

Using RADIUS Authentication for Remote Access VPN

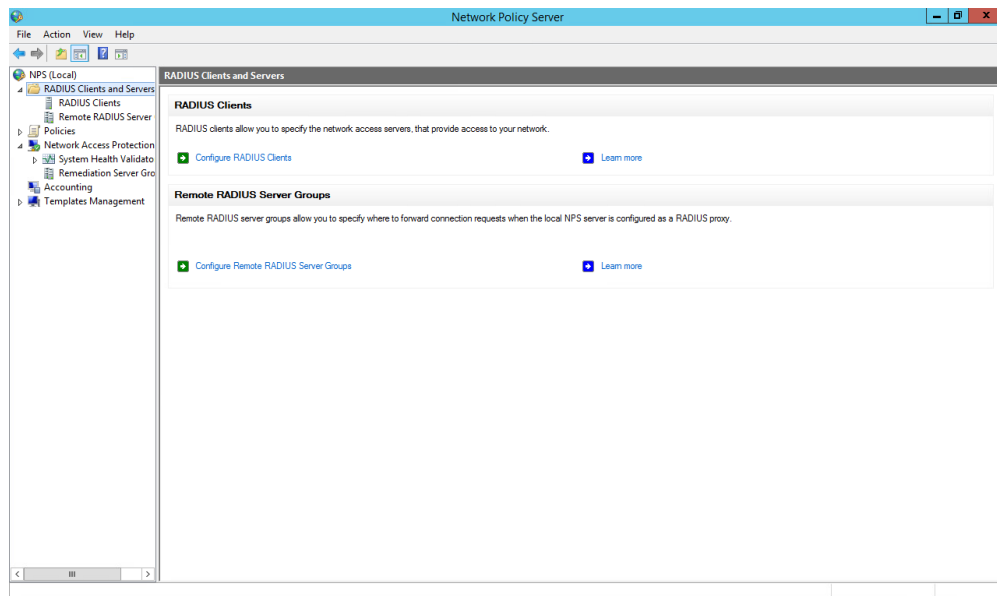
This guide will show step by step instructions for configuring Remote Access VPN to utilize RADIUS authentication. There is also an appendix that includes instructions for integrating DUO MFA with a Check Point Remote Access Gateway.

We will use the following:

- R80.10 Security Management Server
- R80.10 Gateway running NGTX
- Windows Server 2012 for the RADIUS Server
- Windows Server 2012 for the DUO Proxy Server

Step 1: Configure your RADIUS connection on the Windows Server Side.

1. Open the Network Policy Server snap in. This should have been installed/enabled when you added the server as Network Policy Server.



2. Create a RADIUS client by right clicking RADIUS clients and selecting “New”. You will receive the following window shown below.

The screenshot shows the 'New RADIUS Client' dialog box with the 'Advanced' tab selected. The 'Enable this RADIUS client' checkbox is checked. Below it is a dropdown menu for 'Select an existing template:'. The 'Name and Address' section contains a 'Friendly name:' field and an 'Address (IP or DNS):' field with a 'Verify...' button. The 'Shared Secret' section has a dropdown for 'Select an existing Shared Secrets template:' set to 'None'. Below this is a note: 'To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.' There are two radio buttons: 'Manual' (selected) and 'Generate'. Below them are two text input fields for 'Shared secret:' and 'Confirm shared secret:'. At the bottom are 'OK' and 'Cancel' buttons.

3. Fill out the relevant information and take note of the “Shared Secret” you create as you will need it later.

The screenshot shows the 'New RADIUS Client' dialog box with the 'Advanced' tab selected. The 'Enable this RADIUS client' checkbox is checked. Below it is a dropdown menu for 'Select an existing template:'. The 'Name and Address' section contains a 'Friendly name:' field with the text 'Check Point Remote Access VPN' and an 'Address (IP or DNS):' field with the text '10.' followed by a redacted area and a 'Verify...' button. The 'Shared Secret' section has a dropdown for 'Select an existing Shared Secrets template:' set to 'None'. Below this is a note: 'To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.' There are two radio buttons: 'Manual' (selected) and 'Generate'. Below them are two text input fields for 'Shared secret:' and 'Confirm shared secret:', both containing redacted text. At the bottom are 'OK' and 'Cancel' buttons.

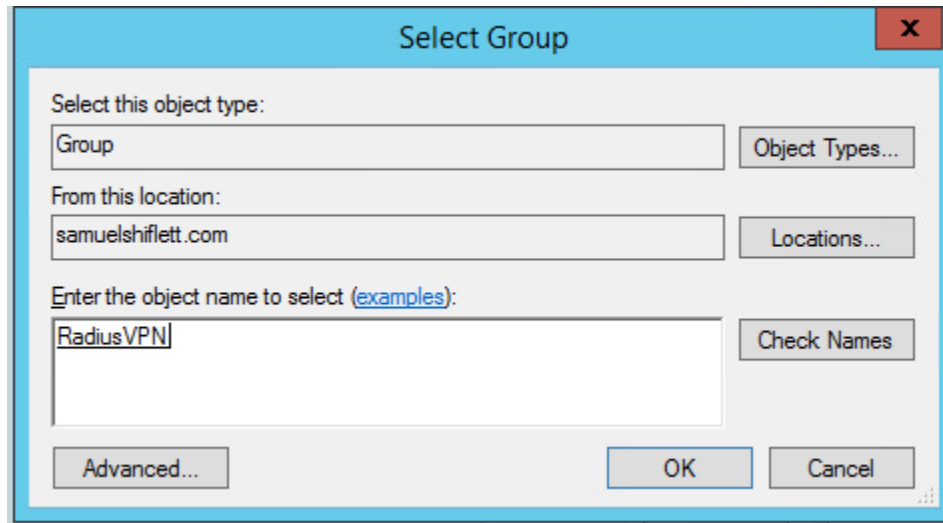
- Click "OK" and proceed to the Network Policy Server window. Right click on "Network Policies" and select "New".

The screenshot shows the 'New Network Policy' dialog box with the title 'Specify Network Policy Name and Connection Type'. The main heading is 'Specify Network Policy Name and Connection Type'. Below the heading is a sub-heading 'Policy name:' followed by a text input field. Underneath is the 'Network connection method' section, which includes a description: 'Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.' There are two radio buttons: 'Type of network access server:' (selected) and 'Vendor specific:'. The 'Type of network access server:' radio button is selected, and its dropdown menu is open, showing 'Unspecified'. The 'Vendor specific:' radio button is unselected, and its dropdown menu shows the number '10'. At the bottom of the dialog box are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

- Enter a name for your policy and leave the network access server field "Unspecified". Then click "Next" on the Specify Conditions page select "Add".

The screenshot shows the 'New Network Policy' dialog box with the title 'Specify Conditions'. The main heading is 'Specify Conditions'. Below the heading is a sub-heading 'Select condition' and a description: 'Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.' There is a list of conditions under the heading 'Select a condition, and then click Add.' The list includes: 'Groups' (with a sub-heading 'Groups'), 'Windows Groups' (with a description: 'The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.'), 'Machine Groups' (with a description: 'The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.'), 'User Groups' (with a description: 'The User Groups condition specifies that the connecting user must belong to one of the selected groups.'), and 'HCAP' (with a sub-heading 'HCAP' and a description: 'The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.'). At the bottom of the dialog box are four buttons: 'Add...', 'Cancel', 'Add...', 'Edit...', 'Remove', and 'Previous', 'Next', 'Finish', 'Cancel'.

6. Select “Windows Groups” and then select “Add Groups”. Enter your group name and click “Check Names”:



Select Group

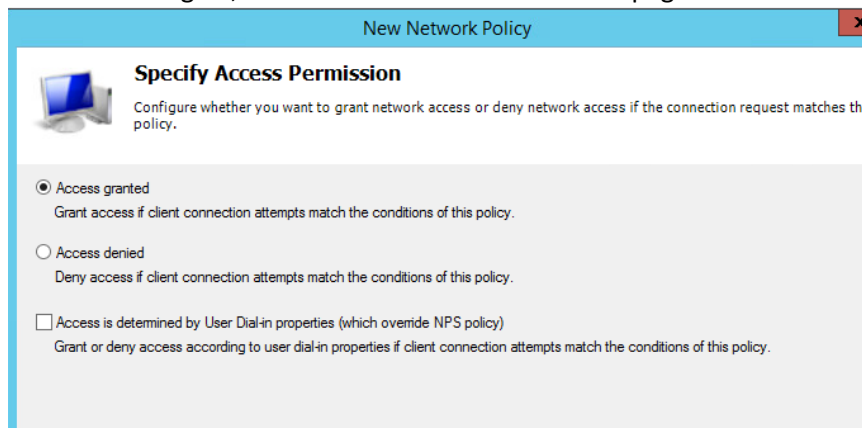
Select this object type:
Group Object Types...

