2FA with Built-in OTP Generator

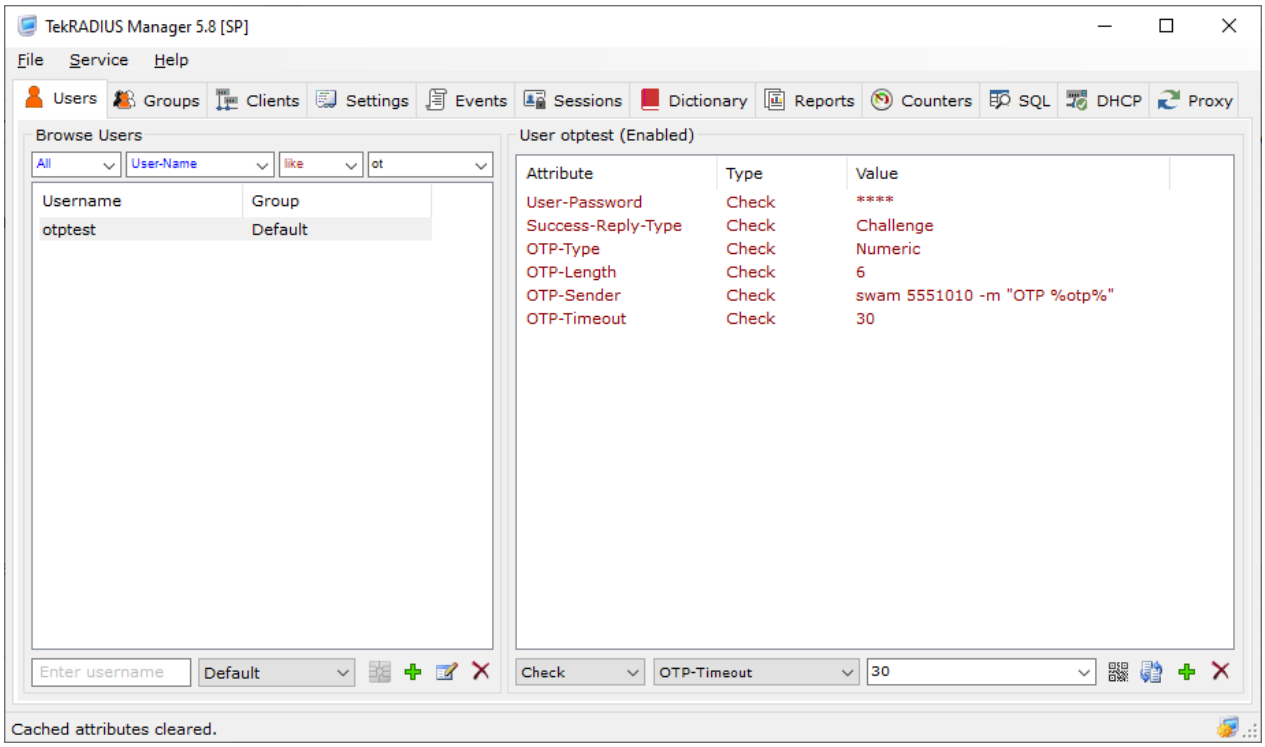
Two factor authentication (2FA) enables increased security when authenticating user sessions. TekRADIUS supports many ways to support 2FA. You can implement 2FA with TekRADIUS built-in OTP Generator. Generated OTPs must be delivered to the users via either e-mail or SMS. You will need an SMTP / SMS account and delivery service/application.

