Parallels RAS Multi-Factor RADIUS Authentication Setup for SMS delivered OTP[1]

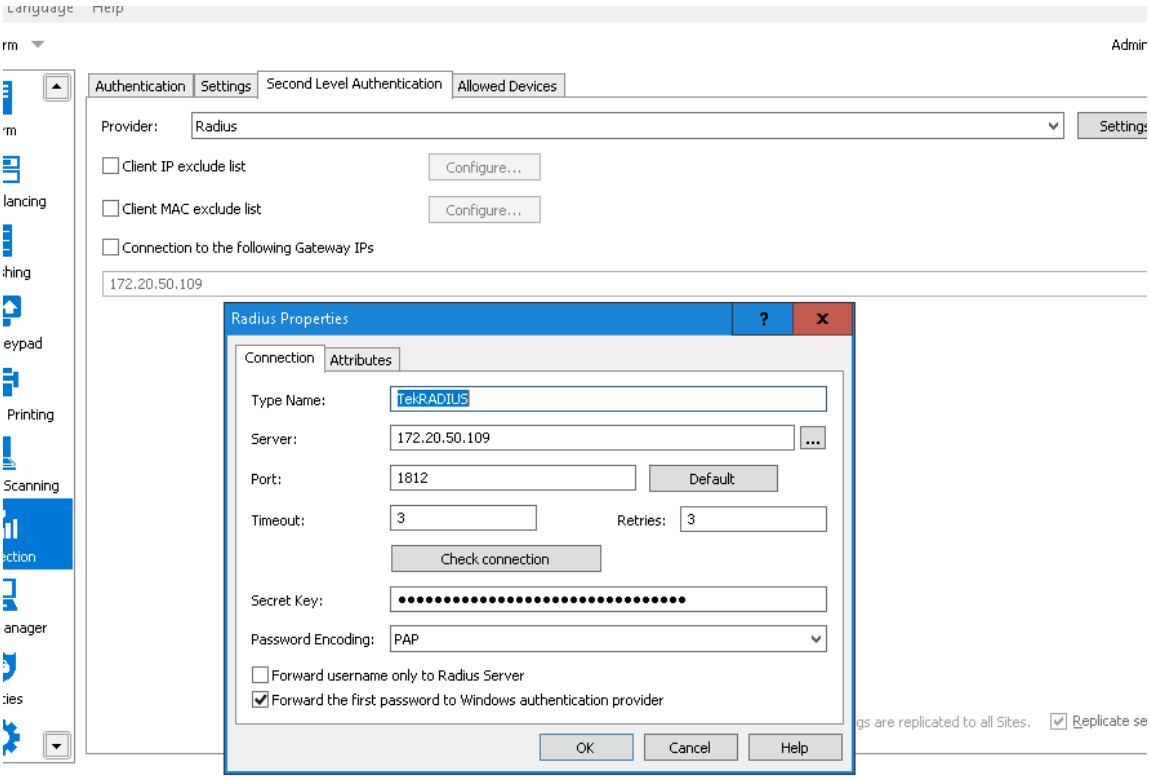
You can deploy TekRADIUS with Parallels RAS for Multi-Factor RADIUS Authentication. Parallels RAS allows you to use multi-factor authentication for access control by configuring a second level authentication.

Parallels Configuration

Parallels RAS allows you to use multi-factor authentication for access control by configuring multiple levels of authentication.

When multi-level authentication is used, users will have to authenticate through two or more successive stages to get the application list. While the first level authentication will always use native authentication (Active Directory / LDAP), other levels can use supported authentication providers like Google Authenticator or OTP authentication.

Multi-level of authentication is more secure because instead of using a standard username and password, it uses a static username and a one-time password generated by a token.
Multi-Level Authentication can be configured from the Second Level Authentication tab in the Connection category.



