SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

Checkpoint R80.10 Integration Guide

SecurAccess Integration Guide

Version 1.0 – 18/09/18

Checkpoint Integration Guide

Contents

1.1 Solution Summary

SecurEnvoy's SecurAccess MFA solution integrates with Checkpoint's R80.10 Firewall through the use of RADIUS for group membership and access control.

1.2 Guide Usage

The information in this guide describes the configuration required for integration with SecurEnvoy and common to most deployments. It is important to note:

- Every organization is different and may require additional or different configuration.
- Some configuration may have other methods to accomplish the same task than those described.
- It is expected that the Checkpoint device has been setup and is already working with LDAP authentication for VPN connectivity.

1.3 Prerequisites

The following conditions are required to set up SecurEnvoy's MFA Solution:

- A SecurAccess MFA server installed, configured and working on a system with:
  - Windows Server 2003 or higher.

  Note: Please see SecurEnvoy's SecurAccess deployment guide on how to setup MFA server solution.
- A Checkpoint firewall appliance or virtual – version GAIA R80.10 and above.
- Checkpoint Endpoint Protection client software E80.65 and above installed on all clients that connect remotely to the network unless the Clientless solution will be used.
- Familiarity with the following technologies:
  - RADIUS configuration
  - Checkpoint Smart Console

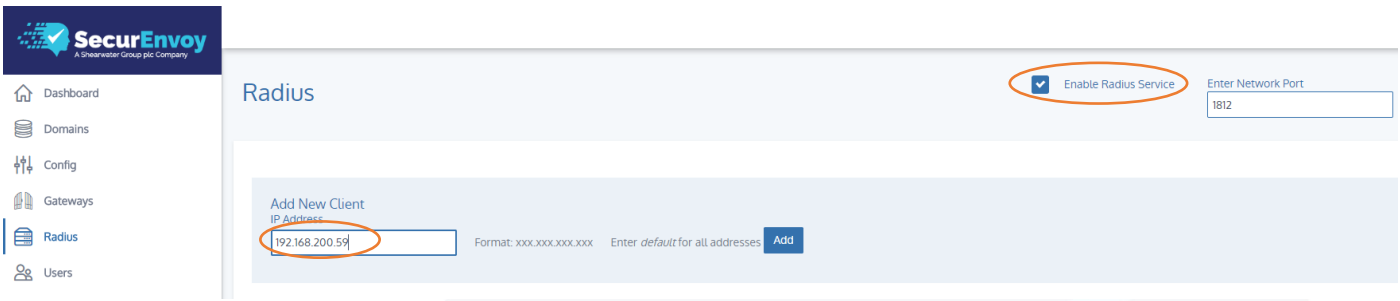
1.4 Authentication

The following section describes the steps required to configure the Checkpoint FW to authenticate users via RADIUS.

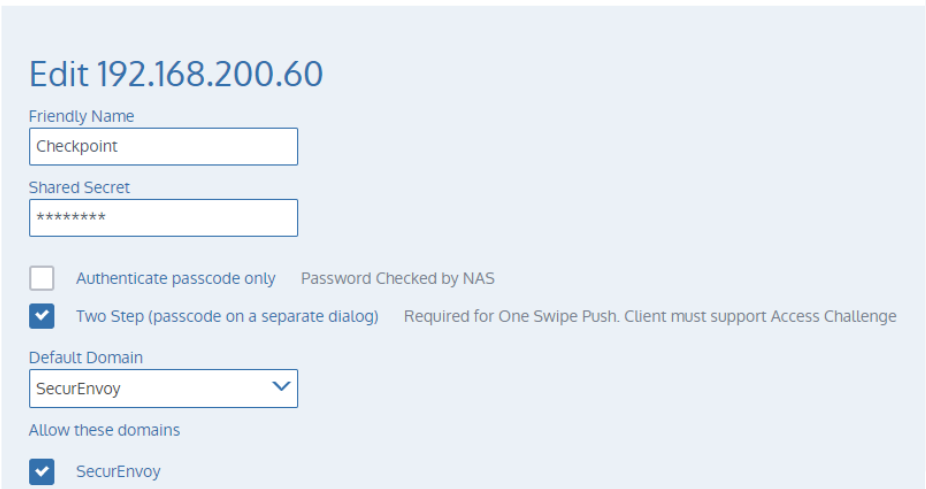
1.41 Setup RADIUS - SecurAccess

Within the SecurAccess configuration, we will need to configure the Checkpoint FW as an authorised RADIUS client.

