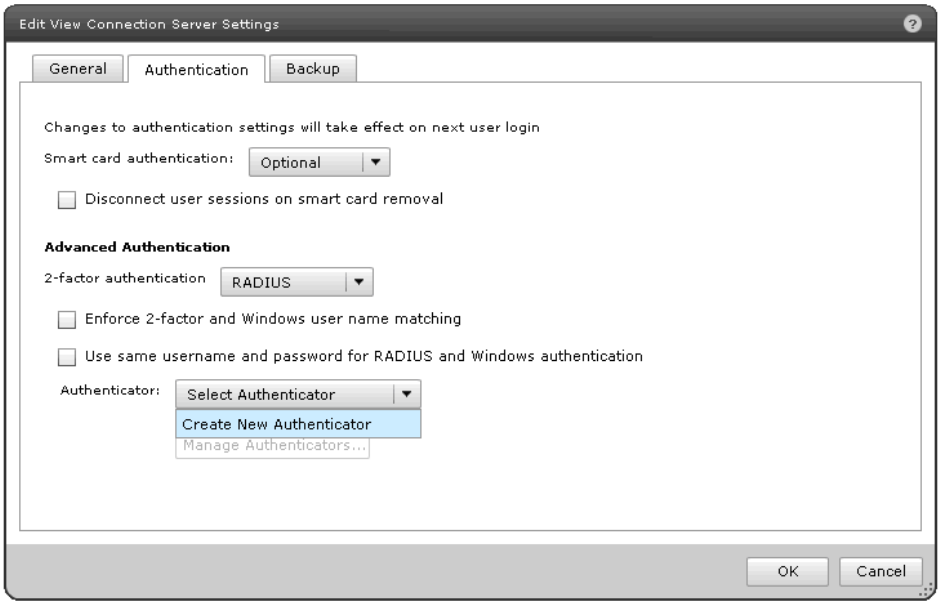
VMware View Two-Factor RADIUS Authentication Setup

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.



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**.

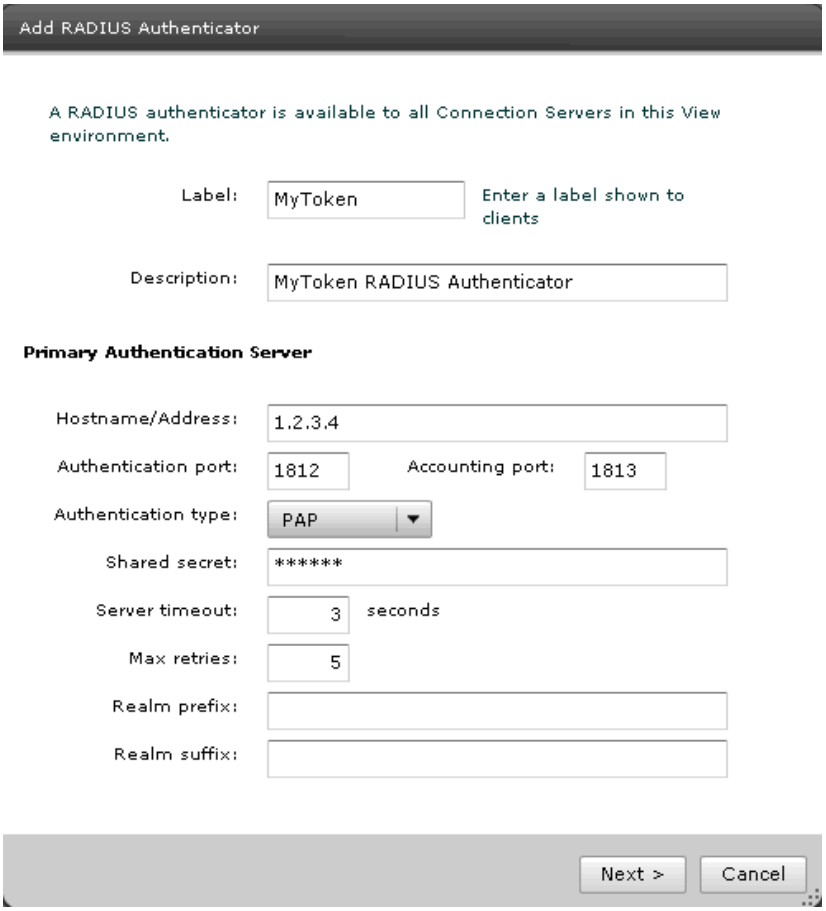
In the admin configuration of RADIUS authentication under **Advanced Authentication**, if **Enforce 2-factor and Windows user name matching** is selected then the Windows login prompt after RADIUS authentication will force the username to be the same as the RADIUS username and the user will not be able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

