP-User-Name and HTTP-User-Password and initialize Google Authenticator by clicking on QR code icon next to the username. Scan displayed QR code by using mobile Google Authenticator application and click on QR code image on the HTTP interface.



Please make sure that your access server supports RADIUS Access-Challenge response. Google Authenticator is supported with TekRADIUS SP license. Please contact to KaplanSoft sales for trial key.

2FA with Local User Profiles using Concatenated-Password Attribute

In this sample configuration, user will be authenticated local user profile and then received OTP will be validated with Google-Authenticator.

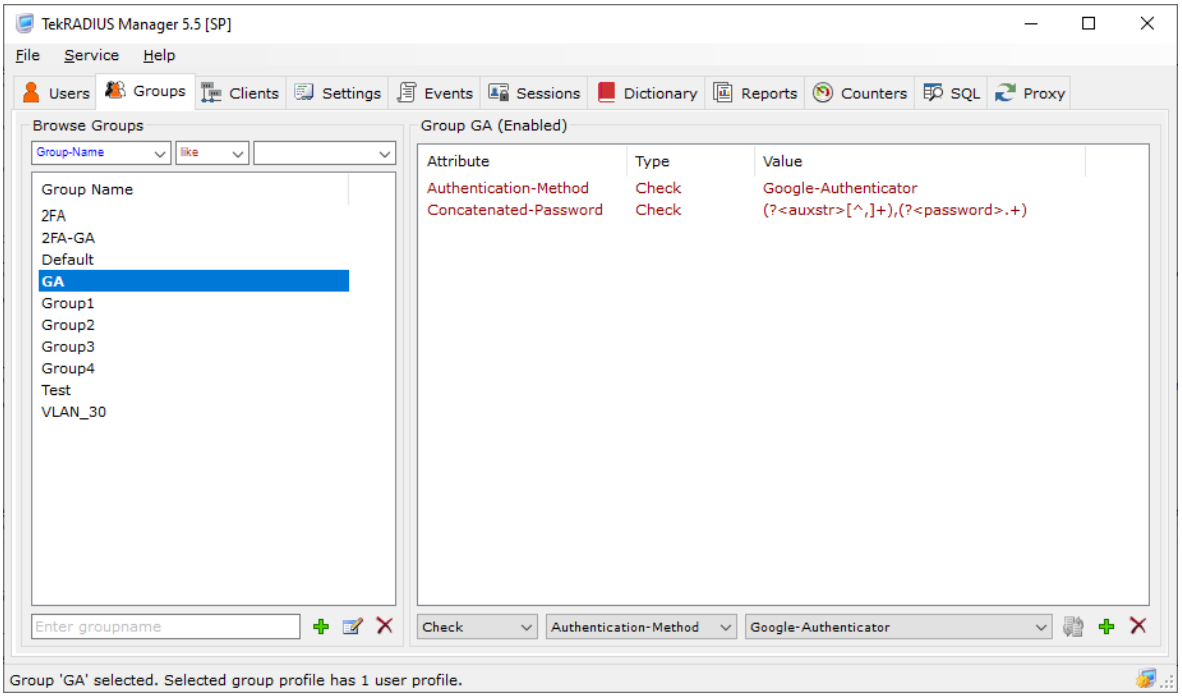


User Profile

User profile must contain a User-Password and HTTP-User-Name and HTTP-User-Password. User should connect to the HTTP interface of TekRADIUS in order to initialize Google-Authenticator. System administrator can send Google-Authentication secret via e-mail if user has an Email-Address configured.

Primary authentication method will be set to Google-Authenticator by adding Authentication-Method = Google-Authenticator as a check attribute to the group profile. User must be enter his/her password in following format;

```
Local account password,Google-Authenticator OTP
```



GA group Profile

Regular expression pattern must contain **password** and **auxstr** named capture groups. Local user password will be matched against **auxstr** whereas **password** will be matched against Google-Authenticatior.