Using RADIUS Authentication for Remote Access VPN

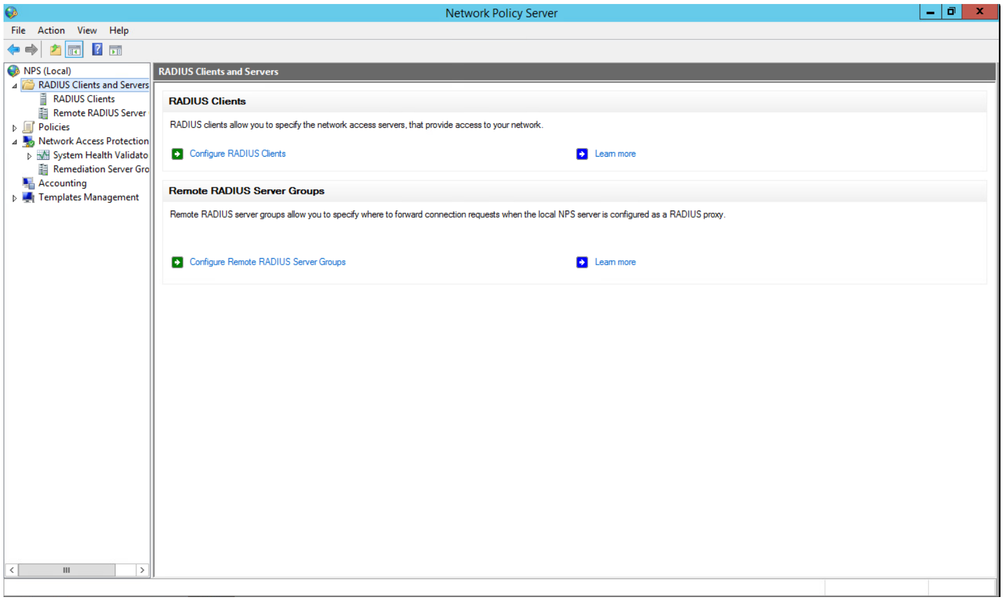
This guide will show step by step instructions for configuring Remote Access VPN to utilize RADIUS authentication. There is also an appendix that includes instructions for integrating DUO MFA with a Check Point Remote Access Gateway.

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.



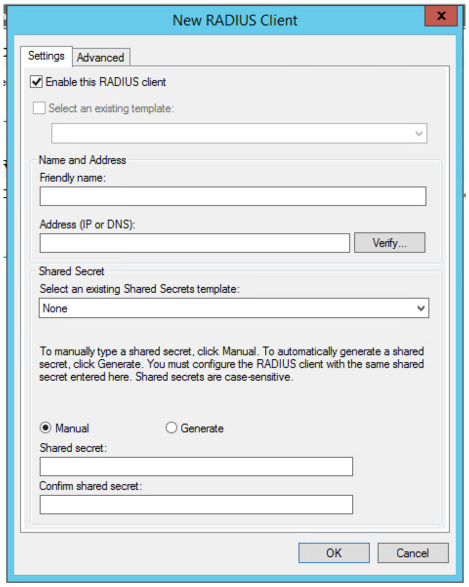
RADIUS Clients

RADIUS clients allow you to specify the network access servers, that provide access to your network.

Remote RADIUS Server Groups

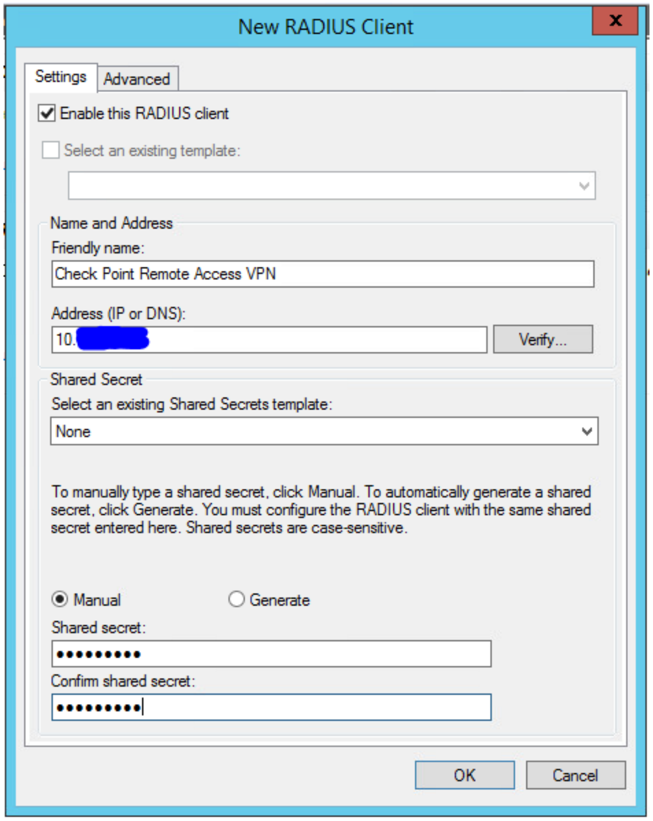
Remote RADIUS server groups allow you to specify where to forward connection requests when the local NPS server is configured as a RADIUS proxy.

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



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.

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



Friendly name: Check Point Remote Access VPN

Address (IP or DNS): 10.[redacted]

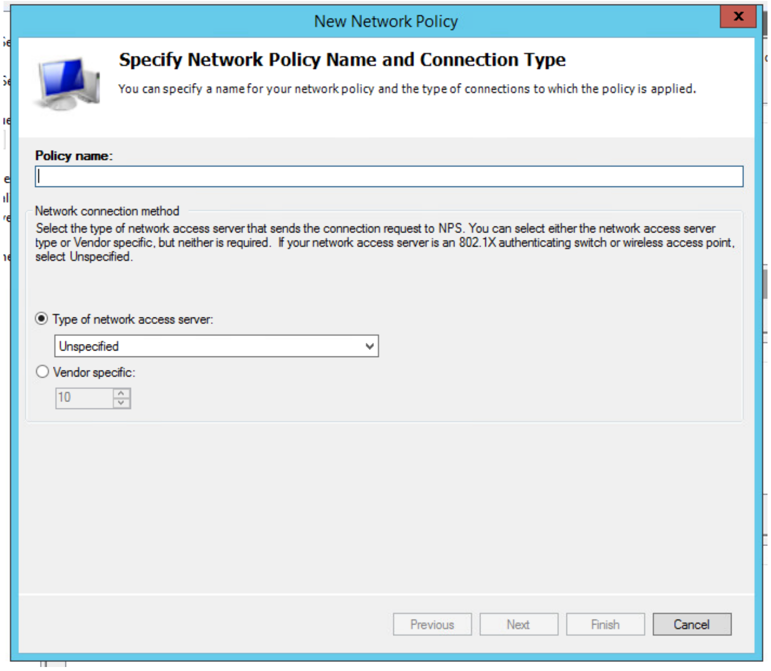
Select an existing Shared Secrets template: None

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.

Shared secret: •••••••••

Confirm shared secret: •••••••••

4. Click “OK” and proceed to the Network Policy Server window. Right click on “Network Policies” and select “New”.



New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:

Network connection method

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.

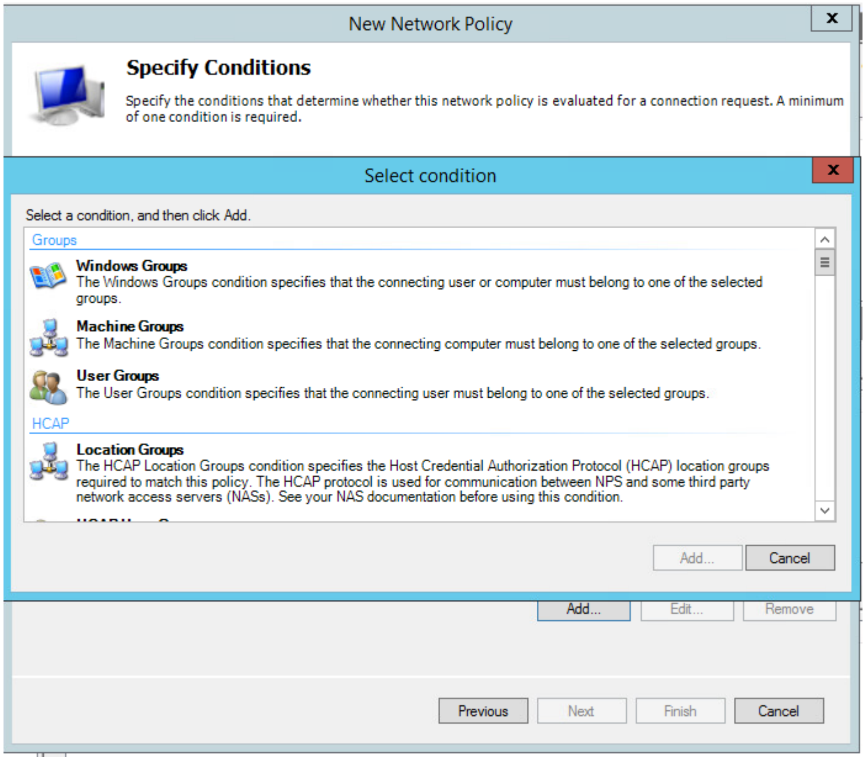
● Type of network access server:

Unspecified

○ Vendor specific:

10

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



New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Select condition

Select a condition, and then click Add.

