SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

Palo Alto Global Protect VPN Integration Guide

PAN-OS 11.0

Global Protect VPN 6.1.0

SecurEnvoy SecurAccess

Index

Index 2
1.0 Prerequisites 3
1.1 Configure Palo Alto GlobalProtect Gateway 4
2.0 Configure SecurEnvoy Radius 10
2.1 Configuration of SecurEnvoy Radius Client (Radius Only Policy) 10
3.0 Test Two-Factor Authentication (GlobalProtect VPN Client) 11
4.0 Notes 13

Palo Alto Global Protect VPN

This document describes how to integrate Palo Alto Global Protect VPN with SecurEnvoy two-factor Authentication solution called 'SecurAccess'

A Virtual Private Network (VPN) uses a public network—such as the Internet—to enable remote users connect securely to the corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as SSH), without the complication of deploying hardware tokens or smartcards.

Two-Factor authentication is provided by the use of (your PIN and your Phone or SecurEnvoy Soft Token app to receive the one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into any LDAP server and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The

Authentication server is directly integrated with LDAP in real time.

The equipment used for the integration process is listed below:

Palo Alto Networks

PAN-OS 11.0

Global Protect VPN – 6.1.0

Microsoft

Microsoft Windows Server 2016 - Windows Server 2021

SecurEnvoy

SecurEnvoy Server

SecurAccess software release v9.x

1.0 Prerequisites

SecurEnvoy Security Server has been installed and configured as per the Installation document. If firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Palo Alto Networks Firewall(s), additional open ports will be required.

1.1 Configure Palo Alto GlobalProtect Gateway

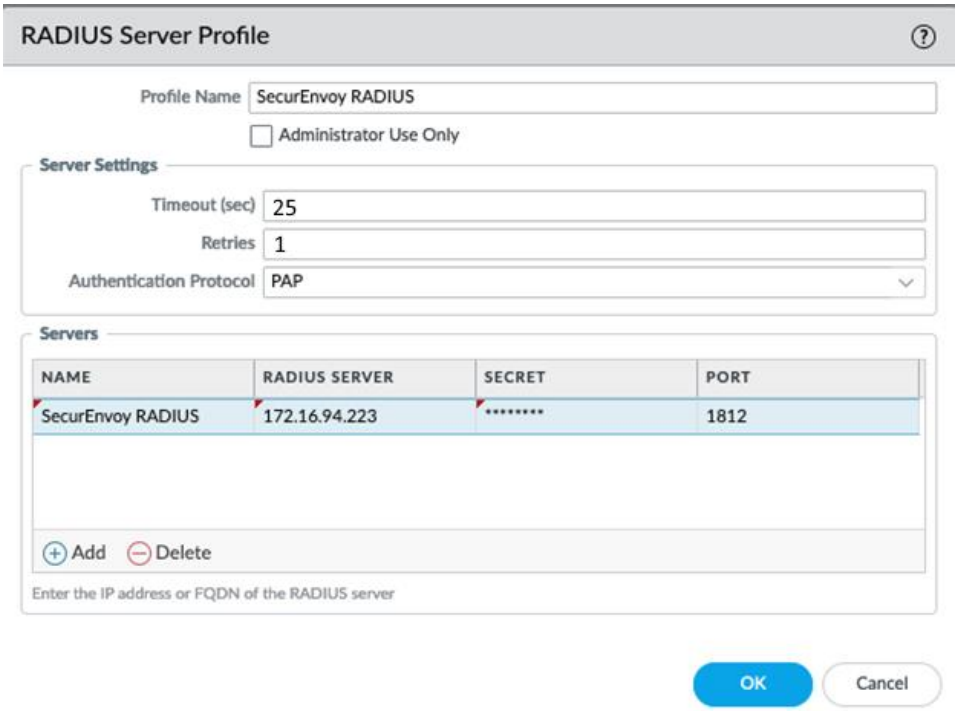
1) Log onto the Palo Alto Admin interface
2) Create a Radius Server Profile by navigating to **Device > Server Profile > Radius > click Add**.
3) In the **Name** field, enter SecurEnvoy RADIUS, and in the **Timeout** field enter 10.
4) In the Authentication Protocol field select: PAP.
5) Add Server to the profile by clicking Add on the bottom of the profile.