- Navigate to RADIUS in the administrator dashboard.
- Ensure the RADIUS Service is enabled in the top right-hand side of the screen and make sure the port number is left as default 1812.
- Enter the IP address of the Checkpoint device and click “Add”

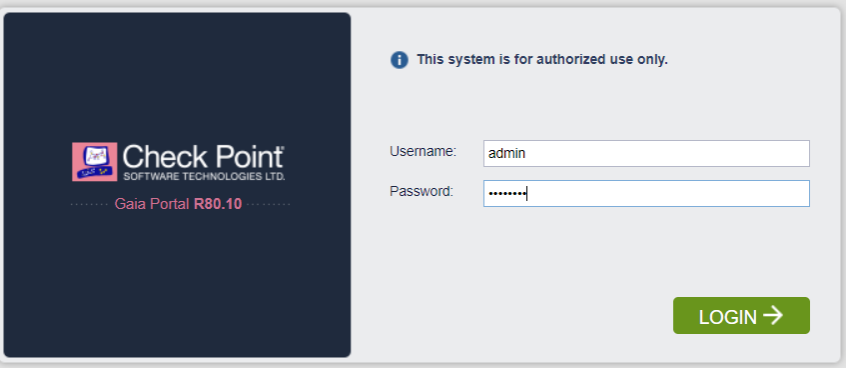


- Enter in a shared secret or common password and select the domains that will be authenticated against (if there is more than one domain configured in SecurAccess)
- Click Update

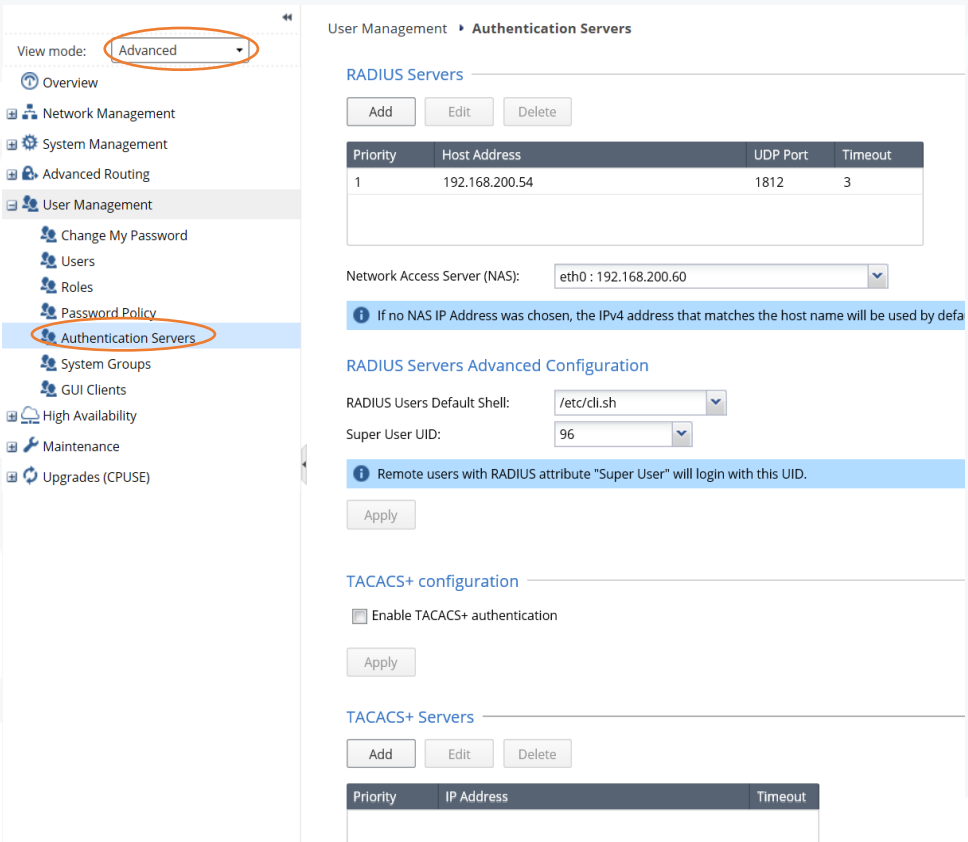


1.42 Setup RADIUS – Checkpoint (Web Portal)

Open a web browser and navigate to the IP or DNS address of your Checkpoint Firewall.
On connection with web-based interface, login using your admin account.