Groups

Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

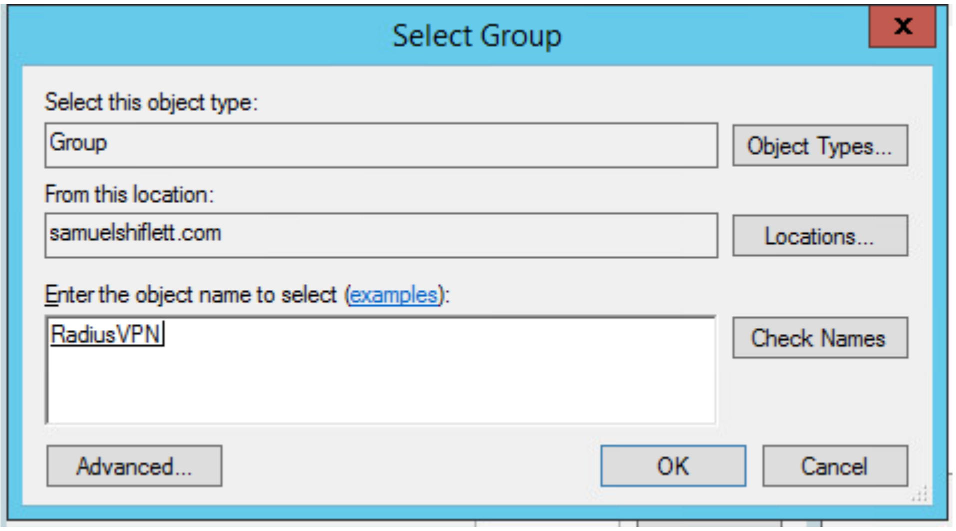
Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

HCAP

Location Groups
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.

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



Select Group

Select this object type:

Group

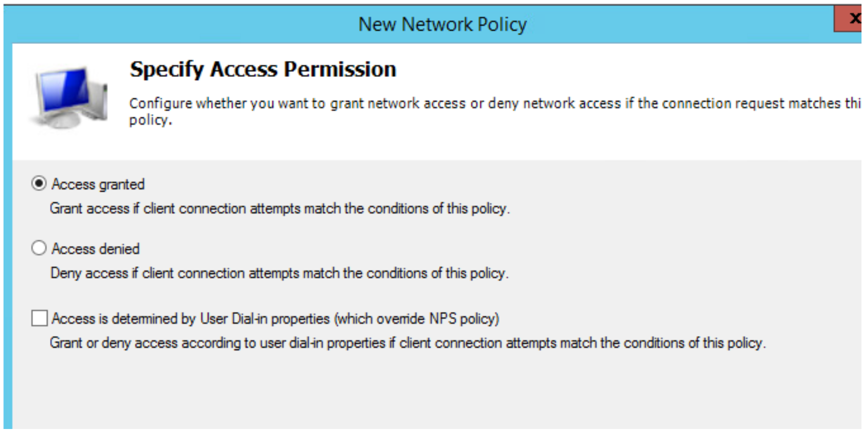
From this location:

samuelshiflett.com

Enter the object name to select (examples):

RadiusVPN

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



New Network Policy

Specify Access Permission

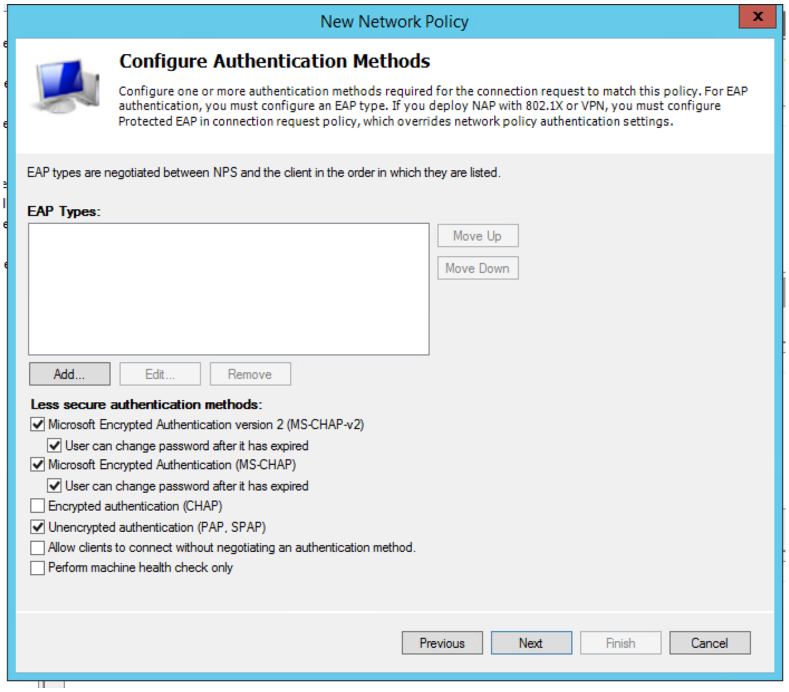
Configure whether you want to grant network access or deny network access if the connection request matches thi policy.

● 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.



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

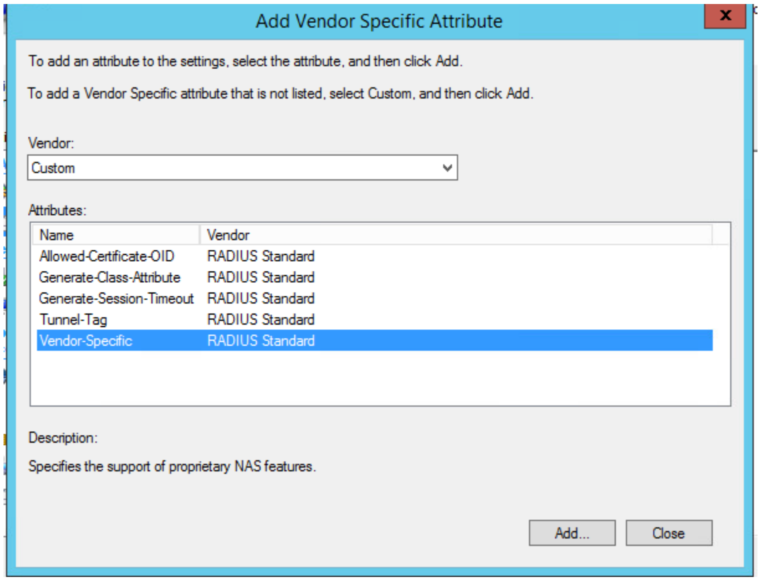
- ☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - ☑ User can change password after it has expired
- ☑ Microsoft Encrypted Authentication (MS-CHAP)
  - ☑ User can change password after it has expired
- ☐ Encrypted authentication (CHAP)
- ☑ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method.
- ☐ Perform machine health check only

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.



Add Vendor Specific Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor: Custom

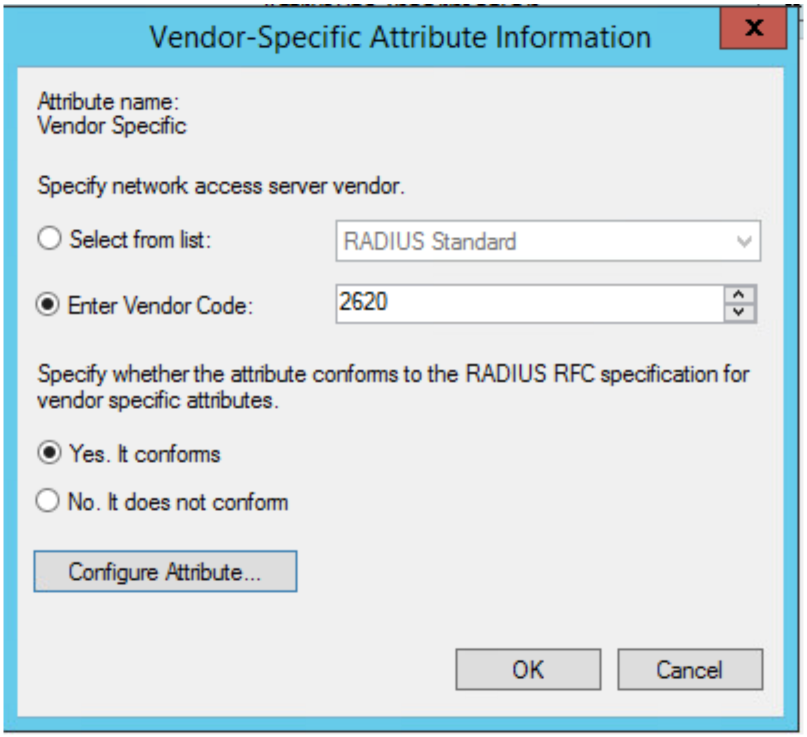
Attributes:

Name	Vendor
Allowed-Certificate-OID	RADIUS Standard
Generate-Class-Attribute	RADIUS Standard
Generate-Session-Timeout	RADIUS Standard
Tunnel-Tag	RADIUS Standard
Vendor-Specific	RADIUS Standard

Description:

Specifies the support of proprietary NAS features.

