VMware View Two-Factor RADIUS Authentication Setup

You can deploy TekRADIUS with VMware View for Two-Factor RADIUS Authentication. TekRADIUS can generate numeric or alphanumeric One Time Passwords (OTP) which can be delivered to authenticated users via telephony methods.

VMware Configuration

From a Web browser, access View Administrator on the View 5.1 Connection Server using https://hostname/admin and log in.

Edit View Connection	Server Settings	3					
General Auti	hentication Backup						
Changes to authe	Changes to authentication settings will take effect on next user login						
Smart card auther	Smart card authentication: Optional 🔍						
Disconnect	Disconnect user sessions on smart card removal						
Advanced Authen 2-factor authentic Enforce 2-fa Use same u Authenticator:	ntication sation RADIUS • actor and Windows user name matching username and password for RADIUS and Windows authentication Select Authenticator • Create New Authenticator						
	Manage Authenticators						
<	OK	Cancel					

Under View **Configuration** > **Servers** > **Connection Servers** select the Connection Server and select **Edit**. Under **Authentication** > **Advanced Authentication**, set the 2-factor authentication option to **RADIUS** and under **Authenticator** select **Create New Authenticator**.

In the admin configuration of RADIUS authentication under **Advanced Authentication**, if **Enforce 2-factor and Windows user name matching** is selected then the Windows login prompt after RADIUS authentication will force the username to be the same as the RADIUS username and the user will not be able to modify this. This feature is the same as is done for RSA SecurID authentication.

Similarly, if **Use same username and password for RADIUS and Windows authentication** is selected then the user will not be prompted for Windows credentials after RADIUS authentication if the RADIUS authentication used Windows username and password. This feature is used in cases where the initial RADIUS authentication uses Windows authentication which triggers an out-of-band transmission of a tokencode which is used as part of a RADIUS challenge. This then avoids the need for the user to re-enter the Windows username and password after RADIUS authentication. This feature will not work in Windows View clients older than 5.1.

Enter IP address of TekRADIUS sever to Hostname / Address and configured shared secret for Connection Server. You should not need to change default RADIUS protocol ports, Authentication for 1812 and Accounting 1813. You can set accounting port to 0 if you do not need RADIUS accounting.

If there is a secondary RADIUS server then complete the settings for the secondary server and select Finish.

Add RADIUS Authenticator	
A RADIUS authenticato environment.	r is available to all Connection Servers in this View
Label:	MyToken Enter a label shown to clients
Description:	MyToken RADIUS Authenticator
Primary Authentication S	erver
Hostname/Address:	1.2.3.4
Authentication port:	1812 Accounting port: 1813
Authentication type:	PAP 🗸 🔻
Shared secret:	****
Server timeout:	3 seconds
Max retries:	5
Realm prefix:	
Realm suffix:	
	Next > Cancel

TekRADIUS Configuration

You can authenticate built-in user profiles or Active Directory users (*Commercial editions only*) with VMware View. Please note that generic OTP generation is supported only in commercial editions of TekRADIUS.

Add a client entry for VMware View in TekRADIUS Manager / Clients tab. Enter IP address of the VMWare View Connection Server and a secret key.

