Palo Alto Networks Integration

Contents

Introduction

This document describes steps to configure a Palo Alto Networks Firewall with Swivel as the authentication server using RADIUS with SMS, Mobile Phone Client, and Taskbar Authentication. The solution is tested with a Palo Alto Networks GlobalProtect client.

Prerequisites

Palo Alto Networks Firewall

Palo Alto Networks documentation

Swivel 3.x, 3.5 or later for RADIUS groups

Baseline

Palo Alto Networks PA-2050

Palo Alto Networks Software 4.1.6

Palo Alto Networks GlobalProtect Client 1.14 and 1.15

Swivel 3.8

Architecture

The Palo Alto Networks makes authentication requests against the PINsafe server by RADIUS.

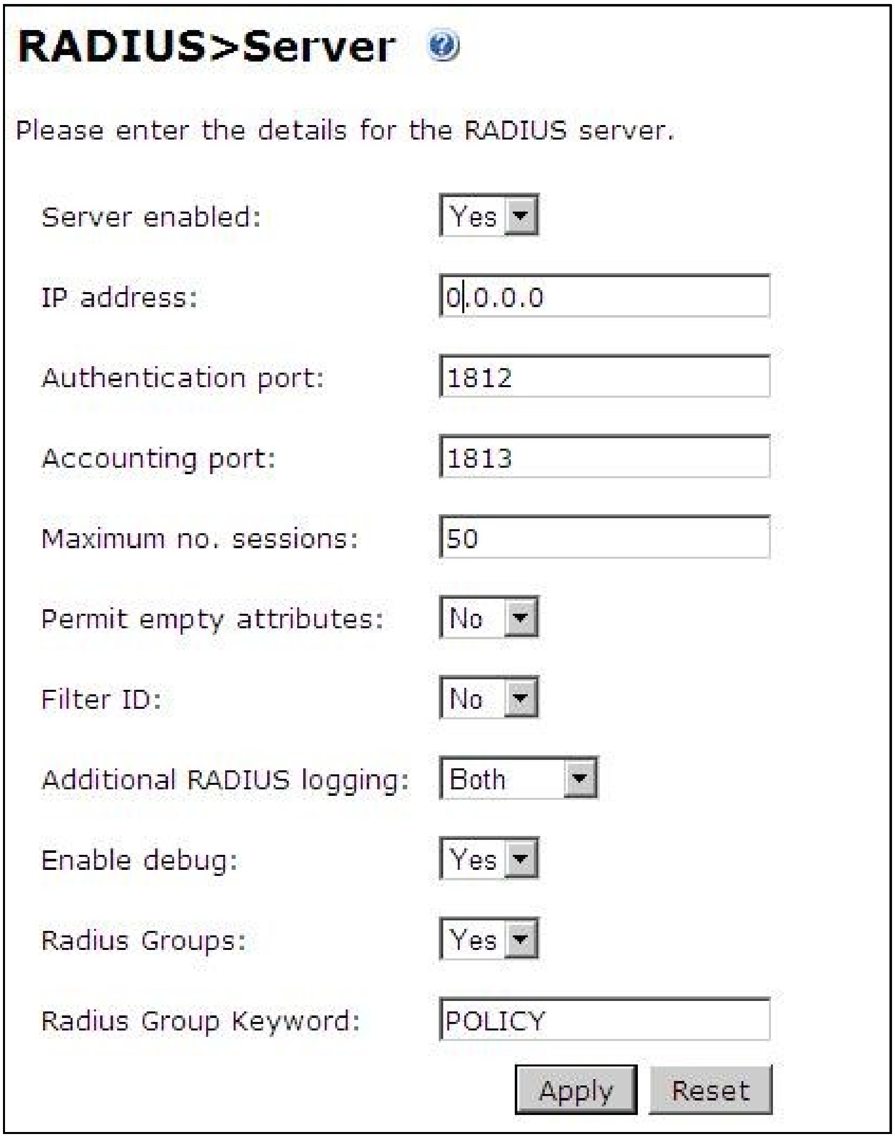
Swivel Configuration

Configuring the RADIUS server

Configure the RADIUS settings using the RADIUS configuration page in the Swivel Administration console by selecting RADIUS Server. To turn on RADIUS authentication set **Server Enabled** to YES. The Host or IP address is the interface which will accept RADIUS requests, leave this blank to allow RADIUS requests on any interface. (In this example the HOST IP is set to 0.0.0.0 which is the same as leaving it blank).

For troubleshooting RADIUS debug can be enabled together with the debug log option, see Debug how to guide

Note: for appliances, the Swivel VIP should not be used as the server IP address, see VIP on PINsafe Appliances



