Parallels RAS Multi-Factor RADIUS Authentication Setup¹

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.

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.

Language	Leib		
rm 💌			Admir
	Authentication Settings Second Level Authentication Allowed D	avices	
m	Provider: Radius		✓ Setting:
9	Client IP exclude list		
lancing	Client MAC exclude list Configure		
	Connection to the following Gateway IPs		
:hing	172.20.50.109		
	Radius Properties	? X	
eypad	Connection Attributes		
P	Type Name: TekRADIUS		
Printing	Server: 172.20.50.109		
Scanning	Port: 1812	Default	
ıl 👘	Timeout: 3	Retries: 3	
ction	Check conne	ction	
3	Secret Key:		
anager	Password Encoding: PAP	~	
3	Forward username only to Radius Serve	r	
:ies	Forward the first password to Windows	authentication provider	
> -		OK Cancel Help	gs are replicated to all Sites. VI Replicate se

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. Google Authenticator will be used as Second Level Authentication in this example. Please note that Google Authenticator 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 Manage	er [SP]						-		×
e <u>S</u> ervice <u>H</u> elp	5								
sers Groups Clie	ents Settings App	lication Log Active S	Sessions Dicti	onary Editor	Reporting	g Monitors F	Proxy		
NAS	Secret	Vendor	Username Pa	rt Enab	led Ir	nterim Update			^
192.168.1.3	test	mikrotik	(^)()(\$)	Ye	s	120			
192.168.1.33	test	ietf		Ye	s	0			
192.168.1.4	test	ietf		Ye	s	0			
192.168.1.43	test	msoft		Ye	s	0			
192.168.1.6	balina	ietf	(^)([a-z]+)(@	⊅.*\$) Ye	s	0			
192.168.1.7	balina	ietf		Ye	s	0			
192.168.13.1	test	mikrotik		Ye	s	60			
192.168.13.3	test	mikrotik		Ye	s	60			
192.168.137.254	ttnet1234	ietf		Ye	s	0			
192.168.88.0/24	test	meraki	(^)()(\$)	Ye	s	120			
192.168.88.13	ttnet1234	ietf		Ye	s	0			
192.168.88.33	test	msoft		Ye	s	120			
192.168.88.4	test	meraki	(^)()(\$)	Ye	s	120			
192.168.88.43	test	ietf		Ye	s	600			
192.168.88.6	test	meraki	(^)()(\$)	Ye	s	120			~
RADIUS Client Pro	perties								
NAS	Secret	Username Part	Vend	lor	Enable	d Interim	Update Period		
192.168.1.4 ~	test		ietf	~	Yes	 ○ ▲ 	seconds		
Kill Command									
							Add/Update	X Dele	te

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.

Users 👗 Groups	📜 Clients 🗔 Settings 🗐 Events 🗳 Sessions	📕 Dictionary 👜 Reports 🔊 Counters 🗊 SQL 🐺	DHCP 2 Prox						
Database 🛛 🏶 F	arameters Accounting Table								
Service	RADIUS Authentication Port	1812							
Authentication	TLS Port	2083							
Accounting	Enabled TLS Versions	TLS10, TLS11, TLS12							
DHCP Server	Include Certificate Chain of Trust	Yes							
Mail Alerting	Server Certificate	New-CA							
Cipher Suites	Trusted CAs	Trust all	\sim						
HTTP Interface	Default EAP Method	PEAP-EAP-MS-CHAP-v2							
FILLE Interface	EAP Server Timeout	60							
	Enable TLS Session Resumption	Yes							
	Session Ticket Encryption Key Lifetime	24							
	Require Local Certificate for EAP-TLS	ficate for EAP-TLS No							
	Authentication Proxy Type	Active Directory							
	Authentication Proxy Domain	lync.kaplansoft.com							
	Keep Domain Name	Yes							
	Add User-Name to Access-Accept Messages	No							
	Failure Count	3							
	Fail on Password Failure	Yes							
	Send Failure Cause	No							
	Trusted CAs Select trusted signing certificate authorities for the cli	ent certificates.							