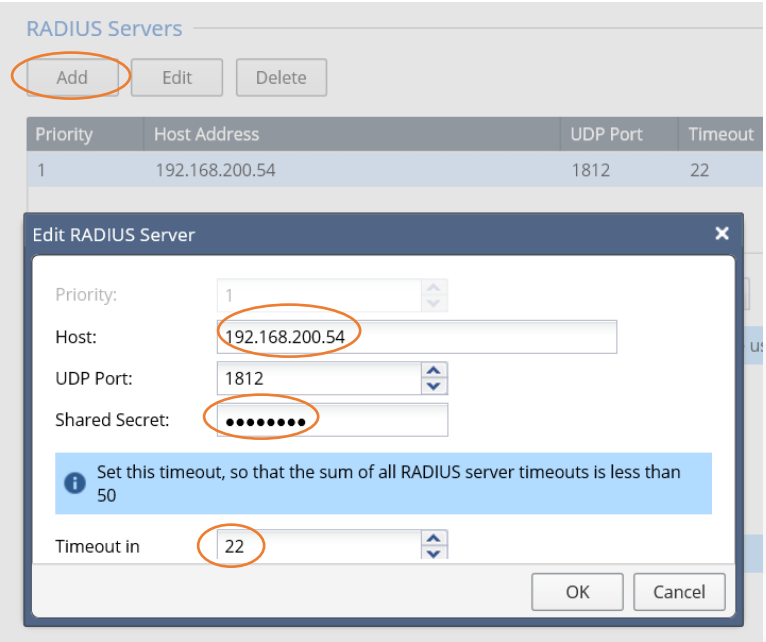


On access to the web portal, make sure View Mode is set to Advanced and navigate to Authentication Servers



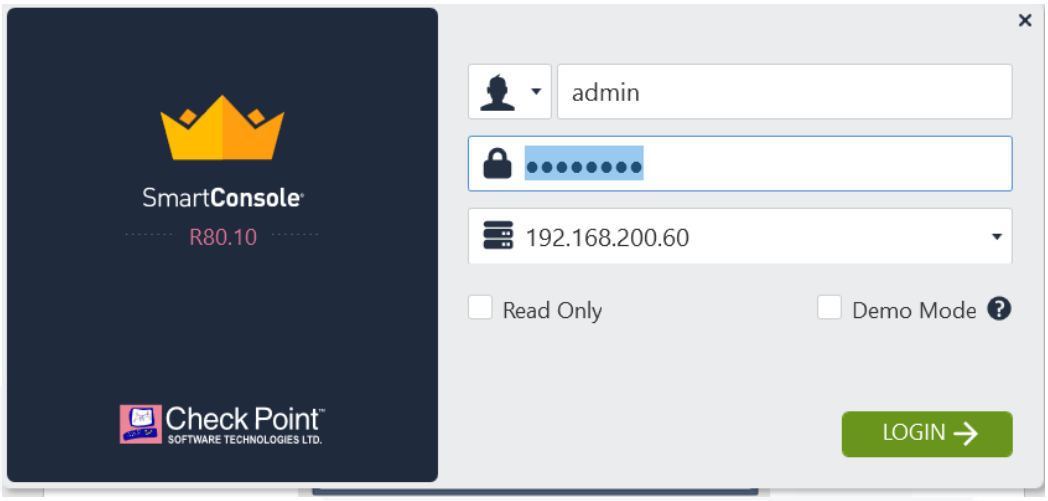
- From within the authentication servers section, click Add under RADIUS Servers to add the SecurEnvoy server.
- Add in the IP address of the SecurEnvoy server, add in the Shared Secret password configured previously and increase the Timeout in to 22 seconds.

Please Note: Select Network Access Server (NAS) interface that will be used to communicate to the SecurEnvoy Server

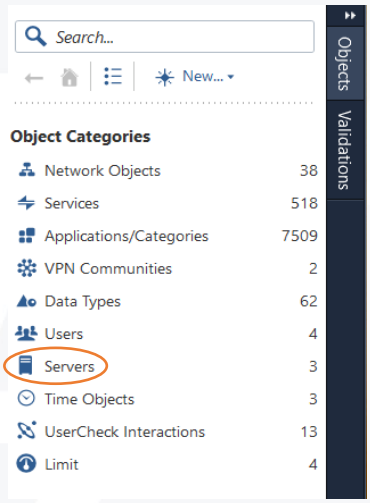


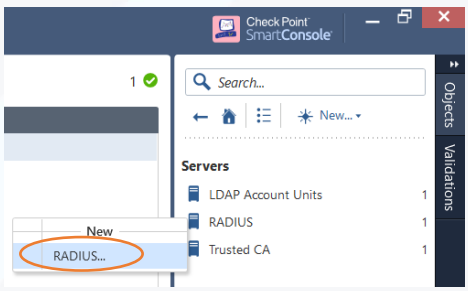
1.43 Setup RADIUS – Checkpoint (Smart Console)

From your Checkpoint SmartConsole Server or Client, login to the Checkpoint Firewall.



