

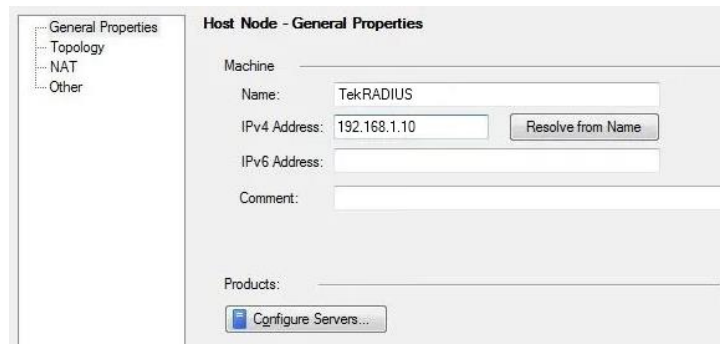
Check Point Security Gateway 2FA RADIUS Authentication Setup

You can deploy TekRADIUS with Check Point Security Gateway for Multi-Factor RADIUS Authentication for VPN sessions.

Check Point Configuration

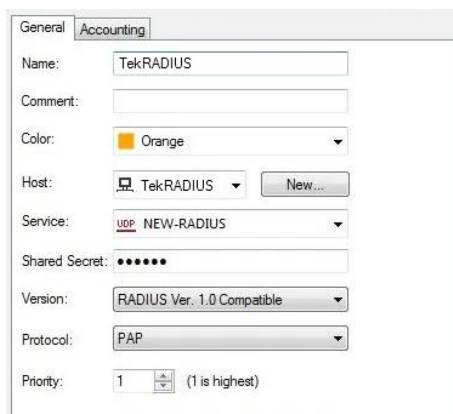
To configure your Checkpoint, log in to the SmartDashboard. Click on the main management button and select Manage > Network Objects > New > Node > Host.

Enter the name and IP address of TekRADIUS server on the General Properties page. Click OK to save the new host, and then click the Close button in the Network Objects window.

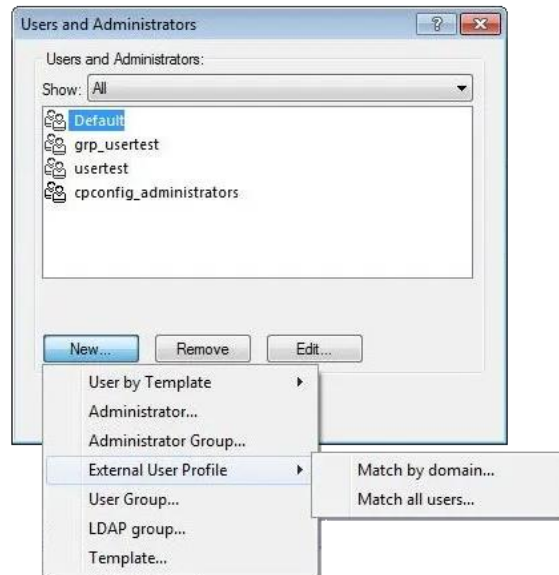


Go back to the main management button and select Manage > Servers and OPSEC Applications > New > RADIUS.

On the General tab, give the server a name such as TekRADIUS. Select the host you created earlier. Be sure to select New-RADIUS as the protocol. This option uses the "new" port of 1812. Click OK and Close.



Create an External User profile. On the main menu, select Manage > Users and Administrators > New > External User Profile > Match all users.

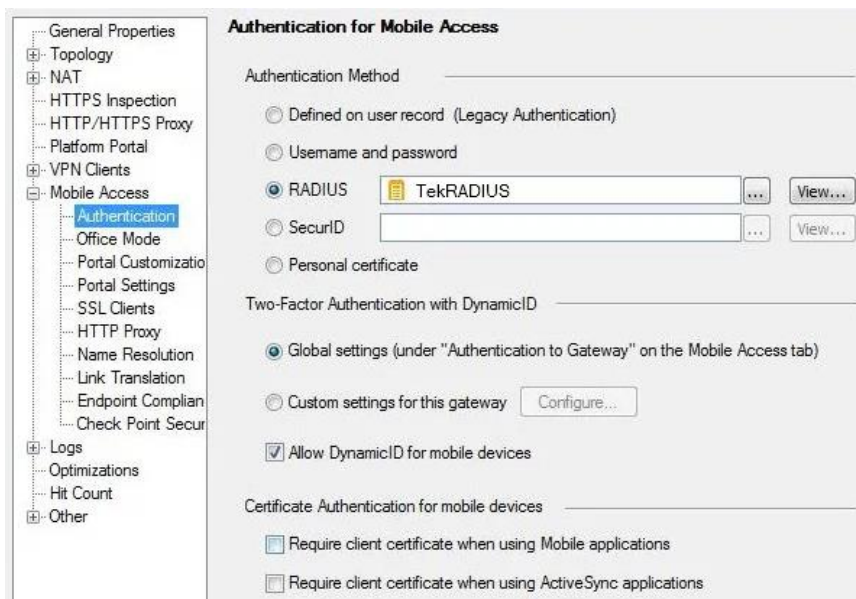


Click on the Authentication page and choose RADIUS as the Authentication Scheme and Select the TekRADIUS host you created earlier.