From this location:
samuelshiflett.com Locations...

Enter the object name to select (examples):
RadiusVPN Check Names

Advanced... OK Cancel

7. Click “OK” and then “OK” again, then select “Next”. On the next page select “Access granted”.



New Network Policy

Specify Access Permission

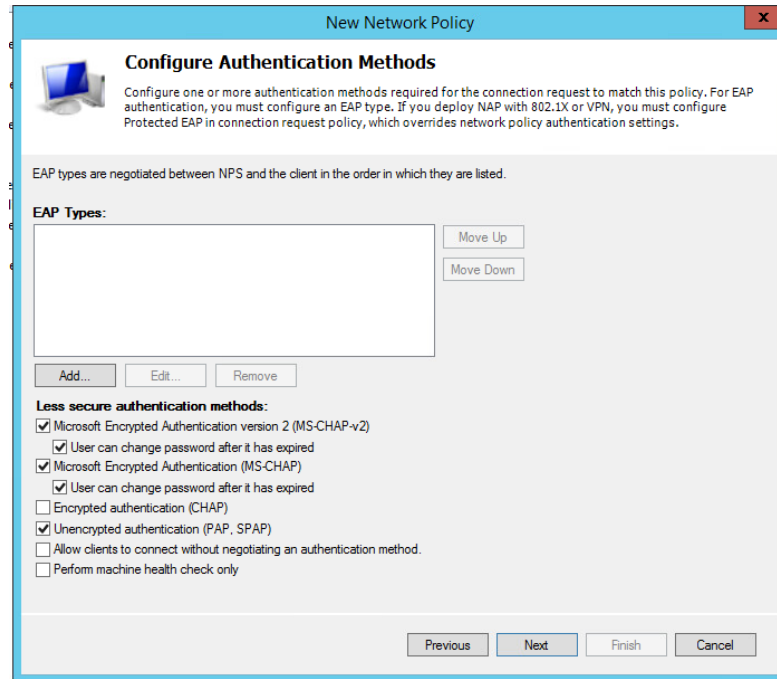
Configure whether you want to grant network access or deny network access if the connection request matches this policy.

Access granted
Grant access if client connection attempts match the conditions of this policy.

Access denied
Deny access if client connection attempts match the conditions of this policy.

Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

8. Click "Next". For authentication methods ensure that at least MS-CHAP-v2 or PAP are checked.

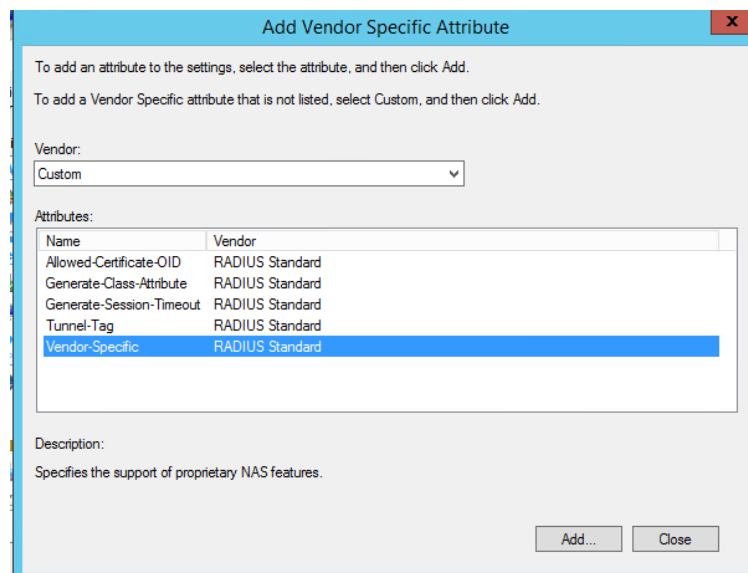


9. Click "Next". Select any additional constraints you'd like to add such as time of day restrictions.

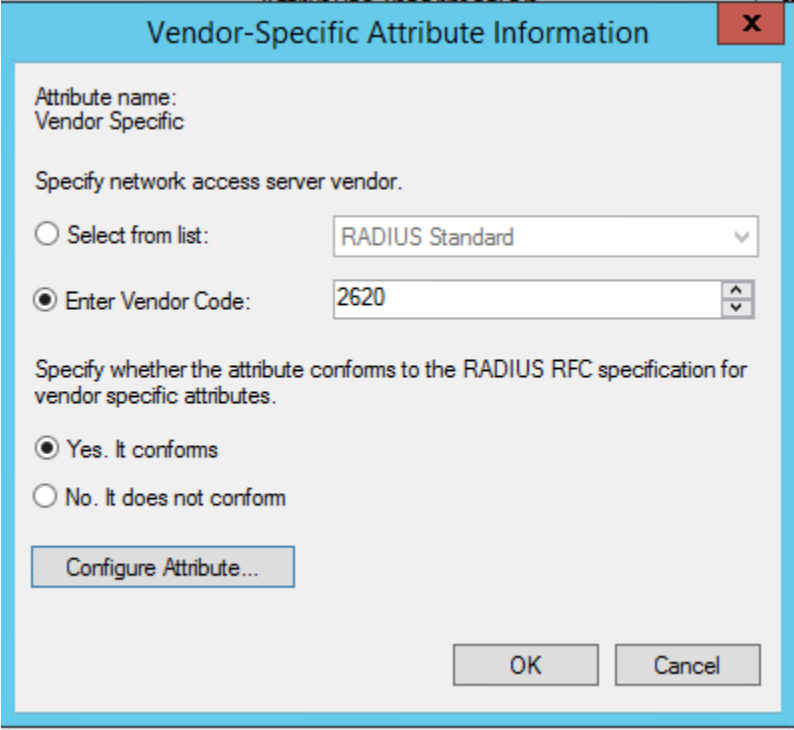
10. Select "Vendor Specific" and click "Add".

11. Click "Add" on the next window.

12. Change the Vendor to Custom and select "Vendor-Specific". Click "Add" again.



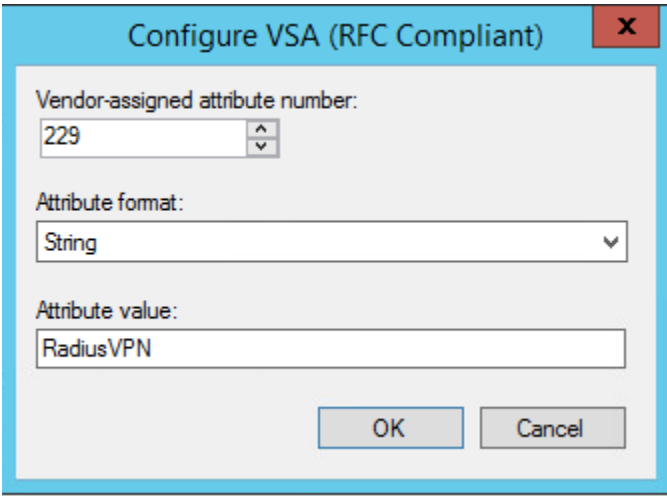
13. Click “Add” again. Change the radio button to Enter Vendor Code and enter “2620”. Select “Yes. It Conforms.” Then click “Configure” attribute.



The screenshot shows a dialog box titled "Vendor-Specific Attribute Information" with a red close button in the top right corner. The dialog contains the following fields and options:

- Attribute name: Vendor Specific
- Specify network access server vendor:
 - Select from list: RADIUS Standard (dropdown menu)
 - Enter Vendor Code: 2620 (text input with up/down arrows)
- Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes:
 - Yes. It conforms
 - No. It does not conform
- Buttons: "Configure Attribute..." (disabled), "OK", and "Cancel".