Name = SecurEnvoy RADIUS

IP address = IP address of the SecurEnvoy Server

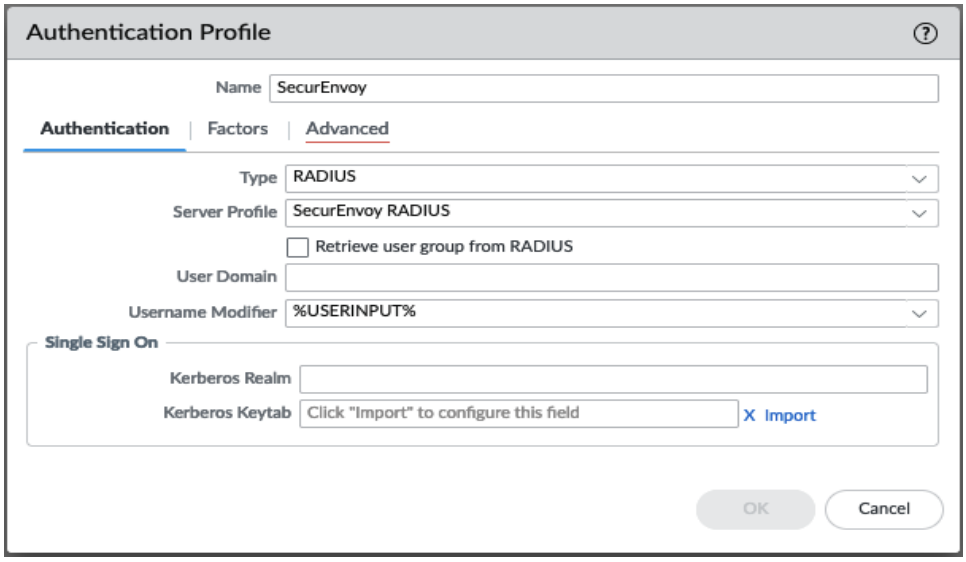
Secret = Secret shared between Palo Alto and SecurEnvoy Radius

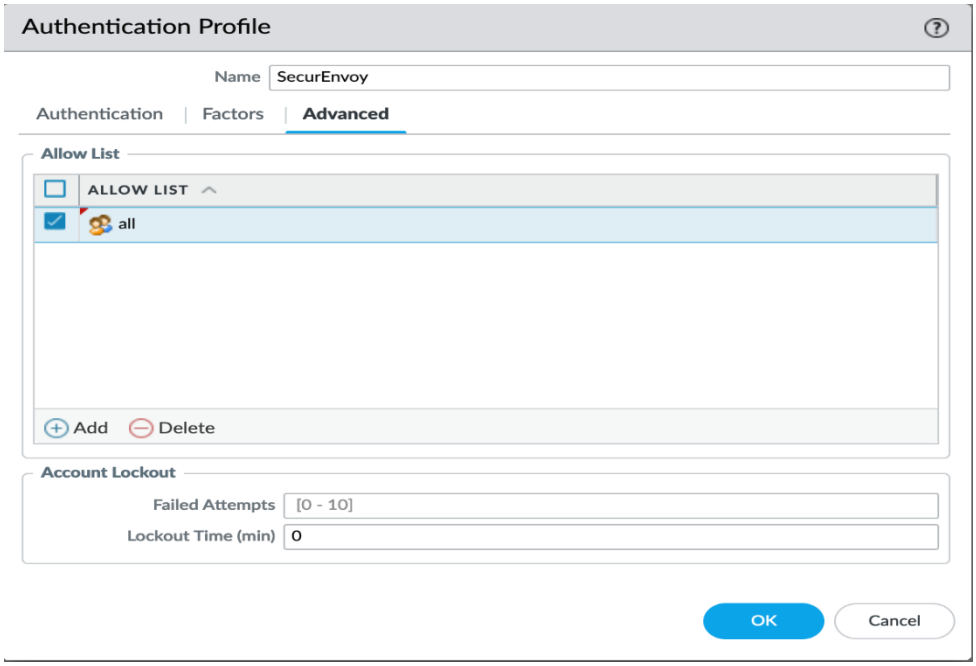
Port = 1812 (UDP)



Click **OK** to save the RADIUS server profile.