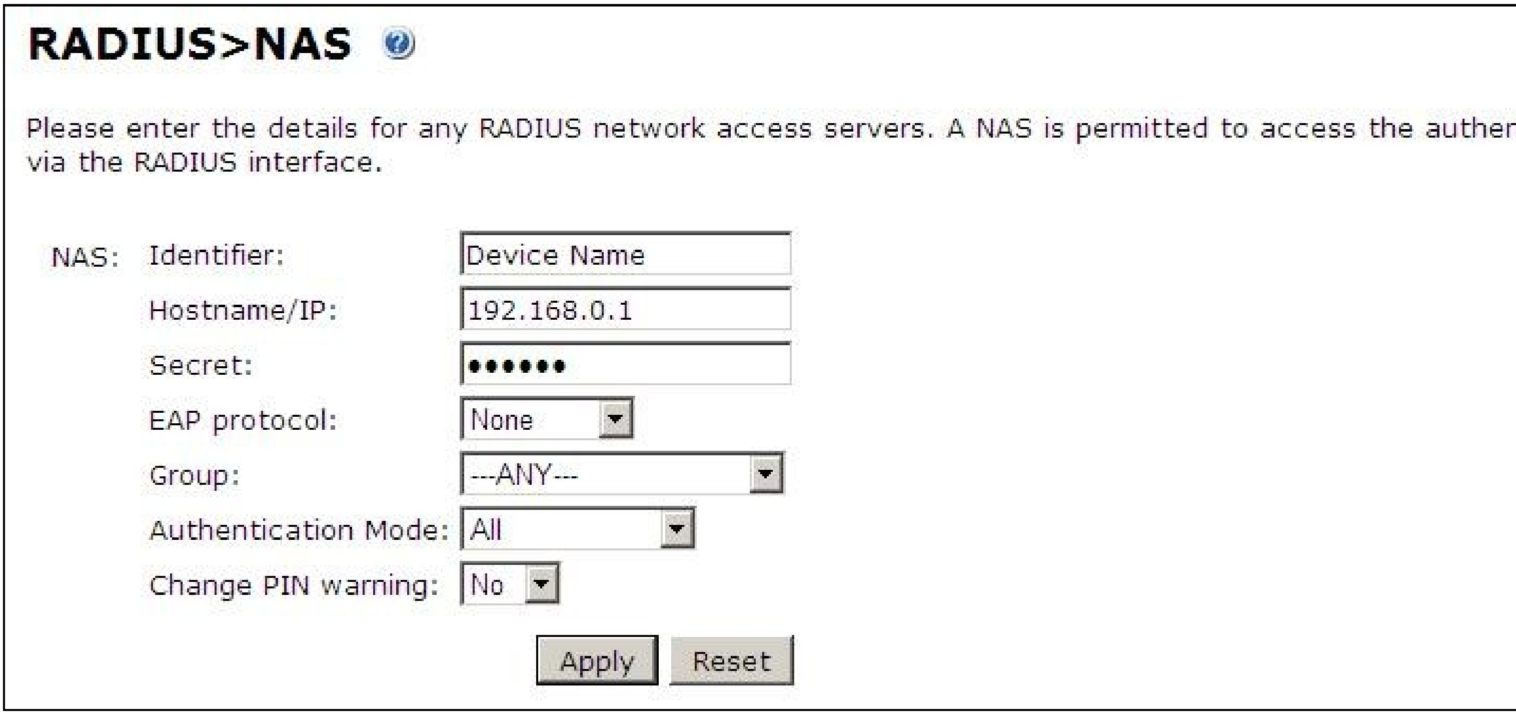
RADIUS>Server

Please enter the details for the RADIUS server.

Server enabled:	Yes
IP address:	0.0.0.0
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No
Filter ID:	No
Additional RADIUS logging:	Both
Enable debug:	Yes
Radius Groups:	Yes
Radius Group Keyword:	POLICY

Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the PINsafe Administration console. Enter a name for the VPN server. The IP address has been set to the IP of the VPN appliance, and the secret ?secret? assigned that will be used on both the PINsafe server and VPN RADIUS configuration.



RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther
via the RADIUS interface.

NAS: Identifier: Device Name

Hostname/IP: 192.168.0.1

Secret: ●●●●●●

EAP protocol: None

Group: ---ANY---

Authentication Mode: All

Change PIN warning: No

You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP are supported. All users will be able to authenticate via this NAS unless authentication is restricted to a specific repository group.

Enabling Session creation with username

The Swivel server can be configured to return an image stream containing a TURing image in the Taskbar

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

To test your configuration you can use the following URL using a valid Swivel username:

Appliance

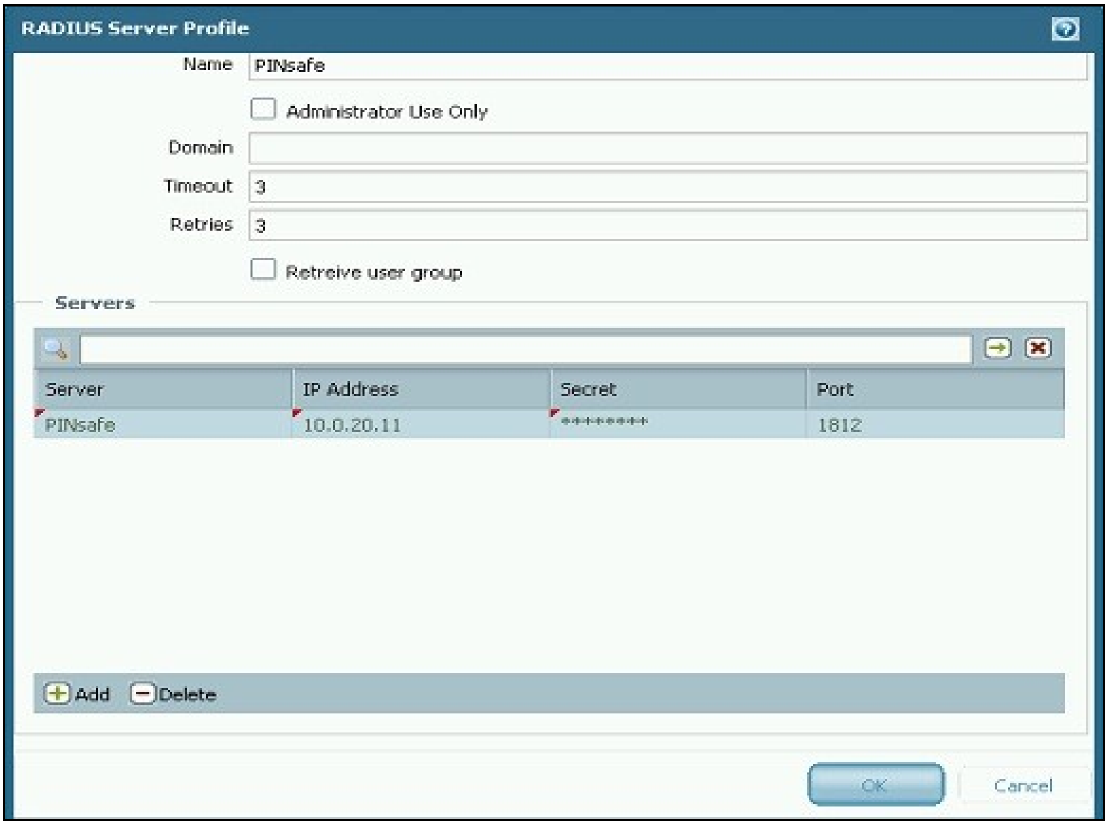
https://Swivel_server_IP:8443/proxy/SCImage?username=testuser