OTP Attributes

You need to configure OTP attributes in user or group profiles. These are

OTP-Type, OTP-Length, OTP-Timeout and OTP-Sender with Success-Reply-Type

Here is a typical local user profile configured for 2FA with built-in OTP generator:



You need to add minimum following attributes as check attributes:

- OTP-Sender = <Built-in or External OTP sender. Generated OTP can be specified in the parameters using %otp% variable>
- Success-Reply-Type = Challenge

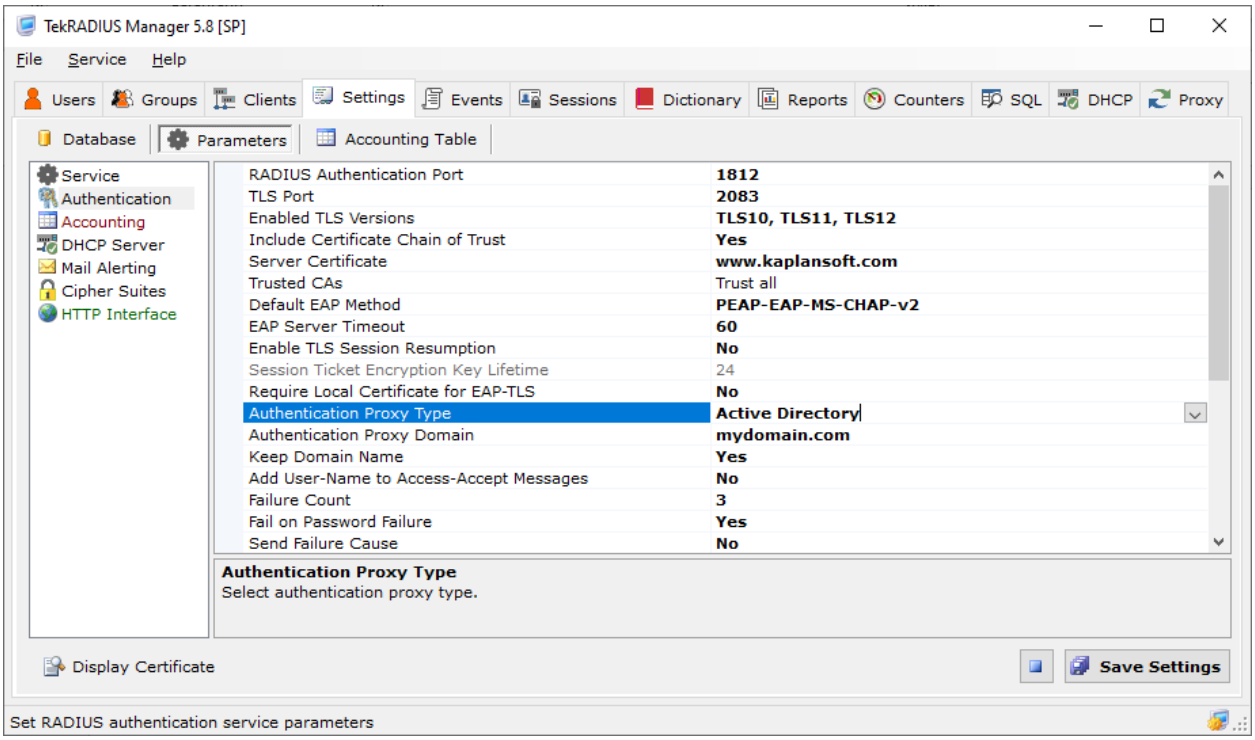
Default OTP-Type is numeric and six digits in length. Default OTP-Timeout is 30 seconds. Attributes other than User-Password can be in the group profile. This will simplify 2FA provisioning if you need the configure multiple user profiles for 2FA.

TekRADIUS will reply with an Access-Challenge and deliver the six digits OTP via an SMS message if user enters the correct User-Password in the **first phase**. Authentication will be successful if the user enters received OTP in the **second phase** of the authentication. OTP expires in 30 seconds in this example.