6) On the **Device** tab, navigate to **Authentication Profile**
7) Click **Add** to add a new profile.
8) Enter a name for the new Authentication Profile and configure the settings.
9) For **Name**, enter: **SecurEnvoy.**
10) For **Authentication**, select **Radius** as the authentication method.
11) Under **Server Profile**, select **SecurEnvoy Radius**
12) Under **Advanced** you see an empty allowlist, click **Add** here and select **All.**

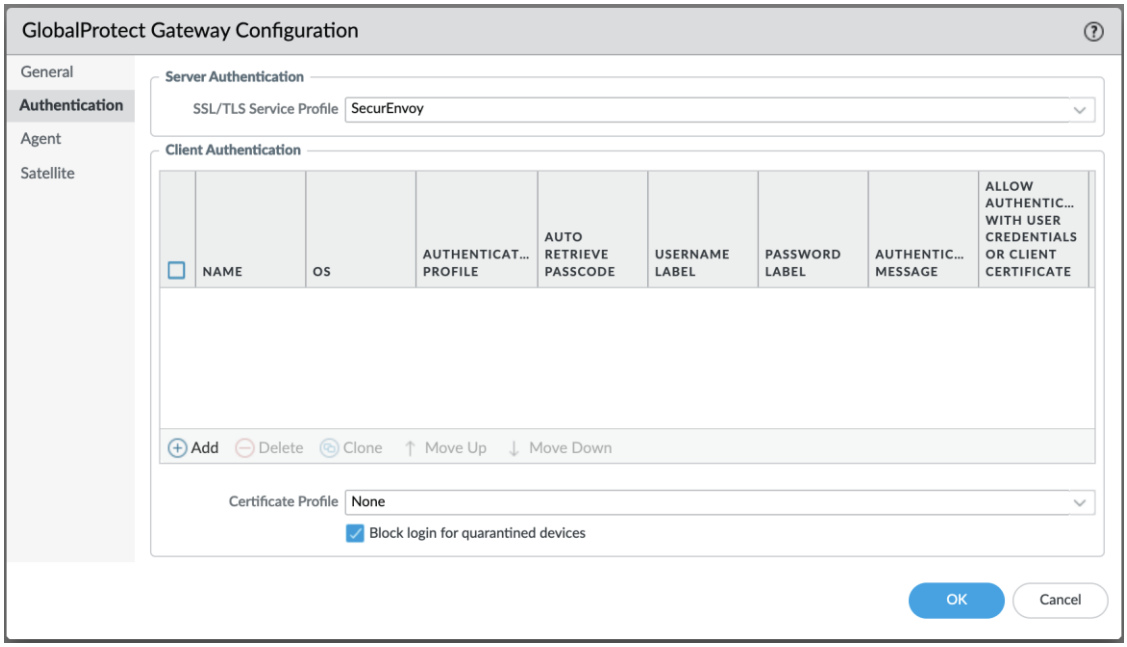




Click **OK** to save.

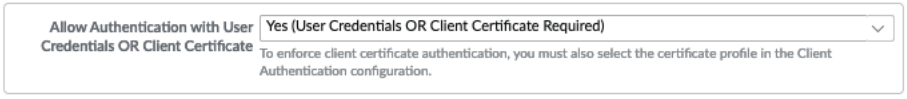
On the **Network** tab, navigate to **GlobalProtect** then **Gateways**.

Click on your configured **GlobalProtect Gateway** and see the properties window.
In the GlobalProtect Gateway **Authentication** properties tab, under **Client Authentication** click on **Add**

