

2FA with Google Authenticator

Two factor authentication (2FA) enables increased security when authenticating user sessions. TekRADIUS supports many 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

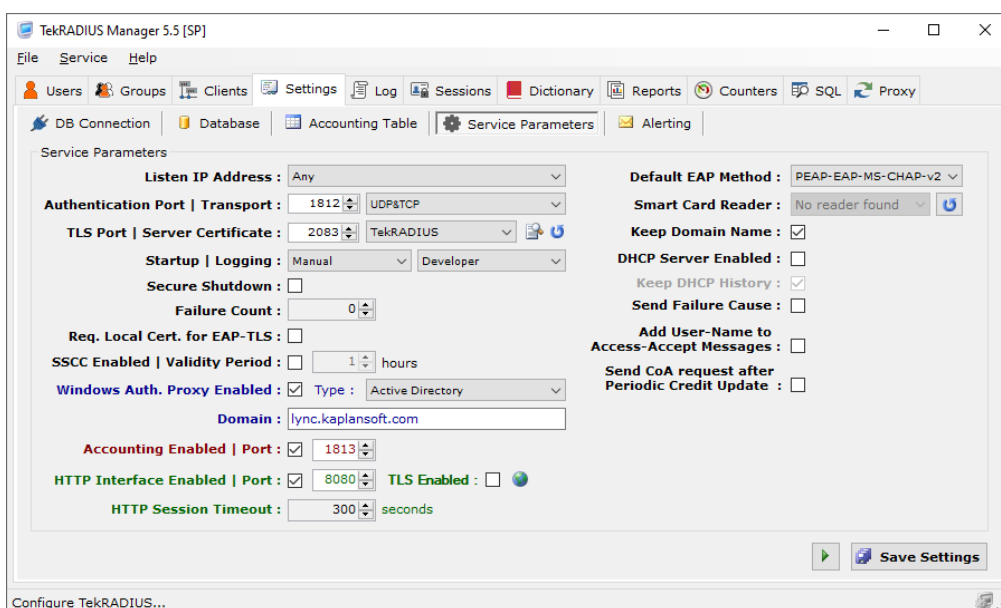
Concatenated-Password attribute allows you to specify a regular expression pattern to split received User-Password in an authentication request. TekRADIUS will update User-Password to value captured with regular expression capture group named **password**. You can get the other part using capture group 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, the user will be authenticated against active directory and then received OTP will be validate with Google-Authenticator.

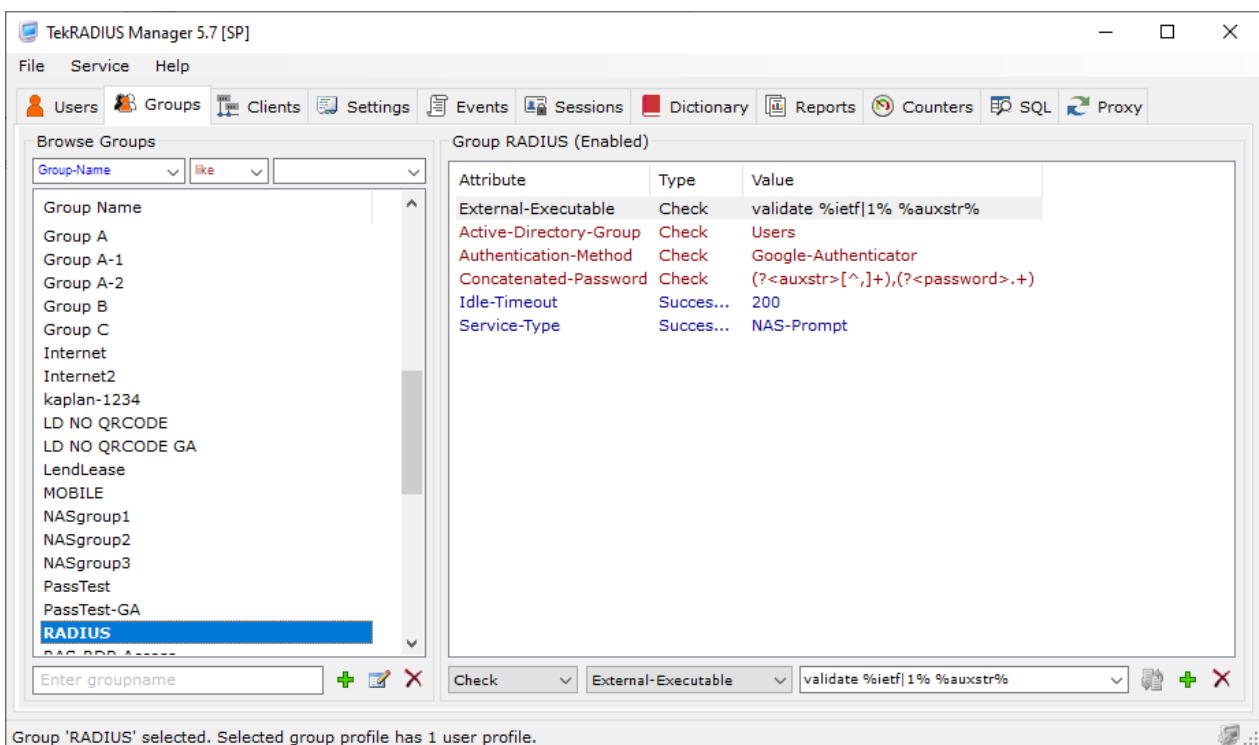


TekRADIUS Settings

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 entering 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. TekRADIUS will invoke an internal function called "Validate" to validate the received Active Directory password.

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

```
05.06.2023 21:38:45.592 - RadAuth req. from 192.168.88.51:55858 [UDP]
Size : 73
Identifier : 2
Attributes :

Service-Type = 2
NAS-IP-Address = 212.58.6.190
User-Name = yasin.kaplan
MS-RAS-Version = 1

05.06.2023 21:38:45.655 - Primary AD group for user 'yasin.kaplan' is 'RADIUS' [66].