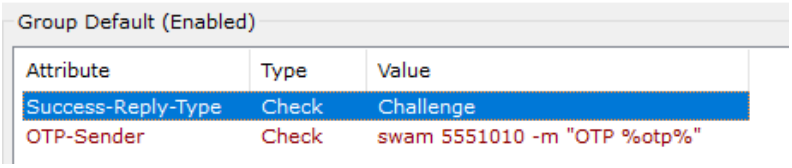
```
02.05.2026 16:38:55.985 - RadAuth req. from 192.168.1.151:63123 [UDP]

 Size             : 68
 Identifier       : 2
 Attributes       :

 User-Name = otptest
 MS-RAS-Version = 1
 Service-Type = 2
 NAS-IP-Address = 192.168.1.51


02.05.2026 16:38:55.985 - PAP authentication commencing for user 'otptest'

02.05.2026 16:38:55.985 - Check items control for user 'otptest' - Start (PAP) [Group: 'default'].

02.05.2026 16:38:55.985 - PAP Authentication is successful for user 'otptest'.

02.05.2026 16:38:55.985 - Check items control for user 'otptest' - Stop [Group: 'default'].

02.05.2026 16:38:55.985 - Authentication is successful for user 'otptest'

02.05.2026 16:38:56.063 - External executable: swam, Parameters: 5551010 -m "OTP 547193"

02.05.2026 16:38:57.219 - External executable exit code: 0

02.05.2026 16:38:57.219 - OTP sent for user 'otptest'.

02.05.2026 16:38:57.219 - Generating Reply Packet for user 'otptest' - Start.

02.05.2026 16:38:57.219 - Generating Reply Packet for user 'otptest' - Stop.

02.05.2026 16:38:57.219 - RadAuth reply to 192.168.1.151:63123 (Challenge)

 Size             : 92
 Identifier       : 2
 Attributes       :

 Reply-Message = Enter OTP
 User-Name = otptest
 State = E420B45C7DDFE94794F4346CEFA770C2

02.05.2026 16:39:20.891 - RadAuth req. from 192.168.1.151:61661 [UDP]

 Size             : 102
 Identifier       : 3
 Attributes       :

 User-Name = otptest
 MS-RAS-Version = 1
 Service-Type = 2
 NAS-IP-Address = 192.168.1.51
 State = E420B45C7DDFE94794F4346CEFA770C2

02.05.2026 16:39:20.891 - PAP authentication commencing for user 'otptest'

02.05.2026 16:39:20.891 - OTP check will be performed for user 'otptest'.

02.05.2026 16:39:20.891 - Check items control for user 'otptest' - Start (PAP) [Group: 'default'].

02.05.2026 16:39:20.891 - PAP Authentication is successful for user 'otptest'.

02.05.2026 16:39:20.891 - Check items control for user 'otptest' - Stop [Group: 'default'].

02.05.2026 16:39:20.891 - Authentication is successful for user 'otptest'
```

2FA with Active Directory Accounts

You can perform 2FA with Active Directory accounts if Authentication Proxy is enabled.

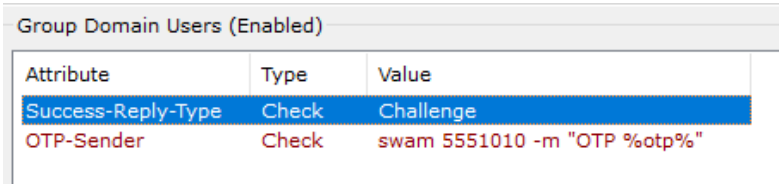


TekRADIUS will perform 2FA for all Active Directory accounts if you put OTP attributes to the Default group profile.



If you plan to perform 2FA for a certain group of AD users you have two options:

Creating group profiles with the same name as the default AD group of the users and putting OTP attributes to this group profile. This may not be practical if you are managing hundreds of users and changing their primary group names. You can use ADGUM.exe which can be found under TekRADIUS application directory to set primary group names.



Group hunting. TekRADIUS will traverse user groups chained with Next-Groups to find a match with Active-Directory-Groups attribute. Create fallback groups named OTP and Regular. Add a

check attribute to the default user group which does not have any matches for all incoming authentication requests.