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



Vendor-Specific Attribute Information

Attribute name:
Vendor Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

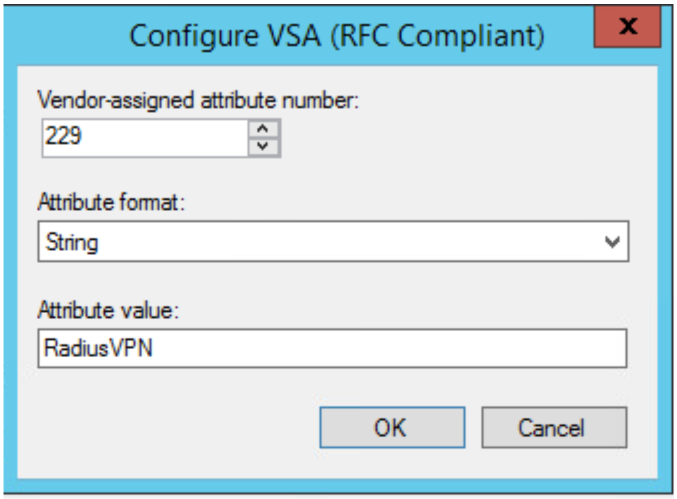
● Enter Vendor Code: 2620

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

● Yes. It conforms

○ No. It does not conform

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.**



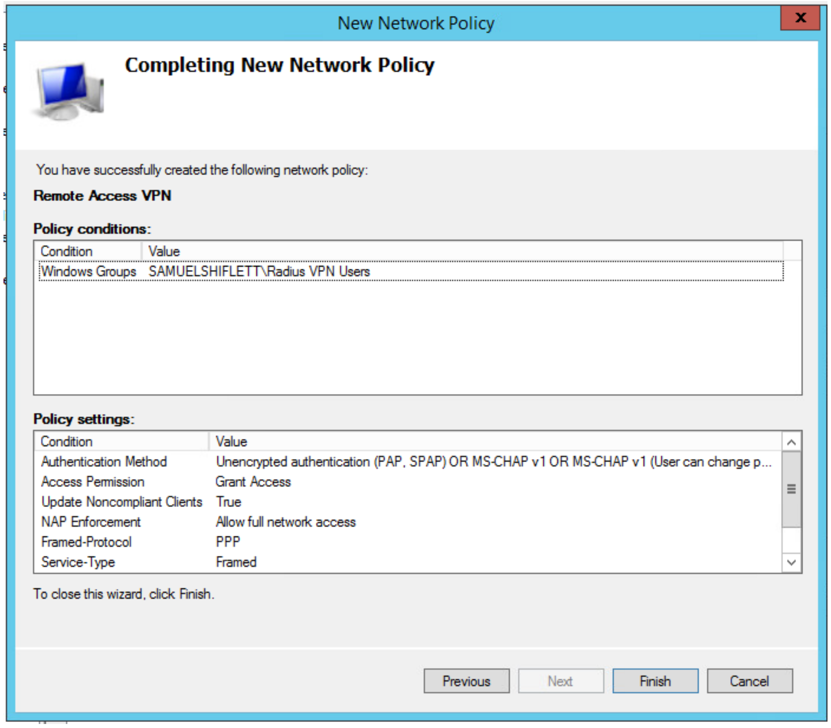
Configure VSA (RFC Compliant)

Vendor-assigned attribute number:
229

Attribute format:
String

Attribute value:
RadiusVPN

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



Completing New Network Policy

You have successfully created the following network policy:

Remote Access VPN

Policy conditions:

Condition	Value
Windows Groups	SAMUELSHIFLETT\Radius VPN Users

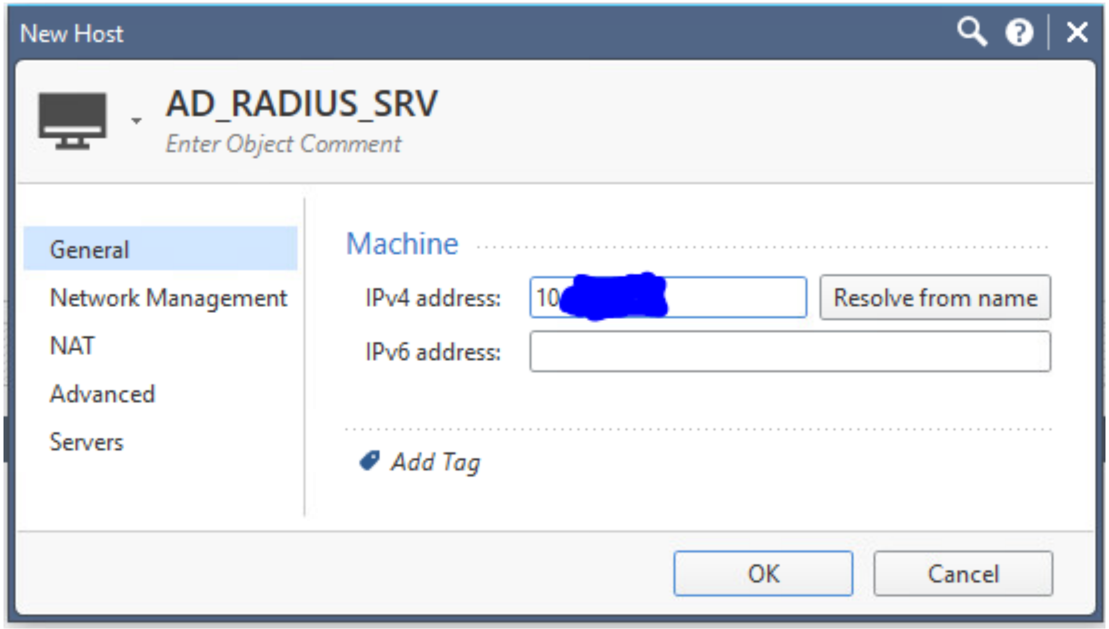
Policy settings:

Condition	Value
Authentication Method	Unencrypted authentication (PAP, SPAP) OR MS-CHAP v1 OR MS-CHAP v1 (User can change p...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

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

1. Create a host object for the RADIUS server.



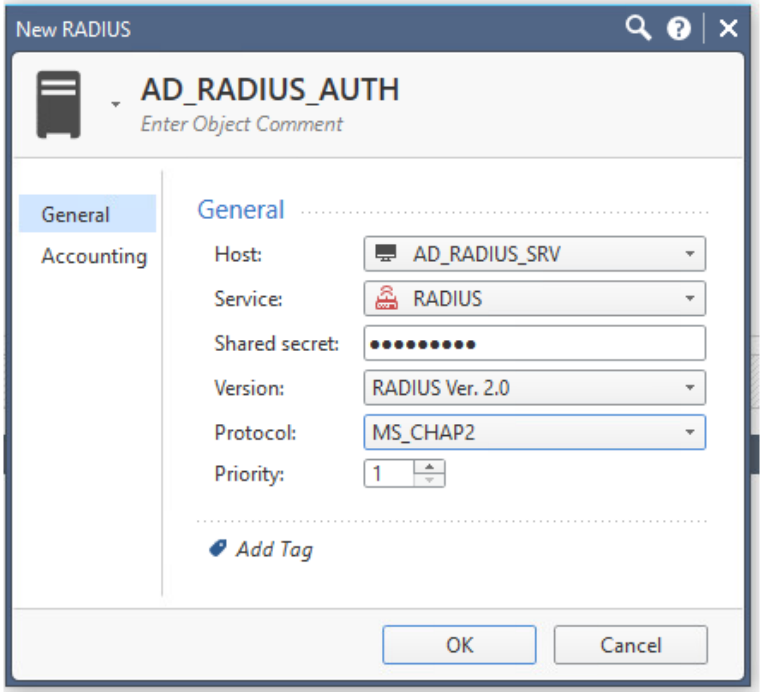
AD_RADIUS_SRV

Enter Object Comment

IPv4 address: 10[redacted]

IPv6 address:

2. Create a RADIUS Server object.



New RADIUS

AD_RADIUS_AUTH

Enter Object Comment

General

Host: AD_RADIUS_SRV

Service: RADIUS

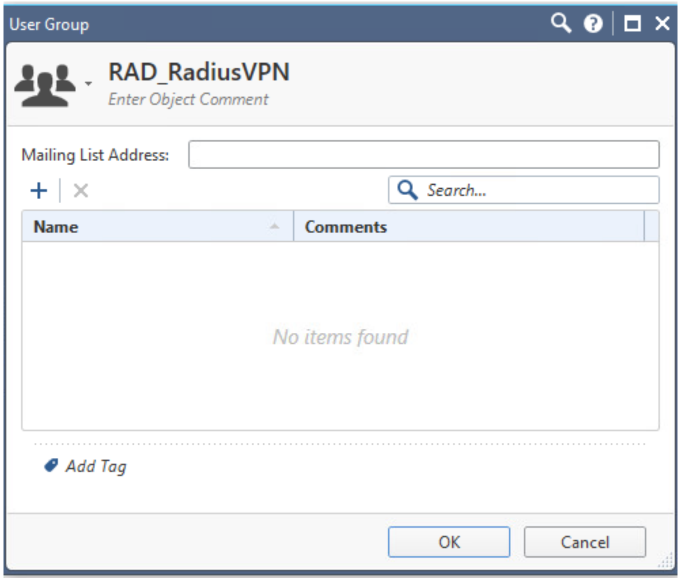
Shared secret: ●●●●●●●●●●

Version: RADIUS Ver. 2.0

Protocol: MS_CHAP2

Priority: 1

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



User Group

RAD_RadiusVPN

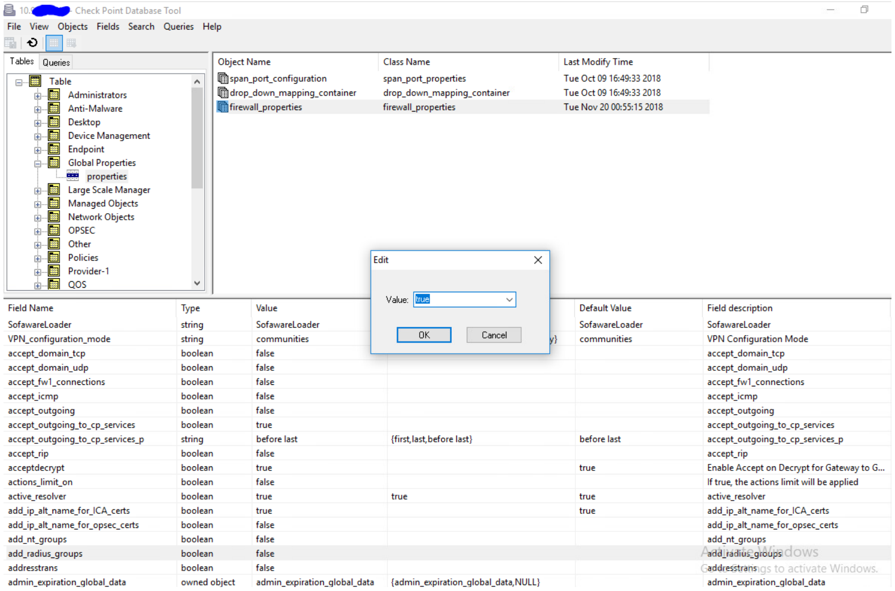
Enter Object Comment

Mailing List Address:

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.