05.06.2023 21:38:45.655 - Group check attribute(s) obtained for user 'yasin.kaplan' - (RADIUS).
05.06.2023 21:38:45.655 - GoogleAuthenticator authentication commencing for user 'yasin.kaplan'
05.06.2023 21:38:45.670 - Performing Active Directory authentication for user 'yasin.kaplan' @ AD.
05.06.2023 21:38:45.686 - (ADProxy) Authentication is successful for user 'AD\yasin.kaplan'.
05.06.2023 21:38:45.686 - Check items control for user 'yasin.kaplan' - Start (GoogleAuthenticator)
05.06.2023 21:38:45.686 - Performing Active Directory authentication for user 'yasin.kaplan' @ AD.
05.06.2023 21:38:45.702 - (ADProxy) Authentication is successful for user 'AD\yasin.kaplan'.
05.06.2023 21:38:45.717 - Google authentication is successful for user 'yasin.kaplan'.
05.06.2023 21:38:45.717 - Check items control for user 'yasin.kaplan' - Stop [Group: 'RADIUS'].
05.06.2023 21:38:45.717 - Google Authenticator authentication is successful for user 'yasin.kaplan'
05.06.2023 21:38:45.717 - Fetching Success-Reply items for user 'yasin.kaplan' - Start.
05.06.2023 21:38:45.717 - Authorization query for user 'yasin.kaplan'; SELECT Attribute, Val from
Users where UserName = 'yasin.kaplan' and Attribute <> 'ietf|2' and Attribute <> 'ietf|3' and
AttrType = 1
05.06.2023 21:38:45.717 - Fetching Success-Reply items for user 'yasin.kaplan' - 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.