Group Default (Enabled)

Attribute	Type	Value
NAS-IP-Address	Check	1.1.1.1
Next-Group	Check	OTP

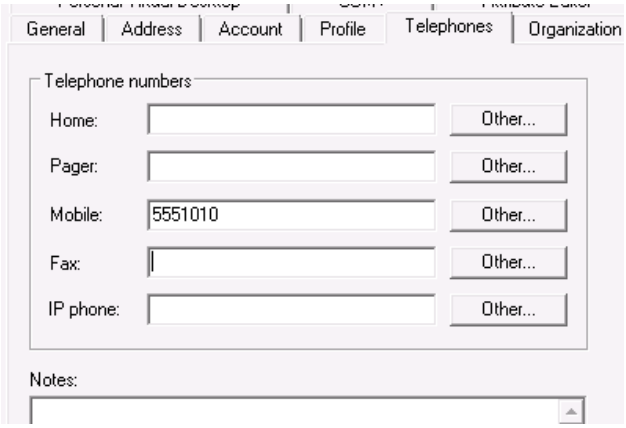
Group OTP (Enabled)

Attribute	Type	Value
Next-Group	Check	CP
Active-Directory-Group	Check	TekTape Users
Success-Reply-Type	Check	Challenge
OTP-Sender	Check	swam %mobile% -m "OTP %otp%"

Group Regular (Enabled)

Attribute	Type	Value

TekRADIUS will fall back to OTP group when an authentication request is received. TekRADIUS will check Active Directory username and password and send a challenge to the access server if the username and password are valid otherwise continue to the next group named “Regular”. OTP will be sent to the user’s mobile number using a command line utility[1]. User’s mobile number is fetched from Active Directory profile of the user.



You can also fetch the e-mail address of the user using %mail% variable.

User will respond to the challenge by entering received OTP and authentication will be successful if the user enter the OTP in a timely manner *(Prior to expiration, user will have 30 seconds to enter the OTP since the OTP-Timeout attribute is absent in the OTP group profile so the default timeout duration will be in effect).* Authentication will be failed if OTP verification fails and TekRADIUS will stop group hunting and will not go to the next group named “Regular” in this setup.

[1] SWAM.exe is a command line utility to send shot messages to the phone numbers via WhatsApp services. You can download it from https://www.kaplansoft.com/tekradius/release/SWAM.zip. Please see Readme.txt for usage and configuration details in the zip archive.

OTP Sending

TekRADIUS provides some internal methods to deliver an OTP:

sendmail

https:// or http://

udp:// tcp:// or tls://

Constant or variable parameters may be specified for the executable. Use *%<RADIUS attribute>%* to use received RADIUS attributes in *Access-Request* messages. TekRADIUS can get user e-mail addresses and mobile phone numbers from Active Directory. You can use `%mail%` and `%mobile%` variables to use user e-mail address and mobile phone number as parameters for the executable.

These are typical valid examples;

```
External-Executable = http://kaplansoft.com/test.php?email=%mail%&otp=%otp%
External-Executable = https://kaplansoft.com/test.php?mobile=%mobile%&otp=%otp%
External-Executable = sendmail %mail% %otp%
External-Executable = [udp|tcp|tls]://kaplansoft.com:600/mail=%amil%,otp=%otp%
```

A return code '0' *(or HTTP return code 200)* is assumed as success and return codes other than '0' are assumed as failure. If the execution fails for any reason, it will be assumed as a failure and authentication will fail.

You must enable Mail Alerting at Settings / Alerting in order to use sendmail internal command.

You can also use command line utilities to send OTPs based on delivery methods. Enter the full path of the executable as the value of the *External-Executable* attribute. Use double quotes (" ") if the path contains space characters

These are typical valid examples;

```
External-Executable = C:\Test.bat %mobile% %mail% %otp%
External-Executable = "C:\Program Files\My App\test.exe" -log %mail% %otp%
External-Executable = "C:\Progra~1\sendotp\sendotp.exe" %mobile% %otp%
```