6. Change add_radius_groups value under Global Properties > Properties > firewall_properties to true.

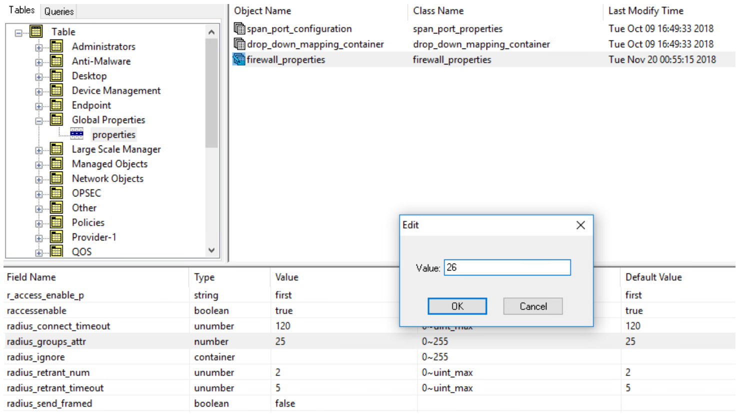


Object Name	Class Name	Last Modify Time
span_port_configuration	span_port_properties	Tue Oct 09 16:49:33 2018
drop_down_mapping_container	drop_down_mapping_container	Tue Oct 09 16:49:33 2018
firewall_properties	firewall_properties	Tue Nov 20 00:55:15 2018

Value: true

Field Name	Type	Value		Default Value	Field description
SofawareLoader	string	SofawareLoader		SofawareLoader	SofawareLoader
VPN_configuration_mode	string	communities	y}	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}	before last	accept_outgoing_to_cp_services_p
accept_rip	boolean	false			accept_rip
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	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

7. Change the radius_groups_atttr from 25 to 26. Save your changes and exit GUIDBedit.

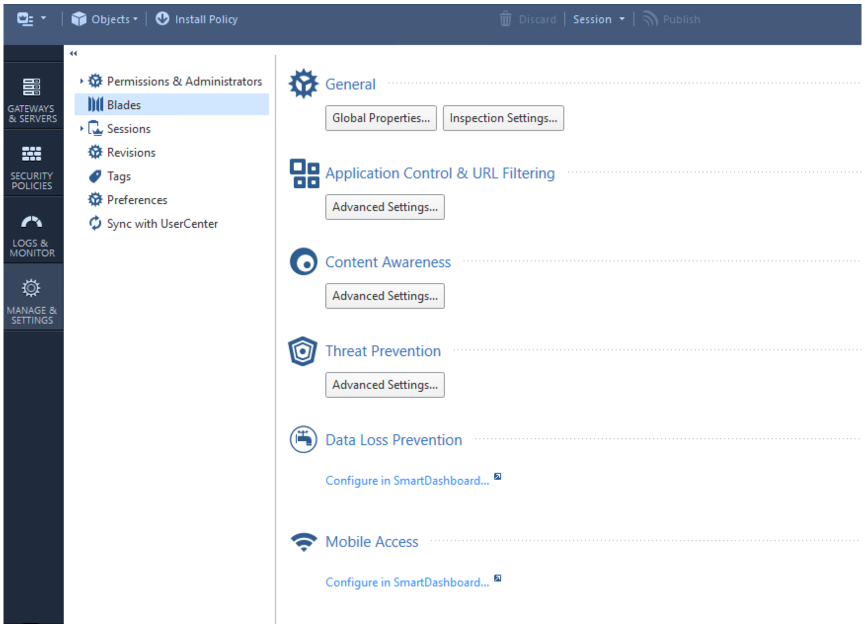


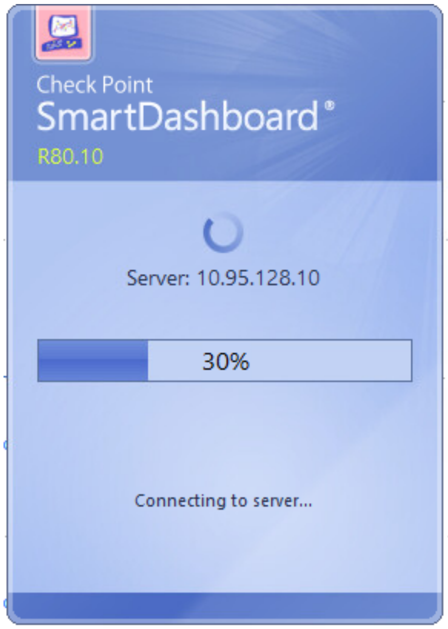
Object Name	Class Name	Last Modify Time
span_port_configuration	span_port_properties	Tue Oct 09 16:49:33 2018
drop_down_mapping_container	drop_down_mapping_container	Tue Oct 09 16:49:33 2018
firewall_properties	firewall_properties	Tue Nov 20 00:55:15 2018

Value: 26

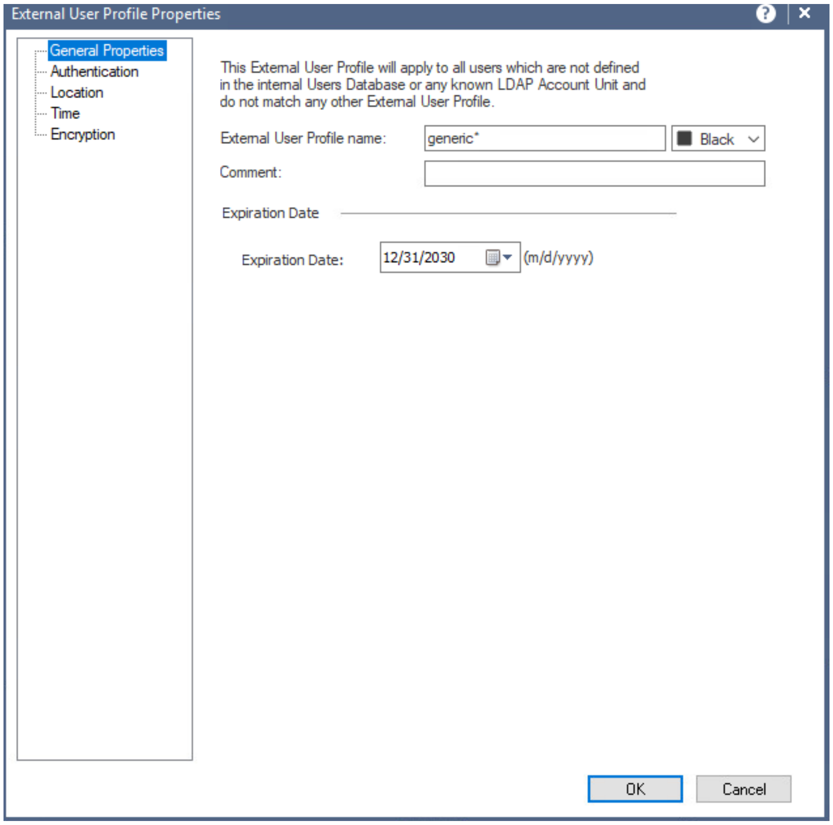
Field Name	Type	Value		Default Value
r_access_enable_p	string	first		first
raccessenable	boolean	true		true
radius_connect_timeout	unumber	120	0~uint_max	120
radius_groups_attr	number	25	0~255	25
radius_ignore	container		0~255	
radius_retrant_num	unumber	2	0~uint_max	2
radius_retrant_timeout	unumber	5	0~uint_max	5
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”.



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.

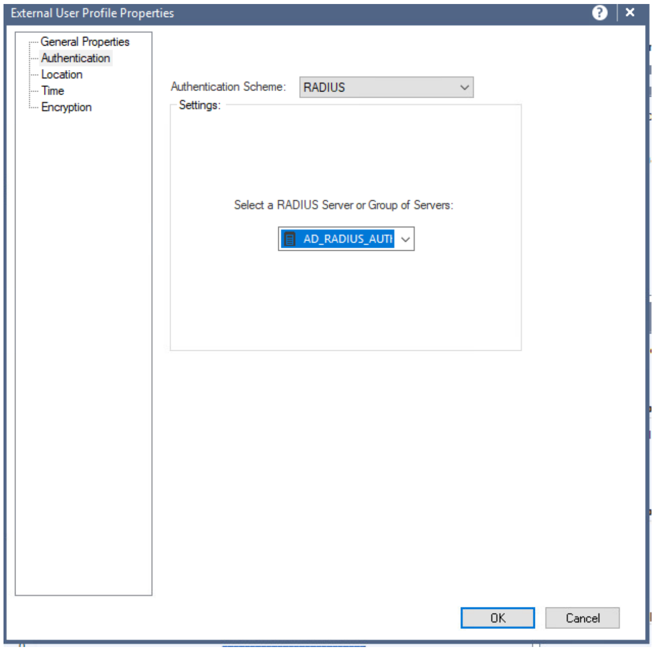
External User Profile name: generic* ■ Black

Comment:

Expiration Date

Expiration Date: 12/31/2030 (m/d/yyyy)

