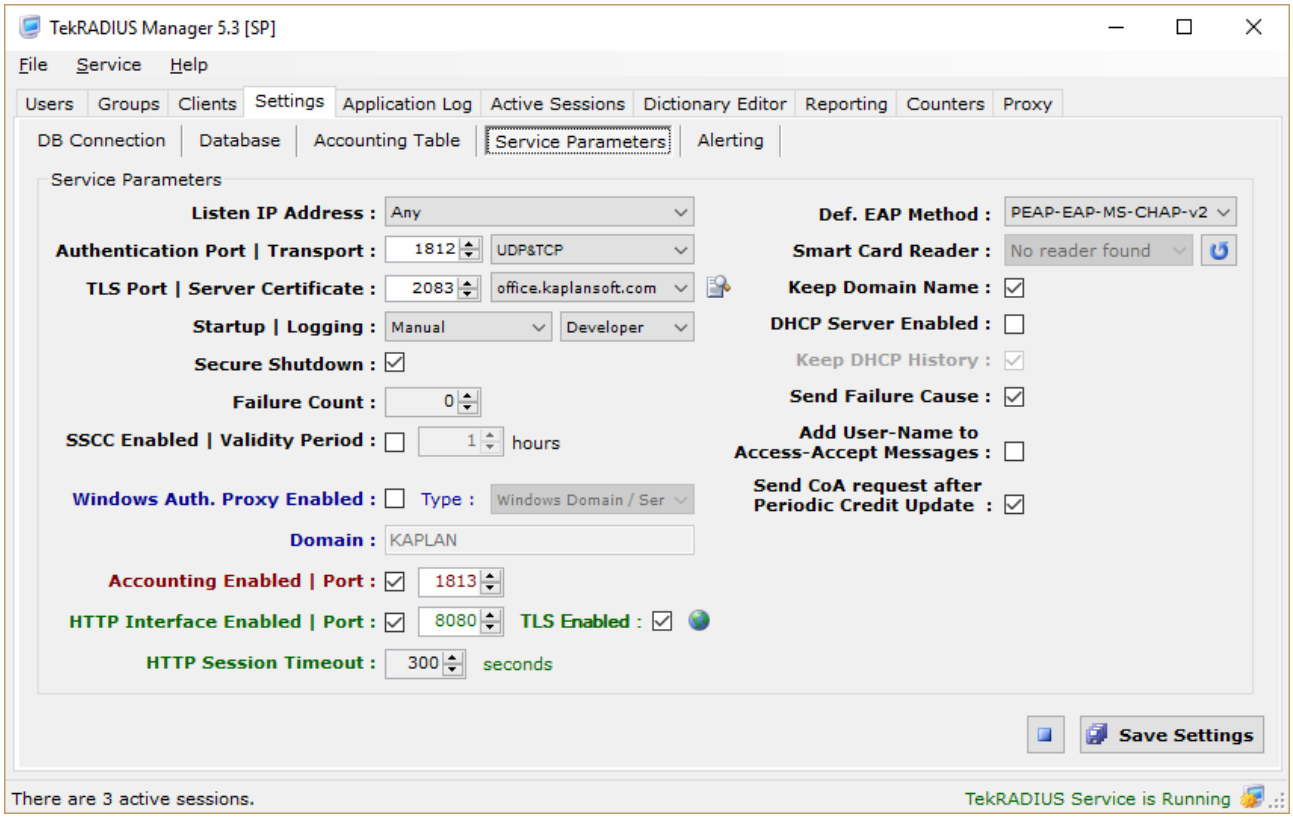
Google Authenticator Setup

Google Authenticator is a multifactor applications 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

TekRADIUS Configuration

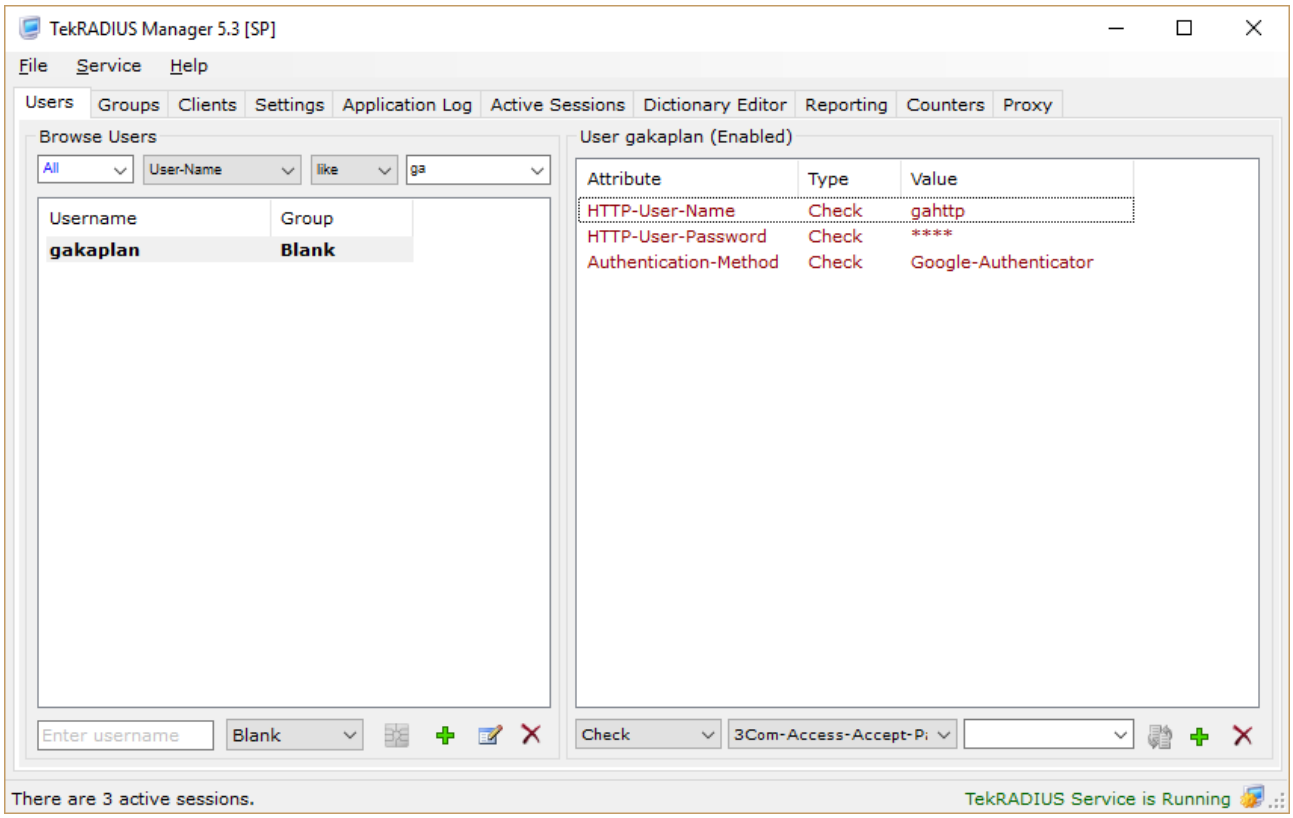
Google Authenticator is supported with SP license of TekRADIUS. You need to enable built-in HTTP server of TekRADIUS which is available only with SP license;



