



## Palo Alto Global Protect VPN Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	<a href="http://www.securenvoy.com">www.securenvoy.com</a>	0845 2600010
	Merlin House Brunel Road Theale Reading RG7 4AB	
Ryan Sheridan	<a href="mailto:rsheridan@securenvoy.com">mailto:rsheridan@securenvoy.com</a>	



## **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.

SecurEnvoy Security Server can be configured in such a way that it can use the existing LDAP password. Utilizing the LDAP password as the PIN, allows the User to enter their UserID, Domain password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. It provides a seamless login into the Windows Server environment by entering three pieces of information. SecurEnvoy utilizes a web GUI for configuration. All notes within this integration guide refer to this type of approach.

### **The equipment used for the integration process is listed below:**

#### **Palo Alto**

Palo Alto Global Protect VPN - PAN-OS 5.0.6 to 7.0.0 and GlobalProtect 1.2.5.

#### **Microsoft**

Microsoft Windows Server 2012, Windows Server 2012 R2

#### **SecurEnvoy**

SecurEnvoy Server

SecurAccess software release v7.3.501

## Index

Palo Alto Global Protect VPN .....	1
Authenticating Users Using SecurAccess Server by SecurEnvoy .....	1
Index .....	3
1.0 Prerequisites .....	3
1.1 Configure Palo Alto GlobalProtect Gateway .....	4
2.0 Configuration of SecurEnvoy .....	6
3.0 Test Two-Factor Authentication .....	7
4.0 Notes .....	9

### 1.0 Prerequisites

*SecurEnvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory. If firewalls are between the SecurEnvoy Security server, Active Directory servers, and the ADFS server(s), additional open ports will be required.*

#### Note

**To avoid duplicating a passcode authentication the bit-length of the CSR private key SSL should be 2048.**

The following table shows what token types are supported.

Token Types Supported	
Real Time SMS or Email	✓
Preload SMS or Email	✓
Soft Token Code	✓
Soft Token Next Code	✓
Voice Call	✓

Token Types Not Supported	
OneSwipe QRCode	✗

## 1.1 Configure Palo Alto GlobalProtect Gateway

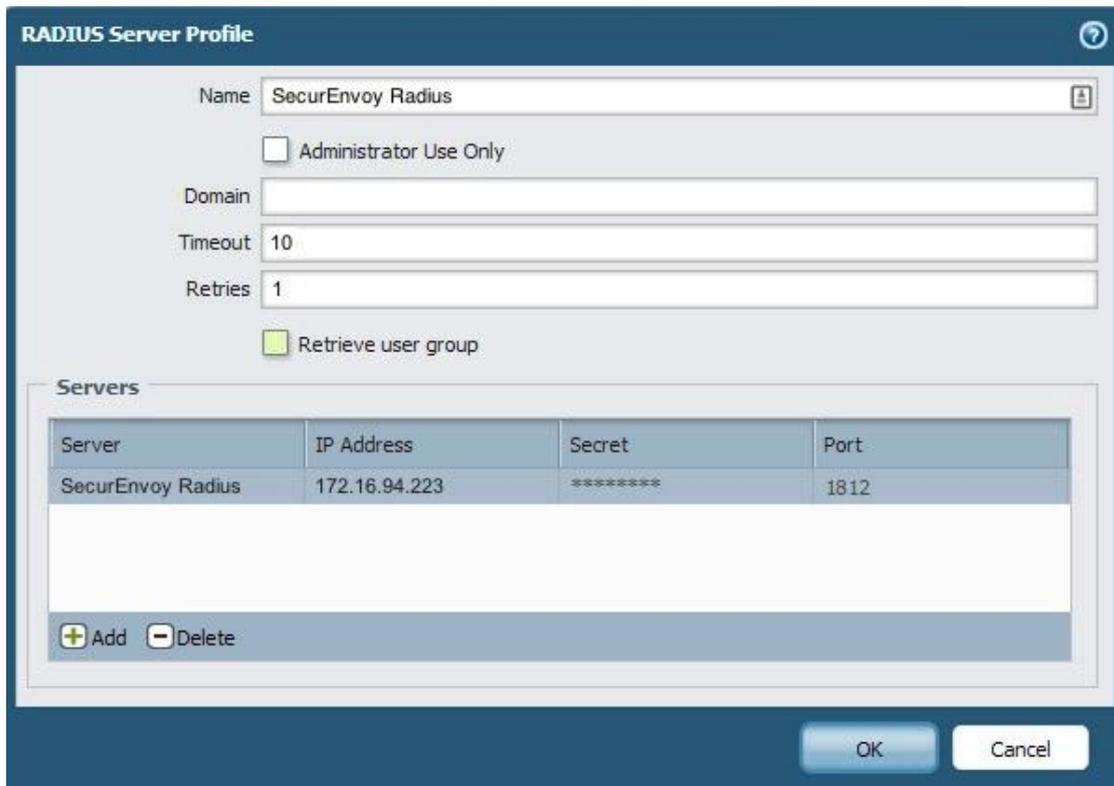
- 1) Log onto the Palo Alto Admin interface
- 2) Create a Radius Server Profile by navigating to **Server Profile > Radius > click Add**.
- 3) In the **Name** field, enter SecurEnvoy RADIUS, and in the **Timeout** field enter 10.
- 4) Add Server to the profile by clicking Add on the bottom of the profile.