NAS Secret Vendor Username Part Enabled Interim Update 192.168.1.3 test mikrotik (^)()(\$) Yes 120 192.168.1.33 test ietf Yes 0 192.168.1.33 test ietf Yes 0 192.168.1.43 test msoft Yes 0 192.168.1.43 test msoft Yes 0 192.168.1.7 balina ietf (^)([a-z]+)(@.*\$) Yes 0 192.168.1.7 balina ietf Yes 0 192.168.1.3.1 test mikrotik Yes 60 192.168.1.3.1 test mikrotik Yes 60 192.168.8.0/24 test meraki (^)()(\$) Yes 120 192.168.8.31 thet1234 ietf Yes 0 192.168.88.33 test msoft Yes 120 192.168.88.44 test meraki (^)()(\$) Yes 120 192.168		ang Homeora Proxy	Kepu	Dictionary Editor	Active Sessions	Application Log A	Circints Settings	Groups	sers
192.168.1.3 test mikrotik (^)()(\$) Yes 120 192.168.1.33 test ietf Yes 0 192.168.1.33 test ietf Yes 0 192.168.1.43 test msoft Yes 0 192.168.1.43 test mikrotik Yes 0 192.168.1.7 balina ietf (^)([a-z]+)(@.*\$) Yes 60 192.168.13.1 test mikrotik Yes 60 192.168.13.2 test mikrotik Yes 0 192.168.8.0/24 test meraki (^)()(\$) Yes 120 192.168.8.3 test msoft Yes 120 121 192.168.8.3 test meraki (^)()(\$) Yes 120 192.168.8.6.4 test meraki (^)()(\$) Yes <td< th=""><th></th><th>Interim Update</th><th>bled</th><th>ne Part Ena</th><th>or Usernan</th><th>Vendo</th><th>Secret</th><th>5</th><th>VAS</th></td<>		Interim Update	bled	ne Part Ena	or Usernan	Vendo	Secret	5	VAS
92.168.1.33 test ietf Yes 0 92.168.1.44 test msoft Yes 0 92.168.1.43 test msoft Yes 0 92.168.1.43 test msoft (^)([a-z]+)(@.*\$) Yes 0 92.168.1.6 balina ietf (^)([a-z]+)(@.*\$) Yes 0 92.168.1.7 balina ietf Yes 0 92.168.13.1 test mikrotik Yes 60 92.168.13.3 test mikrotik Yes 0 92.168.13.1.3 test meraki (^)()(\$) Yes 0 92.168.83.7.254 ttnet1234 ietf Yes 0 92.168.86.13 ttnet1234 ietf Yes 0 92.168.83.3 test msoft Yes 120 92.168.83.3 test meraki (^)()(\$) Yes 120 92.168.84.3 test meraki (^)()(\$) Yes 120		120	es)(\$) Ye	otik (^)(mikrot	test	.168.1.3	92.
92.168.1.4 test ietf Yes 0 92.168.1.43 test msoft Yes 0 92.168.1.43 test msoft Yes 0 92.168.1.43 test msoft Yes 0 92.168.1.6 balina ietf Yes 0 92.168.1.7 balina ietf Yes 0 92.168.13.1 test mikrotik Yes 60 92.168.13.3 test mikrotik Yes 0 92.168.13.2 test meraki (^)()(\$) Yes 0 92.168.81.3 thref1234 ietf Yes 0 92.168.85.3 test msoft Yes 120 92.168.88.4 test meraki (^)()(\$) Yes 120 92.168.88.4 test meraki (^)()(\$) Yes 120 92.168.88.6 test meraki (^)()(\$) Yes 120 92.168.88.6 test meraki (^)()(\$) Yes 120		0	es	Y		ietf	test	.168.1.33	92.
92.168.1.43 test msoft Yes 0 92.168.1.6 balina ietf (^)([a-z]+)(@.*\$) Yes 0 92.168.1.7 balina ietf (^)([a-z]+)(@.*\$) Yes 0 92.168.1.7 balina ietf Yes 0 92.168.1.7 balina ietf Yes 0 92.168.13.1 test mikrotik Yes 60 92.168.13.3 test mikrotik Yes 0 92.168.137.254 thref1234 ietf Yes 0 92.168.88.0/24 test meraki (^)()(\$) Yes 120 92.168.88.3 thref1234 ietf Yes 0 92.168.88.3 test msoft Yes 120 92.168.88.4 test meraki (^)()(\$) Yes 120 92.168.88.4 test meraki (^)()(\$) Yes 120 92.168.88.6 test meraki (^)()(\$) Yes 120		0	es	Y		ietf	test	.168.1.4	92.
92.168.1.6 balina ietf (^)([a-z]+)(@.*\$) Yes 0 92.168.1.7 balina ietf Yes 0 92.168.1.3.1 test mikrotik Yes 60 92.168.13.1 test mikrotik Yes 60 92.168.13.3 test mikrotik Yes 60 92.168.137.254 ttnet1234 ietf Yes 0 92.168.83.1 thret1234 ietf Yes 0 92.168.83.3 test msoft Yes 120 92.168.83.3 test msoft Yes 120 92.168.88.4 test meraki (^)()(\$) Yes 120 92.168.88.4 test meraki (^)()(\$) Yes 120 92.168.88.6 test meraki (^)()(\$) Yes 120		0	es	Ye	t	msoft	test	.168.1.43	92.