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

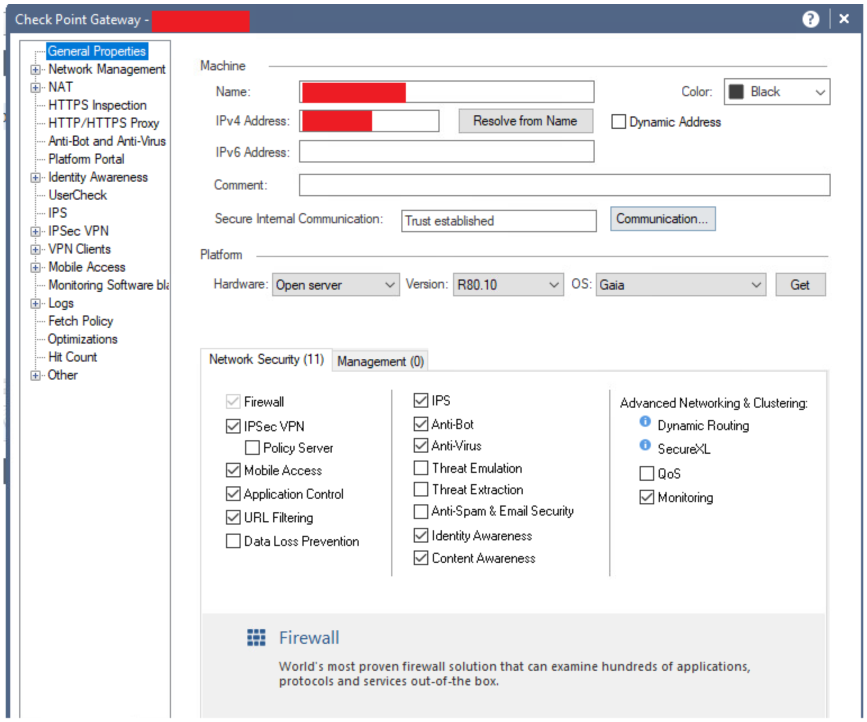


Authentication Scheme: RADIUS

Settings:

Select a RADIUS Server or Group of Servers: AD_RADIUS_AUTI

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.



Check Point Gateway - [redacted]

Machine

Name: [redacted]

Color: Black

IPv4 Address: [redacted]

□ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

Hardware: Open server Version: R80.10 OS: Gaia

☑ Firewall
☑ IPSec VPN
□ Policy Server
☑ Mobile Access
☑ Application Control
☑ URL Filtering
□ Data Loss Prevention

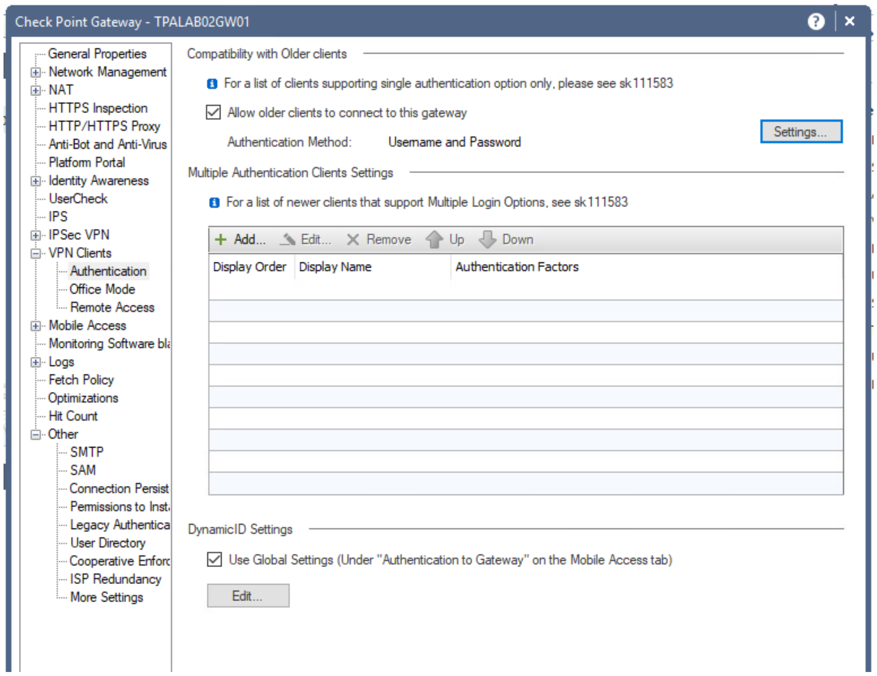
☑ IPS
☑ Anti-Bot
☑ Anti-Virus
□ Threat Emulation
□ Threat Extraction
□ Anti-Spam & Email Security
☑ Identity Awareness
☑ Content Awareness

Advanced Networking & Clustering:
Dynamic Routing
SecureXL
□ QoS
☑ Monitoring

Firewall

World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box.

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



Compatibility with Older clients

For a list of clients supporting single authentication option only, please see sk111583

☑ Allow older clients to connect to this gateway

Authentication Method: Username and Password

Multiple Authentication Clients Settings

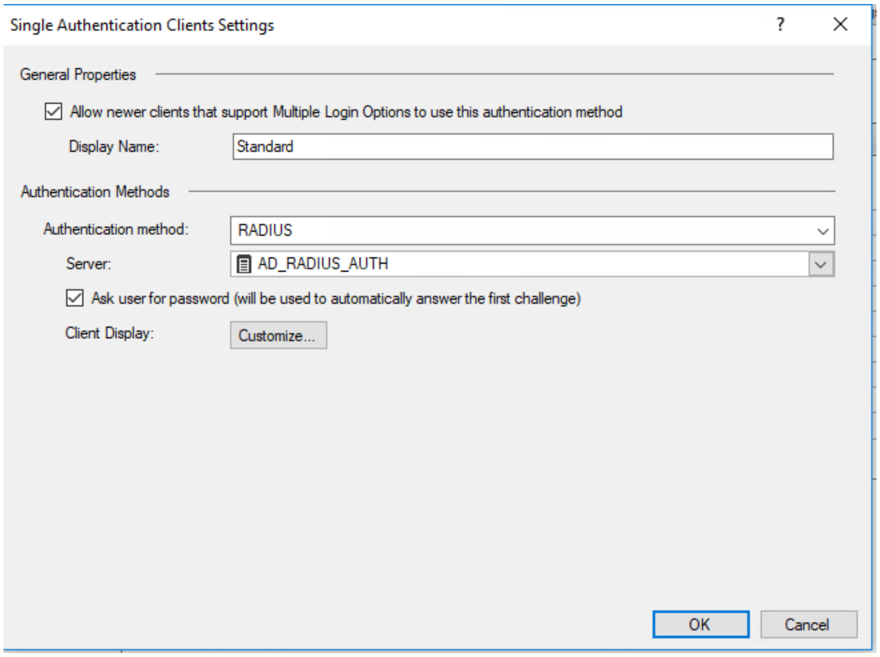
For a list of newer clients that support Multiple Login Options, see sk111583

DynamicID Settings

☑ Use Global Settings (Under "Authentication to Gateway" on the Mobile Access tab)

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 older clients to connect to this gateway” and then click “Settings”.



General Properties

☑ Allow newer clients that support Multiple Login Options to use this authentication method

Display Name: Standard

Authentication Methods

Authentication method: RADIUS

Server: AD_RADIUS_AUTH

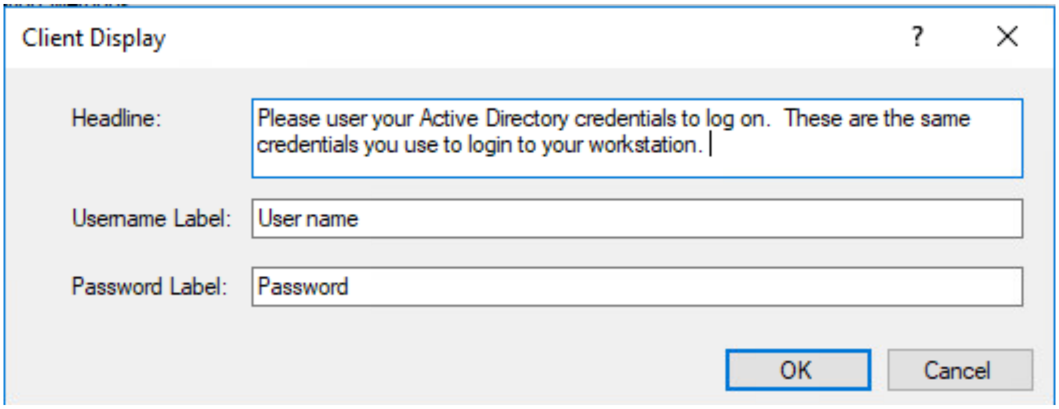
☑ Ask user for password (will be used to automatically answer the first challenge)

Client Display:

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”.



Client Display

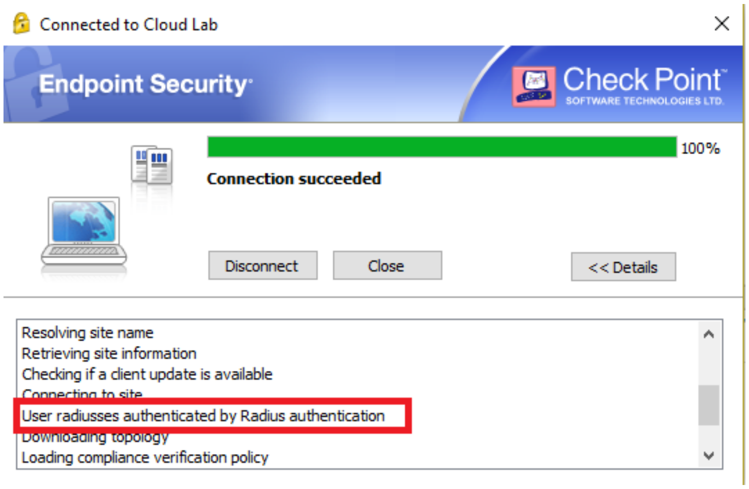
Headline: Please user your Active Directory credentials to log on. These are the same credentials you use to login to your workstation.