**Name** = SecurEnvoy RADIUS

**IP address** = IP address of the SecurEnvoy Server

**Secret** = Secret shared between Palo Alto and SecurEnvoy Radius

**Port** = 1812 (UDP)

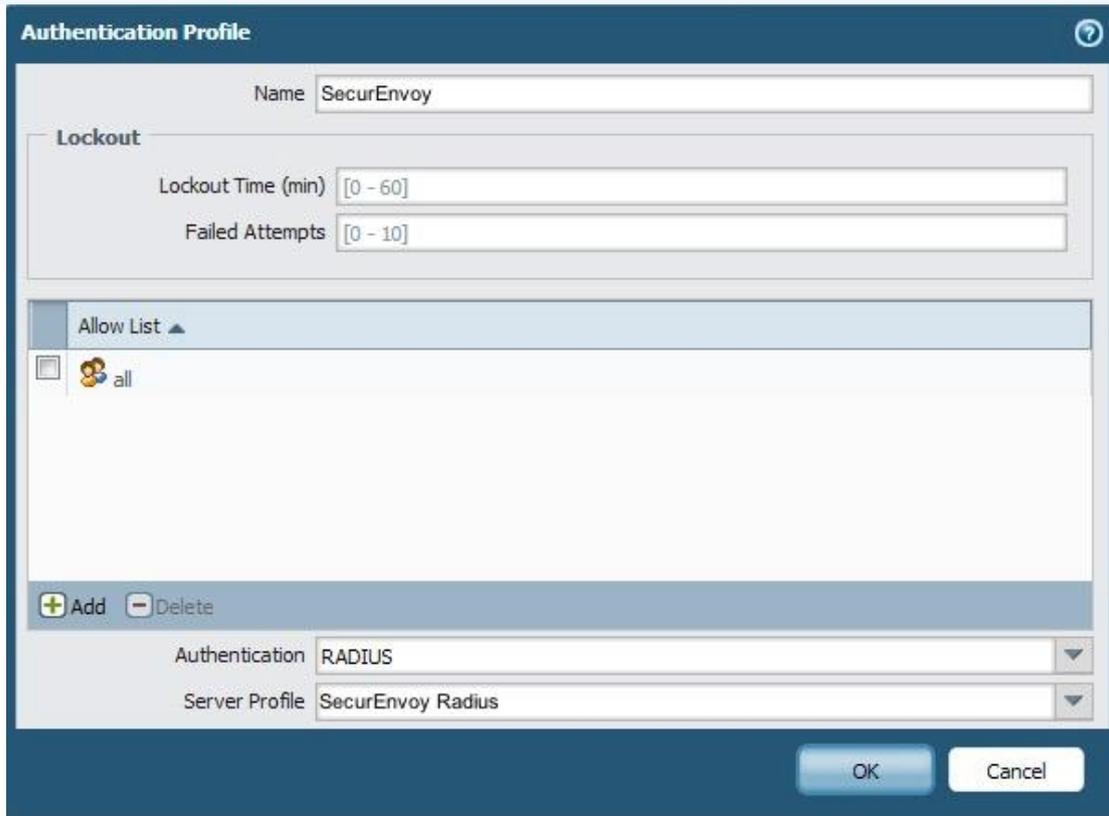


The screenshot shows the 'RADIUS Server Profile' configuration window. The 'Name' field is set to 'SecurEnvoy Radius'. The 'Administrator Use Only' checkbox is unchecked. The 'Domain' field is empty. The 'Timeout' field is set to '10'. The 'Retries' field is set to '1'. The 'Retrieve user group' checkbox is unchecked. Below these fields is a 'Servers' table with one entry: 'SecurEnvoy Radius' with IP Address '172.16.94.223', Secret '\*\*\*\*\*', and Port '1812'. At the bottom of the table are '+ Add' and '- Delete' buttons. The window has 'OK' and 'Cancel' buttons at the bottom right.

Server	IP Address	Secret	Port
SecurEnvoy Radius	172.16.94.223	*****	1812