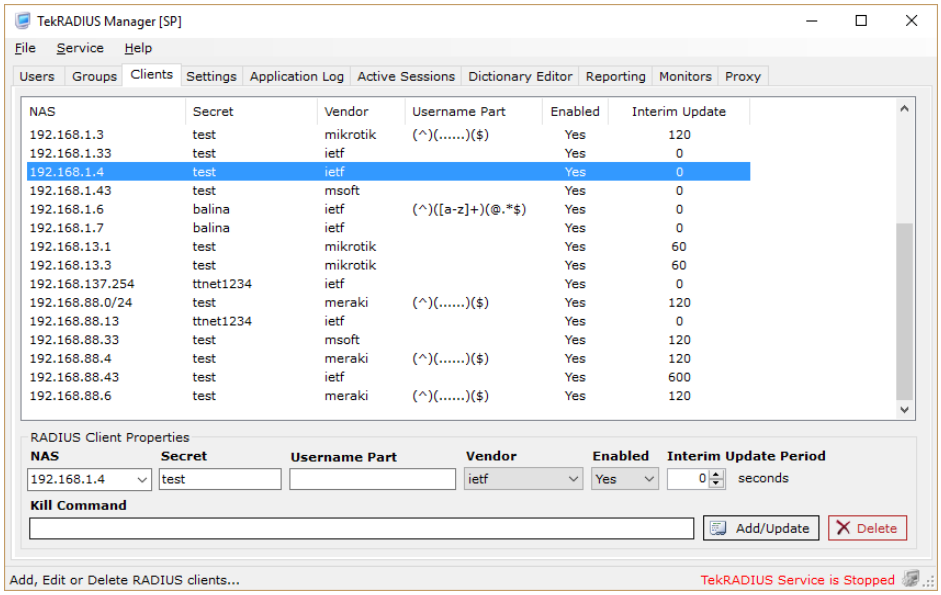
[1] Contributed by Frans Rampen (Frans.Rampen@yoda-ict.nl)

TekRADIUS Configuration

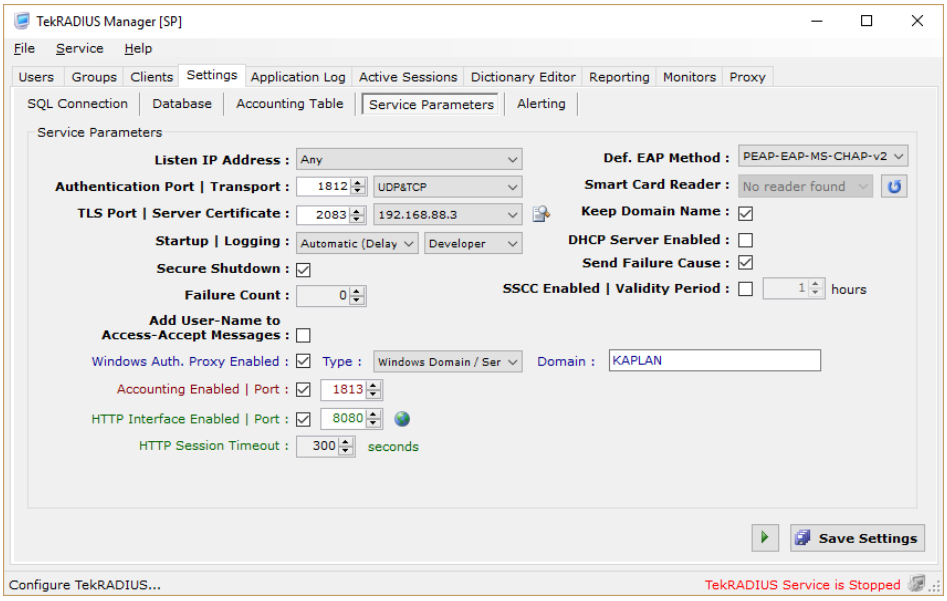
Using second level authentication within Parallels basically replaces standard Authentication provider with TekRADIUS. So TekRADIUS determines if Multi-Level authentication is required or not.

You can authenticate built-in user profiles or Active Directory users *(Commercial editions only)* with TekRADIUS. OTP will be used as Second Level Authentication in this example. Please note that OTP based authenticaton is supported only in commercial editions of TekRADIUS.

Add a client entry for Parallels in TekRADIUS Manager / Clients tab. Enter IP address of the Parallels RAS and a secret key.



Windows Auth. Proxy feature will be used in this sample configuration. You can enable Windows Auth. Directory Proxy at Settings / Service Parameters. TekRADIUS must be installed on domain member server for proper operation.



Some of users do not want to have extra authentication; only username/password. In TekRADIUS we have two group profiles matching active directory groups with or without OTP. You need two extra AD groups in your AD; Standard for plain Active Directory authentication, Access-2FA for OTP authentication after AD authentication and a dummy group called “TekRADIUS-Default”. Group profile configuration in TekRADIUS;