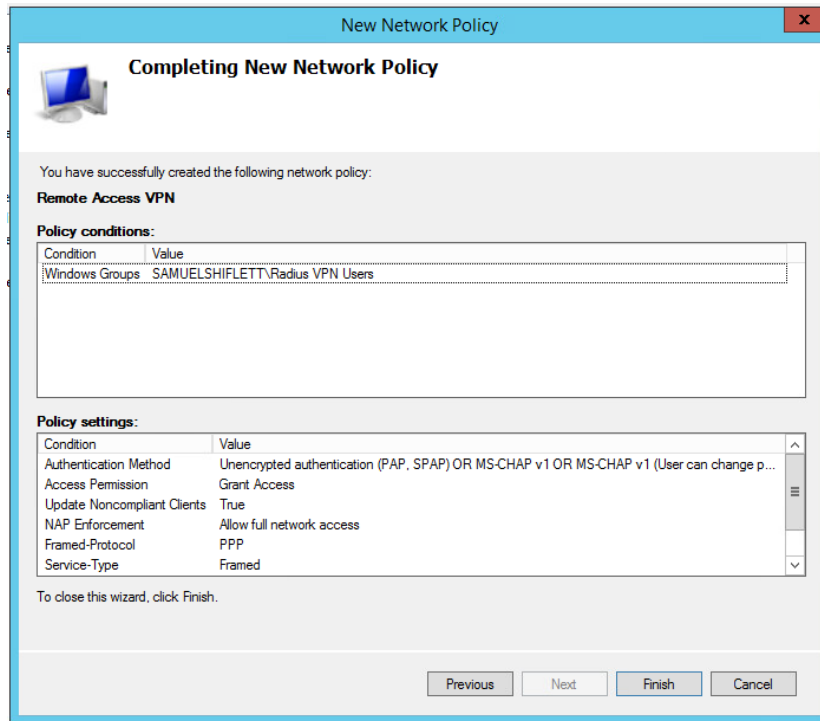
14. Enter “229” for the attributed number, select String for the attribute format and enter the name of the group you created. **This attribute name can’t contain spaces.**



The screenshot shows a dialog box titled "Configure VSA (RFC Compliant)" with a red close button in the top right corner. The dialog contains the following fields and options:

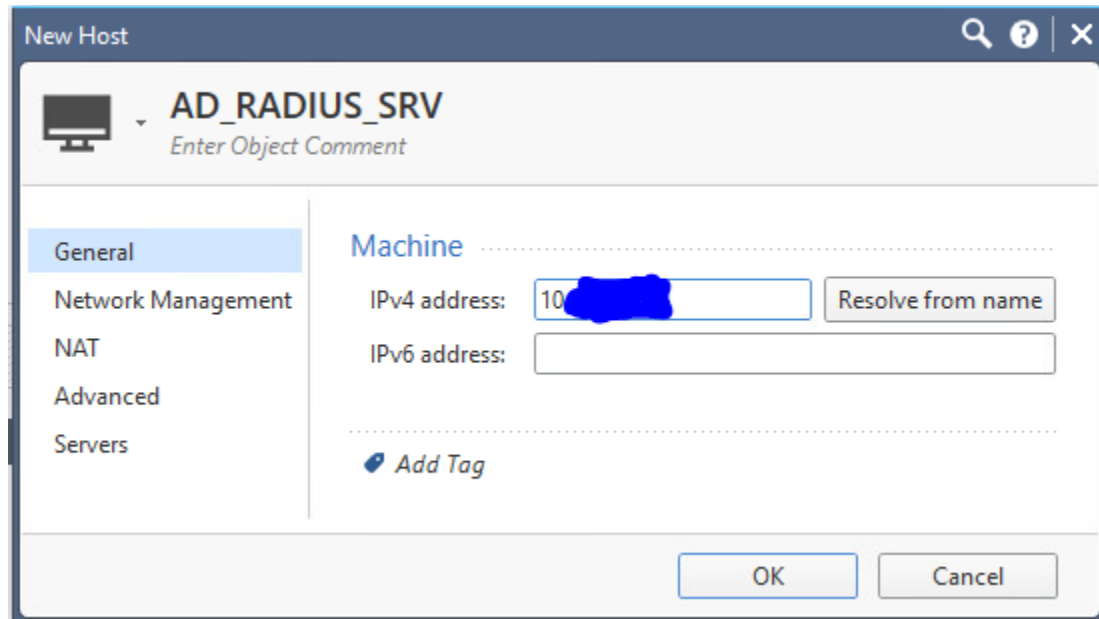
- Vendor-assigned attribute number: 229 (text input with up/down arrows)
- Attribute format: String (dropdown menu)
- Attribute value: RadiusVPN (text input)
- Buttons: "OK" and "Cancel".

15. Click “OK” three times and then select “Next”. Verify your settings and click “Finish”.



Step 2: Configure RADIUS Authentication for Remote Access VPN in SmartConsole

1. Create a host object for the RADIUS server.



2. Create a RADIUS Server object.

The screenshot shows the 'New RADIUS' configuration window. The object name is 'AD_RADIUS_AUTH'. The 'General' tab is active, showing the following settings:

- Host: AD_RADIUS_SRV
- Service: RADIUS
- Shared secret: [masked]
- Version: RADIUS Ver. 2.0
- Protocol: MS_CHAP2
- Priority: 1

There is an 'Add Tag' button and 'OK'/'Cancel' buttons at the bottom.

3. Create an empty group with the name "RAD_yourattributename." This needs to match the attribute name you specified in 1.14.

The screenshot shows the 'User Group' configuration window. The object name is 'RAD_RadiusVPN'. The 'Mailing List Address' field is empty. Below it is a search bar with a magnifying glass icon and the text 'Search...'. A table with columns 'Name' and 'Comments' is shown, containing the text 'No items found'. There is an 'Add Tag' button and 'OK'/'Cancel' buttons at the bottom.

4. Publish your changes and close SmartConsole. **It is recommended to take backup of your SMS prior to making the following changes.**
5. Open GuiDBEdit.

- Change `add_radius_groups` value under Global Properties > Properties > `firewall_properties` to true.

The screenshot shows the Check Point Database Tool interface. The left sidebar displays a tree view of database objects, with 'Global Properties > Properties > firewall_properties' selected. The main window shows a table with columns: Object Name, Class Name, and Last Modify Time. The 'firewall_properties' object is highlighted. An 'Edit' dialog box is open over the table, showing the 'Value' field set to 'true'. The table below the dialog lists various fields and their values.