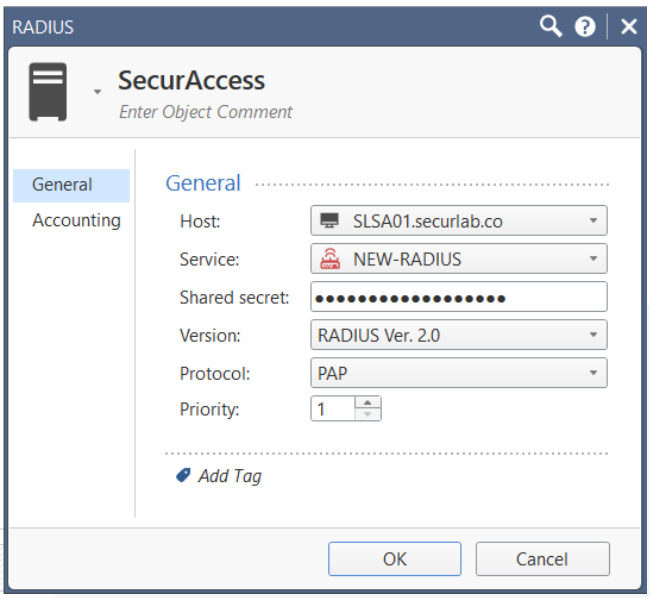
We will need to define a couple of Objects that are specific to the RADIUS and LDAP servers that we will use to check and authenticate the users.
From the Object Category list, select Servers and create a new RADIUS Server





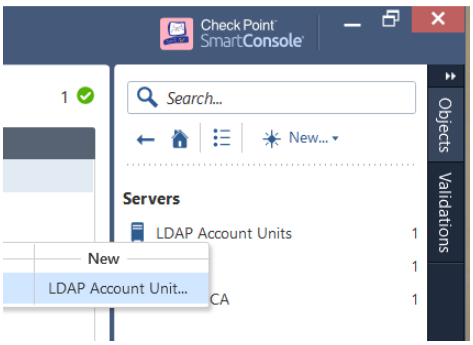
On presentation of the new RADIUS Server Object, complete the following details

Name: Give the Object a new name
Host: Create a Host object that includes the IP address of the SecurAccess Server
Service: Select NEW-RADIUS
Shared Secret: Enter your shared secret as entered in the previous section
Version: Select RADIUS Ver 2.0
Protocol: PAP



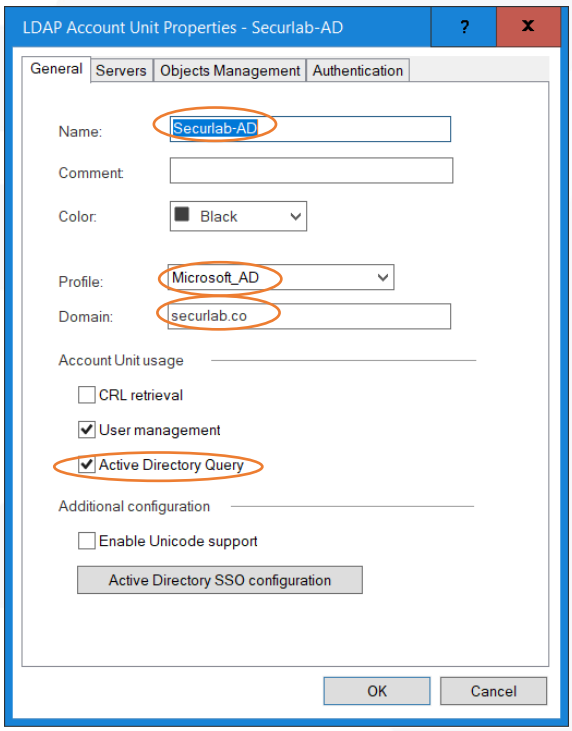
1.44 Setup LDAP – Checkpoint (Smart Console)

So that we do not require individual user accounts to be created on the Checkpoint appliance to match RADIUS authentications, we will create a connection to an LDAP server for the purpose of user matching.
From the Objects list, select LDAP Accounts Unit