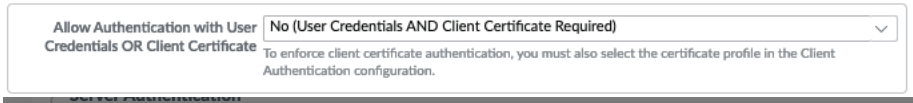


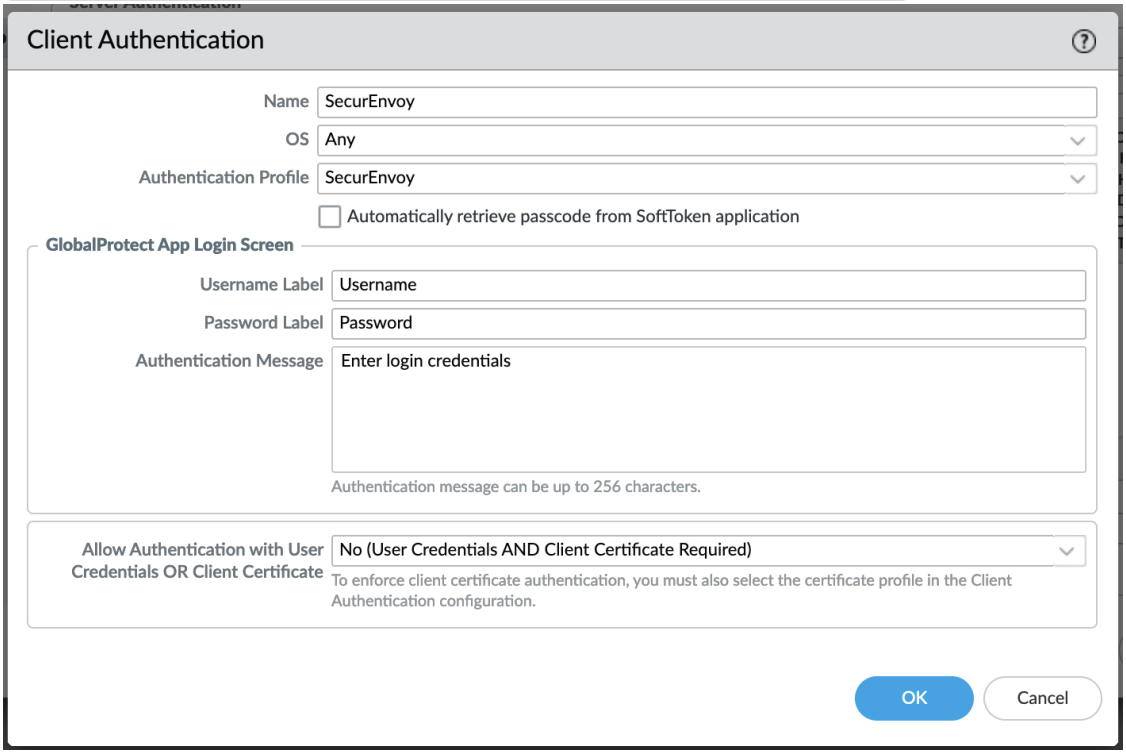
Name = SecurEnvoy
Select Authentication Profile = SecurEnvoy from the drop down list

Note: you need to make a selection here as well, will credentials be enough OR a client certificate



Or enforce BOTH credentials AND a Client Certificate





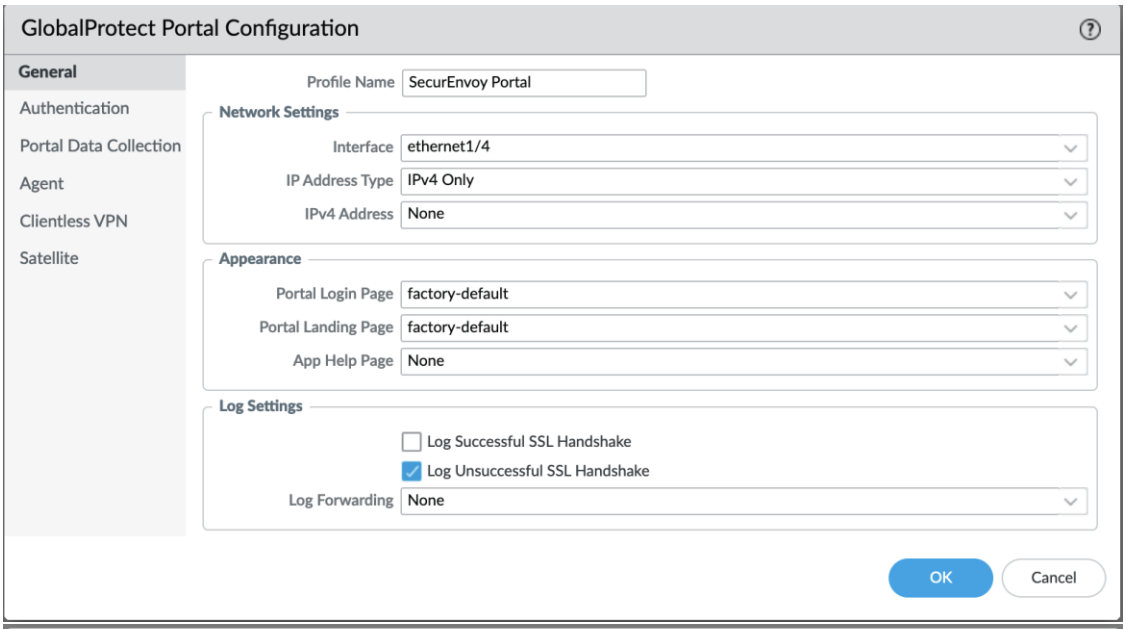
Click **OK** to save.