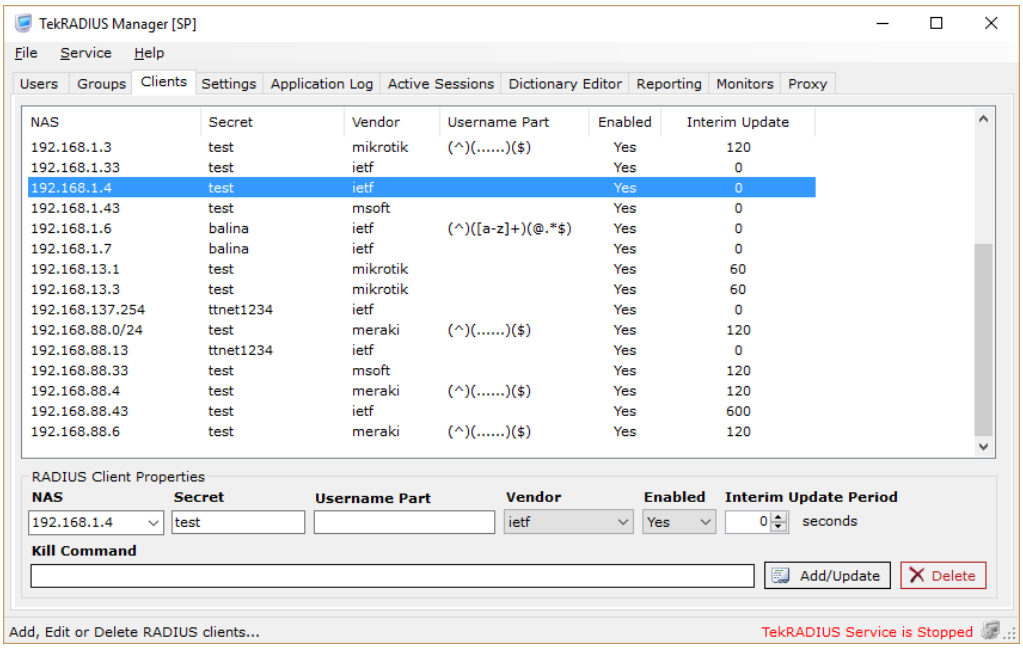
If there is a secondary RADIUS server then complete the settings for the secondary server and select Finish.



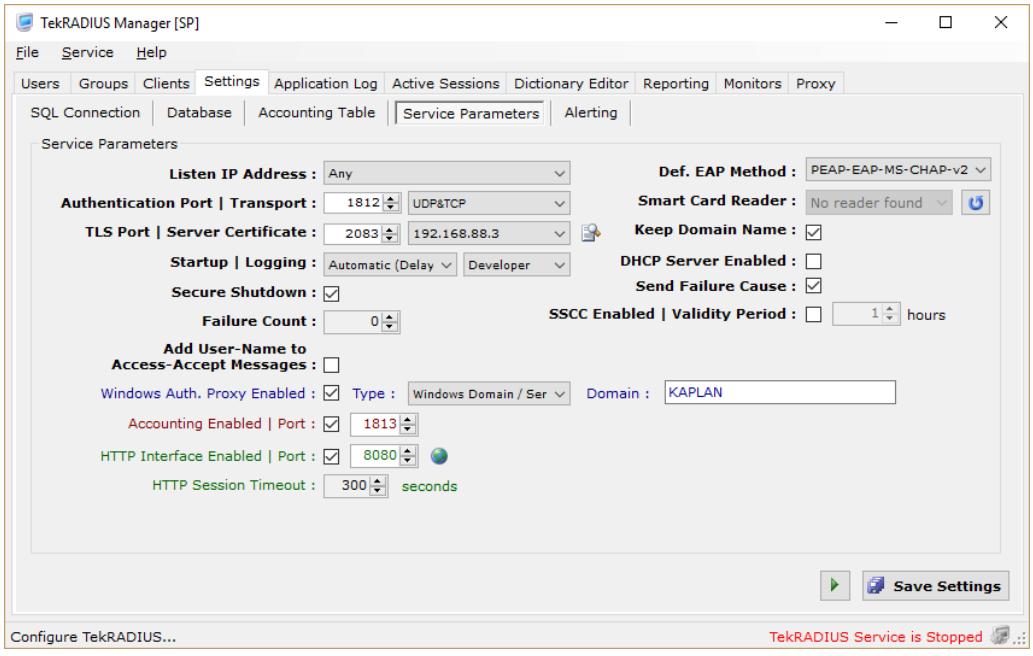
TekRADIUS Configuration

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.