TekRADIUS Settings - Authentication

2										
Users 🗶 Groups	Clients 🖾 Settings	Events	Sessions	Dictionary	Reports	() Counters	🗊 SQL	TO DHCP	2 Pr	
Database	arameters Accountin	ng Table								
Service	Enabled			Yes						
Authentication	HTTP Port			443						
Accounting	Use TLS Transport			Yes						
DHCP Server	Server Certificate			offic	ce.kaplanso	ft.com				
Mail Alerting	Mutual TLS Authentic	ation		No				-1.1-		
Cipher Suites	Trusted CAs			Clas	s 3 Public Prir	mary Certificati	on Authori	ty, DigiCer	t Assure	
HTTP Interface	Session Timeout			0						
	Enable REST API									

TekRADIUS Settings - HTTP Interface

Some of the 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 Google-Authenticator after AD authentication and a dummy group called "TekRADIUS-Default". Group profile configuration in TekRADIUS;

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

sers	Groups	Clients	Settings	Applica	tion Log	Δ	ctive Sessions	Dictionary	Editor	Reporting	Counters	501	Prox	v	
Brows	se Groups		Cottingo	, pp. rea	cion 20g		Group RAS-RE	P-Access (Enabled			- 4-			
Grou Ih 3h Blan Defa RAS RAS setti Teac Wire	k up Name k ult -RDP-Acce RDP-Acces manale thers id	Cess ess-2FA 38-2FA-GA			~		Attribute NA5-IP-Addr Next-Group Active-Direct Success-Repl	ess ory-Group y-Type	Type Check Check Check	Valu 172: RAS Stan Acce	e 20.50.159 -RDP-Access dard dard pt	s-2FA			
RAS-	RDP-Acce	ss-2FA-G	A	•	📝 🗙		Check	✓ Active-I	Director	-Group	~ 0		~ #		×

TekRADIUS Group "RAS-RDP-Access-2FA" (Sends challenge for Google-Authenticator phase if AD authentication is successful)

- Active-Directory-Group = Access-2FA (Check)
- Next-Group = RAS-RDP-Access-2FAGA (Check)
- Success-Reply-Type = Challenge (Check)

ers	Groups	Clients	Settings	Applica	tion Loa	Active Sessions	Dictionary	Editor	Reporting	Counters	SOL	Proxy		
Brows	e Groups					Group RAS-R	DP-Access-1	2E4 (En	abled)			,		
Grou Grou 1h 3h Blan Defa RAS RAS settii Teac Wire	k up Name k ult -RDP-Acces RDP-Acces manale thers d	like ∨ ess cess-2F s-2FA-GA	A		~	Attribute NAS-IP-Addr Next-Group Active-Dired Success-Rep	ess tory-Group Ily-Type	Type Check Check Check Check	Value (172.2 (RAS- (Acces) (Chall	20.50.159 RDP-Access ss-2FA enge	-2FA-GA			
RAS-I	RDP-Acce	ss-2FA-G	A	+	∡ ×	Check	 ✓ Active- 	Director	y-Group	/ 0		- 8	+	×

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

• Authentication-Method = Google-Authenticator (Check)

🥃 TekRADIUS Manager LT 5.4 [SP] - 🗆 🗙
<u>F</u> ile <u>S</u> ervice <u>H</u> elp
Users Groups Clients Settings Application Log Active Sessions Dictionary Editor Reporting Counters SQL Proxy
Browse Groups Group RAS-RDP-Access-2FA-GA (Enabled)
Group-Na V like V Attribute Type Value
Group Name NAS-IP-Address Check 172.20.50.159 1h 3h Blank Default Check Wired Authentication-Method Check Google-Authenticator Blank Default RAS-RDP-Access FAGA Google-Authenticator RAS-RDP-Access-ZFA FAGA Settimanale Teachers Wired Wired Settimanale Settimanale
RAS-RDP-Access-2FA-GA
Group 'RAS-RDP-Access-2FA-GA' selected. TekRADIUS LT Service is stopped 🧔 .

The primary group for a user must be Access-2FA in this configuration and TekRADIUS HTTP interface should display GA initiator icon when a user login to TekRADIUS HTTP interface with AD credentials.

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

RAS Log:

[I 06/000000E/T00001058] Tue Mar 20 11:11:12 2018 - User (user@company.domain) connected from client (10.10.11.9:51501), machine (CLIENT) (14-DD-A9-2B-CB-4D) mode Gateway SSL, using OS: Microsoft Windows 10 Enterprise Edition (x64) , Client version: 16.2 (build 19160). [I 0E/0000000/T00001058] Tue Mar 20 11:11:13 2018 - Radius 172.20.50.109: User user@company.domain from machine CLIENT access allowed. [I 06/000000E/T00001058] Tue Mar 20 11:11:13 2018 - Logon successful user 'user@company.domain' client IP '188.92.60.180' gateway IP '172.21.50.109' [47 31 0 0] [I 06/0000040/T00001058] Tue Mar 20 11:11:13 2018 - Client Rules: rule 'Default Policy' matched. User: user domain Gateway: 172.21.50.109 Mac Address: 14-DD-A9-2B-CB-4D