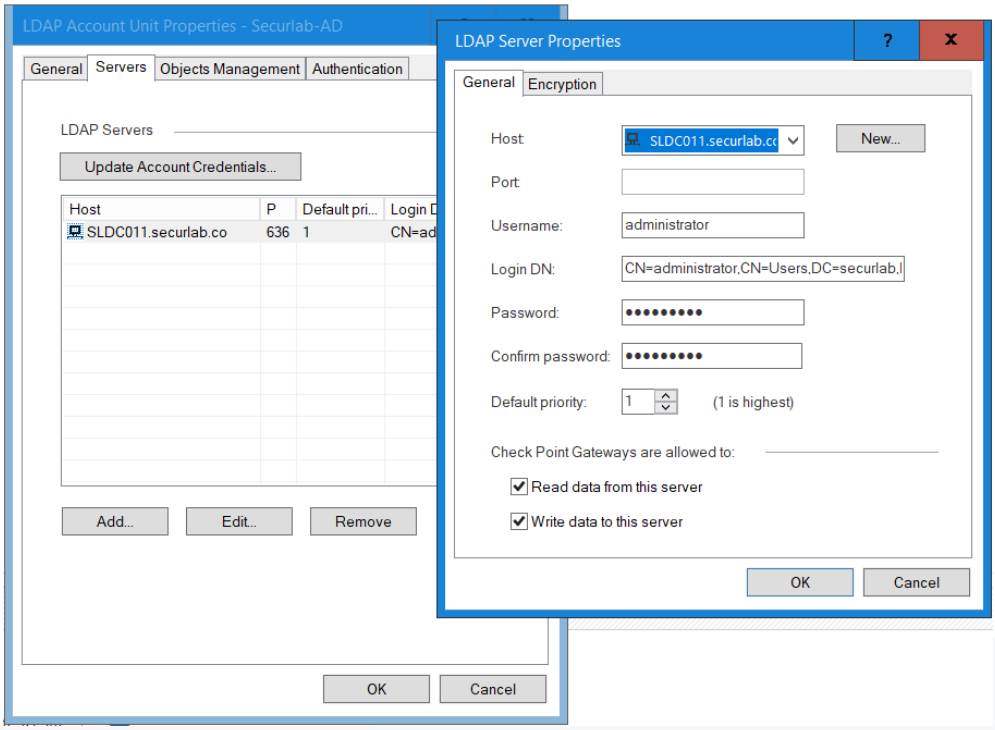


On presentation of the LDAP dialogue box, configure and select the following items on the General tab.

Name: Provide to Server Object with a name
Profile: Select Microsoft_AD
Domain: Active Directory Domain
Account Unit Usage: Make sure User Management and Active Directory Query are selected

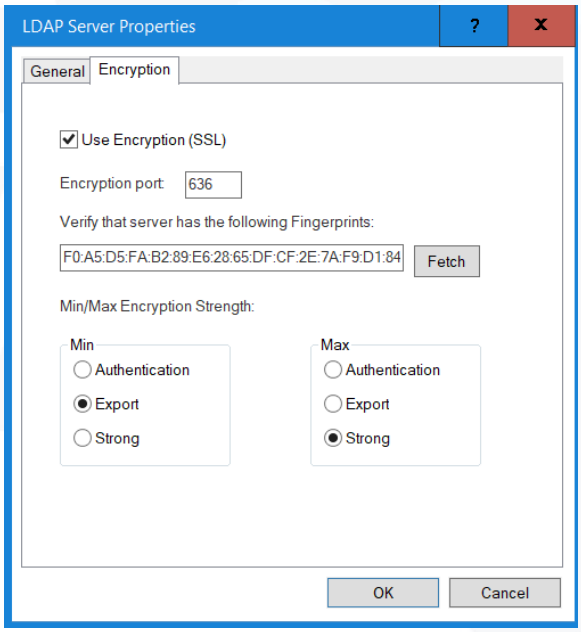


Select the Servers Tab from the dialogue box and select Add to define the LDAP Server properties.



Configure the following details to allow the Checkpoint appliance to query the LDAP server.

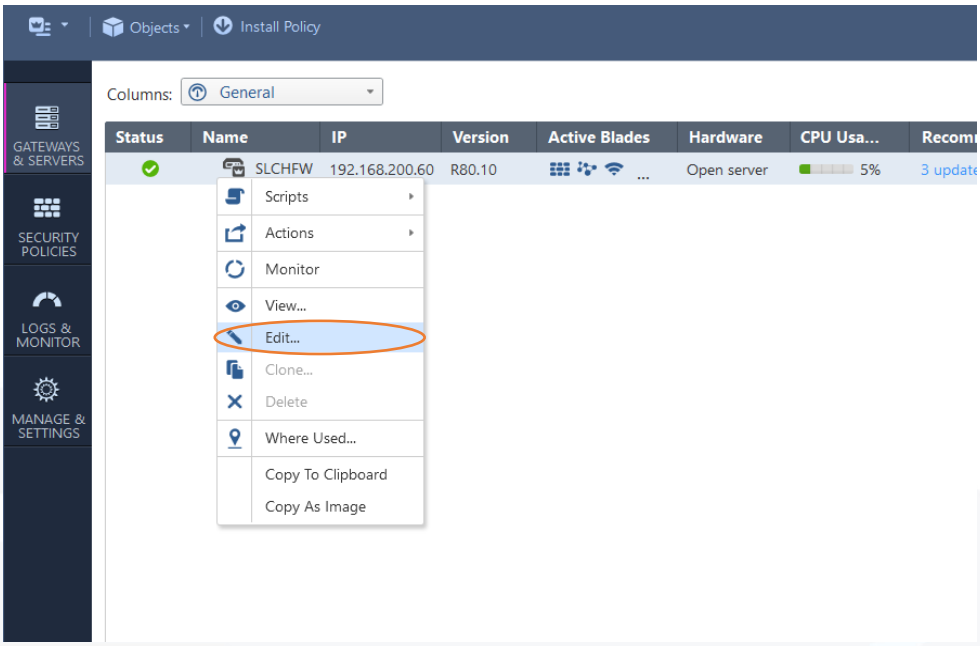
Host: Select or create a New Host (This is Domain Controller you with to query)
Username: An administrator or system account that has rights to query AD
Login DN: Enter the full Distinguished name
Password: Enter Administrator or System account password