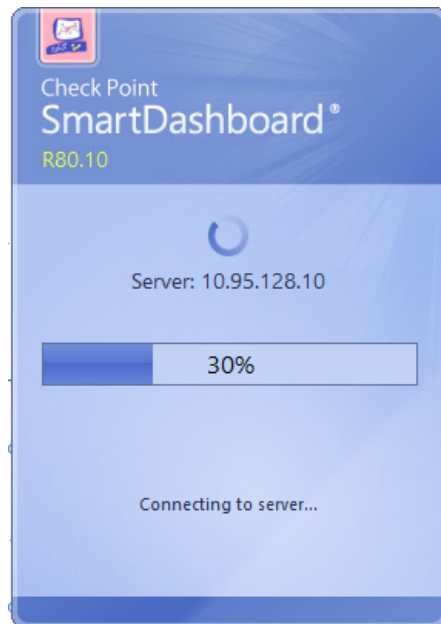
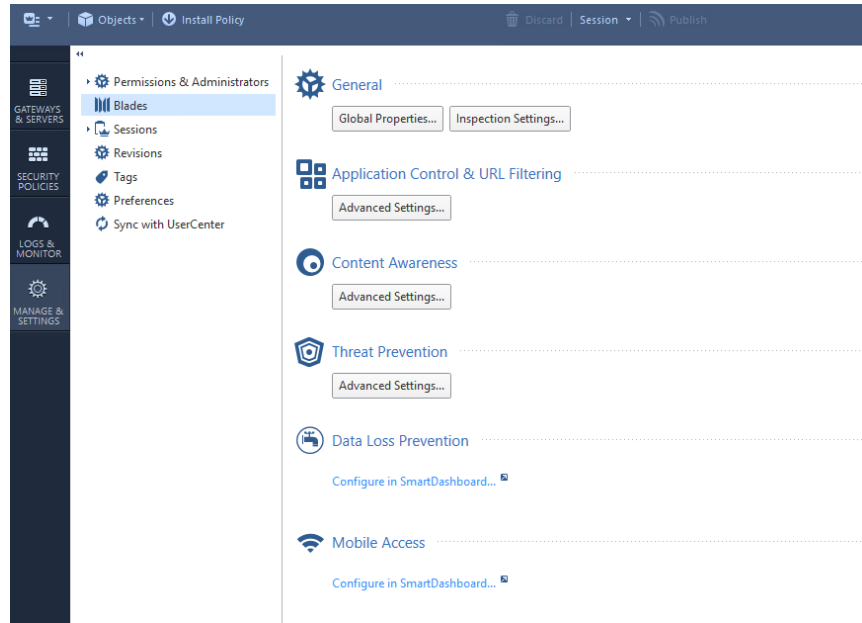
| Field Name | Type | Value | Default Value | Field description |
|----------------------------------|--------------|------------------------------|-------------------------------------|--|
| Software_loader | string | Software_loader | Software_loader | Software_loader |
| VPN_configuration_mode | string | communities | communities | VPN Configuration Mode |
| accept_domain_tcp | boolean | false | | accept_domain_tcp |
| accept_domain_udp | boolean | false | | accept_domain_udp |
| accept_fw1_connections | boolean | false | | accept_fw1_connections |
| accept_icmp | boolean | false | | accept_icmp |
| accept_outgoing | boolean | false | | accept_outgoing |
| accept_outgoing_to_cp_services | boolean | true | | accept_outgoing_to_cp_services |
| accept_outgoing_to_cp_services_p | string | before last | (first,last,before last) | accept_outgoing_to_cp_services_p |
| accept_ip | boolean | false | | accept_ip |
| acceptdecrypt | boolean | true | true | Enable Accept on Decrypt for Gateway to G... |
| actions_limit_on | boolean | false | | If true, the actions limit will be applied |
| active_resolver | boolean | true | true | active_resolver |
| add_ip_alt_name_for_ICA_certs | boolean | true | true | add_ip_alt_name_for_ICA_certs |
| add_ip_alt_name_for_opsec_certs | boolean | false | | add_ip_alt_name_for_opsec_certs |
| add_nt_groups | boolean | false | | add_nt_groups |
| add_radius_groups | boolean | false | | add_radius_groups |
| addresstrans | boolean | false | | addresstrans |
| admin_expiration_global_data | owned object | admin_expiration_global_data | {admin_expiration_global_data,NULL} | admin_expiration_global_data |

- Change the `radius_groups_attr` from 25 to 26. Save your changes and exit GUIDBedit.

The screenshot shows the Check Point Database Tool interface. The left sidebar displays a tree view of database objects, with 'Global Properties > Properties > firewall_properties' selected. The main window shows a table with columns: Object Name, Class Name, and Last Modify Time. The 'firewall_properties' object is highlighted. An 'Edit' dialog box is open over the table, showing the 'Value' field set to '26'. The table below the dialog lists various fields and their values.

| Field Name | Type | Value | Default Value |
|------------------------|-----------|-------|---------------|
| r_access_enable_p | string | first | first |
| r_accessible | boolean | true | true |
| radius_connect_timeout | unumber | 120 | 120 |
| radius_groups_attr | number | 25 | 0-255 |
| radius_ignore | container | | 0-255 |
| radius_retrant_num | unumber | 2 | 0-uint_max |
| radius_retrant_timeout | unumber | 5 | 0-uint_max |
| radius_send_framed | boolean | false | |

8. Reopen SmartConsole. Click on “Manage and Settings” followed by “Blades” and then click “Configure in SmartDashboard.” The legacy SmartDashboard client will open.



9. Click on the user icon in the Object Explorer in the bottom left. Then right click “External User Profiles” and select “New External User Profile > Match all users”.

External User Profile Properties

This External User Profile will apply to all users which are not defined in the internal Users Database or any known LDAP Account Unit and do not match any other External User Profile.

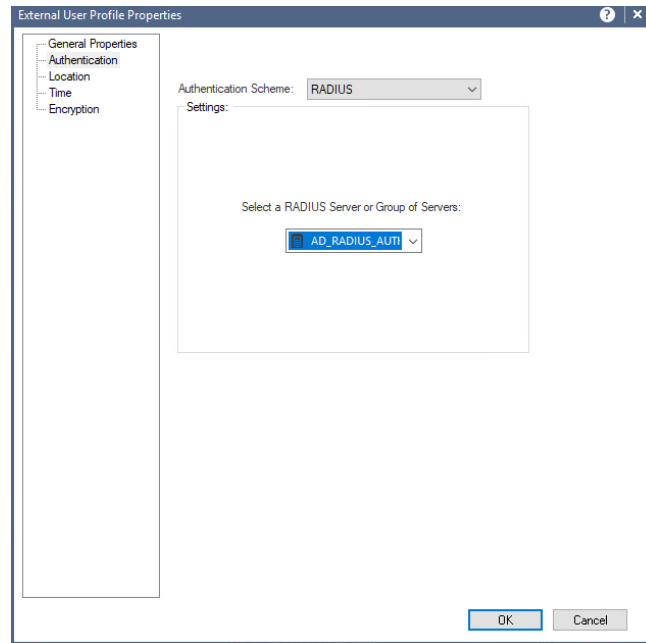
External User Profile name: ▾

Comment:

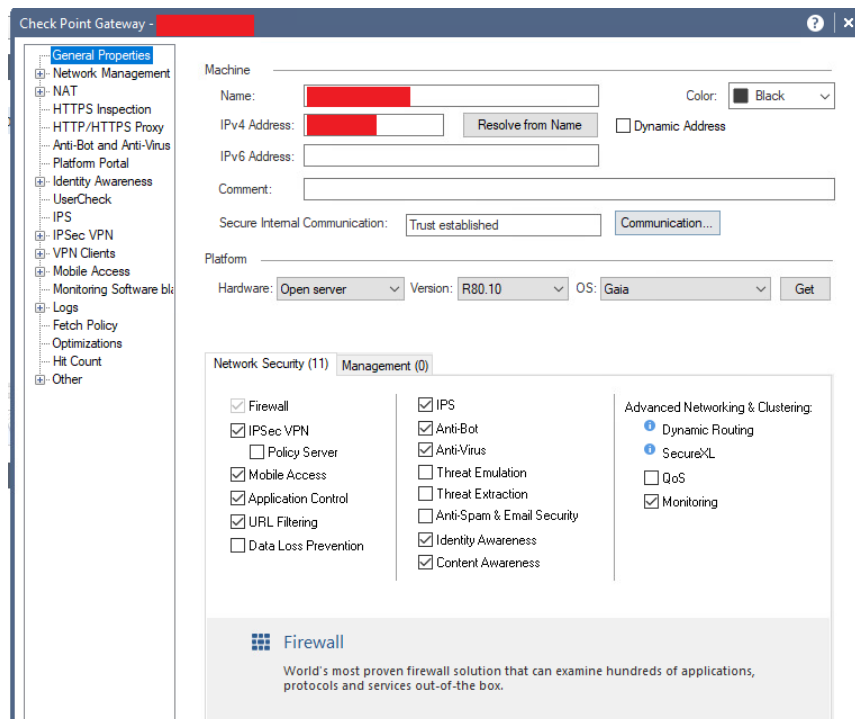
Expiration Date: _____

Expiration Date: (m/d/yyyy)