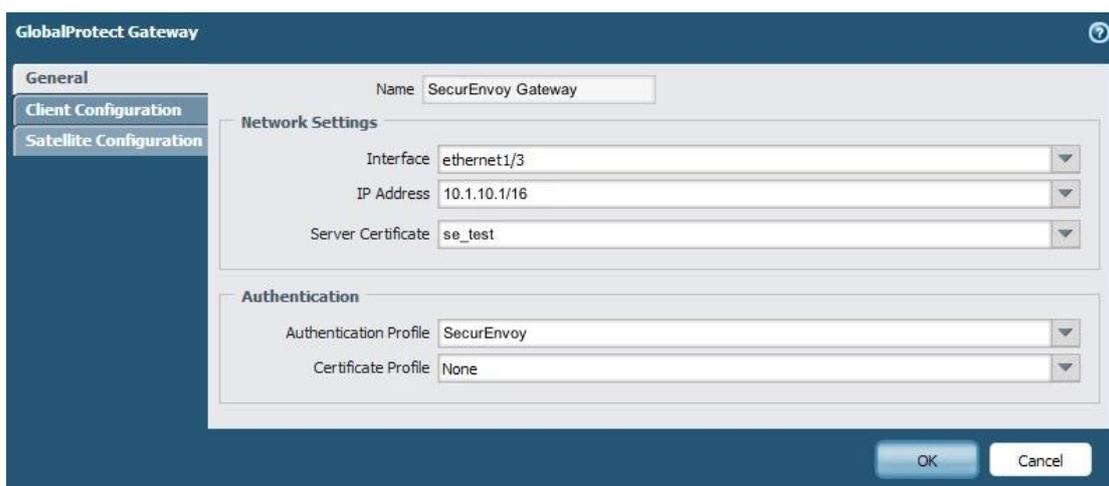
Click **OK** to save the RADIUS server profile.

- 5) On the **Device** tab, navigate to **Authentication Profile**.
- 6) Click **Add** to add a new profile.
- 7) Enter a name for the new Authentication Profile and configure the settings.
- 8) For **Name**, enter: SecurEnvoy
- 9) For **Authentication**, select **Radius** as the authentication method.
- 10) Under **Server Profile**, select SecurEnvoy Radius, and



Click **OK** to save.

- 11) On the **Network** tab, navigate to **GlobalProtect** then **Gateways**.
- 12) Click on your configured **GlobalProtect Gateway** and see the properties window.
- 13) In the GlobalProtect Gateway **General** properties tab, under the **Authentication** section, select the **SecurEnvoy** authentication profile created earlier from the drop-down list.