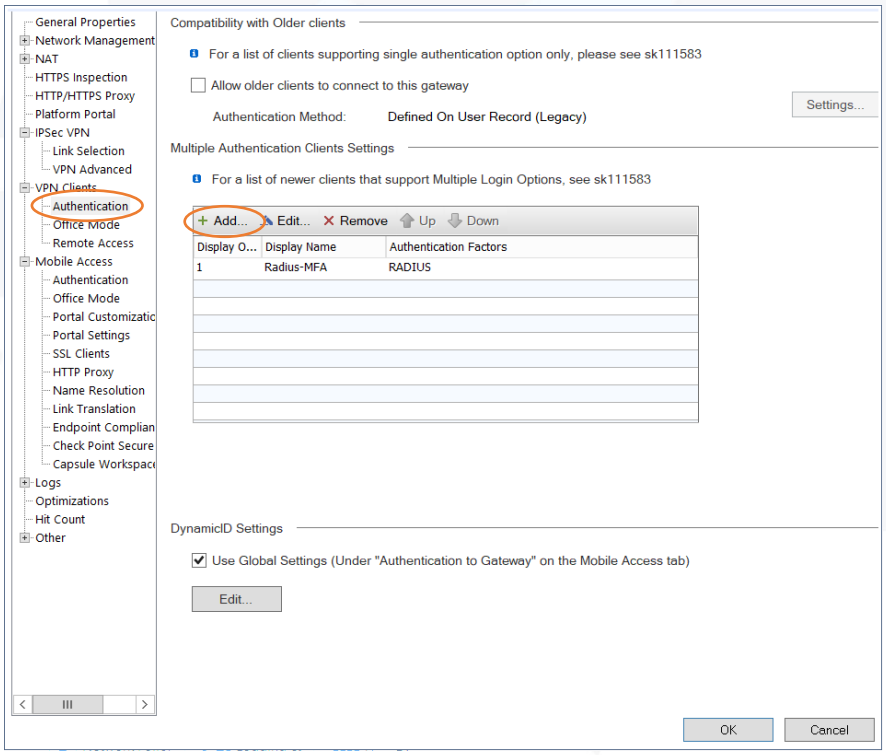
If using SSL, select Use Encryption (SSL) from the Encryption tab and select OK to finish.

1.45 VPN Client – Authentication Policy

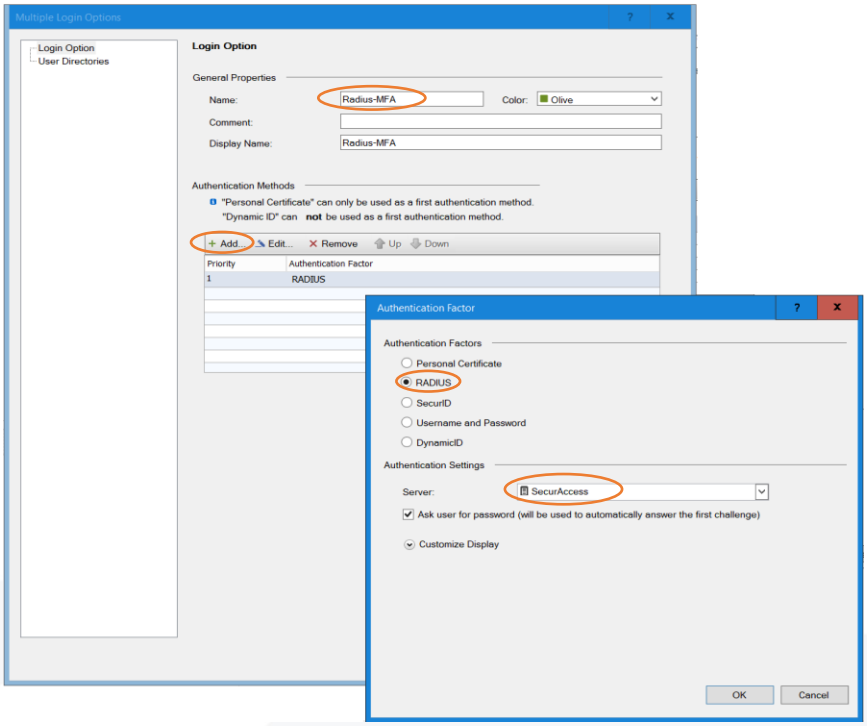
From the Checkpoint Smart Console, right click on the managed gateway and select Edit from the drop-down list.