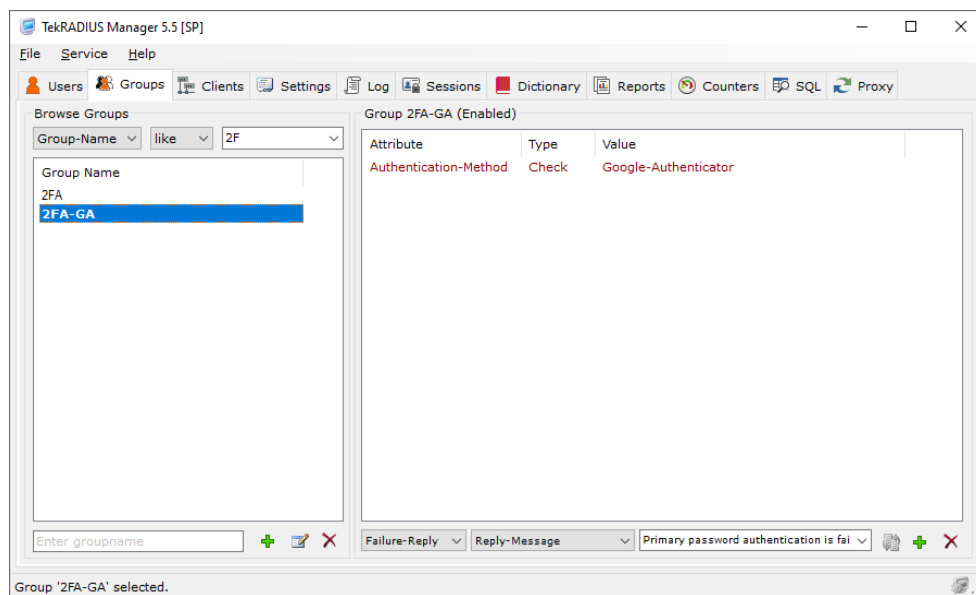
2FA Group. This group contains primary authentication method attributes. 2FA group must also be created in the Active Directory and all users to be authenticated must be members of the 2FA group. You also need to set 2FA as the primary user group for these users in the Active Directory. In this example PAP authentication will be used. 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)

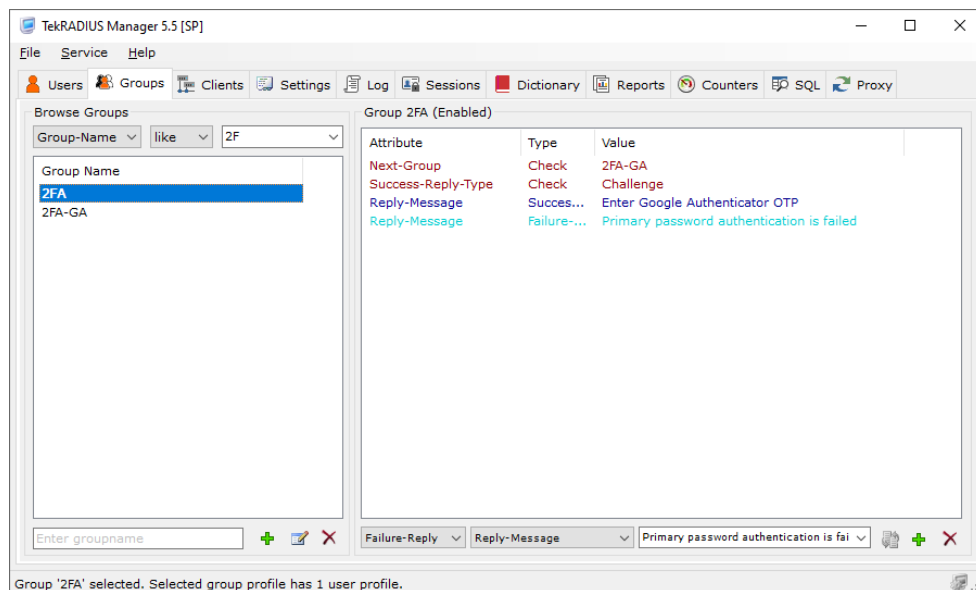
You can use Default group and create Default-GA group in place of 2FA and 2FA-GA if all users in the Active Directory will be authenticated.