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 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.

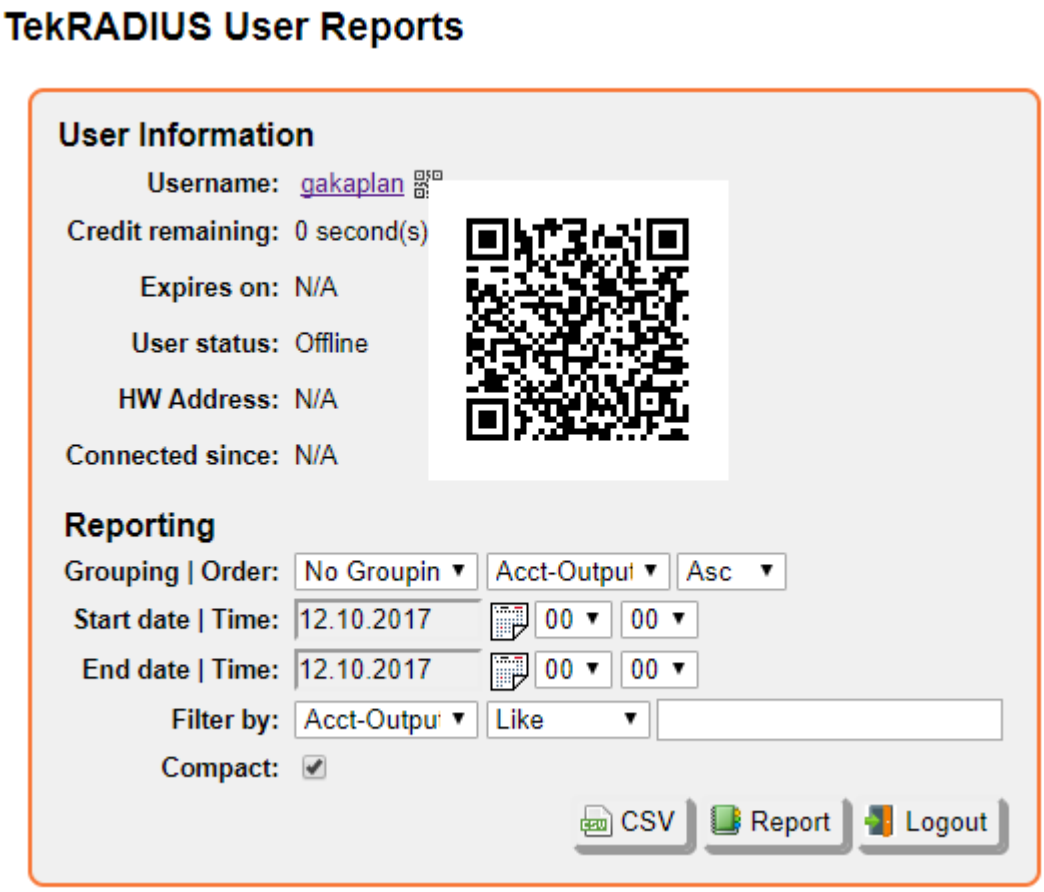


You also need to add HTTP-User-Name and HTTP-User-Password attribute to local user profile as check attributes to allow the user HTTP access.

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 form a previous version TekRADIUS.

Google Authenticator Secret Initialization

User will be asked to enter HTTP username and Password when they have accessed to 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 click the icon. User can scan this QR Code using Google Authenticator application to import the secret. Secret will be reset 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 displayed QR Code. Users should change the HTTP password after first login to the HTTP interface.



Users can enter dynamically generated passwords by Google Authenticator application while logging 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 deploy Google Authenticator with PAP, CHAP, MS-CHAP-v1/v2, PEAP, EAP-MD5, EAP-MS-CHAP-v2, LEAP and EAP-TTLS authentication methods.