Username Label: User name

Password Label: Password

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:



Connected to Cloud Lab

100%

Connection succeeded

```
Resolving site name
Retrieving site information
Checking if a client update is available
Connecting to site
User radiusses authenticated by Radius authentication
Downloading topology
Loading compliance verification policy
```

Troubleshooting

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

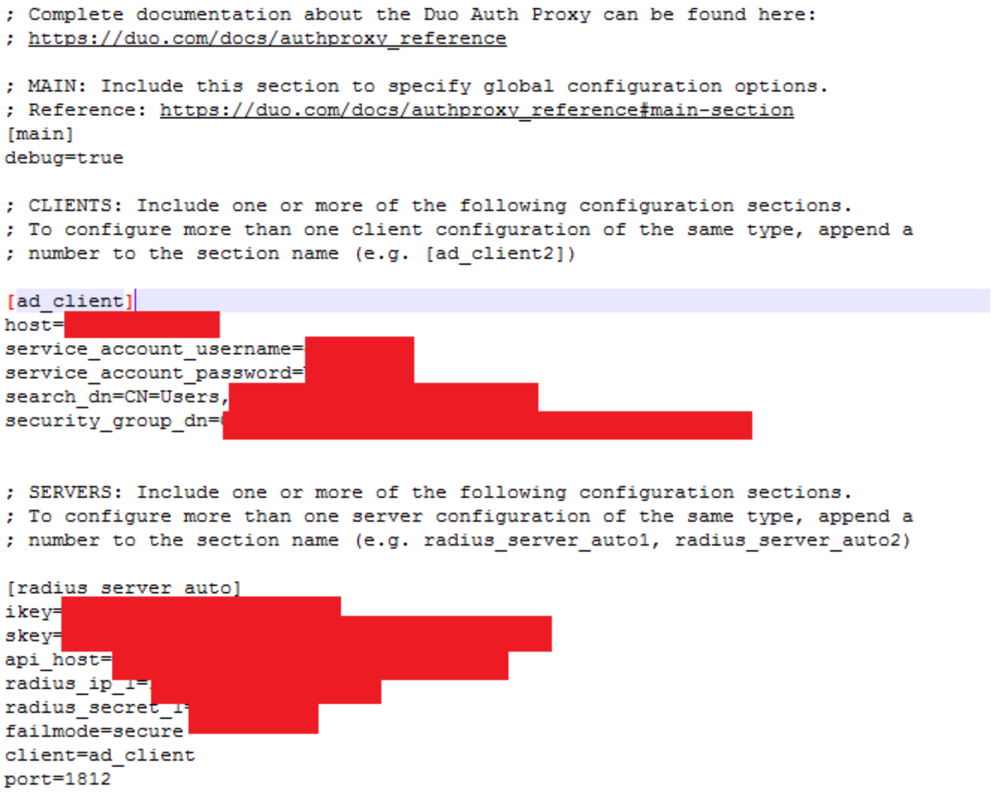
- IP Addresses
- Generic* user profile configuration
- Authentication settings on the gateway object
- Verify connectivity from the gateway to the RADIUS server.
- You may need to add rules to the gateway and other network devices to allow this communication over port 1812.
- You can also verify that the RADIUS request is beings sent by the gateway using "tcpdump -nni *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 configure the proxy can be found here:

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

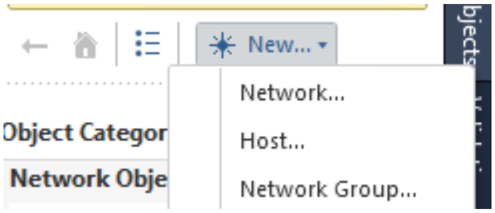
The above guide provides the majority of the steps for configuring the DUO and the Check Point configuration. However, it is designed for Mobile Access. The rest of this guide will assume that the DUO proxy server has already been configured to authenticate to DUO with an AD client as the primary factor:



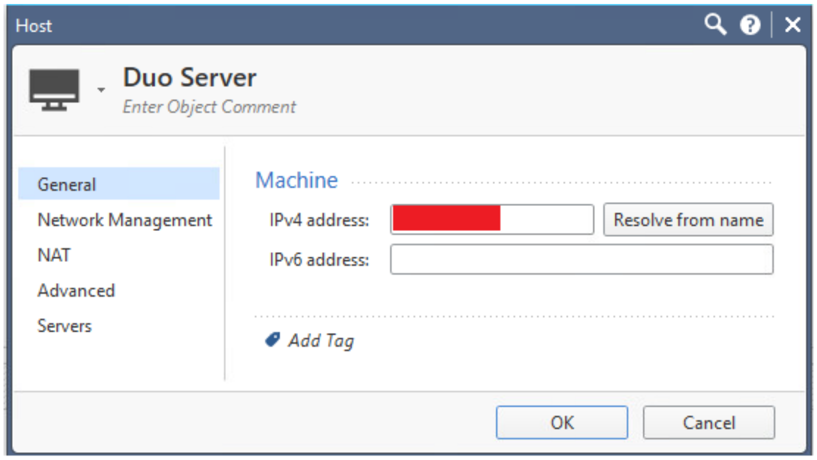
```
; Complete documentation about the Duo Auth Proxy can be found here:
; https://duo.com/docs/authproxy_reference

; 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=[redacted]
service_account_username=[redacted]
service_account_password=[redacted]
search_dn=CN=Users,[redacted]
security_group_dn=[redacted]


; 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=[redacted]
skey=[redacted]
api_host=[redacted]
radius_ip_1=[redacted]
radius_secret_1=[redacted]
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.



Host

Duo Server

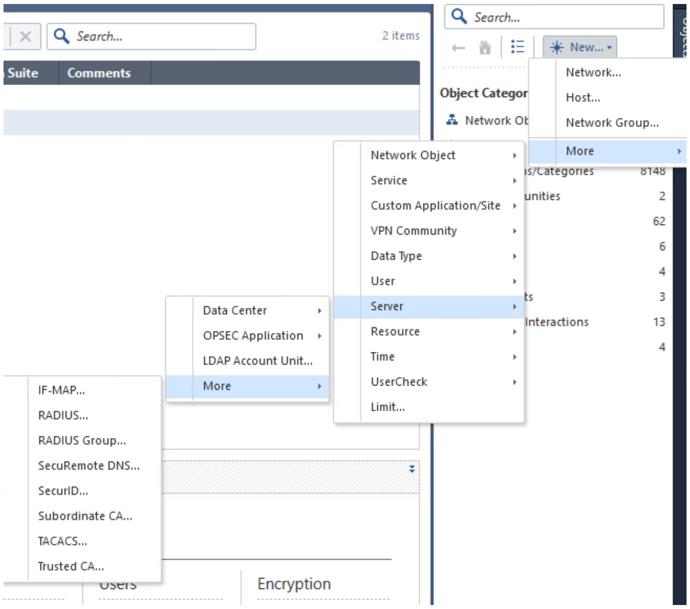
Enter Object Comment

Machine

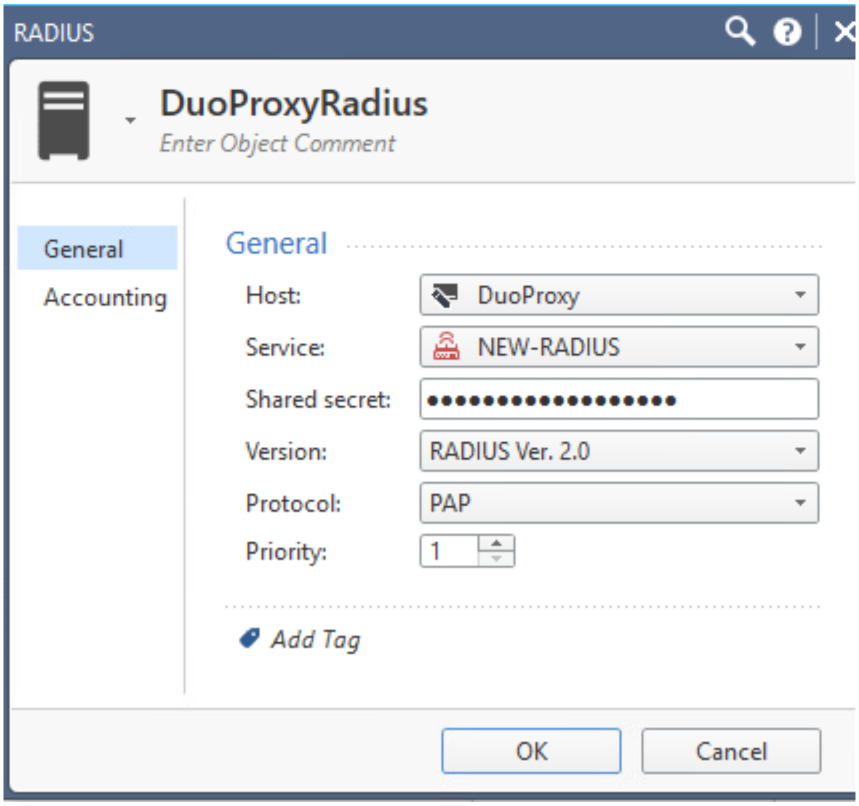
IPv4 address: [redacted]

IPv6 address:

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.



Host: DuoProxy

Service: NEW-RADIUS

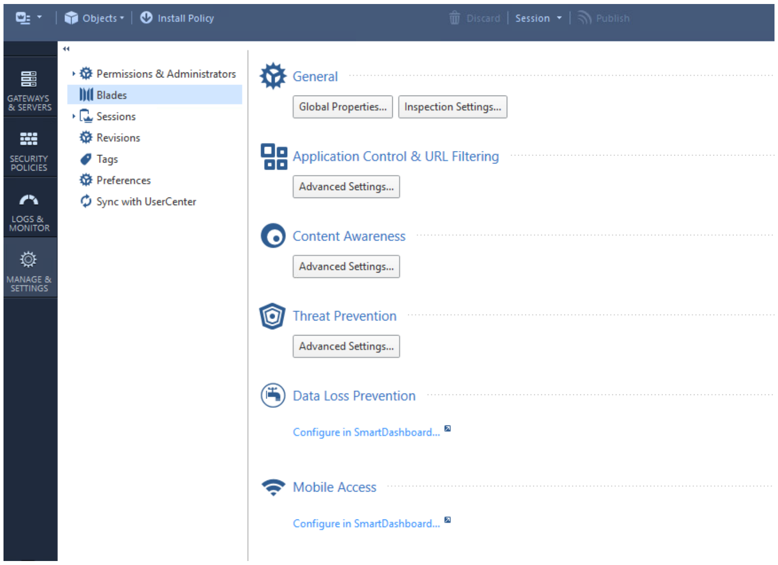
Shared secret: ●●●●●●●●●●●●●●●●●

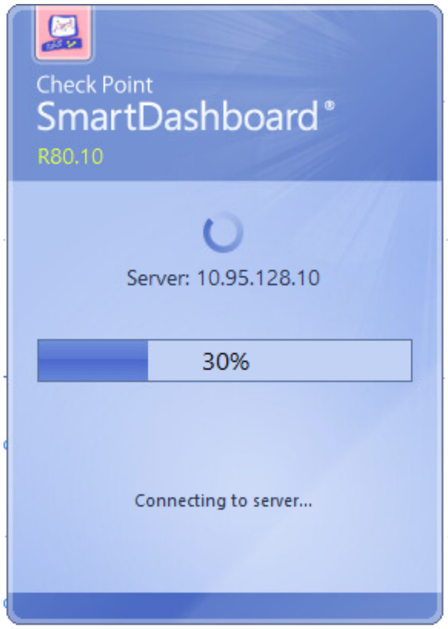
Version: RADIUS Ver. 2.0

Protocol: PAP

Priority: 1

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





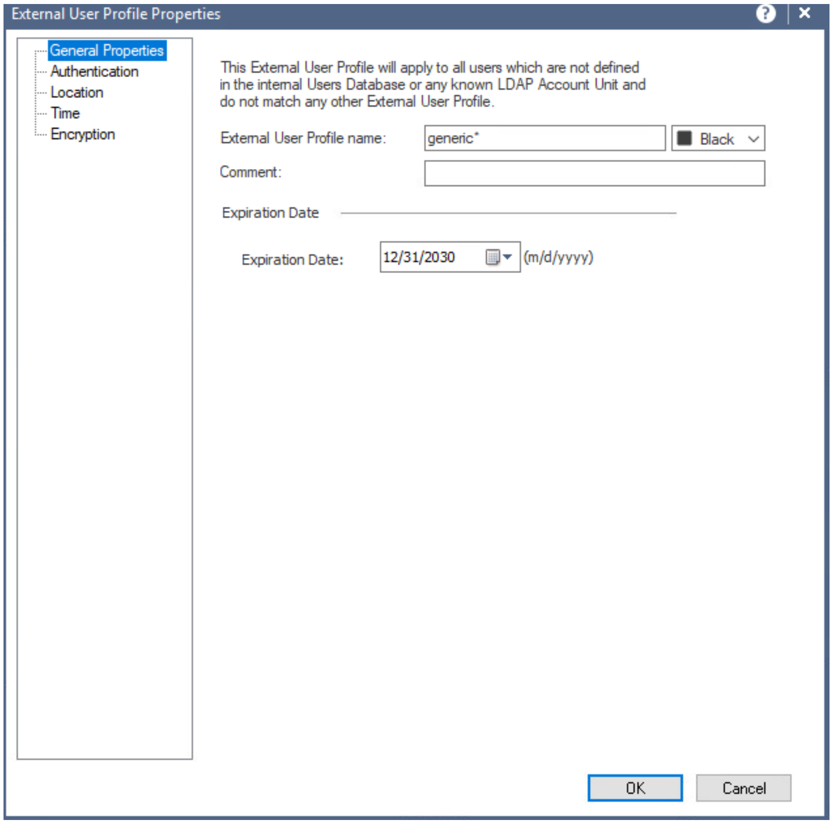
Check Point
SmartDashboard®
R80.10

Server: 10.95.128.10

30%

Connecting to server...

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”.



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.

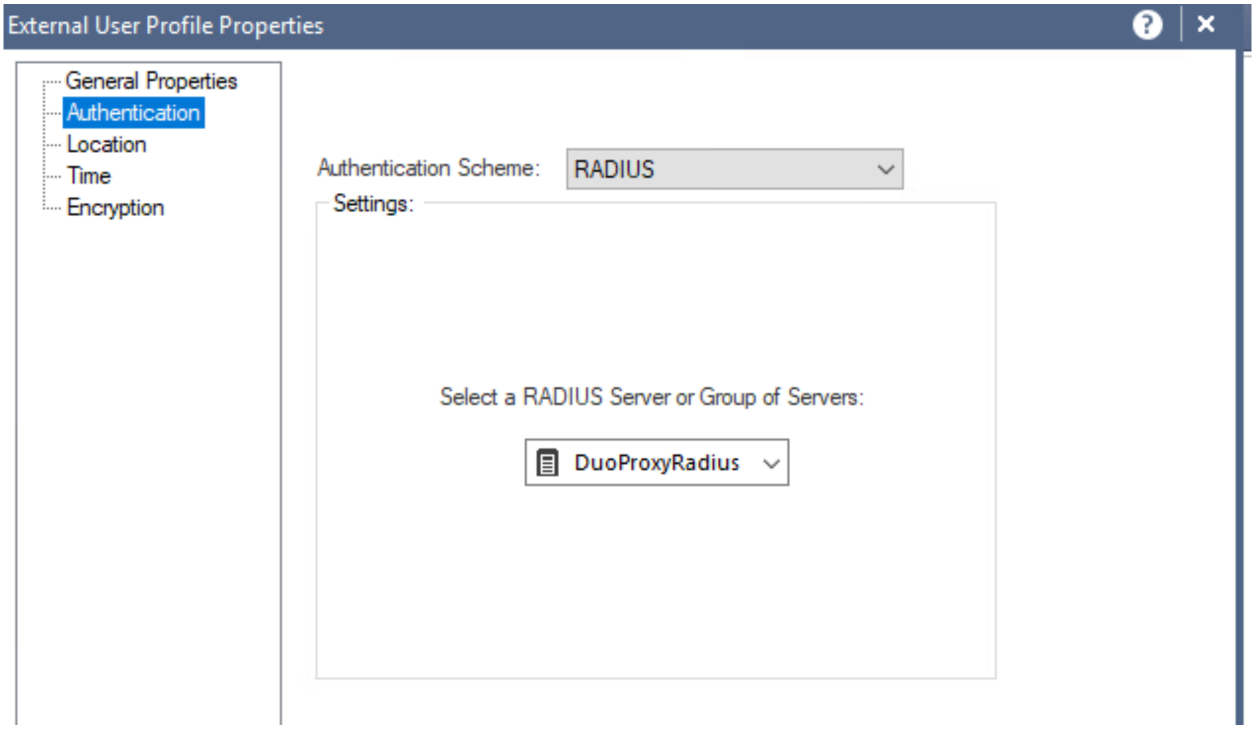
External User Profile name: generic* ■ Black

Comment:

Expiration Date

Expiration Date: 12/31/2030 (m/d/yyyy)

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

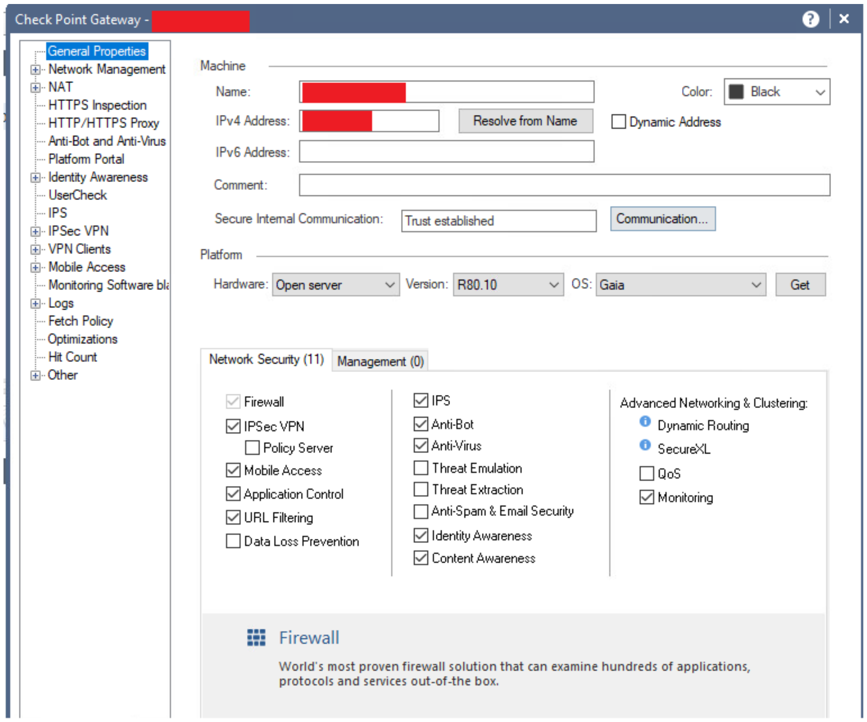


Authentication Scheme: RADIUS

Settings:

Select a RADIUS Server or Group of Servers: DuoProxyRadius

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.



Machine

Name: [redacted]

Color: Black

IPv4 Address: [redacted]

Resolve from Name

□ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Communication...

Platform

Hardware: Open server Version: R80.10 OS: Gaia Get

