Google / Microsoft Authenticator Setup

Google Authenticator is a multifactor authenticator for mobile devices. It generates timed codes used during the 2-step verification process. You need to install to Google Authenticator to your mobile device or PC first;

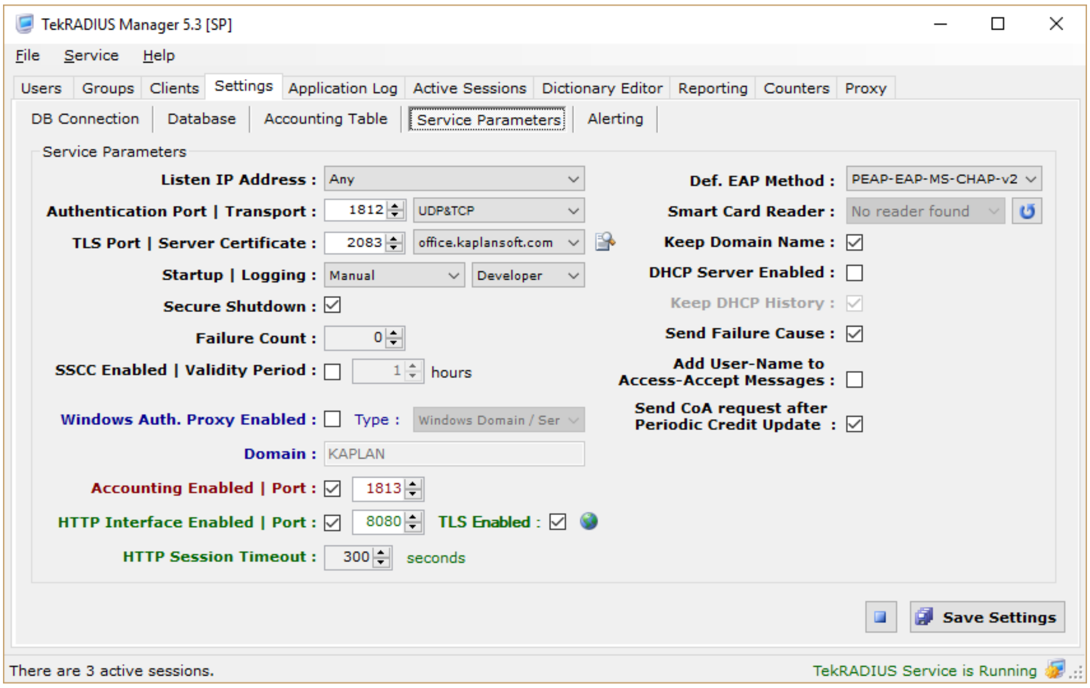
- Windows 8: Google Authenticator on Windows App Store
- Android: Google Authenticator on Google Play
- iOS: Google Authenticator on iTunes App Store
- Windows Phone: Authenticator on Windows Phone App Store
- FireFox: GAuth Authenticator Plugin

For Microsoft Authenticator please visit

- https://www.microsoft.com/en-us/security/mobile-authenticator-app

TekRADIUS Configuration

Google Authenticator is supported with SP license of TekRADIUS. You need to enable built-in HTTP server of TekRADIUS which is available only with SP license;



Service Parameters

Listen IP Address : Any
Authentication Port | Transport : 1812 UDP&TCP
TLS Port | Server Certificate : 2083 office.kaplansoft.com
Startup | Logging : Manual Developer
Secure Shutdown : ☑
Failure Count : 0
SSCC Enabled | Validity Period : □ 1 hours
Windows Auth. Proxy Enabled : □ Type : Windows Domain / Ser
Domain : KAPLAN
Accounting Enabled | Port : ☑ 1813
HTTP Interface Enabled | Port : ☑ 8080 TLS Enabled : ☑
HTTP Session Timeout : 300 seconds