For a software only install see Software Only Installationr

Palo Alto Networks Configuration

Create a RADIUS Server Profile

On the Palo Alto Networks Administration console select the Device tab then Server Profiles and then RADIUS, and click on Add.



RADIUS Server Profile

Name: PINsafe

□ Administrator Use Only

Domain:

Timeout: 3

Retries: 3

□ Retreive user group

Servers

Server	IP Address	Secret	Port
PINsafe	10.0.20.11	********	1812

Enter the following information:

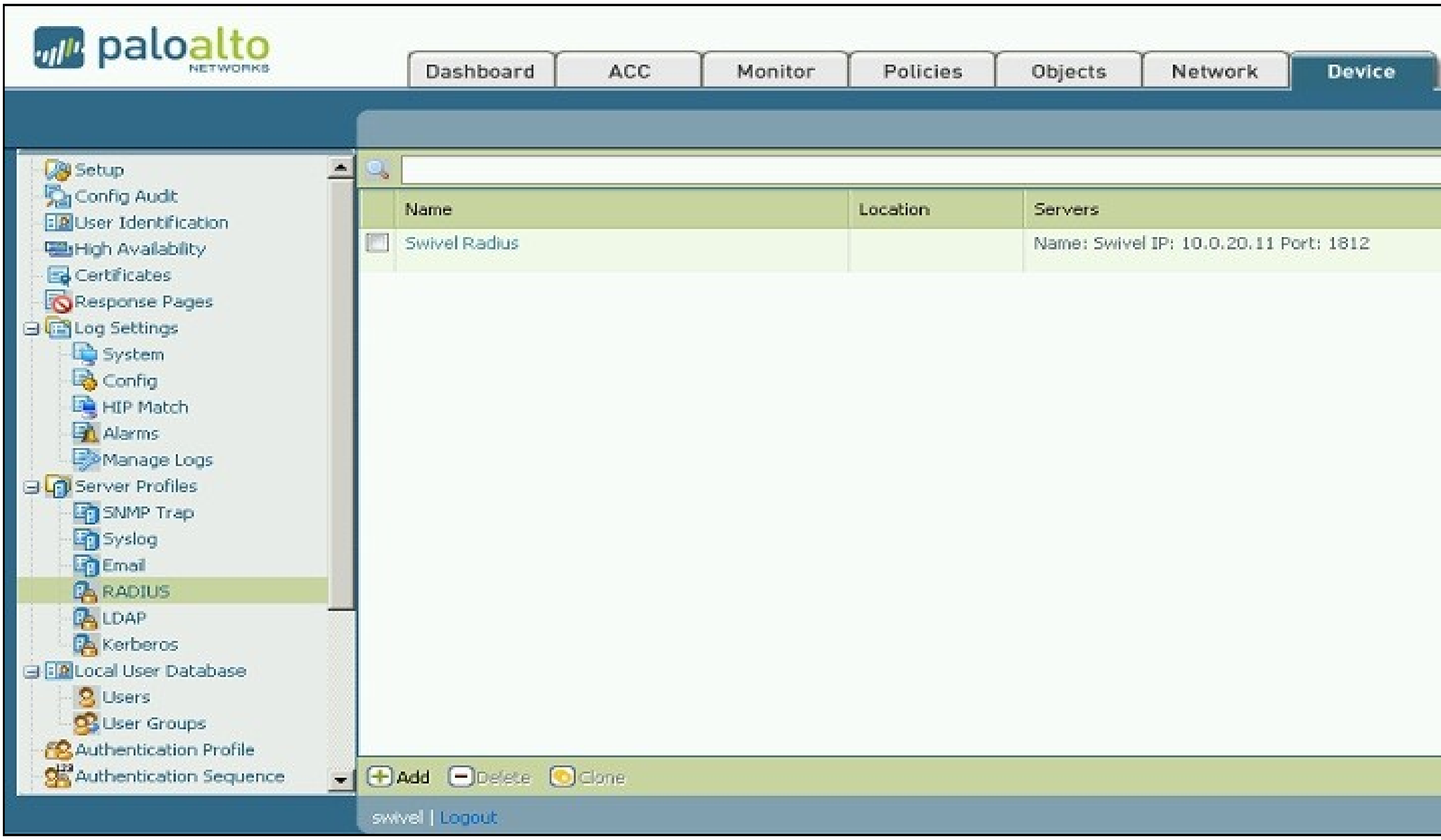
Name Descriptive name for the authentication server