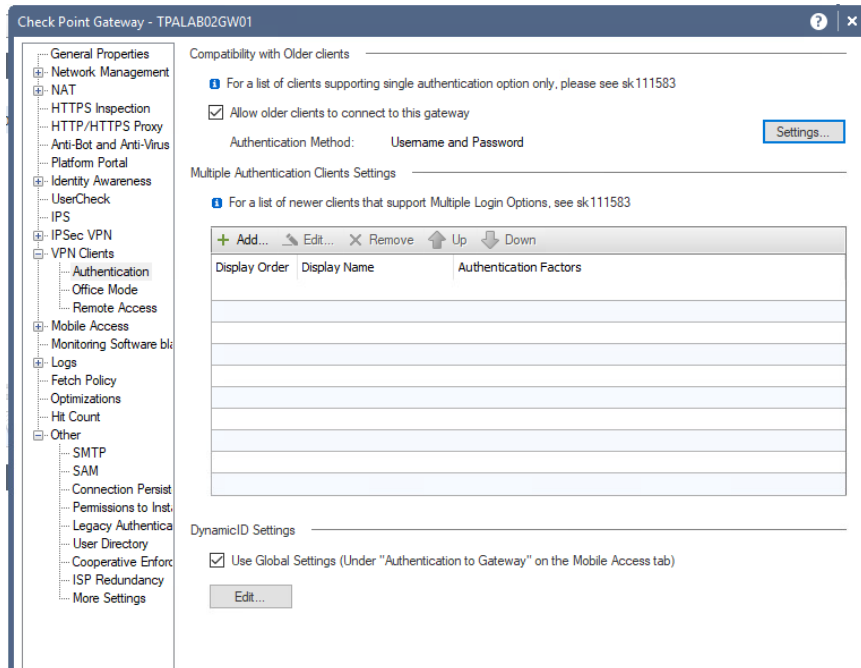
10. Select “Authentication” and change the Authentication Scheme to RADIUS. Then select the RADIUS server object you created in 2.2.



11. Click “OK” and save your changes. Then close the SmartDashboard window.
12. In SmartConsole, open the gateway object for your Remote Access VPN Gateway.

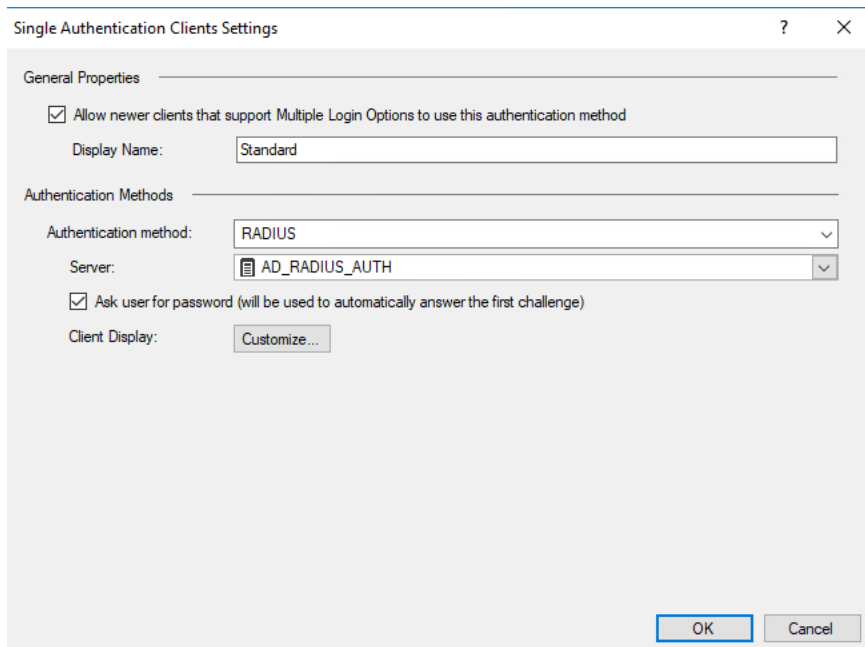


13. Select “VPN Clients” and expand the menu. Then click “Authentication”.



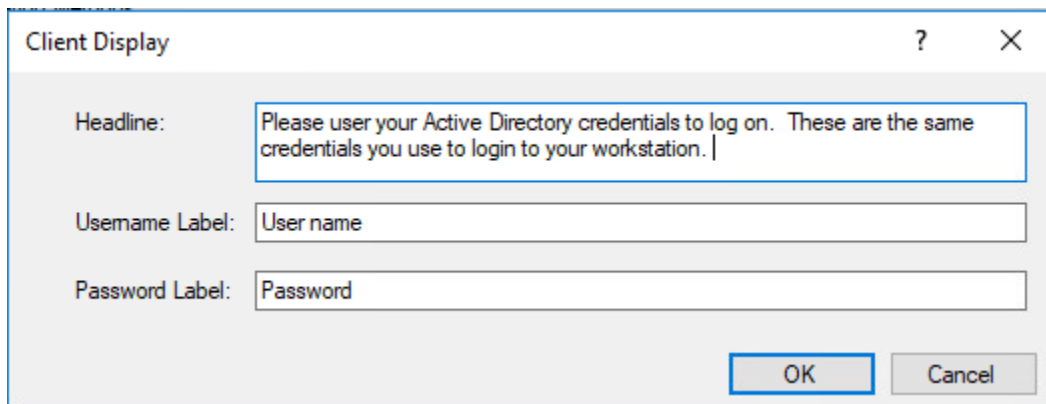
These settings will depend on what version of Endpoint Security/Endpoint connect you have installed, new versions (E80.65 and above support multiple authentication schemes). This guide will utilize the single authentication only option with RADIUS as the authentication method.

14. Check the box “Allow newer clients that support Multiple Login Options to use this authentication method” and then click “Settings”.



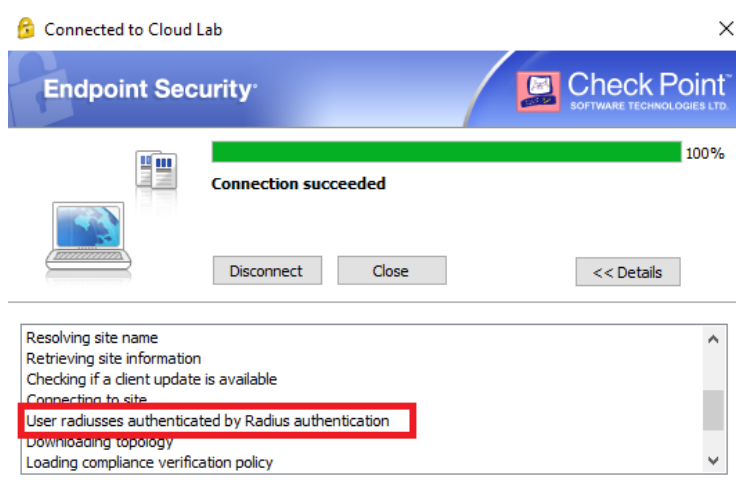
If you are using clients above E80.65 check the top box “Allow newer clients that support Multiple Login Options to use this authentication method. The display name is what your users will see.

15. Change the authentication method to RADIUS and select the server you created in 2.2 as the server.
16. Check the box that says “Ask user for password (will be used to automatically answer the first challenge”. If you leave this unchecked, your end user will be prompted for a username, then a password and they will need to complete two prompts instead of one.
17. Customize what fields your end user sees and the instructions they receive by clicking on “Customize”.



18. Click “OK” on each open window and install policy to the Remote Access gateway.

Your users should now be able to authenticate via their Active Directory Credentials and RADIUS:



Troubleshooting

If you are unable to authenticate, walk through this guide again and verify the following:

- IP Addresses
- Generic* user profile configuration
- Authentication settings on the gateway object
- Verify connectivity from the gateway to the RADIUS server.
- You may need to add rules to the gateway and other network devices to allow this communication over port 1812.
- You can also verify that the RADIUS request is being sent by the gateway using “tcpdump -n *interfacename* host *yourradiusserver*” as you attempt the connection.
- If there is latency or a delay while the gateway waits for a response from the RADIUS server, you may need to increase the timeout according to sk112933. It is recommended to contact TAC for assistance before performing this change to verify that the connection is timing out.
- Verify that the user belongs to the proper security group that you specified in 1.6.
- Check the logs for why the authentication failed. The RADIUS server may not be responding, or the user may not be authorized. The log entry should tell you what caused the failure.