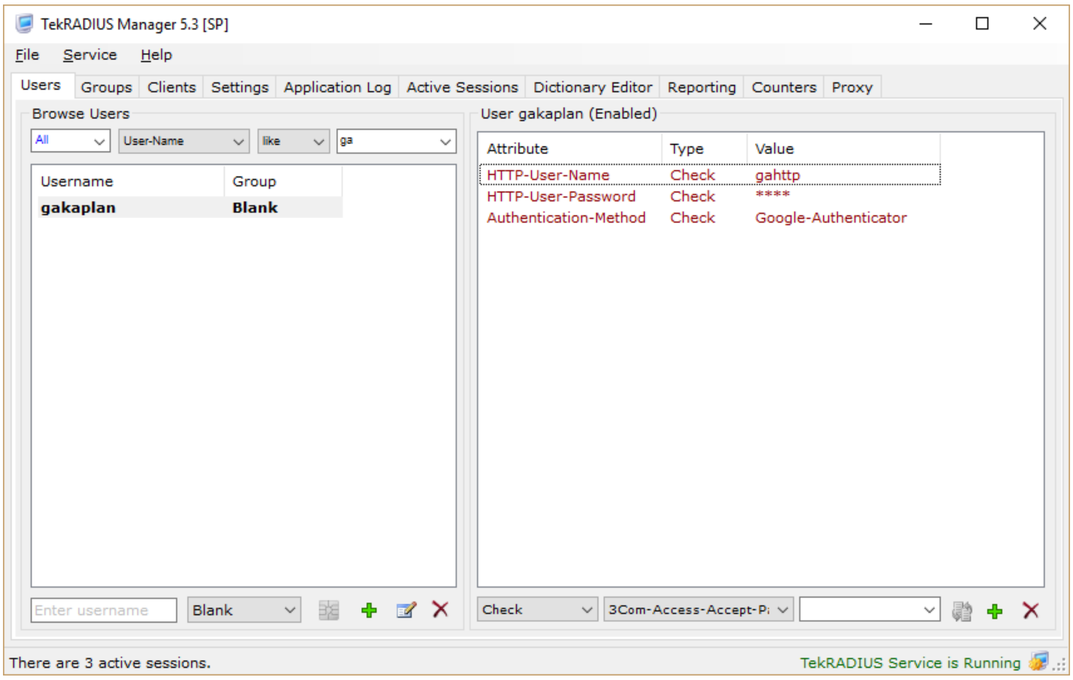
Def. EAP Method : PEAP-EAP-MS-CHAP-v2
Smart Card Reader : No reader found
Keep Domain Name : ☑
DHCP Server Enabled : □
Keep DHCP History : ☑
Send Failure Cause : ☑
Add User-Name to Access-Accept Messages : □
Send CoA request after Periodic Credit Update : ☑

There are 3 active sessions.
TekRADIUS Service is Running

Using TLS transport for HTTP connections is recommended for better security. You need to set a server certificate in Settings / Service Parameters for TLS transport. Users initiate their Google Authenticator secret through the HTTP interface.

Creating User Profiles

You need to create local user profiles for the users. Users must have Authentication-Method = Google-Authenticator as a check attribute either in user or associated group profile. TekRADIUS will add Google-Authenticator-Secret attribute to the user profile when a user initiates Google Authenticator secret. But this attribute is not visible through TekRADIUS Manager and it is kept encrypted in the database if Encrypt Passwords option is set in Settings.



Username	Group
gakaplan	**Blank**

Attribute	Type	Value
HTTP-User-Name	Check	gahttp
HTTP-User-Password	Check	****
Authentication-Method	Check	Google-Authenticator

There are 3 active sessions.

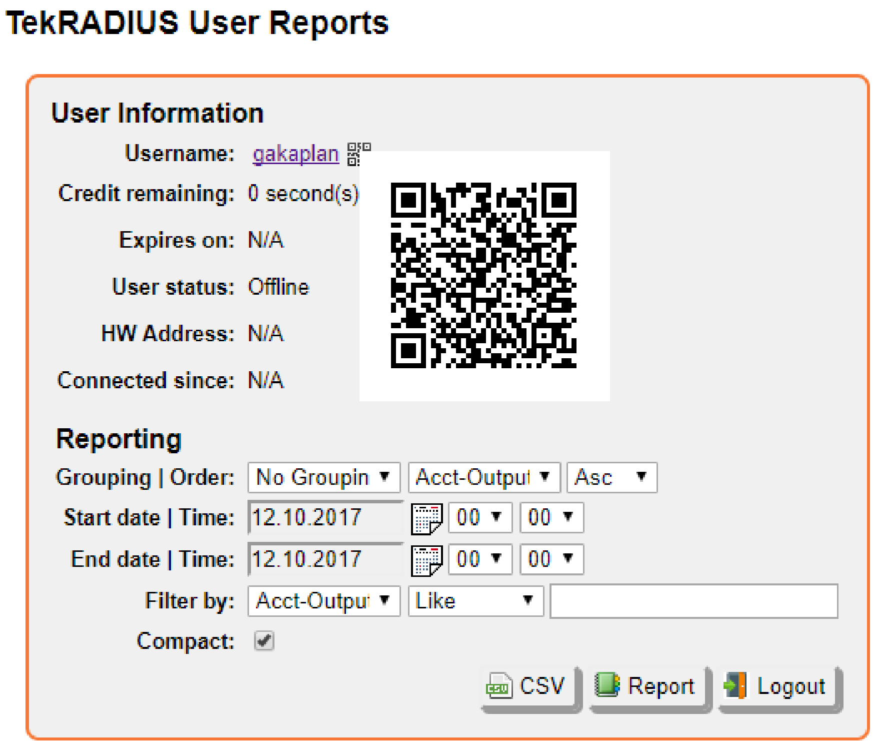
TekRADIUS Service is Running

You also need to add HTTP-User-Name and HTTP-User-Password attribute to local user profile as check attributes to allow the user HTTP access.