Domain A domain to be appended to the authentication request

IP address or hostname of the Swivel server

Shared secret as entered on the PINsafe server

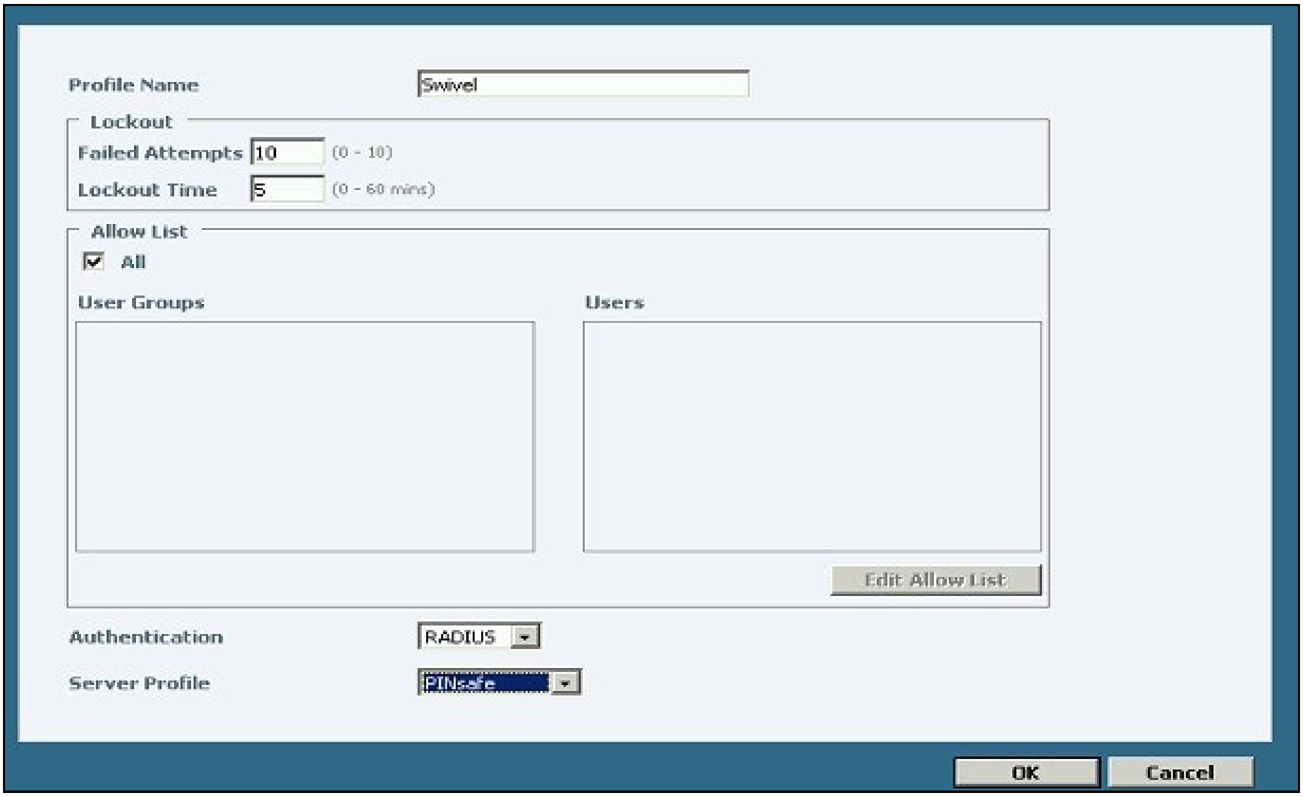
Port usually 1812 by default



	Name	Location	Servers
□	Swivel Radius		Name: Swivel IP: 10.0.20.11 Port: 1812

Create an Authentication Profile

On the Palo Alto Networks Administration console select the Device tab then Authentication profiles, and click on New. Enter a name and select RADIUS as the authentication type, and the Swivel server for the profile.



Profile Name: Swivel

Lockout

Failed Attempts: 10 (0 - 10)

Lockout Time: 5 (0 - 60 mins)