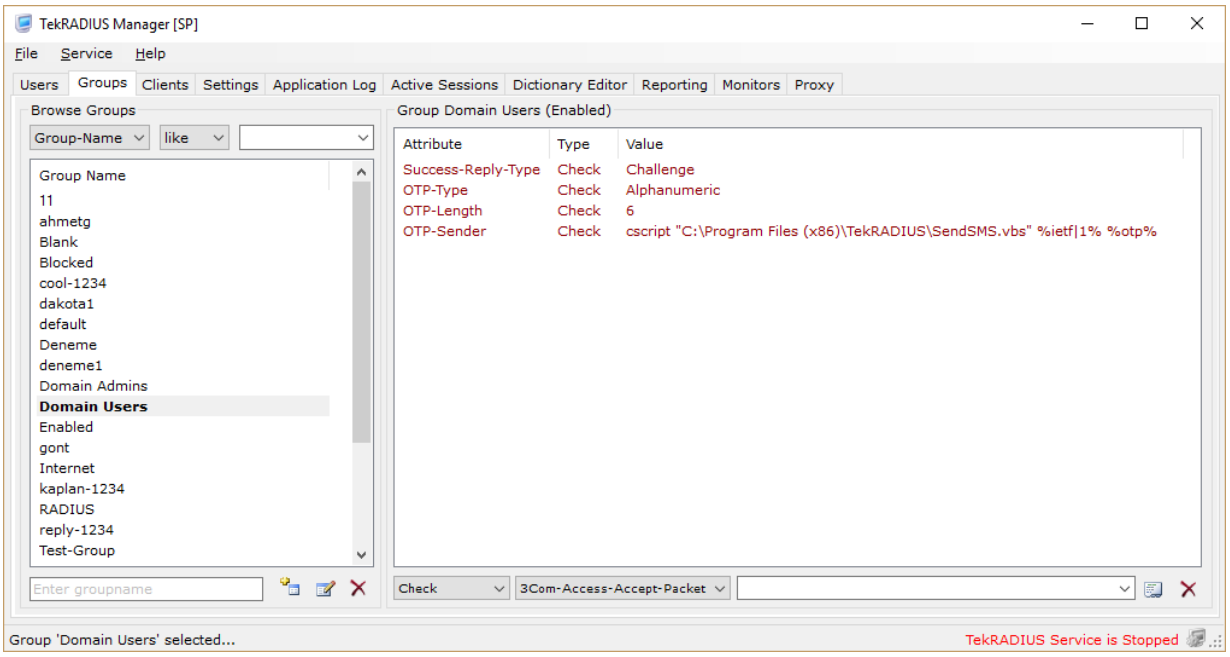
Windows Auth. Proxy feature will be used in this sample configuration. You need to have mobile phone number in active directory user properties. This numbers will be used to deliver TekRADIUS generated OTPs via SMS. You can enable Windows Auth. Directory Proxy at Settings / Service Parameters. TekRADIUS must be installed on domain member server for proper operation.



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%
```



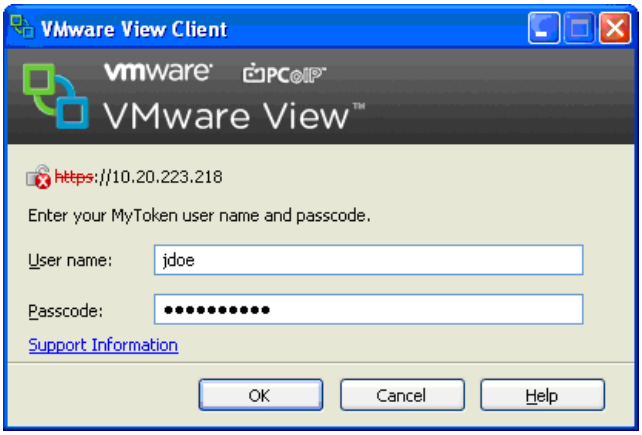
OTP-Sender will invoke following VB script to fetch mobile number for authenticated Active Directory user and deliver OTP via SMS. SMS will be sent using command line utility SMPPCli. SMPPCli can send GSM SMS using SMPP protocol. You can use other utilities or services to deliver OTPs.

```
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
Loop

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.



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.