92.168.1.7 balina ietf Yes 0 92.168.13.1 test mikrotik Yes 60 92.168.13.3 test mikrotik Yes 60 92.168.13.3 test mikrotik Yes 0 92.168.13.3 test mikrotik Yes 0 92.168.13.3 test meraki (^)()(\$) Yes 0 92.168.88.024 test meraki (^)()(\$) Yes 120 92.168.88.13 thet1234 ietf Yes 120 92.168.88.33 test msoft Yes 120 92.168.88.4 test meraki (^)()(\$) Yes 120 92.168.88.6 test meraki (^)()(\$) Yes 120		0	es]+)(@.*\$) Ye	(^)([a-z	ietf	balina	.168.1.6	92.
92.168.13.1 test mikrotik Yes 60 92.168.13.3 test mikrotik Yes 60 92.168.137.254 ttnet1234 ietf Yes 0 92.168.86.0/24 test meraki (^)()(\$) Yes 120 92.168.88.0/24 test msoft Yes 0 92.168.88.0/24 test msoft Yes 0 92.168.88.13 ttnet1234 ietf Yes 120 92.168.88.4 test meraki (^)()(\$) Yes 120 92.168.88.43 test meraki (^)()(\$) Yes 120 92.168.88.6 test meraki (^)()(\$) Yes 120		0	es	Ye		ietf	balina	.168.1.7	92.
92.168.13.3 test mikrotik Yes 60 92.168.137.254 thret1234 ietf Yes 0 92.168.86.0/24 test meraki (^)()(\$) Yes 120 92.168.88.13 thret1234 ietf Yes 0 92.168.88.13 thret1234 ietf Yes 0 92.168.88.13 thret1234 ietf Yes 0 92.168.88.14 test msoft Yes 120 92.168.88.4 test meraki (^)()(\$) Yes 120 92.168.88.43 test meraki (^)()(\$) Yes 120 92.168.88.66 test meraki (^)()(\$) Yes 120		60	es	Y	otik	mikrot	test	.168.13.1	92.
92.168.137.254 ttnet1234 ietf Yes 0 92.168.88.0/24 test meraki (^)()(\$) Yes 120 92.168.88.13 ttnet1234 ietf Yes 0 92.168.88.33 test msoft Yes 120 92.168.88.44 test meraki (^)()(\$) Yes 120 92.168.88.43 test ietf Yes 120 92.168.88.6 test meraki (^)()(\$) Yes 120		60	es	Y	otik	mikrot	test	.168.13.3	92.
92.168.88.0/24 test meraki (^)()(\$) Yes 120 92.168.88.13 ttnet1234 ietf Yes 0 92.168.88.13 ttnet1234 ietf Yes 0 92.168.88.13 test msoft Yes 120 92.168.88.33 test meraki (^)()(\$) Yes 120 92.168.88.4 test meraki (^)()(\$) Yes 120 92.168.88.43 test ietf Yes 600 92.168.88.6 test meraki (^)()(\$) Yes 120		0	es	Ye		4 ietf	4 ttnet123	.168.137.2	92.
92.168.88.13 ttnet1234 ietf Yes 0 92.168.88.33 test msoft Yes 120 92.168.88.4 test meraki (^)()(\$) Yes 120 92.168.88.43 test ietf Yes 600 92.168.88.6 test meraki (^)()(\$) Yes 120		120	es)(\$) Ye	ki (^)(merak	4 test	.168.88.0/2	92.
92.168.88,33 test msoft Yes 120 92.168.88,4 test meraki (^)()(\$) Yes 120 92.168.88,4 test ietf Yes 600 92.168.88,6 test meraki (^)()(\$) Yes 120 92.168.88,6 test meraki (^)()(\$) Yes 120		0	es	Ye		4 ietf	ttnet123	.168.88.13	92.
92.168.88.4 test meraki (^)()(\$) Yes 120 92.168.88.43 test ietf Yes 600 92.168.88.6 test meraki (^)()(\$) Yes 120 ADIUS Client Properties		120	es	Ye	t	msoft	test	.168.88.33	92.
92.168.88.43 test ietf Yes 600 92.168.88.6 test meraki (^)()(\$) Yes 120		120	es	.)(\$) Ye	ki (^)(merak	test	.168.88.4	92.
92.168.88.6 test meraki (^)()(\$) Yes 120 ADIUS Client Properties		600	es	Ye		ietf	test	.168.88.43	92.
ADIUS Client Properties		120	es	.)(\$) Ye	ki (^)(merak	test	.168.88.6	92.
							Properties	DIUS Client	
IAS Secret Username Part Vendor Enabled Interim Update Period	e Period	oled Interim Update Pe	Ena	Vendor	e Part	Username	Secret	5	IAS
92.168.1.4 v test ietf v Yes v 0 - seconds	ıds	✓ 0	 Yes 	ietf >			✓ test	.168.1.4	92.
üll Command							l	Comman	äll