Please delete C:\Program Files (x86)\TekRADIUS\TekRADIUS.db file and re-start TekRADIUS, if you are not seeing attributes and values mentioned above and you have upgraded from a previous version of TekRADIUS.

Google / Microsoft Authenticator Secret Initialization

Users will be asked to enter HTTP username and Password when they have accessed the HTTP interface of TekRADIUS. User can initialize their secret by clicking QR Code icon displayed next to their usernames on the HTTP interface. TekRADIUS will display a QR Code when the user clicks the icon. User can scan this QR Code using Google / Microsoft Authenticator application to import the secret. Secret will be reset with every click on the QR Code icon so please make sure that you do not click the icon more than one time. Otherwise, you need to scan the QR Code to re-initialize the secret. Click on QR Code image to hide the displayed QR Code. Users should change the HTTP password after first login to the HTTP interface.



TekRADIUS User Reports

User Information

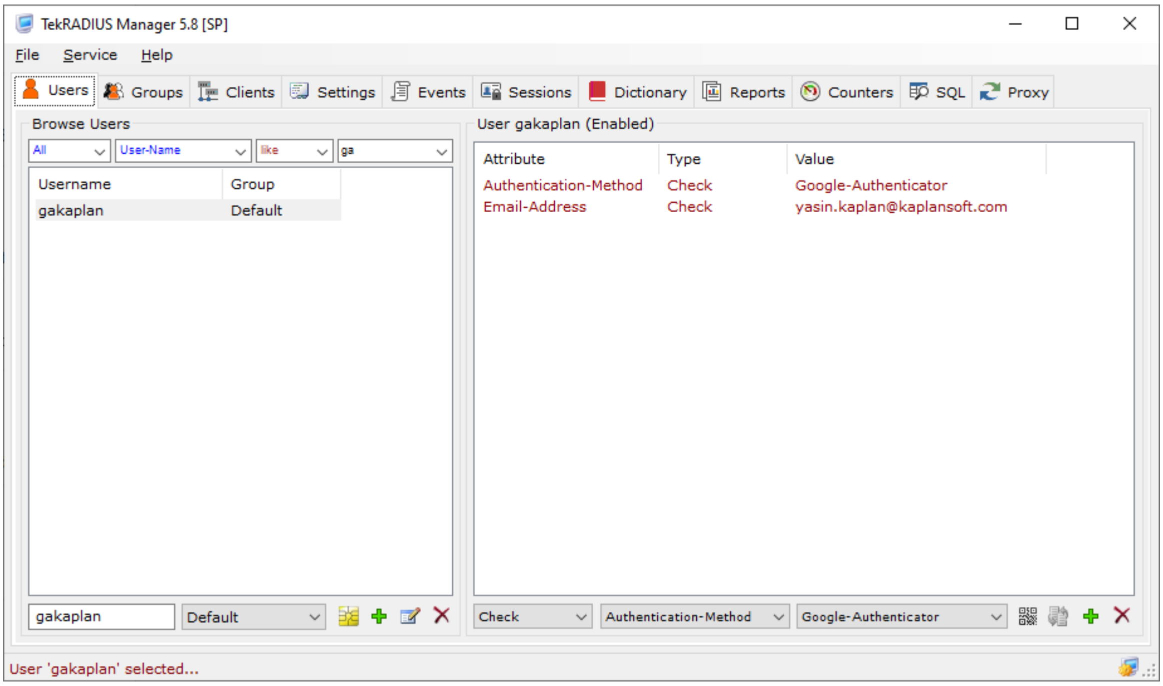
Username:	gakaplan
Credit remaining:	0 second(s)
Expires on:	N/A
User status:	Offline
HW Address:	N/A
Connected since:	N/A

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-Outpu ▾ Like ▾
Compact:	☑

Users can use dynamically generated passwords by Google Authenticator application while logging in after this procedure. TekRADIUS applies hard coded 5 minutes tolerance for the generated passwords, so it is recommended to synchronize time settings in TekRADIUS server and client device with a Time server.