Allow List

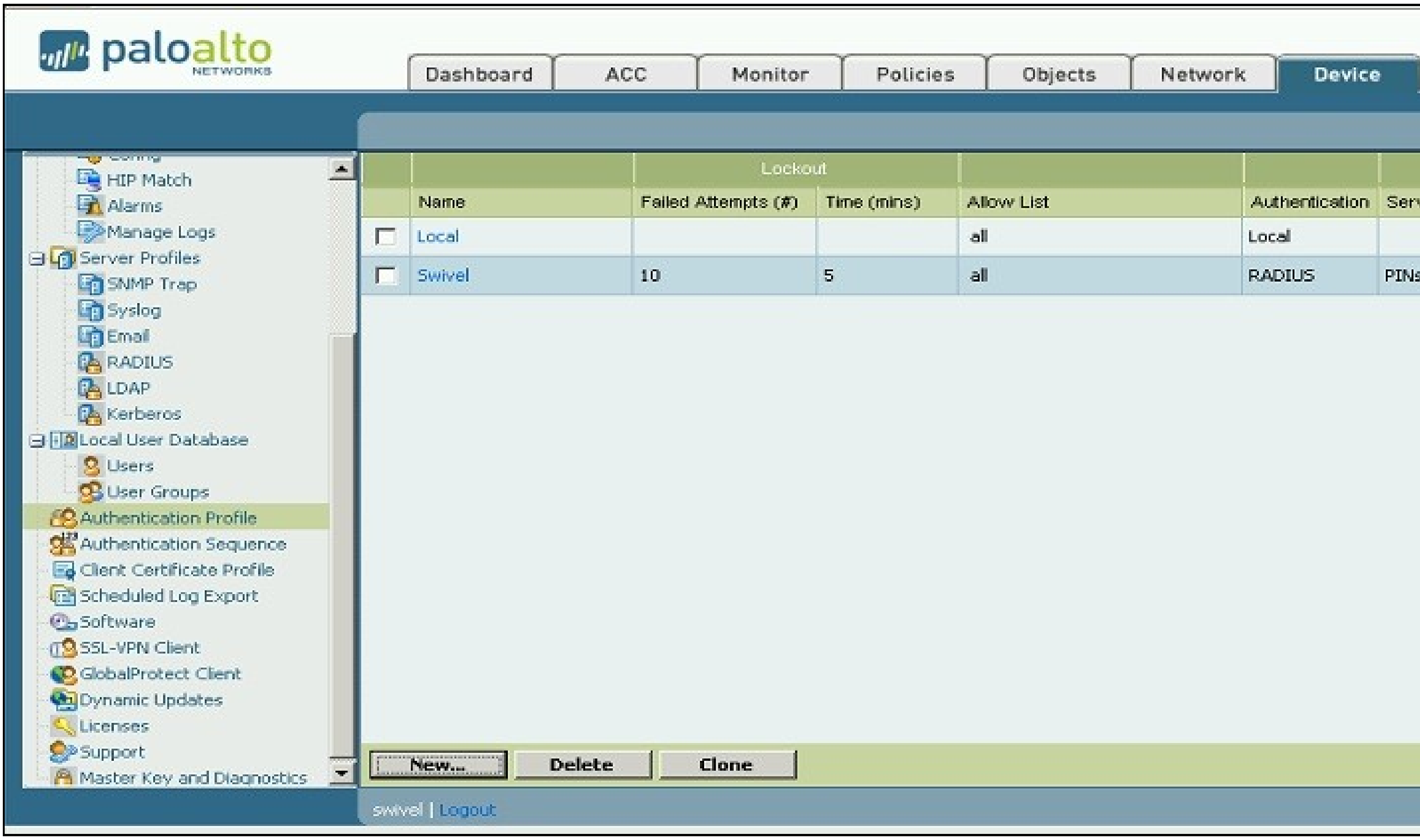
☑ All

User Groups

Users

Authentication: RADIUS

Server Profile: PINsafe

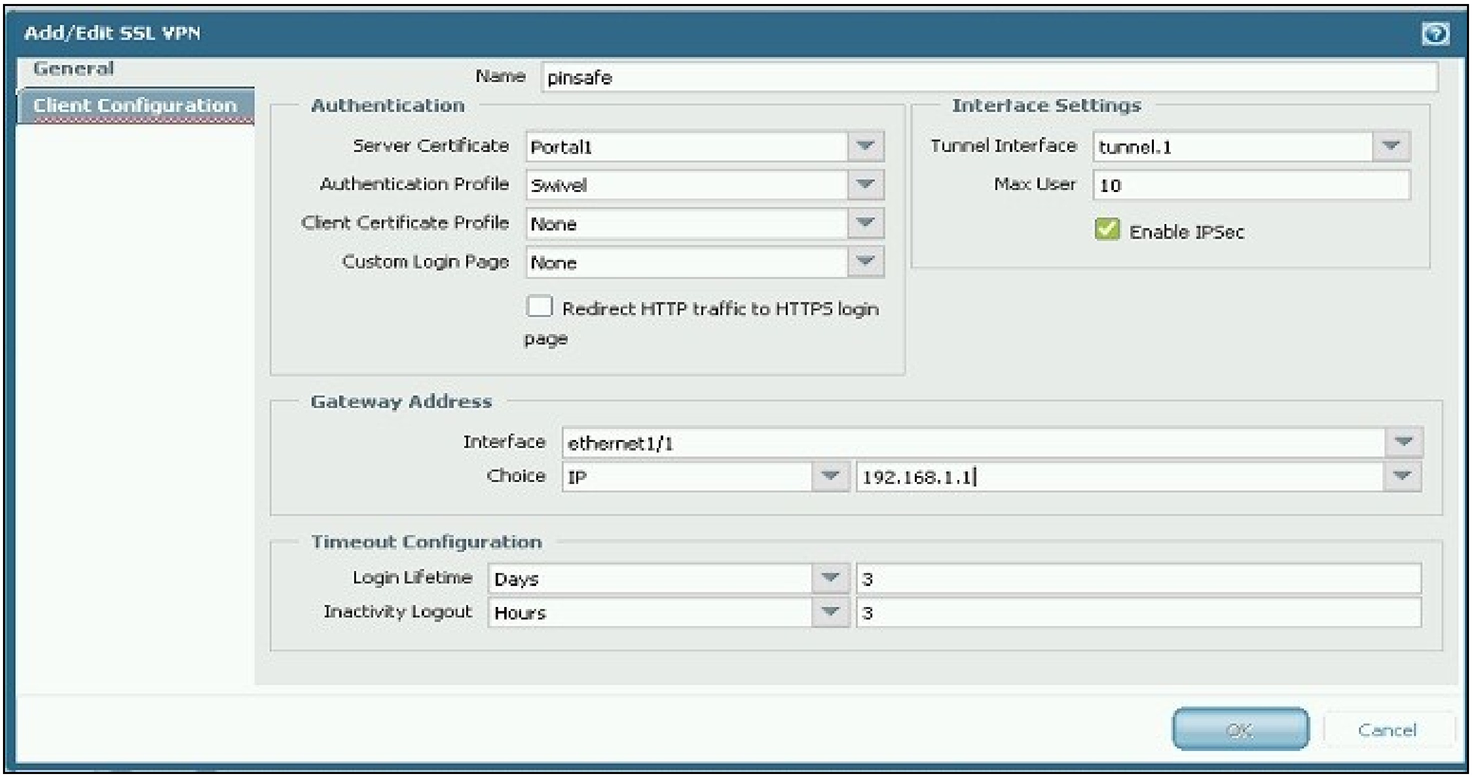


		Lockout				
	Name	Failed Attempts (#)	Time (mins)	Allow List	Authentication	Ser
□	Local			all	Local	
□	Swivel	10	5	all	RADIUS	PINs

Configure the GlobalProtect Portal to use Swivel RADIUS Authentication

On the Palo Alto Networks Administration console select the Network tab then SSL-VPN, either edit an existing GlobalProtect Portal or configure a new one by clicking on New.

Configure the **Authentication Profile** to use the authentication profile created above.