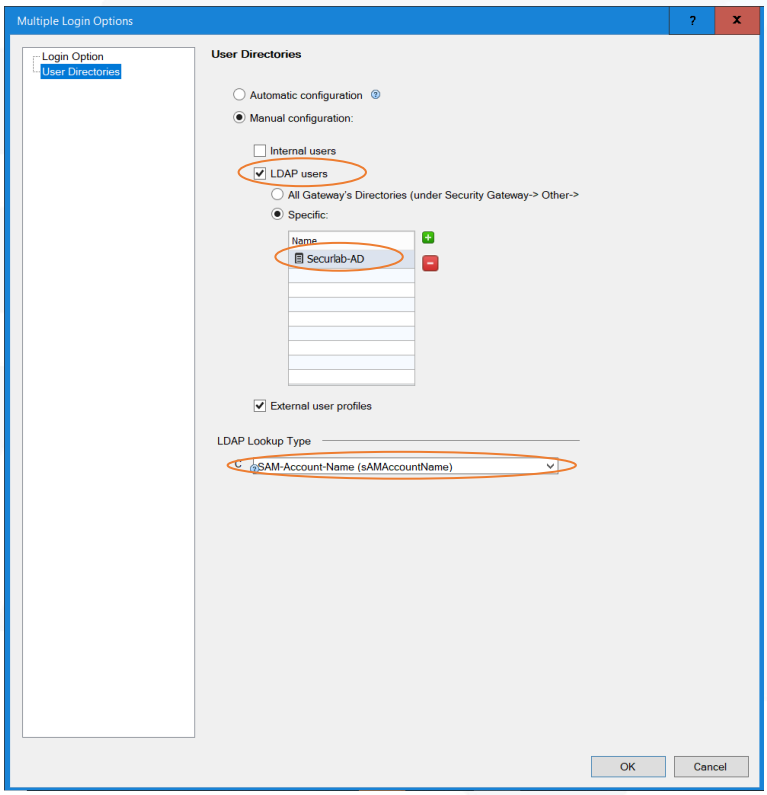
In order to complete the RADIUS configuration, an authentication server needs to be assigned to the VPN client and Mobile Access policy.
From the VPN Clients\Authentication section, select Add to define a RADIUS server profile



Create a name for the new RADIUS Server and select Add to define the configuration details of the server.



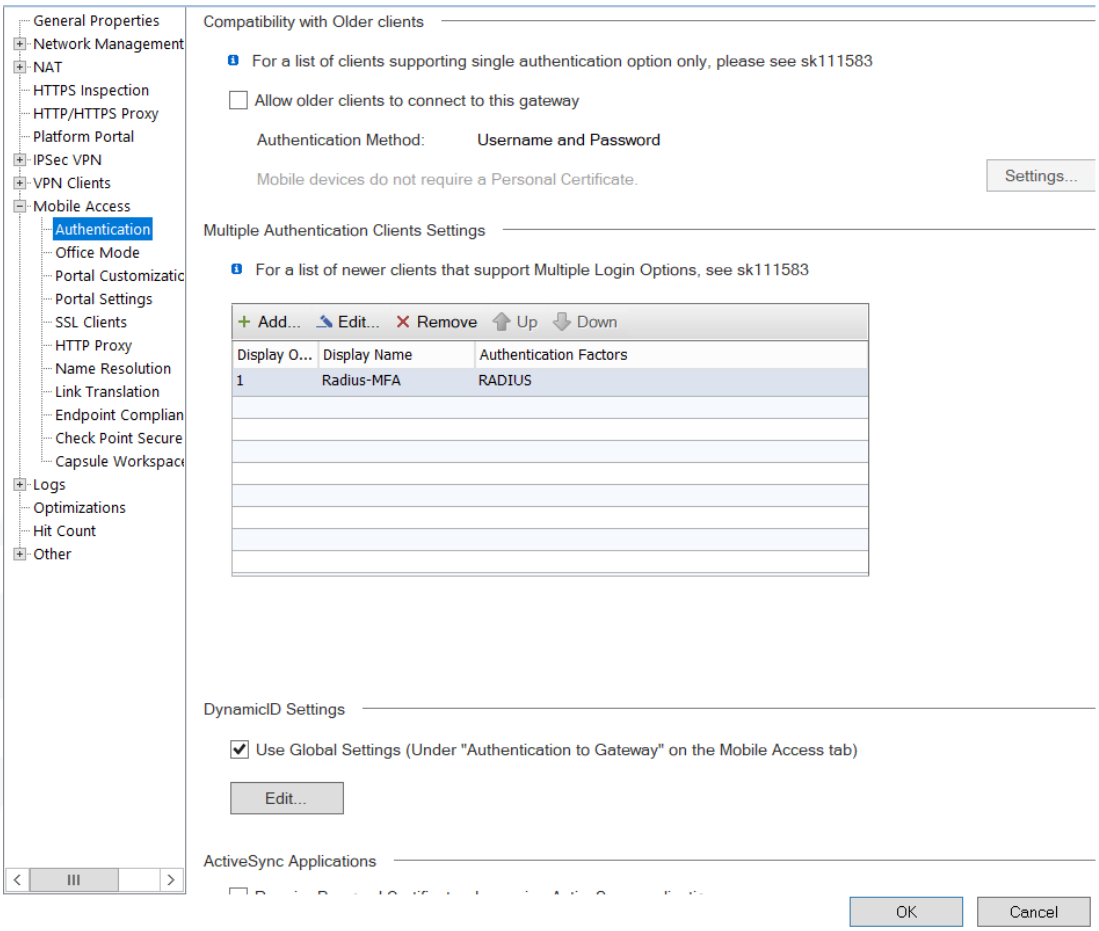
Configure the authentication factor as RADIUS and select the Server created previously under the Checkpoint objects section