Appendix: Using DUO MFA as a RADIUS Server for Remote Access VPN Authentication

This guide can easily be adapted to use a third-party RADIUS server (in this case DUO). DUO is typically deployed with a proxy server running on either Linux or Windows Server. In our case we will use a DUO proxy server running Windows Server 2012 R2. The specific steps for configuring the proxy can be found here:

<https://duo.com/docs/checkpoint?ikey=DIRUR3RRWHRDVFC84VDS&host=api-b7f86f92.duosecurity.com#overview>

The above guide provides the majority of the steps for configuring the DUO and the Check Point configuration. However, it is designed for Mobile Access. The rest of this guide will assume that the DUO proxy server has already been configured to authenticate to DUO with an AD client as the primary factor:

```

; Complete documentation about the Duo Auth Proxy can be found here:
; https://duo.com/docs/authproxy\_reference

; MAIN: Include this section to specify global configuration options.
; Reference: https://duo.com/docs/authproxy\_reference#main-section
[main]
debug=true

; CLIENTS: Include one or more of the following configuration sections.
; To configure more than one client configuration of the same type, append a
; number to the section name (e.g. [ad_client2])

[ad_client]
host=
service_account_username=
service_account_password=
search_dn=CN=Users,
security_group_dn=

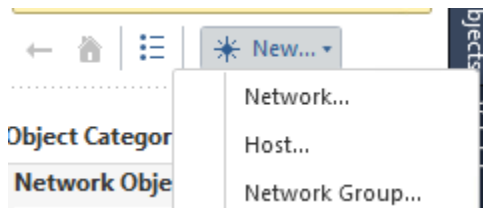
; SERVERS: Include one or more of the following configuration sections.
; To configure more than one server configuration of the same type, append a
; number to the section name (e.g. radius_server_auto1, radius_server_auto2)

[radius server auto]
ikey=
skey=
api_host=
radius_ip_1=
radius_secret_1=
failmode=secure
client=ad_client
port=1812

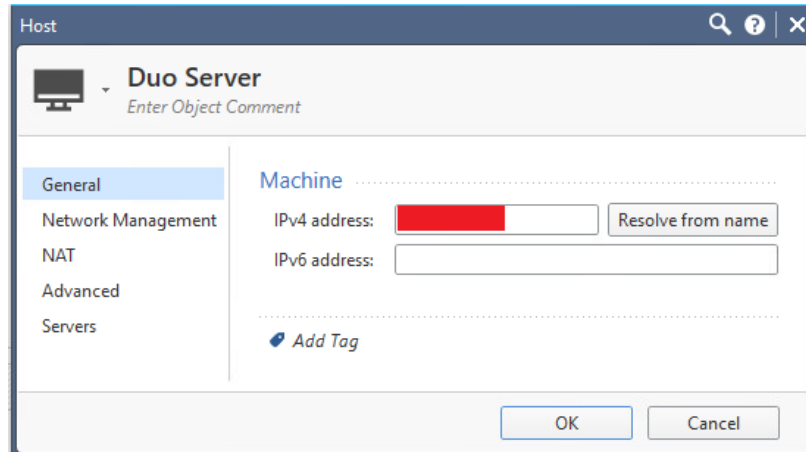
```

Configuring a Check Point Gateway to use DUO

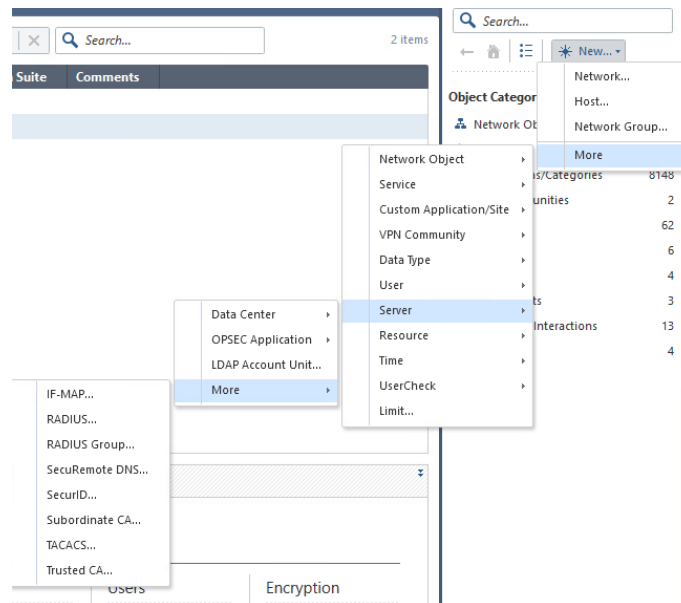
1. Create a new host by selecting New... > Host... in the Object Explorer.



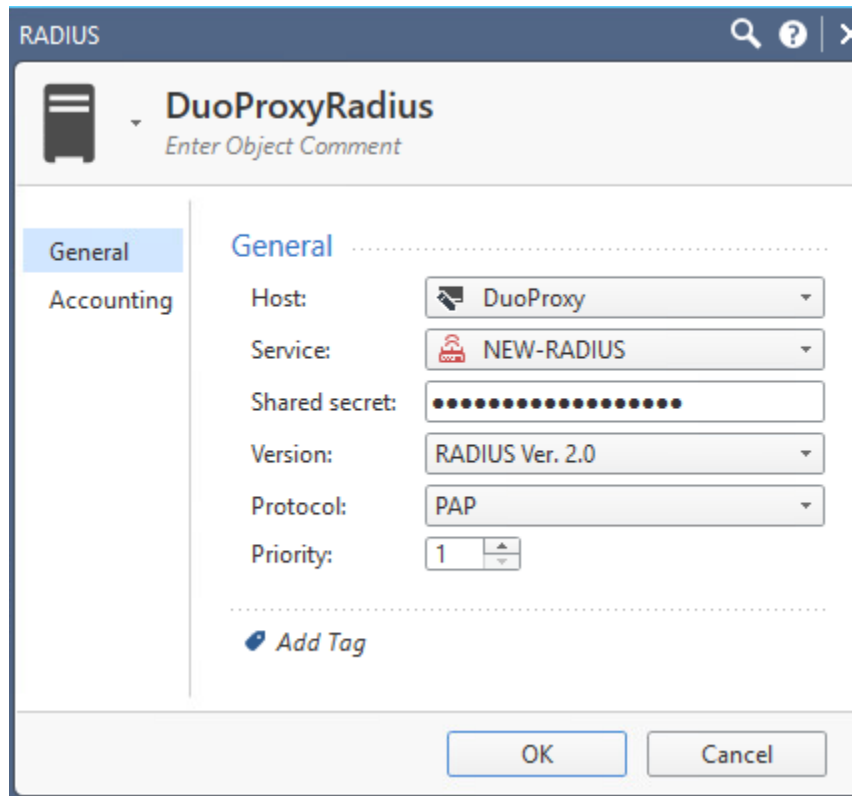
2. Fill in the Name and IP address of the DUO proxy server. Click OK.



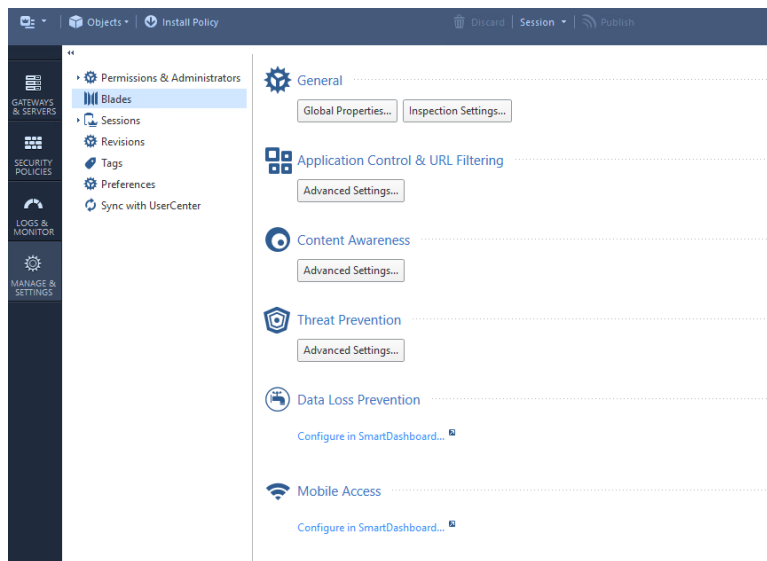
3. Create a RADIUS server object by clicking “New.. > More... > Server > More > RADIUS” in the Object Explorer.