Network Security (11) Management (0)

☑ Firewall
☑ IPSec VPN
□ Policy Server
☑ Mobile Access
☑ Application Control
☑ URL Filtering
□ Data Loss Prevention

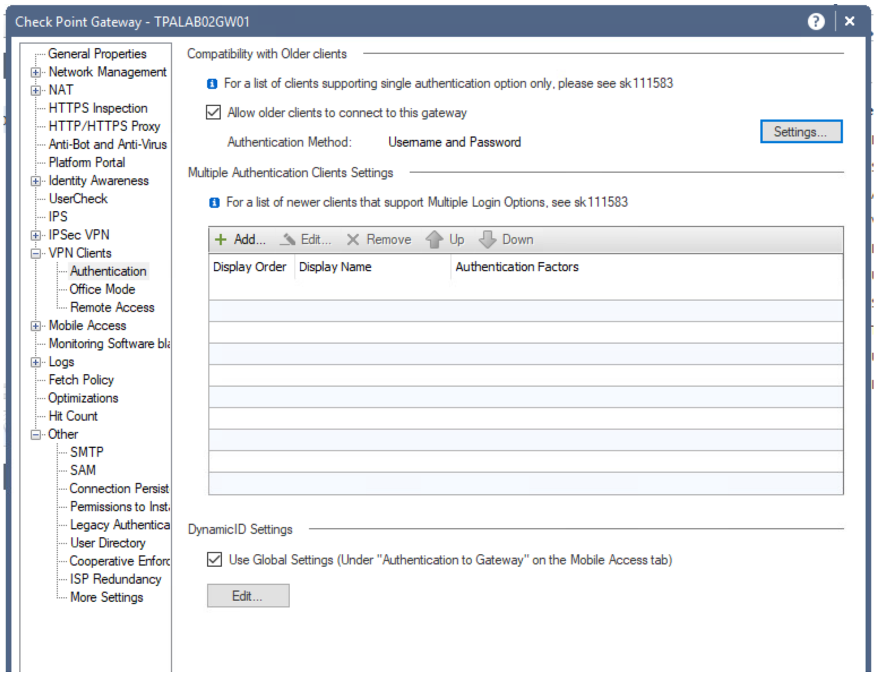
☑ IPS
☑ Anti-Bot
☑ Anti-Virus
□ Threat Emulation
□ Threat Extraction
□ Anti-Spam & Email Security
☑ Identity Awareness
☑ Content Awareness

Advanced Networking & Clustering:
Dynamic Routing
SecureXL
□ QoS
☑ Monitoring

Firewall

World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box.

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



Compatibility with Older clients

For a list of clients supporting single authentication option only, please see sk111583

☑ Allow older clients to connect to this gateway

Authentication Method: Username and Password

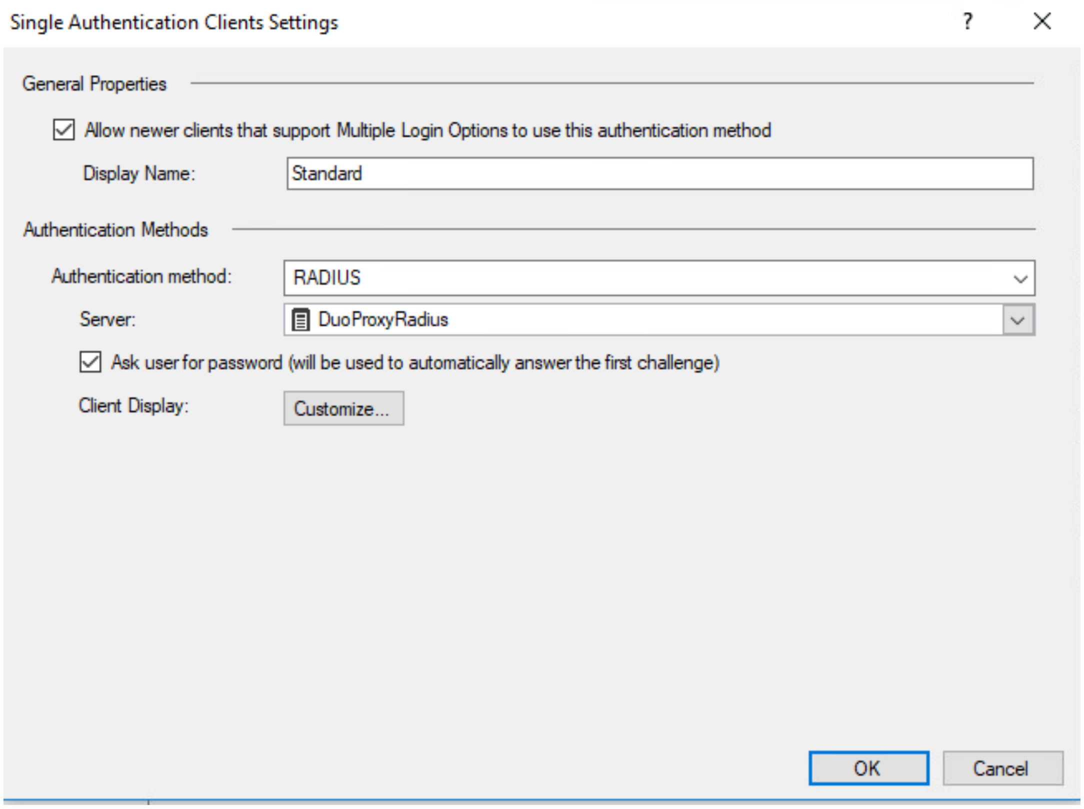
Multiple Authentication Clients Settings

For a list of newer clients that support Multiple Login Options, see sk111583

DynamicID Settings

☑ Use Global Settings (Under "Authentication to Gateway" on the Mobile Access tab)

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



General Properties

☑ Allow newer clients that support Multiple Login Options to use this authentication method

Display Name: Standard

Authentication Methods

Authentication method: RADIUS

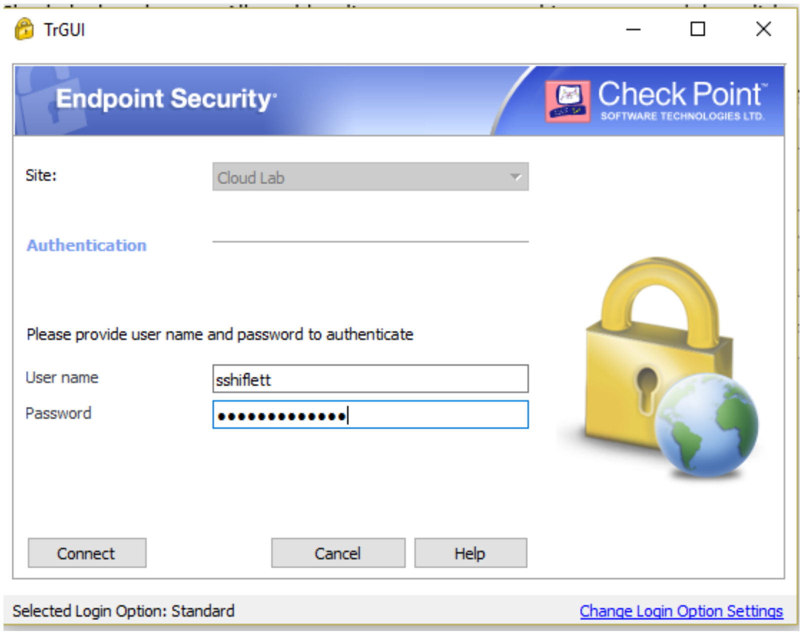
Server: DuoProxyRadius

☑ Ask user for password (will be used to automatically answer the first challenge)

Client Display:

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.



TrGUI

Endpoint Security

Check Point SOFTWARE TECHNOLOGIES LTD.

Site: Cloud Lab

Authentication

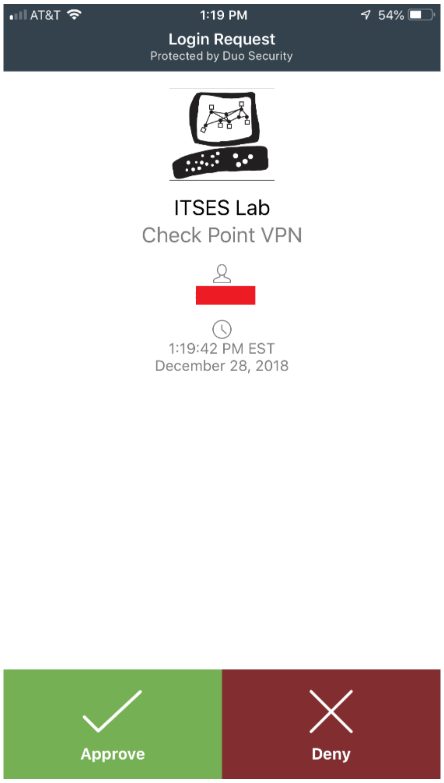
Please provide user name and password to authenticate

User name: sshiflett

Password: •••••••••••••

Selected Login Option: Standard

Change Login Option Settings



AT&T 1:19 PM 54%

Login Request

Protected by Duo Security

ITSES Lab

Check Point VPN

[redacted]

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.