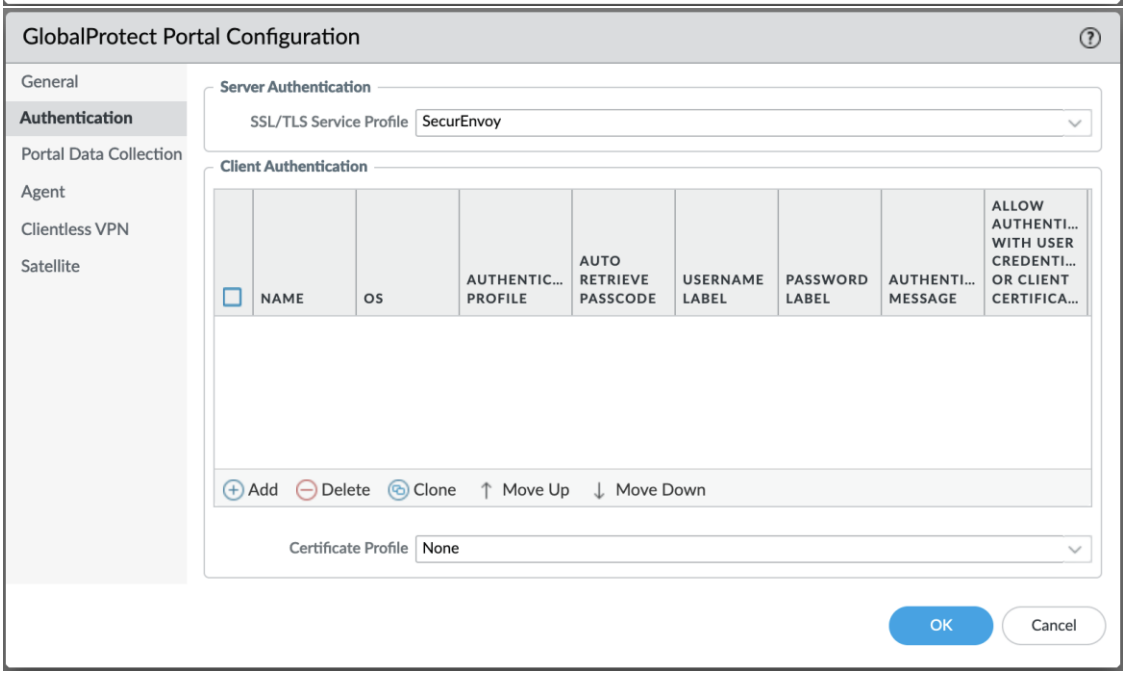
On the **Network** tab, navigate to **GlobalProtect** then **Portal**.