TekRADIUS log:

20.03.2018 11:11:12.549 - RadAuth req. from : 172.20.50.109:51592 [UDP] Size : 64 / 64 Identifier : 1 Attributes • NAS-IP-Address = 172.20.50.109 User-Name = user@company.domain 20.03.2018 11:11:12.550 - Authentication query; for user 'user@company.domain'; SELECT Attribute, Val from Users where UserName = 'user@company.domain' and AttrType = 0 20.03.2018 11:11:12.587 - Active Directory Authentication commencing for user 'user@company.domain' 20.03.2018 11:11:12.814 - Check items control for user 'user@company.domain' - Start (Group: Default) [ActiveDirectory]. 20.03.2018 11:11:12.829 - Validating Active Directory group membership for user 'user@company.domain' (TekRADIUS-Default, company.domain). 20.03.2018 11:11:12.829 - Getting Active Directory group membership information for user 'user@company.domain' (TekRADIUS-Default, company.domain [company.domain]). 20.03.2018 11:11:13.038 - Active Directory group membership validation failed for user 'user@company.domain'. No group information obtained. 20.03.2018 11:11:13.038 - Active Directory group does not match (TekRADIUS-Default). 20.03.2018 11:11:13.038 - Check items control for user 'user@company.domain' - Stop (Default). 20.03.2018 11:11:13.056 - Check items control for user 'user@company.domain' - Start (Group: RAS-RDP-Access) [ActiveDirectory]. 20.03.2018 11:11:13.073 - Validating Active Directory group membership for user 'user@company.domain' (Standard, company.domain). 20.03.2018 11:11:13.073 - Getting Active Directory group membership information for user 'user@company.domain' (Standard, company.domain [company.domain]). 20.03.2018 11:11:13.138 - Active Directory group membership validation successful for user 'user@company.domain'. 20.03.2018 11:11:13.138 - Check items control for user 'user@company.domain' - Stop (RAS-RDP-Access). 20.03.2018 11:11:13.138 - Active Directory authentication successfull for user 'user@company.domain' 20.03.2018 11:11:13.138 - Fetching Success-Reply items for user 'user@company.domain' - Start. 20.03.2018 11:11:13.139 - Fetching Success-Reply items for user 'user@company.domain' - Stop.

TekRADIUS sends challenge back top RAS if windows authentication was successful followed by Google Authentication.

RAS Log:

[I 06/000000E/T00000F24] Tue Mar 20 11:19:32 2018 - User (rastest@company.domain) connected from client (10.10.11.9:51760), machine (CLIENT) (14-DD-A9-2B-CB-4D) mode Gateway SSL, using OS: Microsoft Windows 10 Enterprise Edition (x64) , Client version: 16.2 (build 19160). [I 0E/0000000/T00000F24] Tue Mar 20 11:19:32 2018 - Radius 172.20.50.109: User rastest@company.domain from machine CLIENT is challenged. [I 0E/0000000/T00000F24] Tue Mar 20 11:19:41 2018 - Radius 172.20.50.109: User rastest@company.domain from machine CLIENT access allowed. [I 06/0000000E/T00000F24] Tue Mar 20 11:19:41 2018 - Logon successful user 'rastest@company.domain' client IP '188.92.60.180' gateway IP '172.21.50.109' [47 31 0 0] [I 06/0000040/T0000F24] Tue Mar 20 11:19:41 2018 - Client Rules: rule 'YodaCLoud Default Policy' matched. User: rastest domain Gateway: 172.21.50.109 Mac Address: 14-DD-A9-2B-CB-4D

TekRADIUS Log:

20.03.2018 11:19:32.147 - RadAuth req. from : 172.20.50.109:63709 [UDP] : 58 / 58 Size Identifier : 1 Attributes • NAS-IP-Address = 172.20.50.109 User-Name = rastest@company.domain 20.03.2018 11:19:32.147 - Authentication query; for user 'rastest@company.domain'; SELECT Attribute, Val from Users where UserName = 'rastest@company.domain' and AttrType = 0 20.03.2018 11:19:32.173 - Active Directory Authentication commencing for user 'rastest@company.domain' 20.03.2018 11:19:32.195 - Check items control for user 'rastest@company.domain' - Start (Group: Default) [ActiveDirectory]. 20.03.2018 11:19:32.207 - Validating Active Directory group membership for user 'rastest@company.domain' (TekRADIUS-Default, company.domain). 20.03.2018 11:19:32.207 - Getting Active Directory group membership information for user 'rastest@company.domain' (TekRADIUS-Default, company.domain [company.domain]). 20.03.2018 11:19:32.316 - Active Directory group membership validation failed for user 'rastest@company.domain'. No group information obtained. 20.03.2018 11:19:32.316 - Active Directory group does not match (TekRADIUS-Default). 20.03.2018 11:19:32.316 - Check items control for user 'rastest@company.domain' - Stop (Default). 20.03.2018 11:19:32.330 - Check items control for user 'rastest@company.domain' - Start (Group: RAS-RDP-Access) [ActiveDirectory]. 20.03.2018 11:19:32.342 - Validating Active Directory group membership for user 'rastest@company.domain' (Access-2FA, company.domain). 20.03.2018 11:19:32.342 - Getting Active Directory group membership information for user 'rastest@company.domain' (Access-2FA, company.domain [company.domain]). 20.03.2018 11:19:32.412 - Active Directory group membership validation failed for user 'rastest@company.domain'. No group information obtained. 20.03.2018 11:19:32.412 - Active Directory group does not match (Access-2FA). 20.03.2018 11:19:32.412 - Check items control for user 'rastest@company.domain' - Stop (RAS-RDP-Access). 20.03.2018 11:19:32.425 - Check items control for user 'rastest@company.domain' - Start (Group: RAS-RDP-Access-2FA) [ActiveDirectory]. 20.03.2018 11:19:32.437 - Validating Active Directory group membership for user 'rastest@company.domain' (Access-2FA). 20.03.2018 11:19:32.437 - Getting Active Directory group membership information for user 'rastest@company.domain' (Access-2FA, company.domain [company.domain]). 20.03.2018 11:19:32.504 - Active Directory group membership validation successful for user 'rastest@company.domain'. 20.03.2018 11:19:32.504 - Check items control for user 'rastest@company.domain' - Stop (RAS-RDP-Access-2FA). 20.03.2018 11:19:32.504 - Active Directory authentication successful for user 'rastest@company.domain' 20.03.2018 11:19:32.504 - Fetching Success-Reply items for user 'rastest@company.domain' - Start. 20.03.2018 11:19:32.504 - Fetching Success-Reply items for user 'rastest@company.domain' - Stop. 20.03.2018 11:19:32.504 - Generating Reply Packet - Start. 20.03.2018 11:19:32.505 - Generating Reply Packet - Stop. 20.03.2018 11:19:32.505 - RadAuth reply to : 172.20.50.109:63709 (Failure) Size : 54 Identifier : 1 Attributes : State = 5417647261A3D24A94B9E8C5E445FF08 20.03.2018 11:19:41.779 - RadAuth req. from : 172.20.50.109:63709 [UDP] Size : 92 / 92 Identifier : 1 Attributes : State = 5417647261A3D24A94B9E8C5E445FF08NAS-IP-Address = 172.20.50.109 User-Name = rastest@company.domain

20.03.2018 11:19:41.782 - GoogleAuthenticator Authentication commencing for user 'rastest@company.domain' 20.03.2018 11:19:41.782 - Check items control for user 'rastest@company.domain' - Start (Group: RAS-RDP-Access-2FA-GA) [GoogleAuthenticator]. 20.03.2018 11:19:41.782 - Check items control for user 'rastest@company.domain' - Stop (RAS-RDP-Access-2FA-GA). 20.03.2018 11:19:41.782 - Google Authenticator authentication successful for user 'rastest@company.domain' 20.03.2018 11:19:41.782 - Fetching Success-Reply items for user 'rastest@company.domain' - Start. 20.03.2018 11:19:41.782 - Fetching Success-Reply items for user 'rastest@company.domain' - Start.

If a third level authentication is required; just return 'Challenge' as Reply-Type on Google Authenticator and configure another authentication method using groups.

You must initialize Google Authenticator prior to make an authentication attempt. Connect to TekRADIUS HTTP interface with Active Directory username and password and initialize Google Authenticator by clicking on QR code icon next to the username. Scan displayed QR code by using mobile Google Authenticator application and click on QR code image on the HTTP interface.

User Informatio	on	
Username:	gakaplan 뫎	3
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 V Asc V
Start date Time:	12.10.2017	00 ▼ 00 ▼
End date Time:	12.10.2017	00 ▼ 00 ▼
Filter by:	Acct-Outpu	t V Like V
Compact:		
		E CSV Report Logout

TekRADIUS User Reports