Name: pinsafe

Authentication

Server Certificate: Portal1
Authentication Profile: Swivel
Client Certificate Profile: None
Custom Login Page: None
□ Redirect HTTP traffic to HTTPS login page

Interface Settings

Tunnel Interface: tunnel.1
Max User: 10
☑ Enable IPSec

Gateway Address

Interface: ethernet1/1
Choice: IP 192.168.1.1

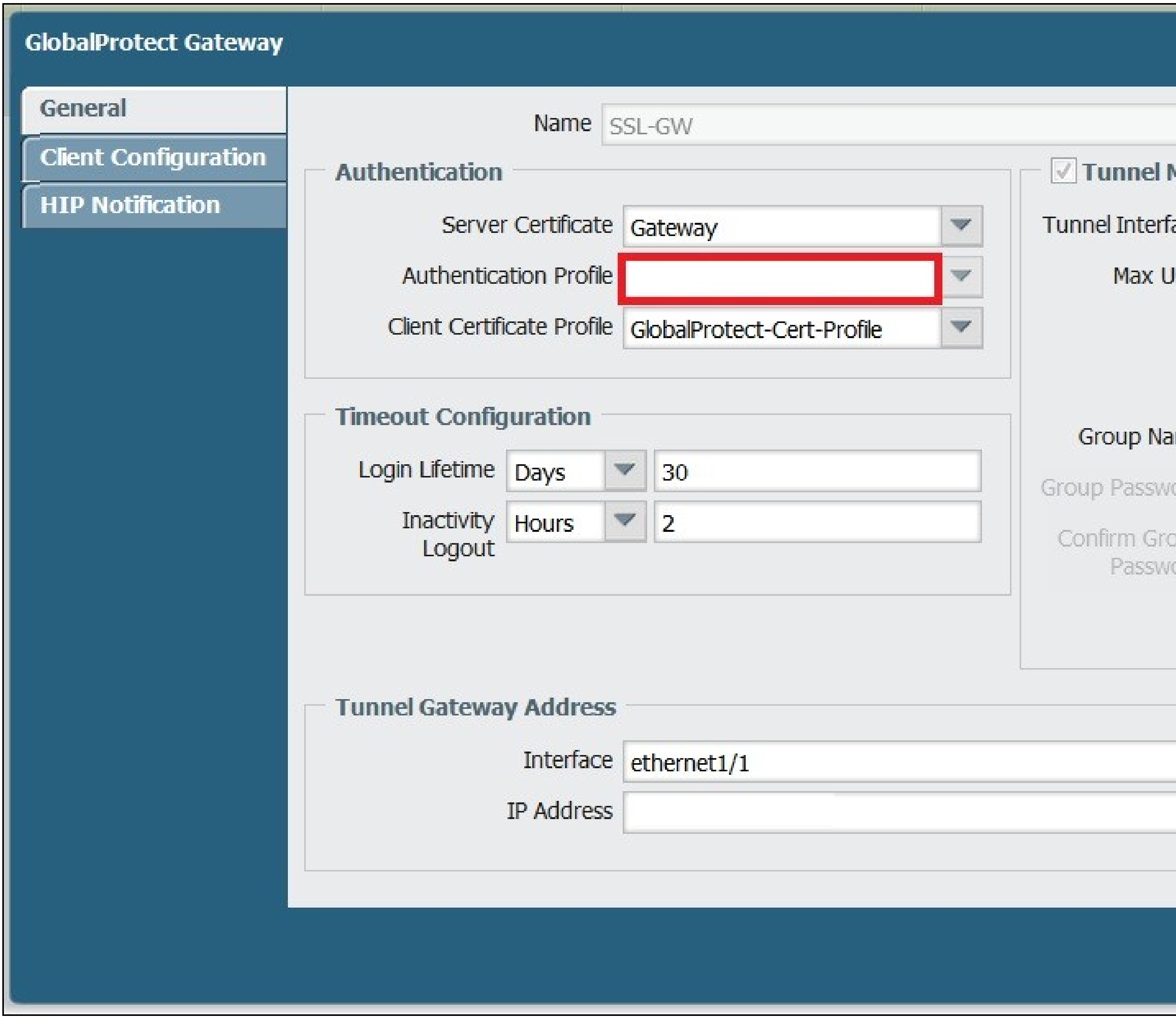
Timeout Configuration

Login Lifetime: Days 3
Inactivity Logout: Hours 3

Configure the GlobalProtect Gateway to use Swivel RADIUS Authentication

On the Palo Alto Networks Administration console select the Network tab then SSL-VPN, either edit an existing GlobalProtect Gateway or configure a new one by clicking on New.

Configure the **Authentication Profile** to use the authentication profile created above.