Next, click on the Mobile Access tab and the Policy page. Right click on the Policy and select Edit. Move the generic* from **Available Members** to **Selected Members**.

Configure the Mobile Access VPN

Configure the Checkpoint SSL-VPN, bring up the Authentication page under Mobile Access. Select the RADIUS and the TekRADIUS server setup previously. Click OK. And then the Install Policy button.



Configuring the IPSec VPN for RADIUS

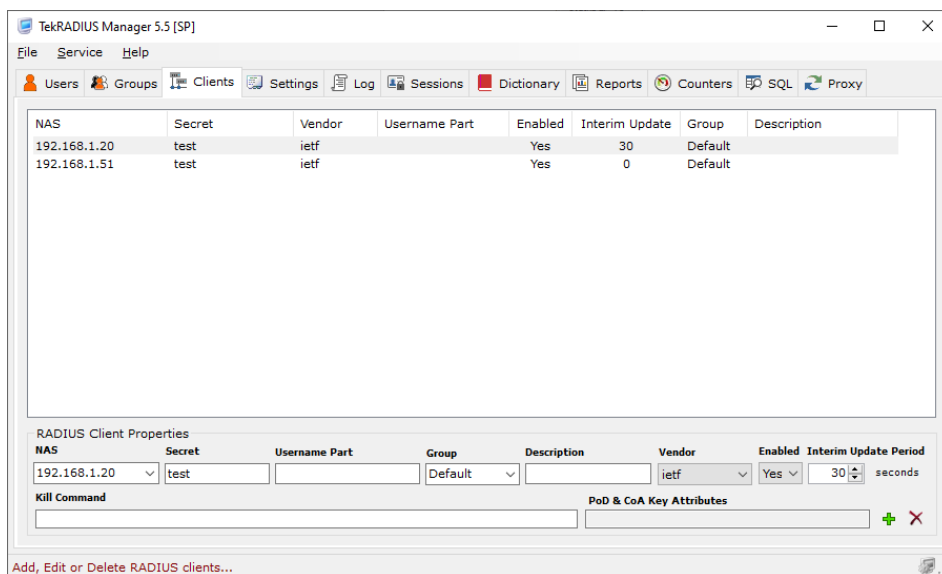
Configure the Checkpoint IPSec -VPN. Click on the IPSec VPN tab and click on Gateways in the left window.

Right click on your Gateway and select Edit. Click on VPN Clients and then Authentication. Click on RADIUS and select the TekRADIUS server you added as RADIUS server above. Click OK. And then the Install Policy button.

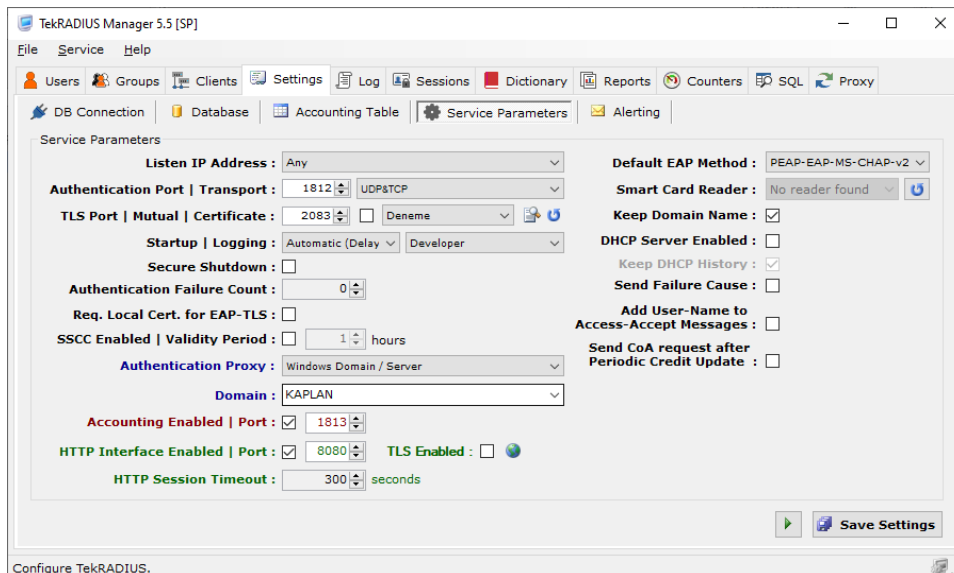
TekRADIUS Configuration

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 Check Point Security Gateway in TekRADIUS Manager / Clients tab. Enter IP address of the Check Point Security Gateway and the shared secret key specified earlier in Check Point Security Gateway configuration.