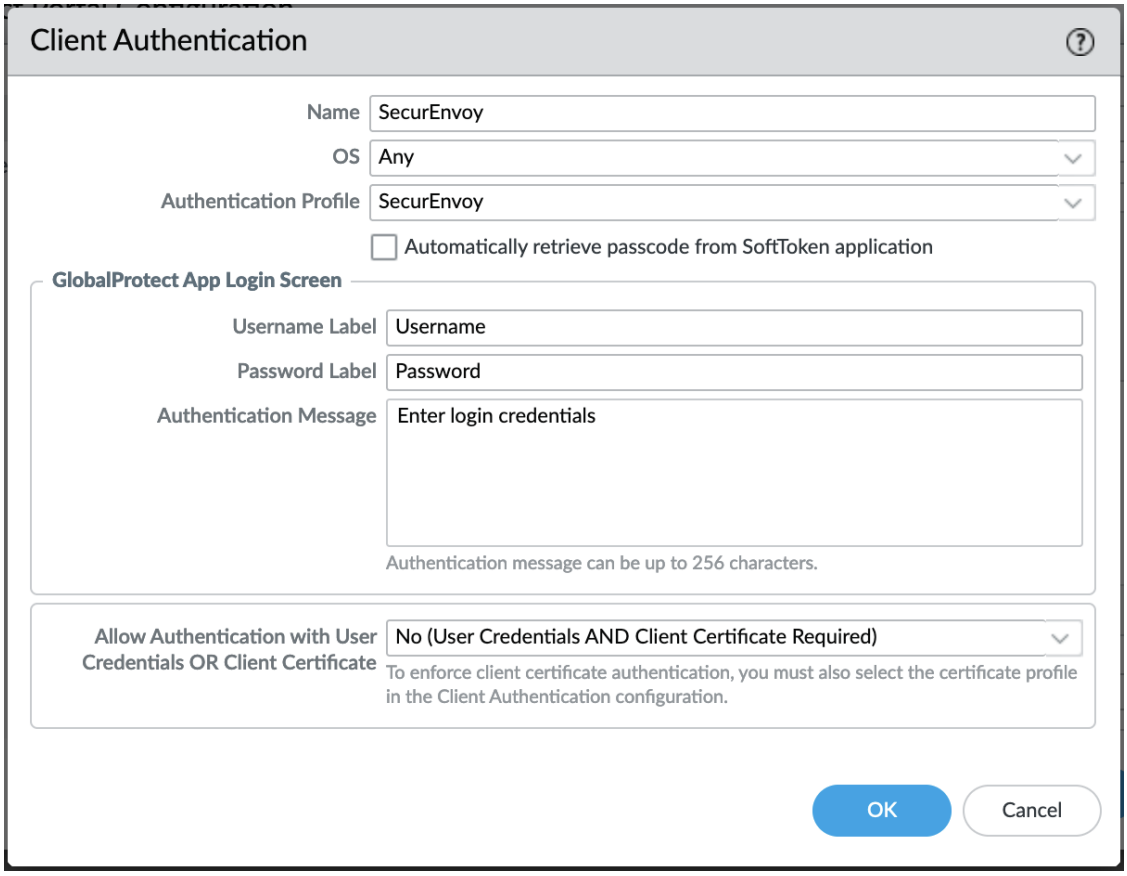
Click on your configured **GlobalProtect Portal** to see the properties window.

Click on the **Authentication** tab on the left.

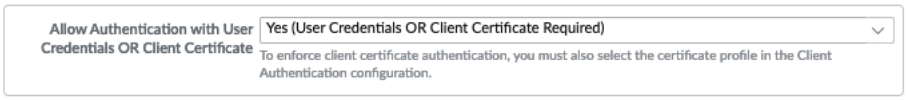
section of the GlobalProtect **Portal Configuration** properties tab, select the **SecurEnvoy** Authentication Profile from the drop-down list.