GlobalProtect Gateway

Name SSL-GW

Authentication

Server Certificate Gateway

Authentication Profile

Client Certificate Profile GlobalProtect-Cert-Profile

Timeout Configuration

Login Lifetime Days 30

Inactivity Logout Hours 2

☑ Tunnel M

Tunnel Interfa

Max U

Group Na

Group Passw

Confirm Gro Passw

Tunnel Gateway Address

Interface ethernet1/1

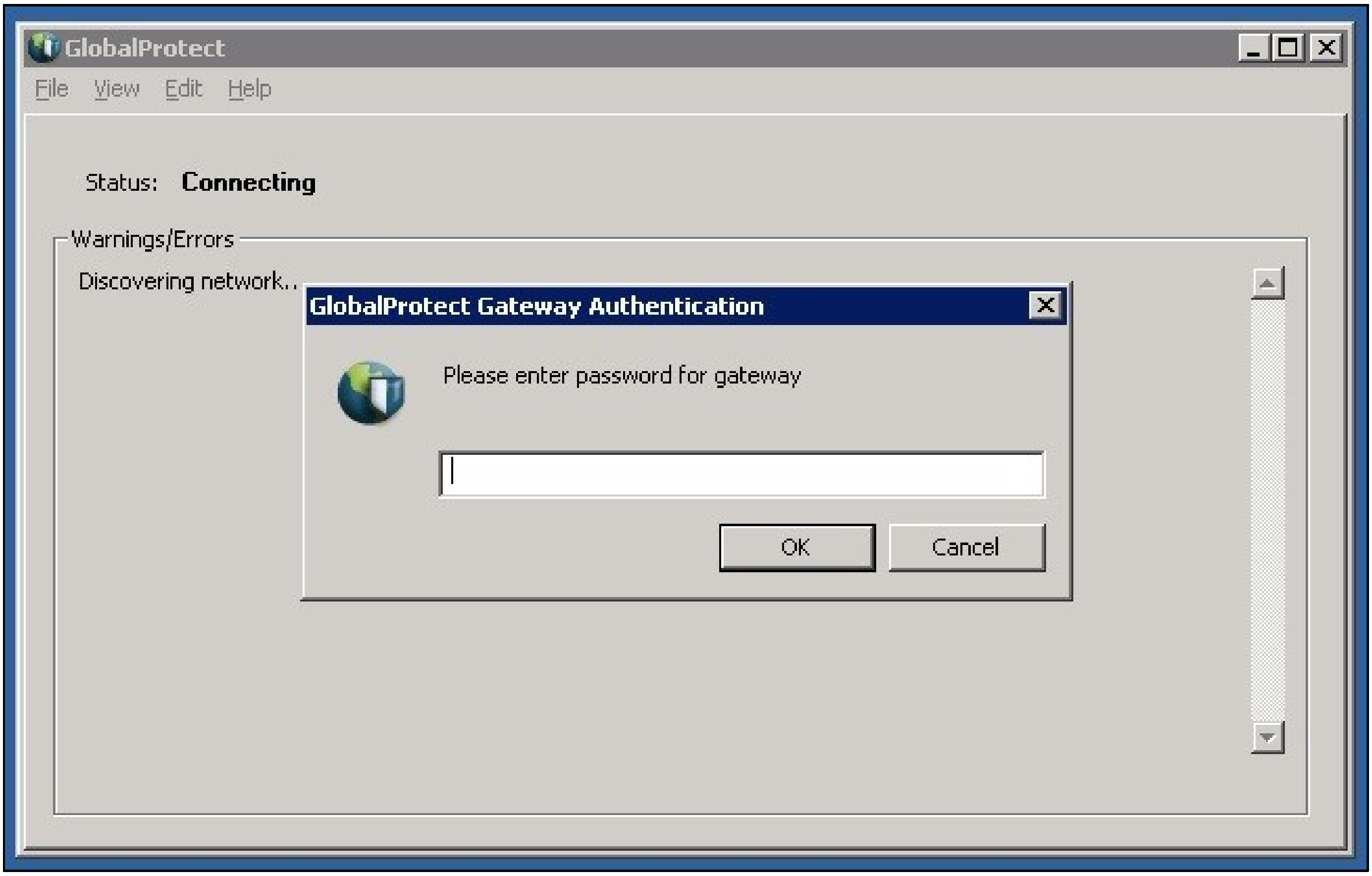
IP Address

Additional Configuration Options

Challenge and Response with Two Stage Authentication

Challenge and Response is supported by using Two Stage authentication and Check Password with Repository using RADIUS PAP authentication. See Challenge and Response How to Guide.