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.



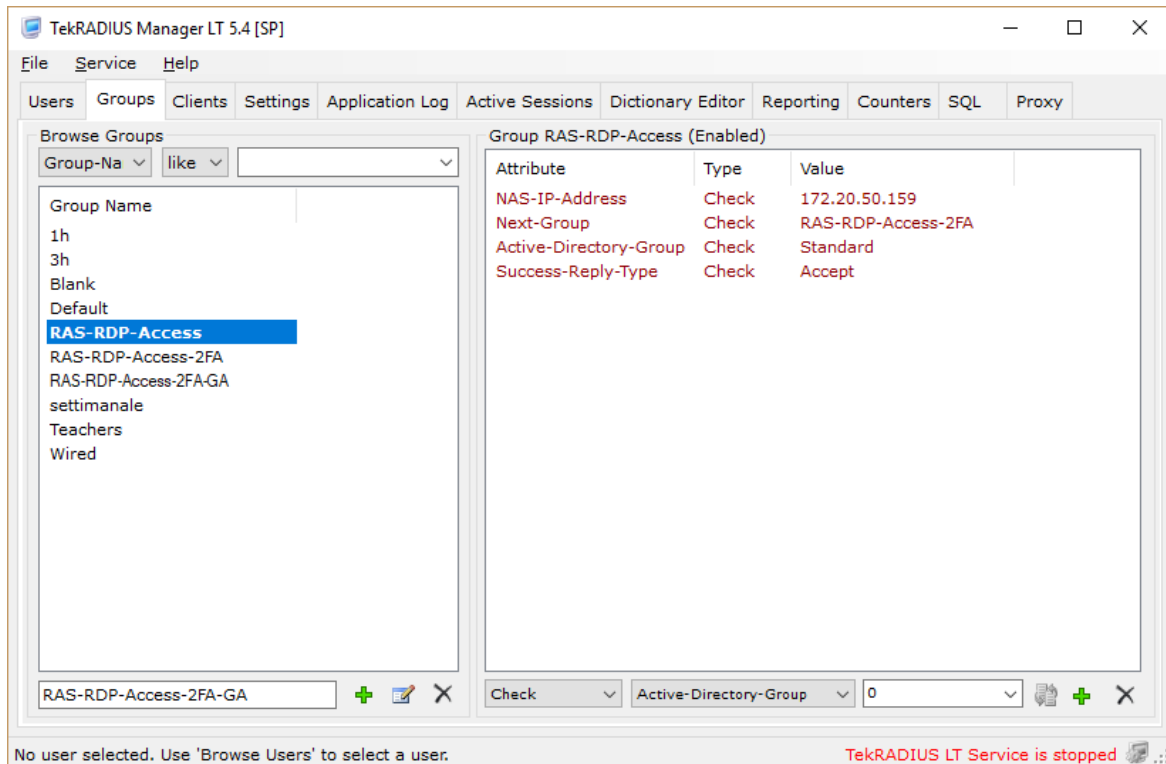
Some of users do not want to have extra authentication; only username/password. In TekRADIUS we have two group profiles matching active directory groups with or without OTP. You need two extra AD groups in your AD; Standard for plain Active Directory authentication, Access-2FA for Google-Authenticator 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)