You can optionally add Reply-Message attributes;

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



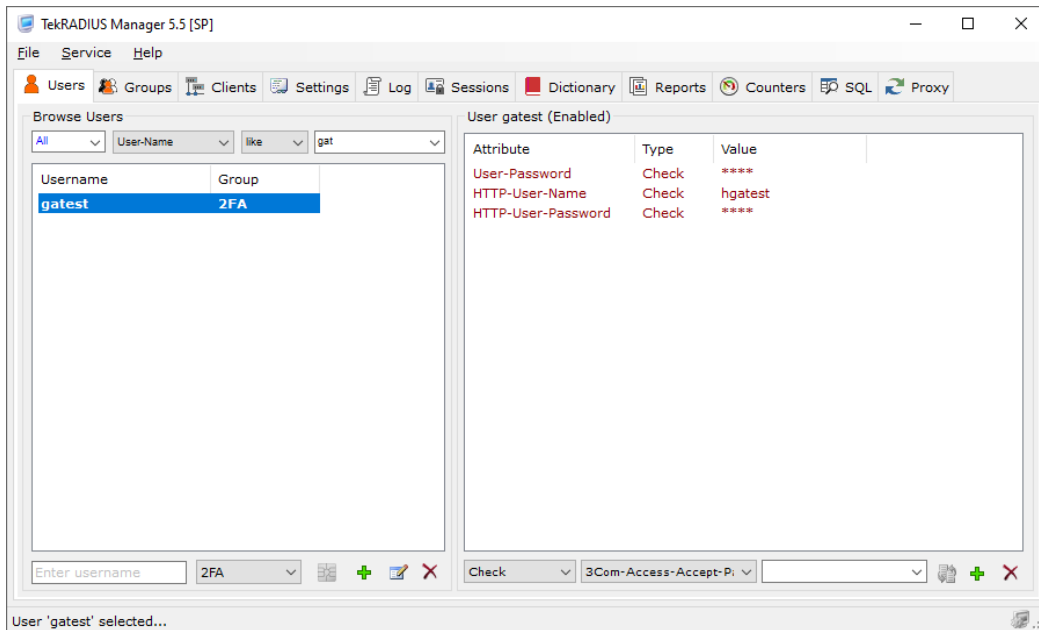
2FA-GA group Profile



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 making 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.

TekRADIUS User Reports

User Information

Username: [gakaplan](#) 


Credit remaining: 0 second(s)

Expires on: N/A

User status: Offline

HW Address: N/A

Connected since: N/A



Reporting




Grouping | Order: No Groupin | Acct-Output | Asc

Start date | Time: 12.10.2017 | 00 | 00

End date | Time: 12.10.2017 | 00 | 00

Filter by: Acct-Output | Like |

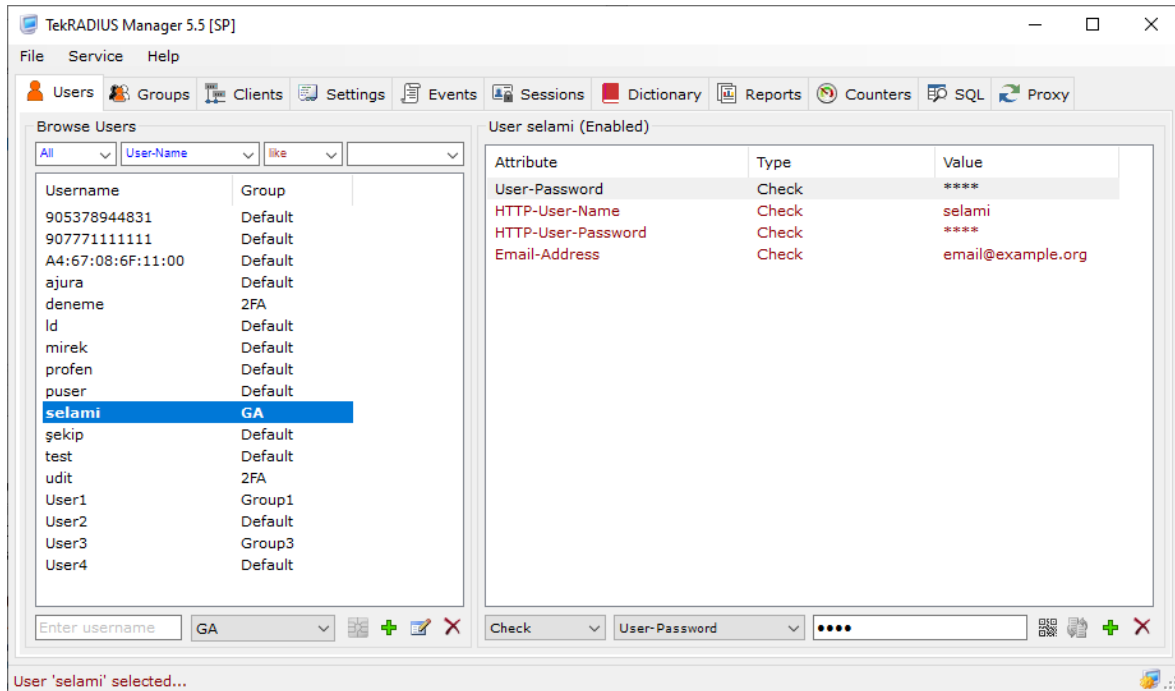
Compact:

Please make sure that your access server supports RADIUS Access-Challenge response. Google Authenticator is supported with TekRADIUS SP license. Please contact 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.