Enter Password



Status: Connecting

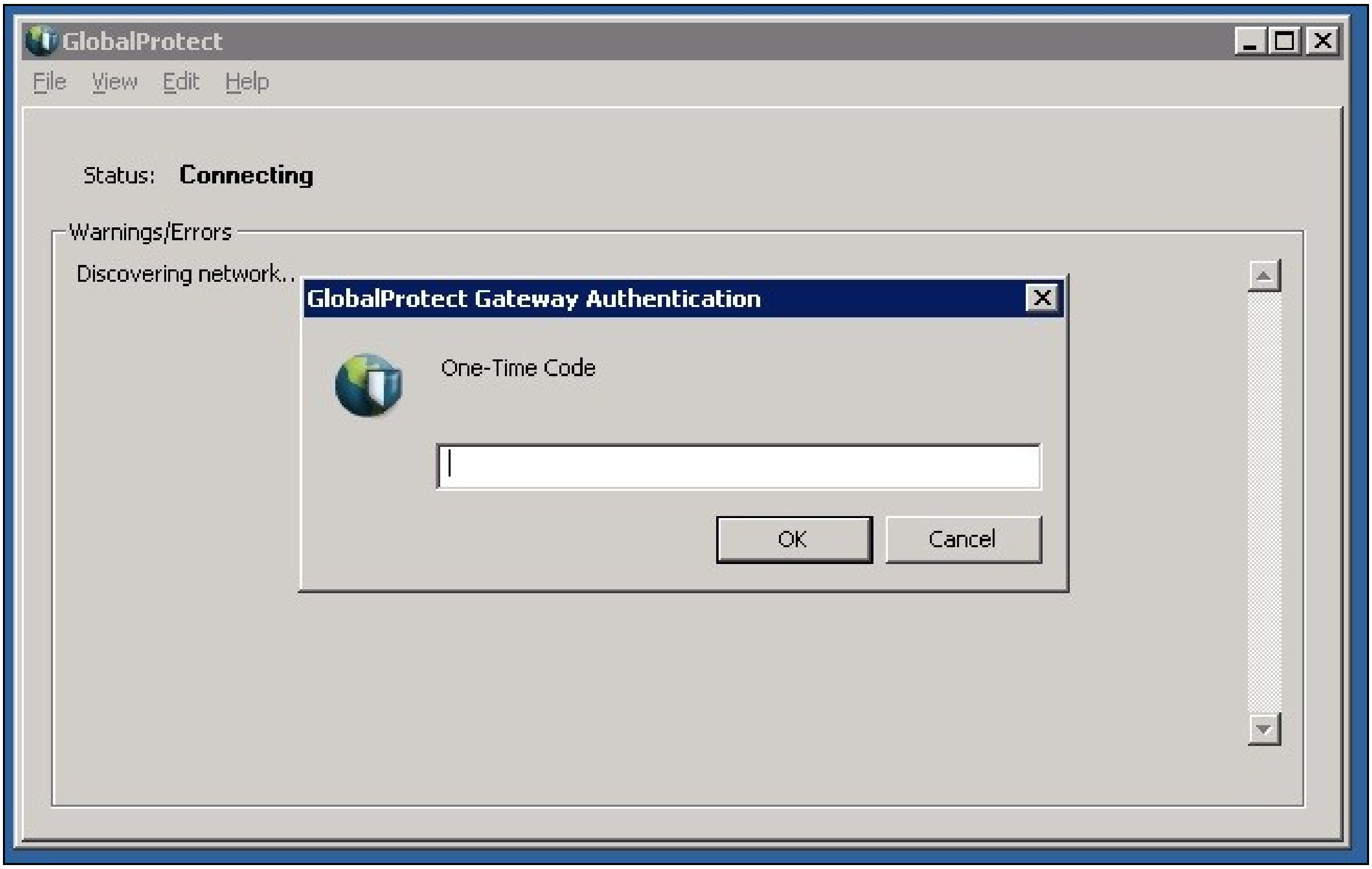
Warnings/Errors

Discovering network..

GlobalProtect Gateway Authentication

Please enter password for gateway

Enter OTC



Status: Connecting

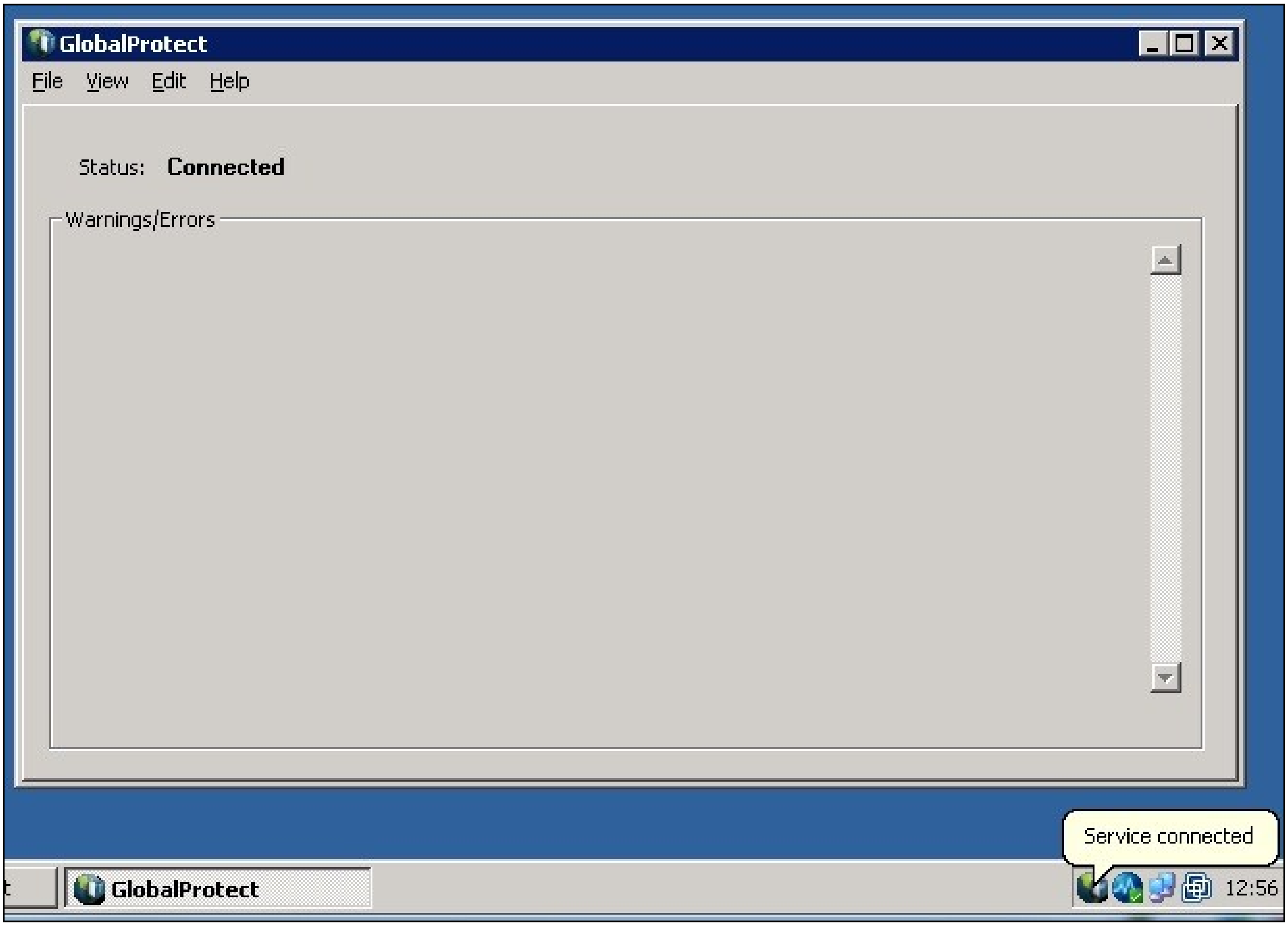
Warnings/Errors

Discovering network..

GlobalProtect Gateway Authentication

One-Time Code

IF OTC is correct then connection will be established



Testing

Connect to the GlobalProtect Client and authenticate using RADIUS authentication.

Troubleshooting

Check the PINsafe logs for RADIUS requests.

Known Issues and Limitations

None

Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com