Click **OK** to save.

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



- 15) Click on your configured **GlobalProtect Portal** to see the properties window.
- 16) In the **Authentication** section of the GlobalProtect **Portal Configuration** properties tab, select the **SecurEnvoy** Authentication Profile from the drop-down list.

The screenshot shows the 'GlobalProtect Portal' configuration window. The 'Portal Configuration' tab is selected. The 'Name' field is set to 'SecurEnvoy Portal'. Under 'Network Settings', the 'Interface' is 'ethernet1/3', 'IP Address' is '10.1.10.1/16', and 'Server Certificate' is 'se\_test'. Under 'Authentication', the 'Authentication Profile' is 'SecurEnvoy', 'Client Certificate' is 'None', and 'Certificate Profile' is 'None'. Under 'Appearance', both 'Custom Login Page' and 'Custom Help Page' are set to 'factory-default'. 'OK' and 'Cancel' buttons are at the bottom right.

Click **OK** to save.

- 17) Save the **GlobalProtect** configuration. Click **Commit** in the upper-right corner of the Palo Alto administrative interface.

## 2.0 Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can be set up to use the existing Windows password as the PIN component. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP), which is sent to the user's SecurEnvoy mobile soft token application

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click the **"Radius"** tab

TRIAL ENDS IN 1482 DAYS 282 FREE SMS WEB TEXTS LEFT

SecurEnvoy Security Server Admin

License CustomerID 10000  
Access/Password:2 of 500  
SecurMail:1 of 500  
ICE:0 of 100 (29 days left)

Config Radius SecurMail Log Viewer Users Reporting Alerting Help **Log Out**

Radius License Expires 1st Jan 2020

**Network Access Server (NAS)**

127.0.0.1  
 172.16.94.227

**Delete Selected**

**NAS IP Address** 172.16.94.227 Format xxx.xxx.xxx.xxx or default for undefined IP's

**Shared Secret** \*\*\*\*\*

Authenticate passcode only  Password Checked by NAS

Passcode prompt is on a separate dialog  Requires Access Challenge

Default Domain testdomain.local Allow these  testdomain.local domains

Only allow users in LDAP group (nested ) **Change Group**

Leave group blank to authenticate all users

Override customer name in SMS message with  Max 20  
Leave blank to use default

Pass Back Data To Radius Client in Attribute 25

No information is passed back  
 Password is passed back  
 LDAP group members (nested ) (return distinguished names )  
 User's Distinguished Name

Trusted Networks (no 2FA required)

Blocked Networks (black listed IP's)

Must send IP address in attribute 31 (Example 10.\* 172.16.\* 192.168.1.\* 192.168.5.5)

**Update** **New**

2013 Copyright SecurEnvoy. All rights reserved Integration Guides FAQ Version 7.3.501

Enter IP address and Shared secret for the Palo Alto device that wish to use SecurEnvoy Two-Factor authentication.

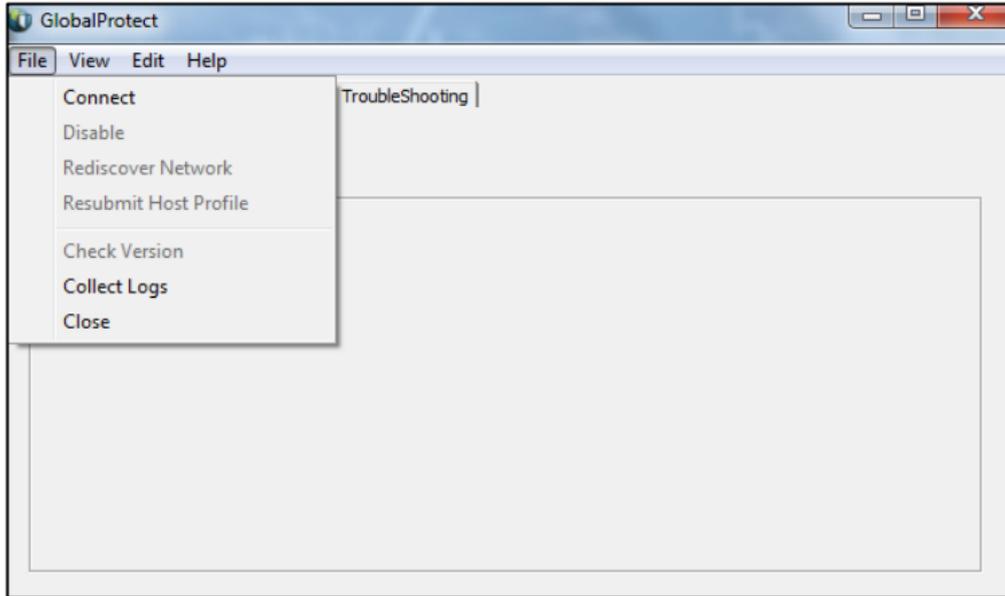
Click to **Check** the box "Passcode prompt is on a separate dialog".