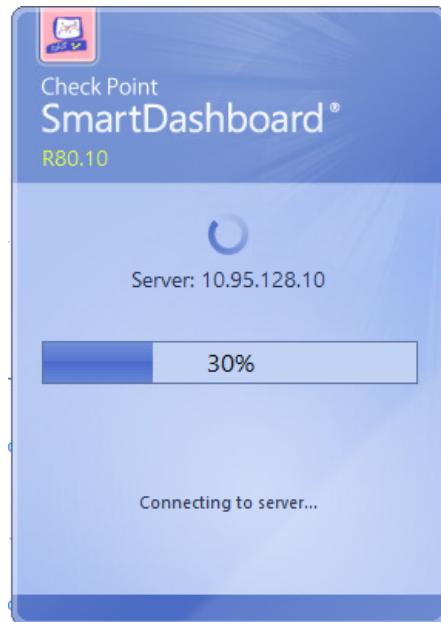


4. Select the Host you created in Step 2 as the Host. The Service must be NEW-RADIUS. The Shared secret was configured in the DUO proxy configuration file. Select RADIUS Ver 2.0 and PAP as the protocol.

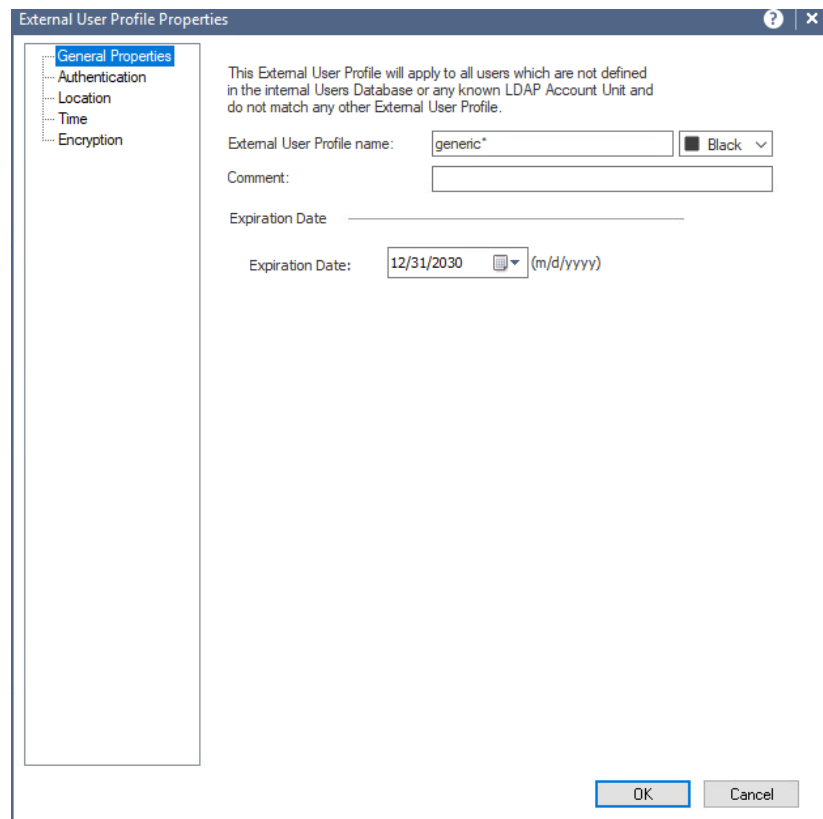


5. Go to Manage and Settings followed by Blades and then Click "Configure in SmartDashboard". The legacy SmartDashboard client will open.

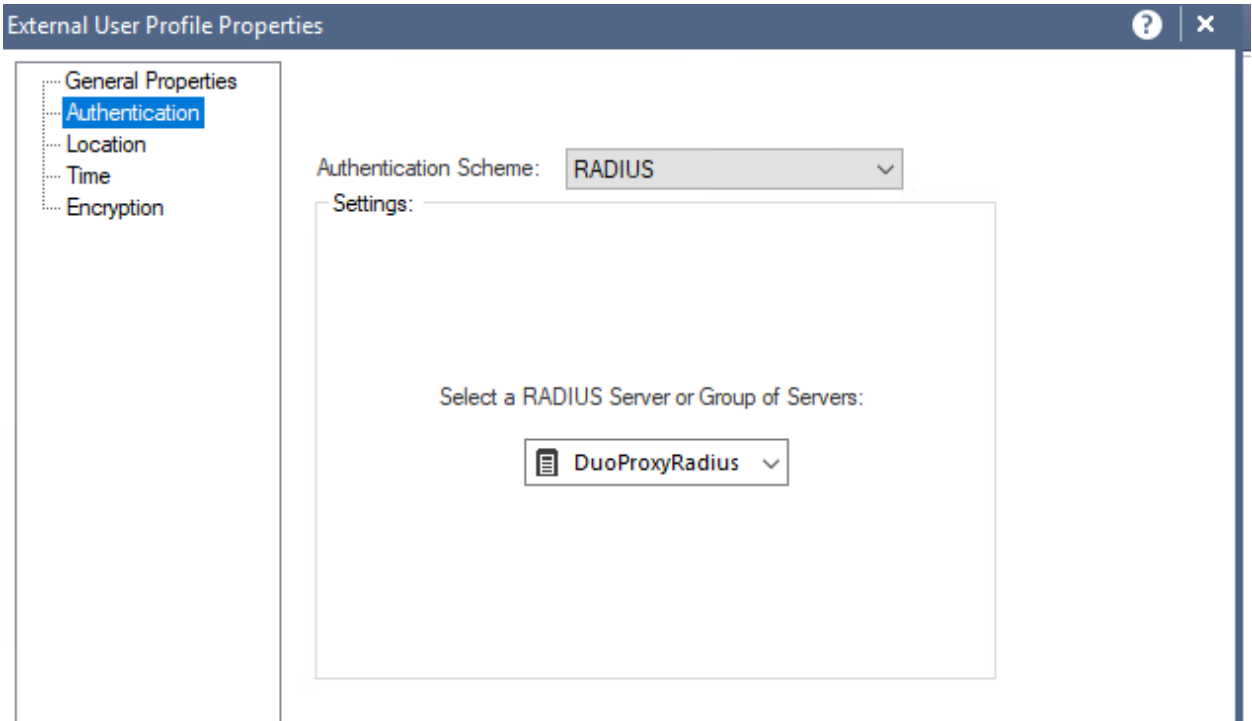




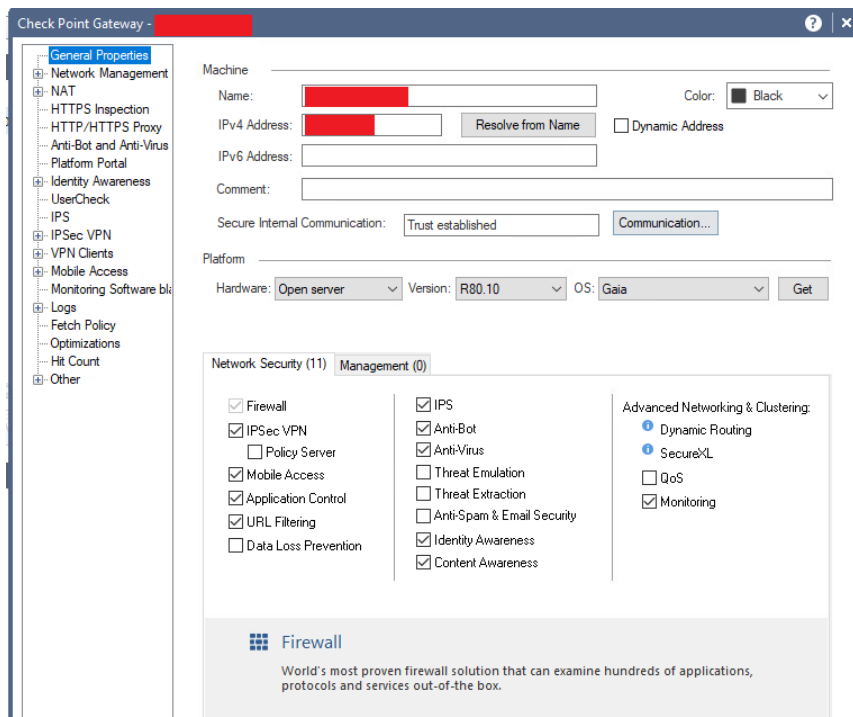
6. Click on the “User” icon in the Object Explorer in the bottom left. Then right click “External User Profiles” and select “New External User Profile > Match all users”.