You can optionally deliver Google Authenticator secret via e-mail to the users. You need to add Email-Address attribute as a check attribute to the user profiles and configure and active Mail Alerting in TekRADIUS settings. TekRADIUS will send the Google Authenticator secret as a QR Code to be scanned to the user by default. You can force TekRADIUS to deliver Google Authenticator secret in text format.



TekRADIUS Manager 5.8 [SP]

File Service Help
Users Groups Clients Settings Events Sessions Dictionary Reports Counters SQL Proxy
Browse Users
All User-Name like ga

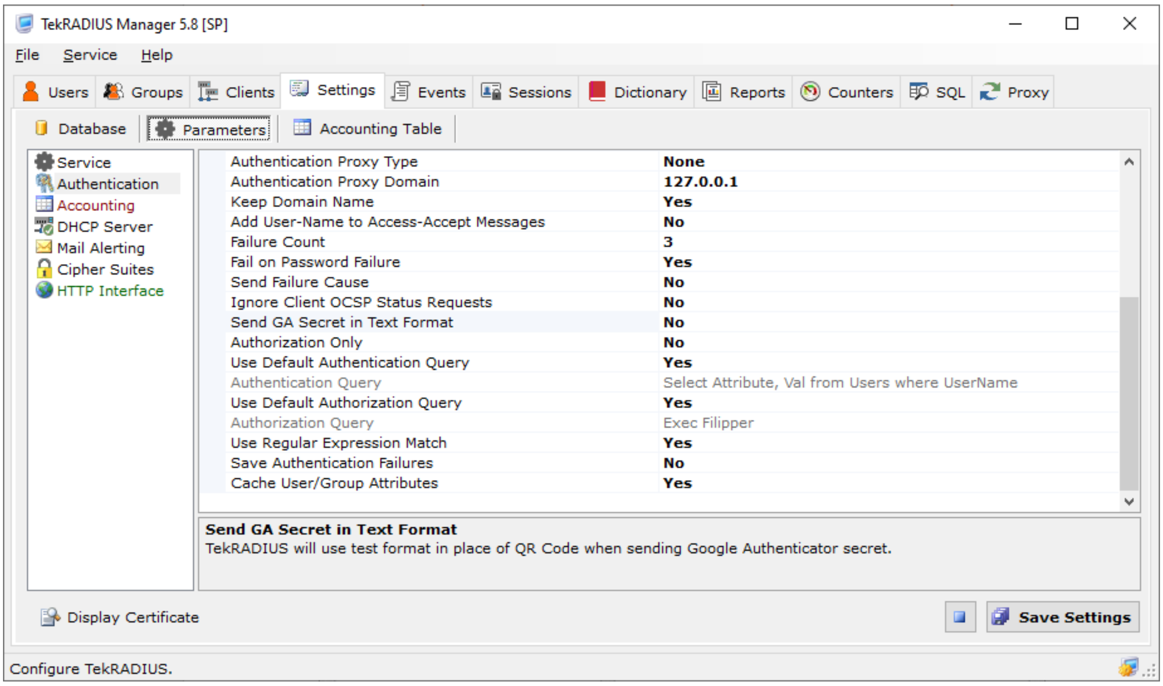
Username	Group
gakaplan	Default

User gakaplan (Enabled)

Attribute	Type	Value
Authentication-Method	Check	Google-Authenticator
Email-Address	Check	yasin.kaplan@kaplansoft.com

gakaplan Default
Check Authentication-Method Google-Authenticator

User 'gakaplan' selected...



Authentication Proxy Type	None
Authentication Proxy Domain	127.0.0.1
Keep Domain Name	Yes
Add User-Name to Access-Accept Messages	No
Failure Count	3
Fail on Password Failure	Yes
Send Failure Cause	No
Ignore Client OCSP Status Requests	No
Send GA Secret in Text Format	No
Authorization Only	No
Use Default Authentication Query	Yes
Authentication Query	Select Attribute, Val from Users where UserName
Use Default Authorization Query	Yes
Authorization Query	Exec Filipper
Use Regular Expression Match	Yes
Save Authentication Failures	No
Cache User/Group Attributes	Yes

Send GA Secret in Text Format
TekRADIUS will use test format in place of QR Code when sending Google Authenticator secret.

Configure TekRADIUS.

You can deploy Google / Microsoft Authenticator with PAP, CHAP, MS-CHAP-v1/v2, PEAP, EAP-MD5, EAP-MS-CHAP-v2, LEAP and EAP-TTLS authentication methods.