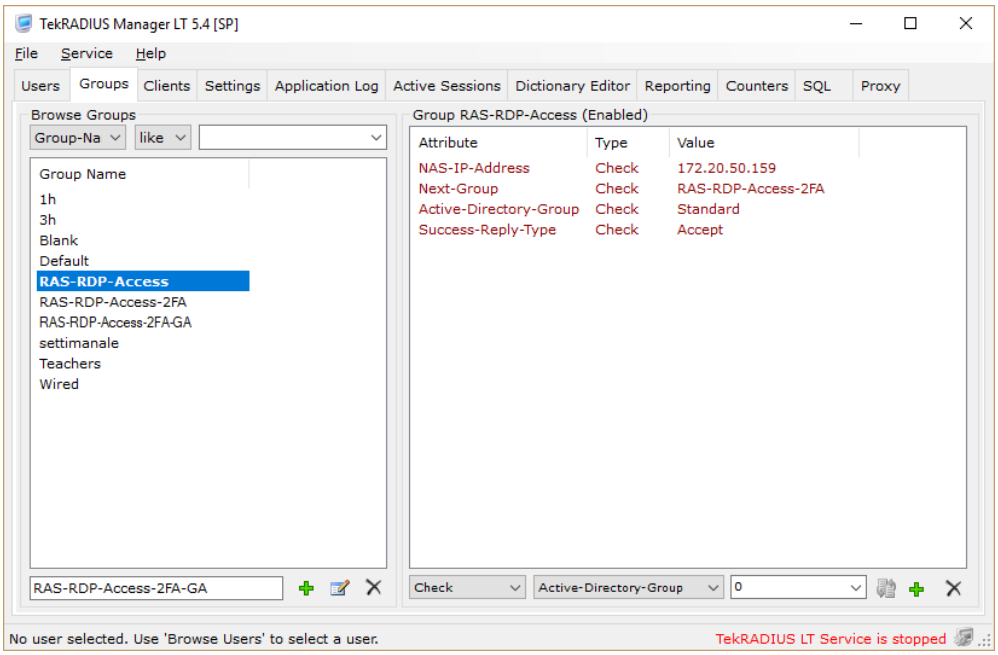
NAS-IP-Address attribute can be optionally added to group profile to restrict access from a specific NAS(es).

TekRADIUS Group "Default" *(This is entry group)*

- Active-Directory-Group = TekRADIUS-Default *(Check)*
- Next-Group = RAS-RDP-Access *(Check)*

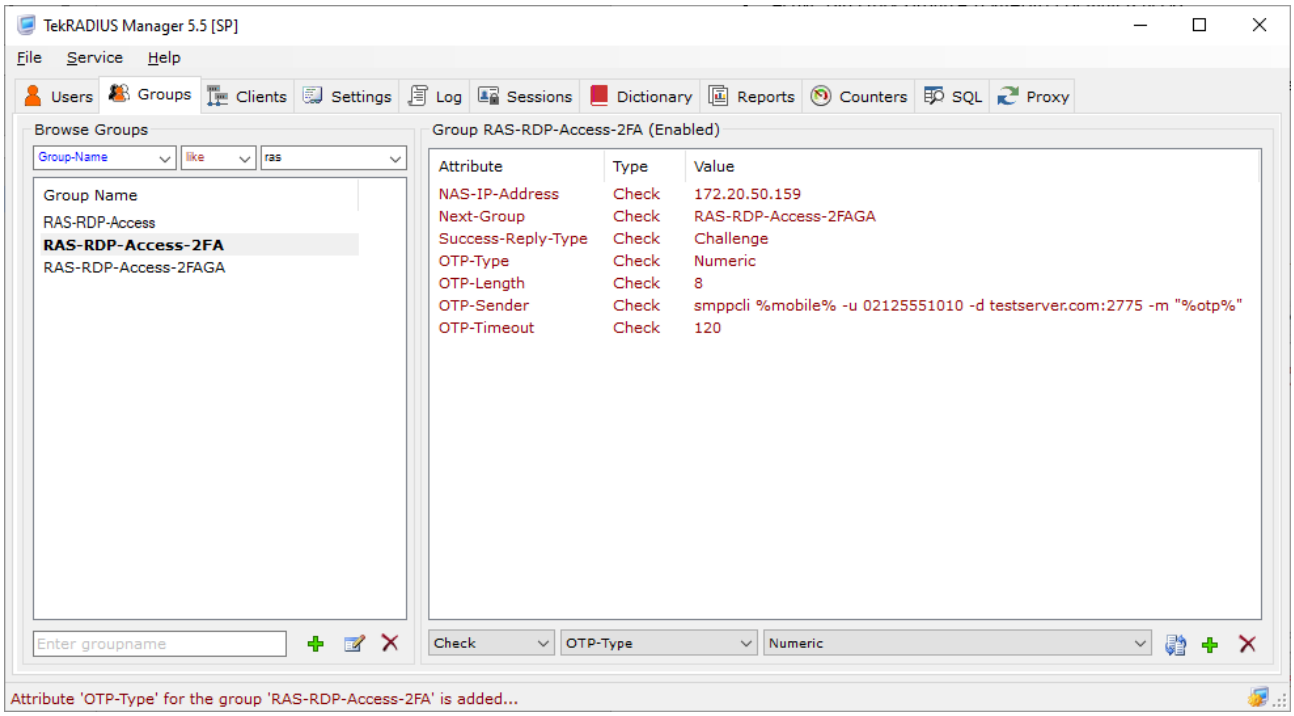
TekRADIUS Group "RAS-RDP-Access" *(This one authenticates plain AD users, falls back to RAS-RDP-Access-2FA if authentication fails)*