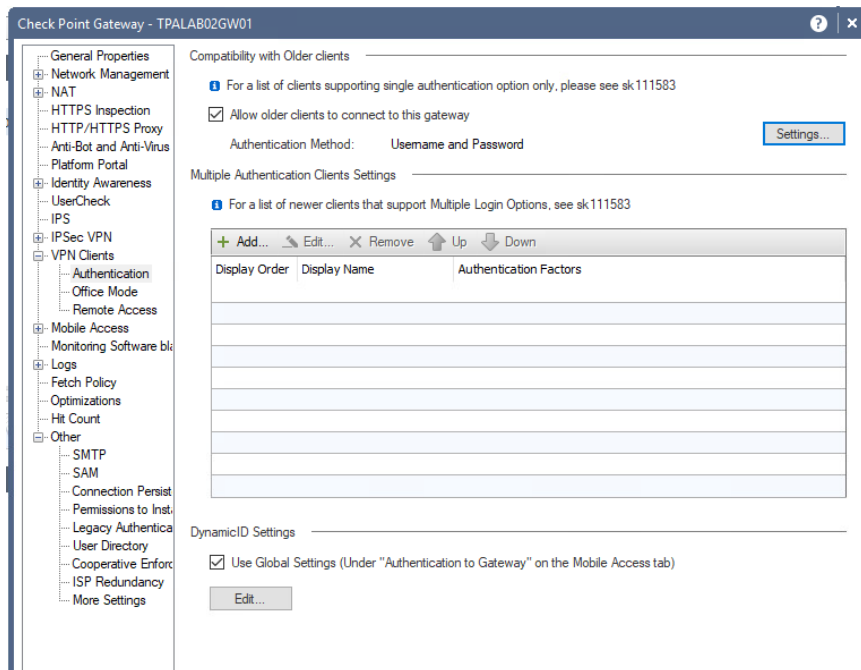
7. Select Authentication on the left pane. Change the Authentication Scheme to RADIUS and select the RADIUS server object you created in Step 4.



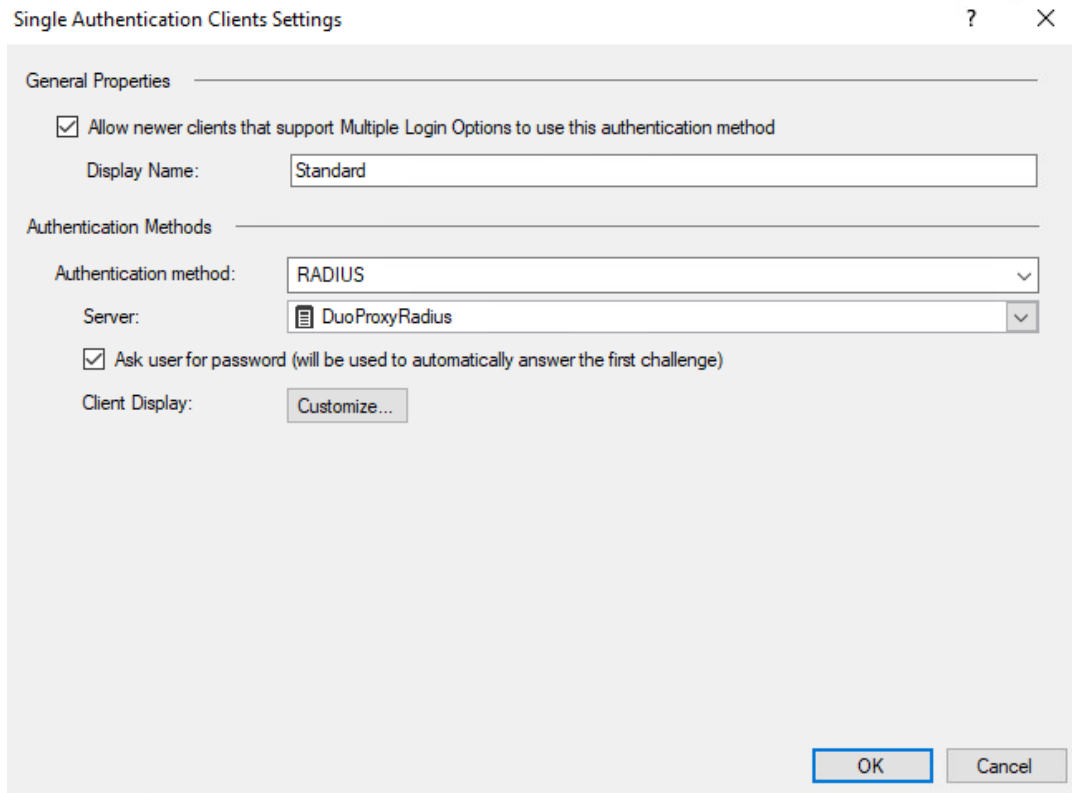
8. Click "OK" and save your changes. Then close the SmartDashboard window.
9. In SmartConsole, open the gateway object for your Remote Access VPN Gateway.



10. Select VPN Clients and expand the menu. Then click Authentication.

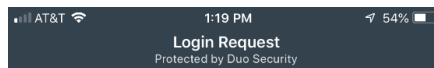
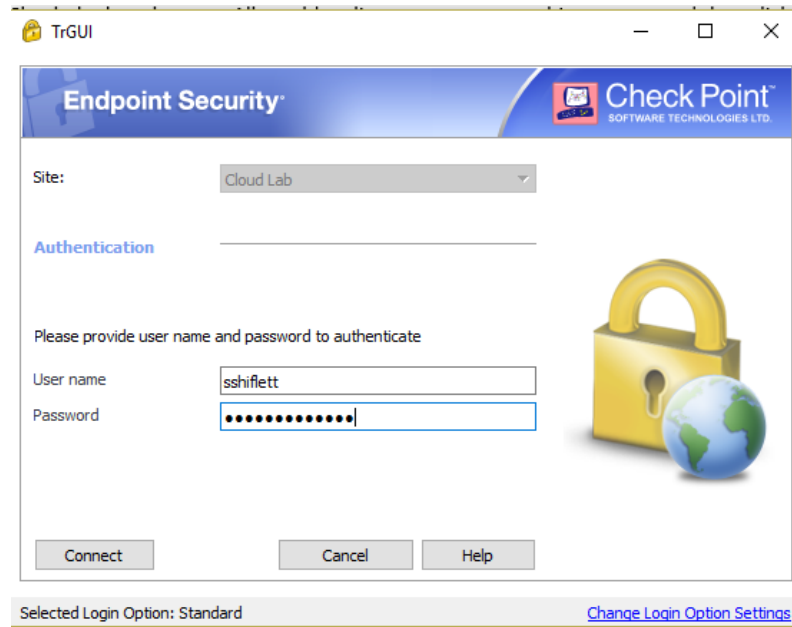


11. Check the box that says Allow older clients to connect to this gateway and then click Settings...



12. Select the RADIUS server you created in Step 4 as the server. Click OK.

13. Publish your changes and install policy to the Remote Access gateway. Your user should now be prompted for both their password via the Check Point client and an authorization via the DUO client.



ITSES Lab
Check Point VPN



1:19:42 PM EST
December 28, 2018



Additional Steps

At this point, your users should be able to use DUO to authenticate to the VPN. However, the default RADIUS timeouts are too short in some cases leading to users failing to approve the push notification in time. For this reason it is recommended that you increase the RADIUS timeout values according to sk102557. DUO also recommends the timeout settings found here https://help.duo.com/s/article/1170?language=en_US.