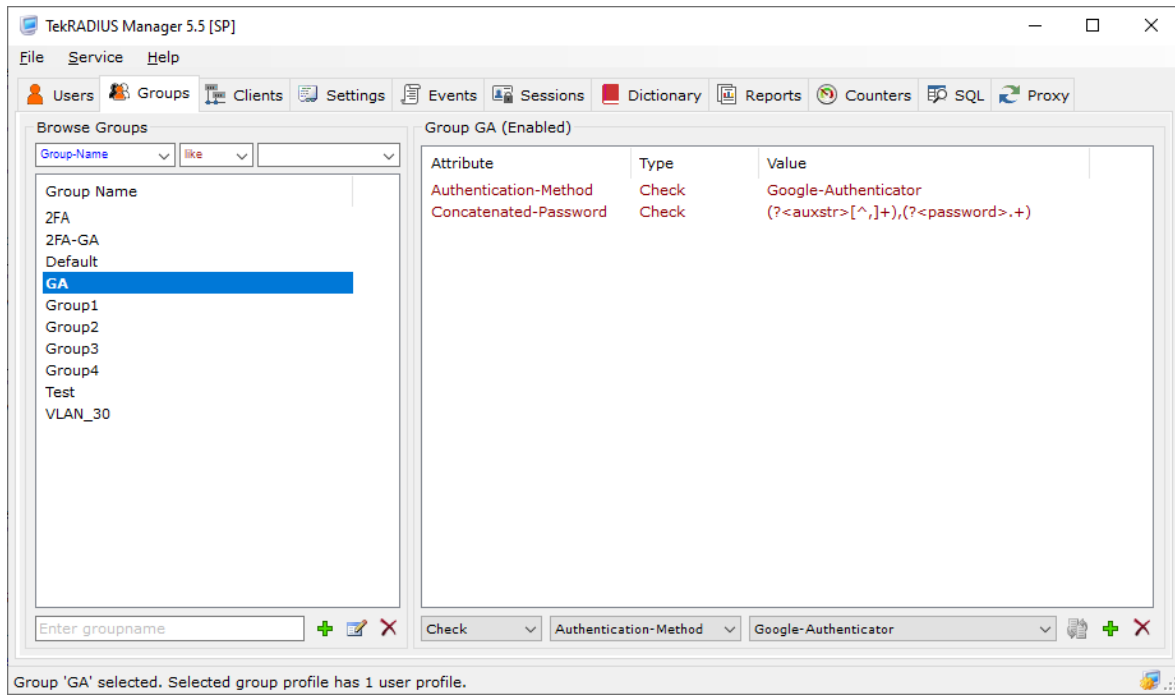
User Profile

User profile must contain a User-Password and HTTP-User-Name and HTTP-User-Password. User should connect to the HTTP interface of TekRADIUS to initialize Google-Authenticator. System administrators can send Google-Authenticator 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 entering his/her password in following format;

Local account password,Google-Authenticator OTP

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-Authenticator.



GA group Profile