2FA with Concatenated-Password

Two factor authentication (2FA) enables increased security when authenticating user sessions. 2FA may be hard to implement, especially your access servers do not support RADIUS challenges from the RADIUS server.

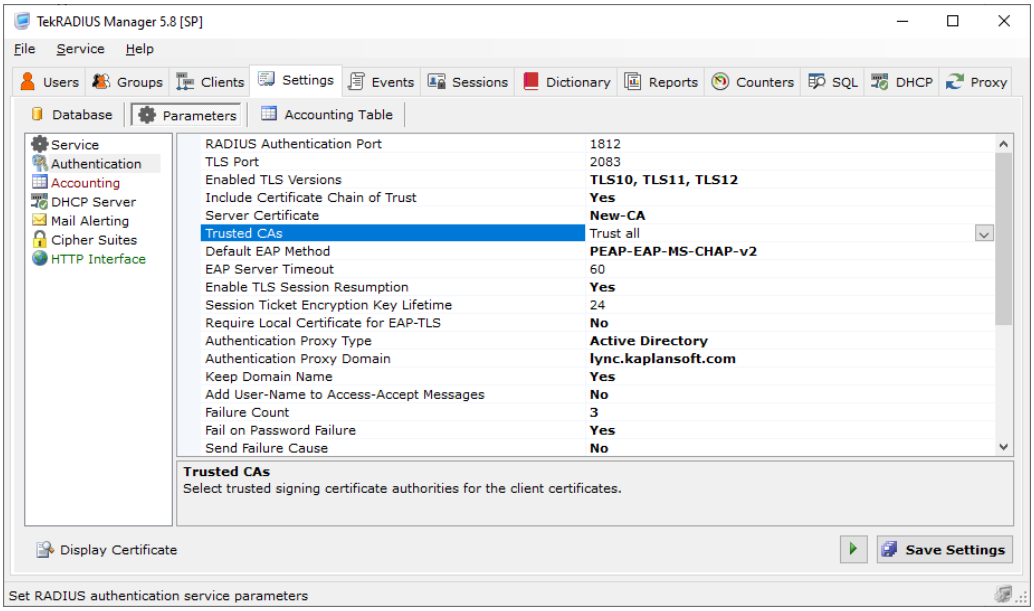
Concatenated-Password attribute allows you to specify a regular expression pattern to split received User-Password in an authentication request. TekRADIUS will update User-Password to value captured with regular expression capture group named **password**. You can get other parts using a capture group 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. This attribute requires a commercial license. Here is a sample;

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

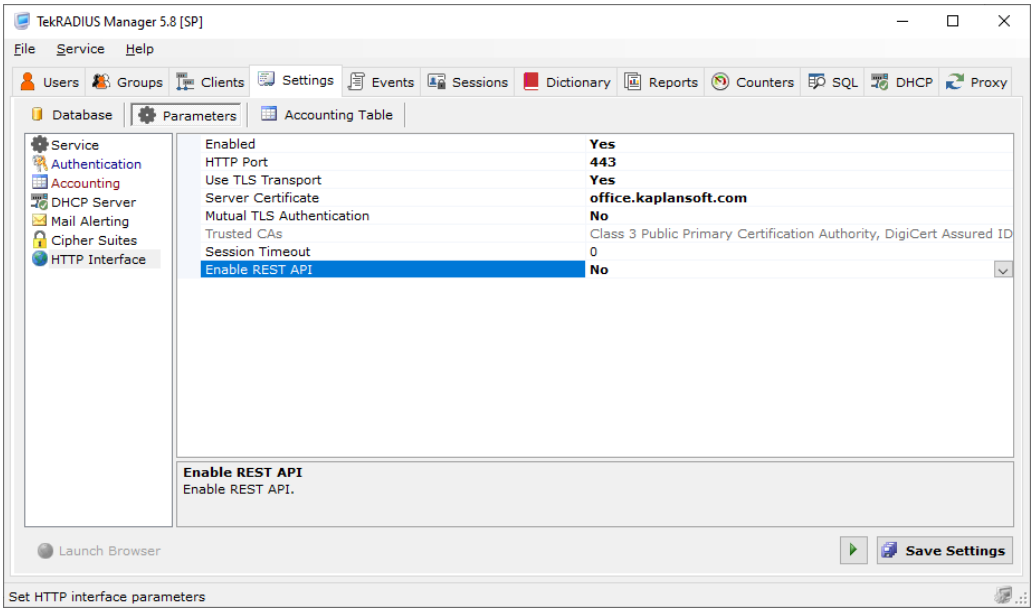
Regular expression pattern must contain **password** and **auxstr** named capture groups. This regular expression splits received passwords concatenated with a comma in User-Password attribute and sets User-Password to second part of the original User-Password value. Captured first part value assigned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

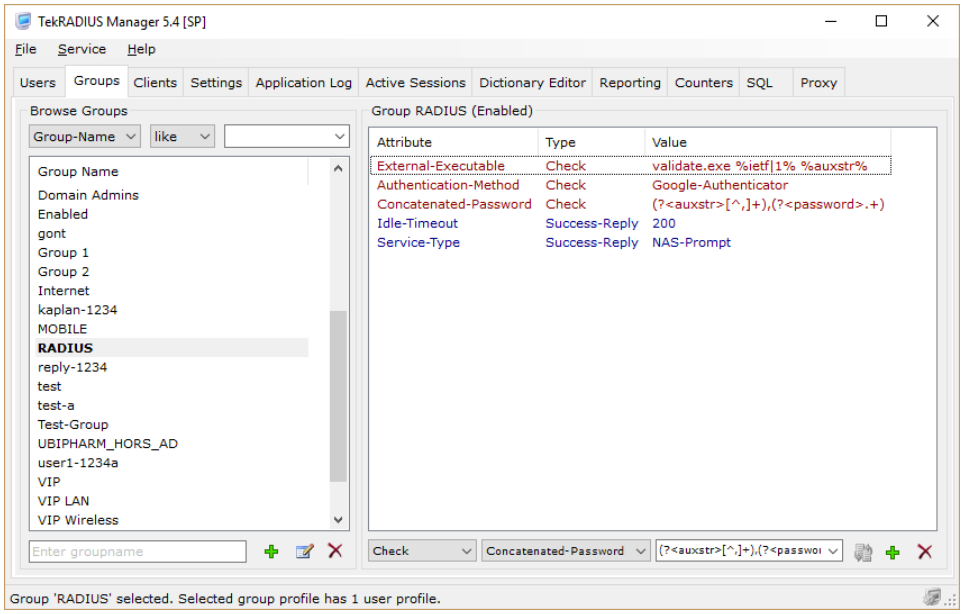


TekRADIUS Settings – HTTP Interface

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. The 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 acccount 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 an Active Directory account called validate.exe. This can be downloaded from https://www.kaplansoft.com/TekRADIUS/release/Validate.zip. Validate.exe, validates Active Directory username 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.