On selecting the User Directories tab, make sure the following areas of configured as per the above config.

1.46 Mobile Access – Authentication Policy

In order to complete the RADIUS configuration for the Mobile Access Policy, an authentication server needs to be assigned.
From the Mobile Access\Authentication section, select Add to define a RADIUS server profile and select the previously configured RADIUS profile.

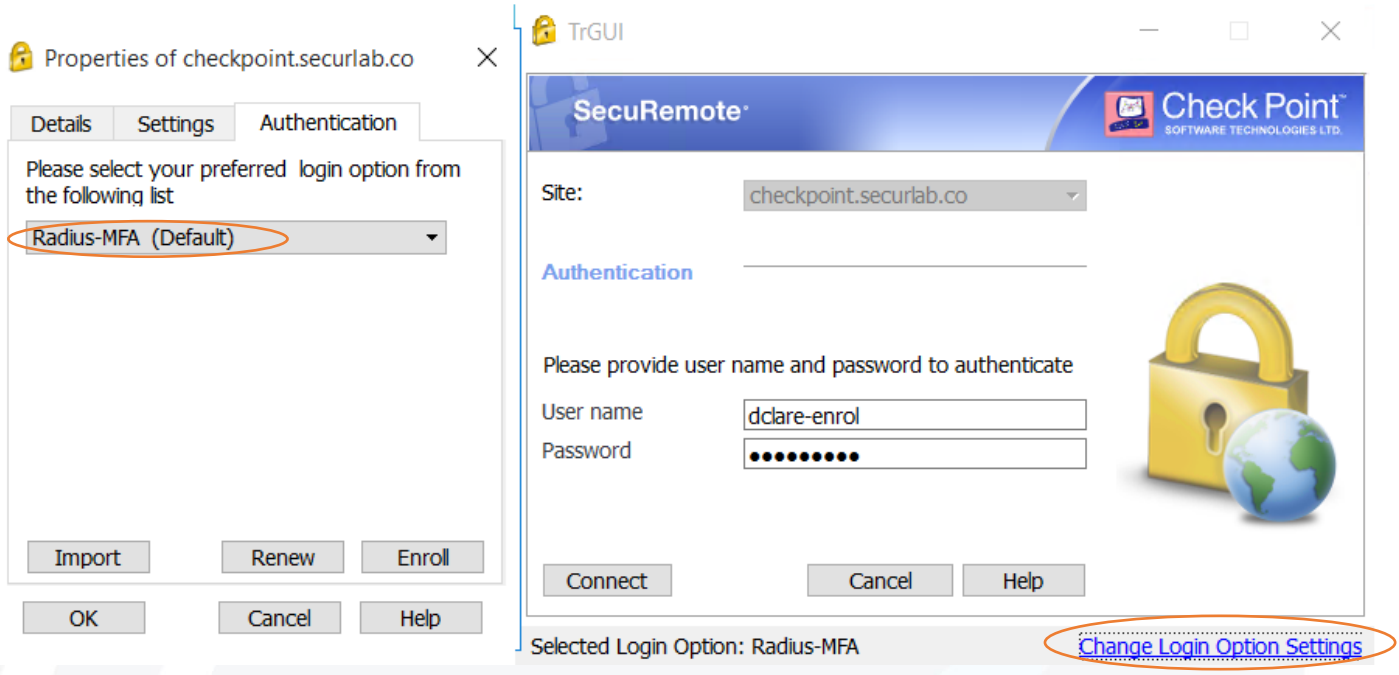


1.5 Checkpoint Endpoint Client

The following section describes steps required to configure the Checkpoint Endpoint client to authenticate with SecurEnvoy's MFA solution.

1.5.1 SecuRemote

- Run the Checkpoint Endpoint Client and change the Login Option Settings.
- Make sure you select the RADIUS profile you configured in the previous section.



Click Connect to establish a connection to the Checkpoint firewall. Dependent on the SecurEnvoy Token type selected by the user, the login screen will present different views

PUSH Notifications

Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012

EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 89 70074522

ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

Sales

E info@SecurEnvoy.com
T +612 9911 7778

USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA – East Coast

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com