# Parallels RAS Multi-Factor RADIUS Authentication Setup for SMS delivered OTP<sup>1</sup>

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.

Lanyuaye	нер			
rm 💌				Admir
	Authentication Sett	ngs Second Level Authentication Allowed Devices		
m	Provider: Radiu	IS		✓ Setting:
3	Client IP exclude	list Configure		
lancing	Client MAC exclu	de list Configure		
	Connection to th	e following Gateway IPs		
:hing	172.20.50.109			
		Radius Properties ? X		
eypad		Connection Attributes		
Printing		Type Name:		
		Server: 172.20.50.109		
Scanning		Port: 1812 Default		
		Timeout: 3 Retries: 3		
ection		Check connection		
5		Sacrat Keur		
anager				
		Password Encoding: PAP		
2		Forward username only to Radius Server		
lies		Forward the first password to windows authentication provider	gs are replicated to all Sites.	✓ <u>R</u> eplicate se
7		OK Cancel Help		

<sup>&</sup>lt;sup>1</sup> 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.

TekRADIUS Manag	er [SP]							-		×
le <u>S</u> ervice <u>H</u> el	p									
Jsers Groups Cl	ients Settings A	pplication Log Act	ive Sessions	Dictionary	Editor	Reporting	Monitors	Proxy		
NAS	Secret	Vendor	Usernam	ne Part	Enable	ed Inte	erim Update			^
192.168.1.3	test	mikrotik	(^)(	)(\$)	Yes		120			
192.168.1.33	test	ietf			Yes		0			
192.168.1.4	test	ietf			Yes		0			
192.168.1.43	test	msoft			Yes		0			
192.168.1.6	balina	ietf	(^)([a-z	]+)(@.*\$)	Yes		0			
192.168.1.7	balina	ietf			Yes		0			
192.168.13.1	test	mikrotik			Yes		60			
192.168.13.3	test	mikrotik			Yes		60			
192.168.137.254	ttnet1234	ietf			Yes		0			
192.168.88.0/24	test	meraki	(^)(	)(\$)	Yes		120			
192.168.88.13	ttnet1234	ietf			Yes		0			
192.168.88.33	test	msoft			Yes		120			
192.168.88.4	test	meraki	(^)(	)(\$)	Yes		120			
192.168.88.43	test	ietf			Yes		600			
192.168.88.6	test	meraki	(^)(	)(\$)	Yes		120			~
RADIUS Client Pro	operties									
NAS	Secret	Username P	art	Vendor		Enabled	Interim	Update Period	l	
192.168.1.4 、	/ test			ietf	$\sim$	Yes 🗸	0	seconds		
Kill Command										
								Add/Update	X Dele	ete
, Edit or Delete R/	ADIUS clients						Tek	RADIUS Service	is Stopp	ed 🎲

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.

TekRADIUS Manager [SP]	-		×
le <u>S</u> ervice <u>H</u> elp			
Jsers Groups Clients Settings Application Log Active Sessions Dictionary Editor Reporting Monitors Proxy			
SQL Connection Database Accounting Table Service Parameters Alerting			
Service Parameters			
Listen IP Address : Any V Def. EAP Method : PEAP-E	AP-MS-CH	AP-v2 V	-
Authentication Port   Transport : 1812 🖨 UDP&TCP 🗸 Smart Card Reader : No read	ler found	~ <b>U</b>	1
TLS Port   Server Certificate : 2083 🛊 192.168.88.3 🗸 🏠 Keep Domain Name : 🗸			
Startup   Logging : Automatic (Delay > Developer > DHCP Server Enabled :			
Secure Shutdown : 🕢 Send Failure Cause : 🗸			
Failure Count : 0 🔹 SSCC Enabled   Validity Period : 🗌	1 🔹 ho	urs	
Add User-Name to Access-Accept Messages :			
Windows Auth. Proxy Enabled : 🗹 Type : Windows Domain / Ser 🗸 Domain : KAPLAN			
Accounting Enabled   Port : 🔽 1813 💼			
HTTP Interface Enabled   Port : 🗹 🛛 8080 🖨 🕥			
HTTP Session Timeout : 300 🜩 seconds			
Þ	🗐 Save	e Settin	gs
nfigure TekRADIUS TekRADIUS S	ervice is	Stopped	Ug

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

2	ervice	нер													
ers	Groups	Clients	Settings	Applicat	ion Log	A	ctive Sessions	Dictionary	Editor	Reporting	Counters	SQL	Pro	ху	
rows	se Groups					_	Group RAS-RI	DP-Access (	Enable	d)					
Grou	p-Na 🗸	like 🗸			~		Attribute		Туре	Value	•				
Group-Na v like v Group Name 1h 3h Blank Default RAS-RDP-Access RAS-RDP-Access-2FA RAS-RDP-Access-2FA RAS-RDP-Access-2FA Settimanale Teachers Wired					NAS-IP-Addr Next-Group Active-Direct Success-Rep	ess ory-Group ly-Type	Check Check Check	: 172.1 RAS- Stann Acce	20.50.159 RDP-Access dard ot	:-2FA					
AS-	RDP-Acce	ss-2FA-G	A	+	<b>∀</b> X		Check	~ Active-	Directory	-Group	/ 0		~	Þ +	×

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)

Users 👫 Groups 🏢 Clients 🗔 S	ettings 🗐 Log	Sessions	E Dictionary	Reports	(Notes Section 1997)	🗊 sql	2 Prox	у	
rowse Groups	Gro	up RAS-RDP-Acc	ess-2FAGA (Enabl	led)					
roup-Name 🗸 like 🗸 ras	Att	ribute Ty	ype V	alue					_
Group Name	Re	ply-Message S	uccess-Reply A	uthentication	n is successful				
AS-RDP-Access									
AS-RDP-Access-2FA									
AS-RDP-Access-2FAGA									

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.