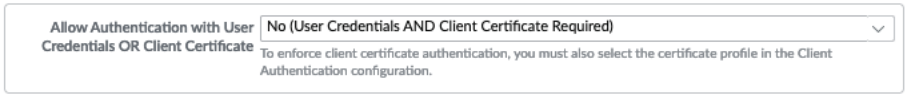


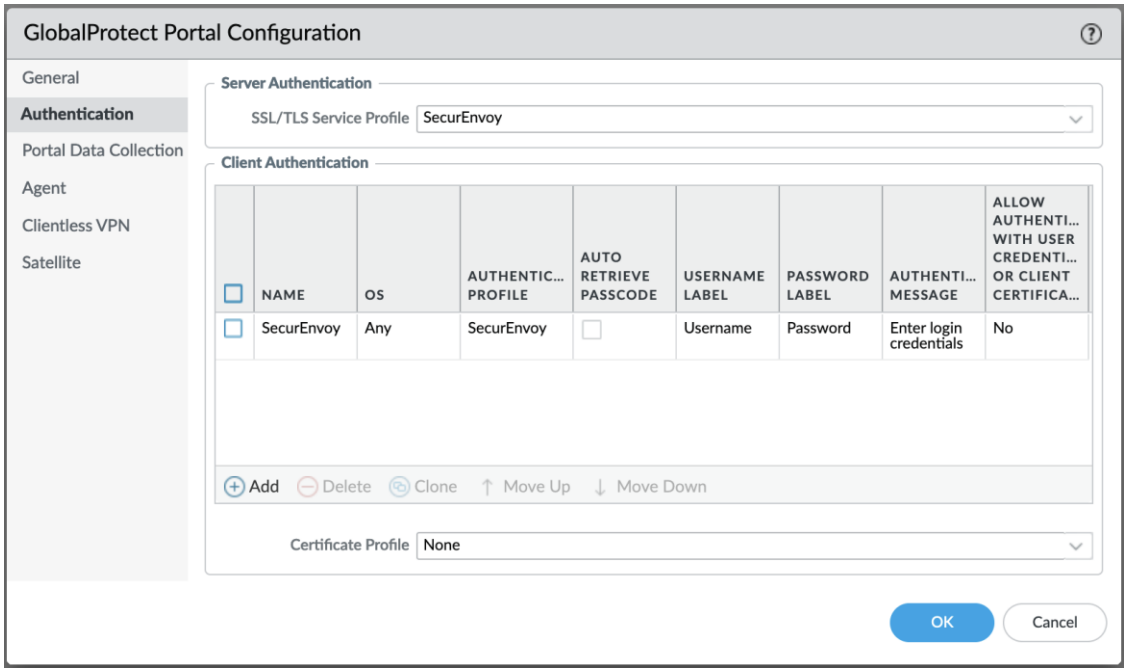


Note: you need to make a selection here as well, will credentials be enough OR a client certificate



Or enforce BOTH credentials AND a Client Certificate





Click **OK** to save.

7) Activate the **GlobalProtect** configuration by clicking **Commit** in the upper-right corner of the administrative interface.

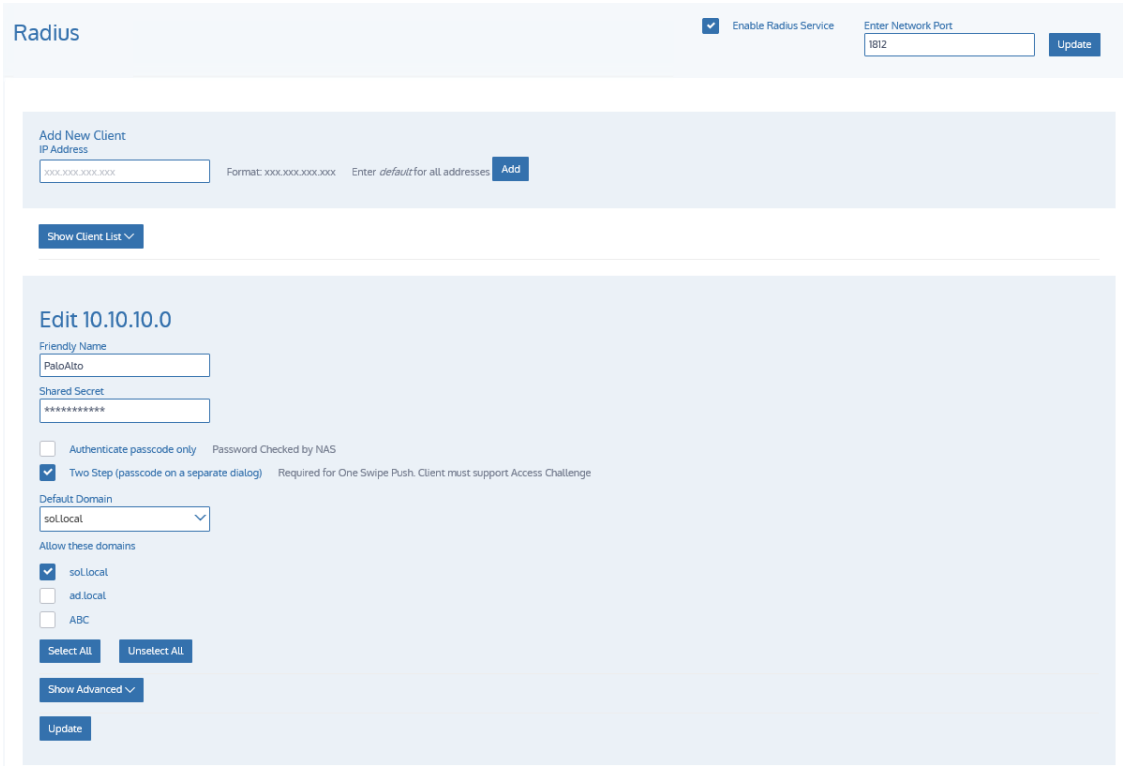
2.0 Configure SecurEnvoy Radius

SecurEnvoy supplies the second factor of authentication in the form of a one time passcode (OTP). This is sent to the user via their preferred authentication method.