Windows Auth. Proxy feature will be used in this sample configuration. You need to have mobile phone number in active directory user properties. This numbers will be used to deliver TekRADIUS generated OTPs via SMS. 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]	- 0
<u>File S</u> ervice <u>H</u> elp	
Users Groups Clients Settings Application Log Active Sessions Dictionary Editor Reporting Monitors Proxy	У
SQL Connection Database Accounting Table Service Parameters Alerting	
Service Parameters	
Listen IP Address : Any V Def. EAP Method : PEA	AP-EAP-MS-CHAP-v2 V
Authentication Port Transport : 1812 🛉 UDP&TCP 🗸 Smart Card Reader : No	reader found \vee 😈
TLS Port Server Certificate : 2083 🛊 192.168.88.3 🗸 🏠 Keep Domain Name : 🗸	
Startup Logging : Automatic (Delay \lor Developer \lor DHCP Server Enabled :	
Secure Shutdown : 🕢 Send Failure Cause : 🖓	
Failure Count : 0	1 🜩 hours
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	
	Save Setting
Configure TekRADIUS TekRADI	(US Service is Stopped

You need to have following attributes in the Default user group or Domain Users group;

```
Success-Reply-Type = Challenge (Check) You may not use this attribute in older versions of VMware View.
OTP-Type = Alphanumeric (Check)
OTP-Length = 6
OTP-Sender = cscript "C:\Program Files (x86)\TekRADIUS\SendSMS.vbs" %ietf|1% %otp%
```



OTP-Sender will invoke following VB script to fetch mobile number for authenticated Active Directory user and deliver OTP via SMS. SMS will be sent using command line utility SMPPCli. SMPPCli can send GSM SMS using SMPP protocol. You can use other utilities or services to deliver OTPs.

```
Option Explicit
Dim ret, WshShell
Dim adoCommand, adoConnection
Dim varBaseDN, varFilter
Dim objRootDSE, strQuery, adoRecordset, strmobile
Dim varSearchName
Set adoCommand = CreateObject("ADODB.Command")
Set adoConnection = CreateObject("ADODB.Connection")
adoConnection.Provider = "ADsDSOObject"
adoConnection.Open "Active Directory Provider"
Set adoCommand.ActiveConnection = adoConnection
Set objRootDSE = GetObject("LDAP://RootDSE")
varBaseDN = "<LDAP://" & objRootDSE.Get("defaultNamingContext") & ">"
varSearchName = WScript.Arguments.Item(0)
varFilter = "(&(objectCategory=person)(objectClass=user)(samaccountname="& varSearchName &"))"
strQuery = varBaseDN & ";" & varFilter & ";mobile;subtree"
adoCommand.CommandText = strQuery
adoCommand.Properties("Page Size") = 1000
adoCommand.Properties("Timeout") = 20
adoCommand.Properties("Cache Results") = False
Set adoRecordset = adoCommand.Execute
Do Until adoRecordset.EOF
    strmobile = adoRecordset.Fields("mobile").Value
    adoRecordset.MoveNext
qool
adoRecordset.Close
adoConnection.Close
```

```
If strmobile = "" then
WScript.Quit 99
else
Set WshShell = CreateObject("Wscript.Shell")
ret = WshShell.Run("""C:\Program Files (x86)\TekRADIUS\SMPPCli.exe"" " & strmobile & " -m """
& WScript.Arguments.Item(1) & """", 0, True)
WScript.Quit ret
End if
```

This script, SendSMS.vbs and SMPPCli.exe should be placed in TekRADIUS application directory (*C*:*Program Files* (*x86*)*TekRADIUS by default*).

Test this setup from any View Client. Clients with RADIUS support will show the appropriate token label in text prompts. Older View clients will still work but will refer to RSA SecurID in text prompts. If possible, use a Windows View Client 5.1. At the View Client login prompt, the label in the text prompt will show the label configured in View for this authenticator.

R VMware View	w Client 🚺 🗌 🔀						
vm ware: ლec⊚⊪.							
™⊡ VMware View [™]							
📸 https://10.20.223.218							
Enter your MyToken user name and passcode.							
<u>U</u> ser name:	jdoe						
Desserved							
Passcode:							
Support Information							
OK Cancel <u>H</u> elp							

After authenticating to RADIUS, you will get another prompt if the RADIUS server responded with a supported Access Challenge. You will then enter OTP received via SMS message to complete authentication.

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