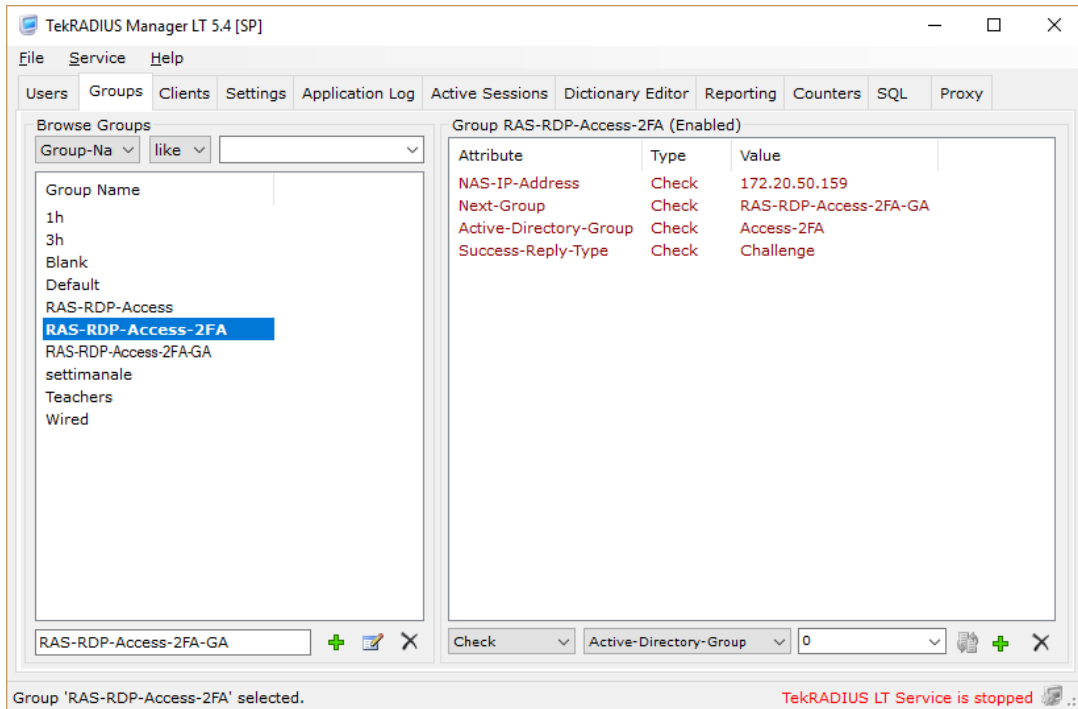
TekRADIUS Group "RAS-RDP-Access" (This one authenticates plain AD users, falls back to RAS-RDP-Access-2FA if authentication fails)

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



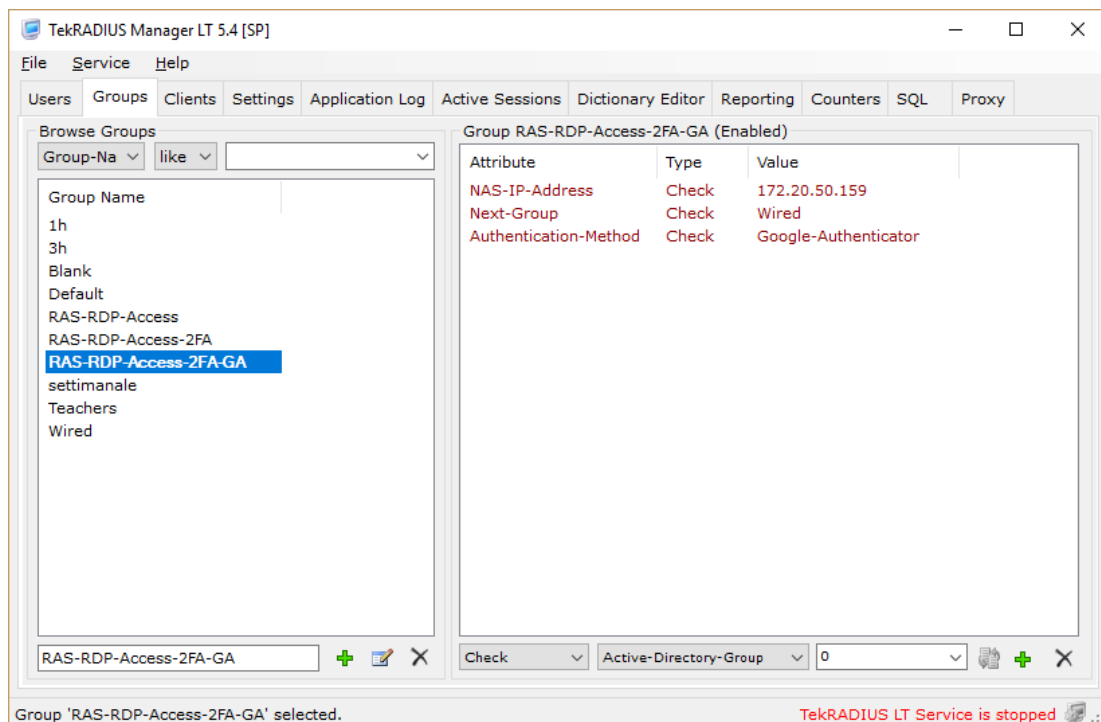
TekRADIUS Group "RAS-RDP-Access-2FA" (Sends challenge for Google-Authenticator phase if AD authentication is successful)

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



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

- Authentication-Method = Google-Authenticator (Check)



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


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

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.

TekRADIUS User Reports

User Information

Username: [gakaplan](#) 


Credit remaining: 0 second(s)

Expires on: N/A

User status: Offline

HW Address: N/A

Connected since: N/A



Reporting




Grouping | Order:

Start date | Time:

End date | Time:

Filter by:

Compact:

 CSV  Report  Logout