2.1 Configuration of SecurEnvoy Radius Client (Radius Only Policy)

The Radius only policy is preferred when checking against user information in the form of:

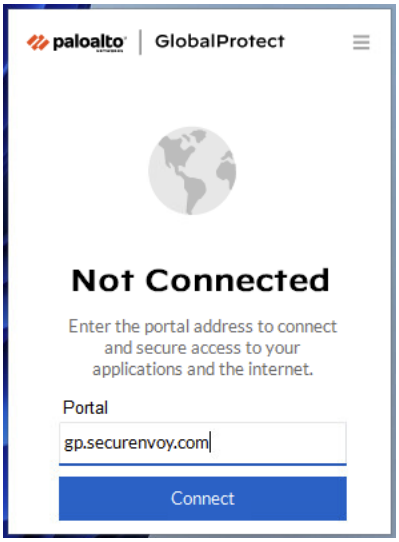
- Username (SecurEnvoy Auth)
- Password (SecurEnvoy Auth)
- Passcode (SecurEnvoy Auth)



1. Log onto the SecurEnvoy Admin console
2. Select the “Radius” Tab
3. To configure a new Radius client, enter the IP address of the Palo Alto device in the “Add New Client IP Address” field and select “Add”.
4. Enter a Friendly name: - Palo Alto?
5. Enter the Shared Secret (same as the Palo Alto Radius setting)
6. Uncheck “Authenticate passcode Only.
7. Click the **Check** box “Passcode prompt is on a separate dialog”.
8. Click **“Update”** to confirm settings.

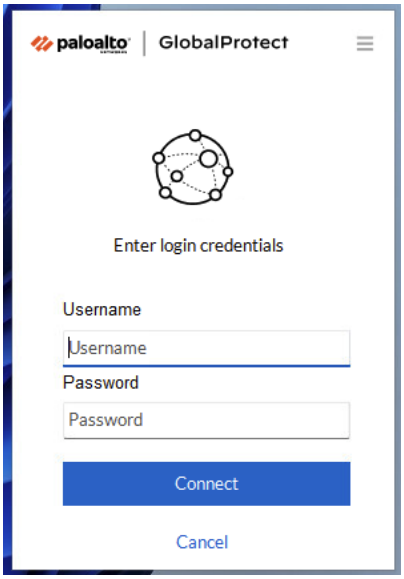
3.0 Test Two-Factor Authentication (GlobalProtect VPN Client)

1. Launch the GlobalProtect app by clicking the system tray icon. Then enter the Global Protect Portal name (DNS name pointing to the IP address of the Portal) and press connect

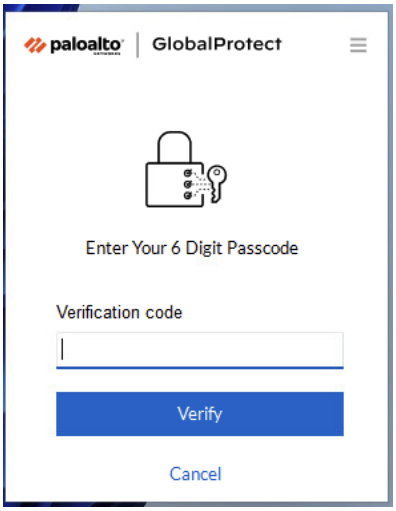


2. Select “Connect”.

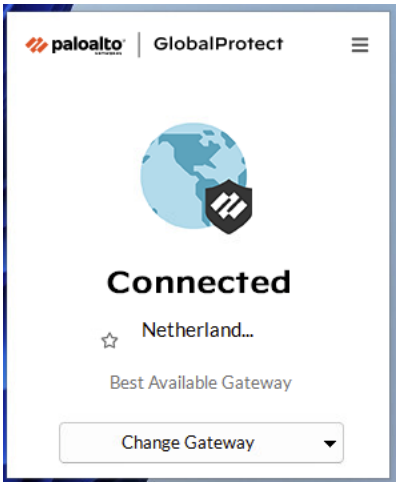
3. At the prompt, enter your **Username** and **Password.**



4. The user is then prompted to enter their Passcode (OTP) from SecurEnvoy to complete the authentication process.



5. Authentication process complete.



4.0 Notes