- Active-Directory-Group = Standard *(Check)*
- Success-Reply-Type = Accept *(Check)*
- Next-Group = RAS-RDP-Access-2FA

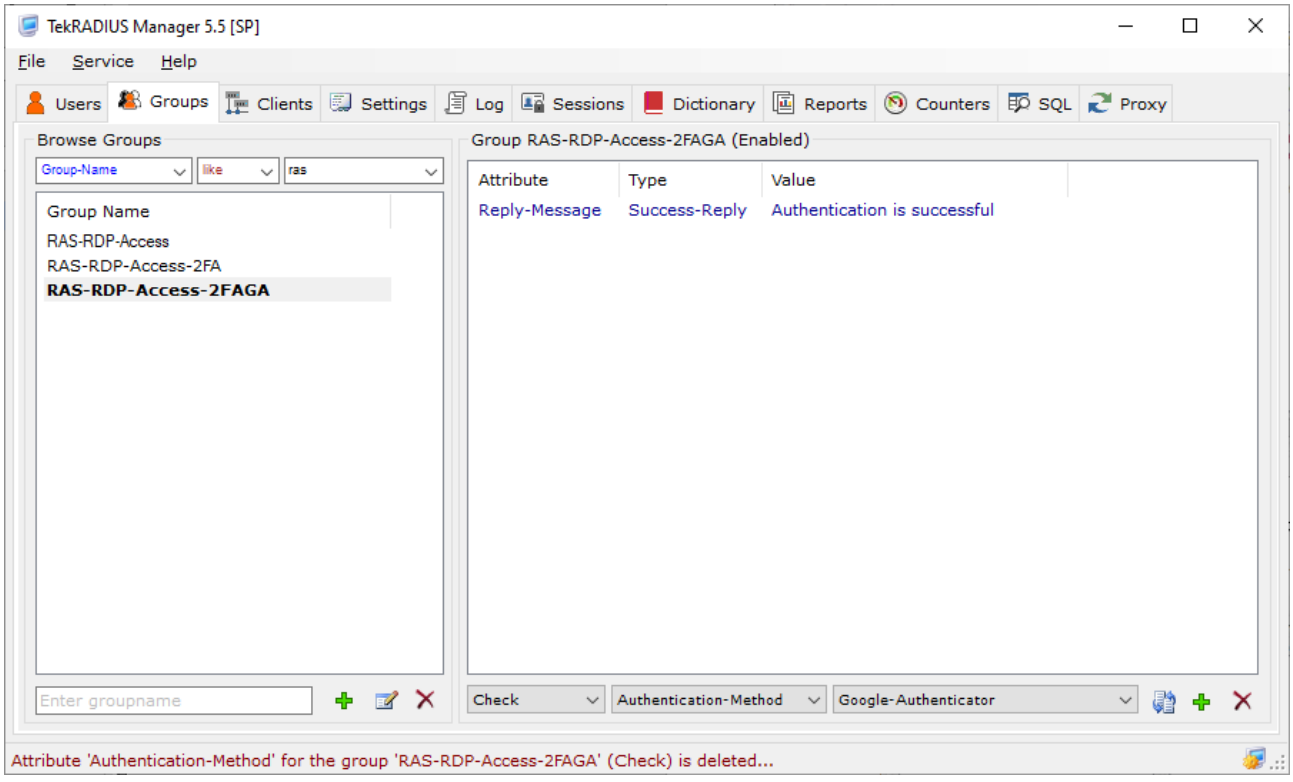


TekRADIUS Group "RAS-RDP-Access-2FA" *(Sends OTP in a challenge if AD authentication is successful)*

- Active-Directory-Group = Access-2FA *(Check)*
- Next-Group = RAS-RDP-Access-2FAGA *(Check)*
- Success-Reply-Type = Challenge *(Check)*
- OTP-Type = Numeric *(Check)*
- OTP-Length = 6 *(Check)*
- OTP-Sender = <Depends on your SMS sending method> *(Check)*



TekRADIUS Group "RAS-RDP-Access-2FAGA" *(This is the final phase for authentication)*



TekRADIUS sends an Accept Reply-Type after authentication of the credentials and active directory membership.

You can download trial version of SMPPCli.exe from KaplanSoft website.