Click **"Update"** to confirm settings.

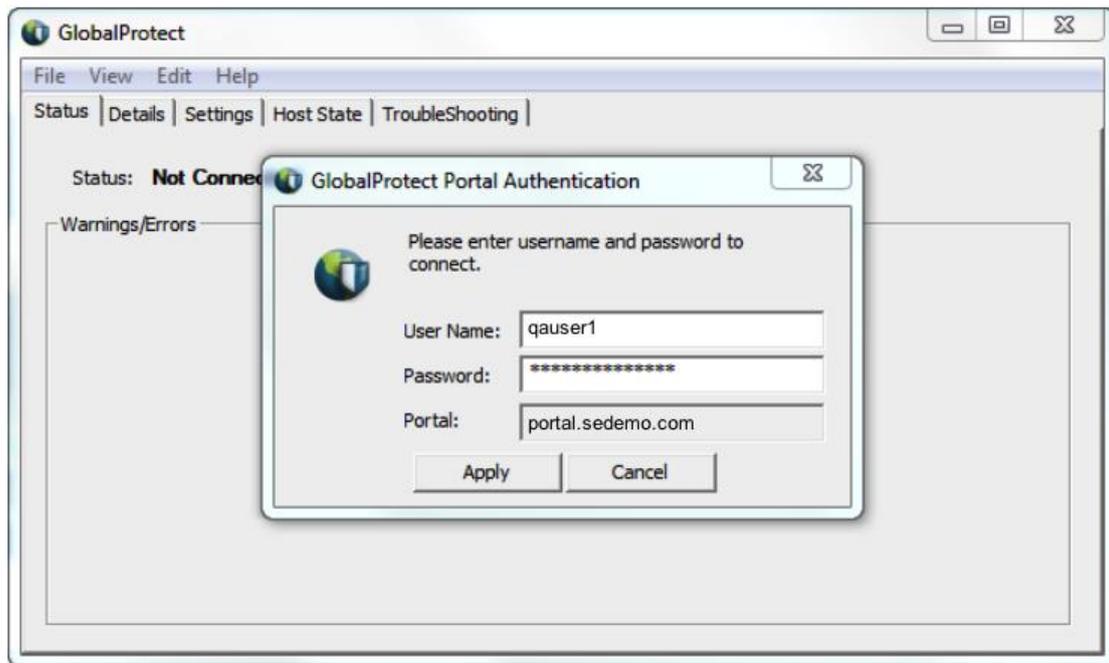
Click **"Logout"** when finished. This will log out of the Administrative session.

### 3.0 Test Two-Factor Authentication

- 1) A user opens the GlobalProtect client, and then clicks **File**, then **Connect**.



2) The user enters their **LDAP Username / Password** for the GlobalProtect **Portal** Authentication



3) The user is then prompted to enter their Passcode (OTP) from their SecurEnvoy soft token.



(Passcode delivered via Soft Token in this example)

4) Finally, the user is successfully connected.

#### 4.0 Notes