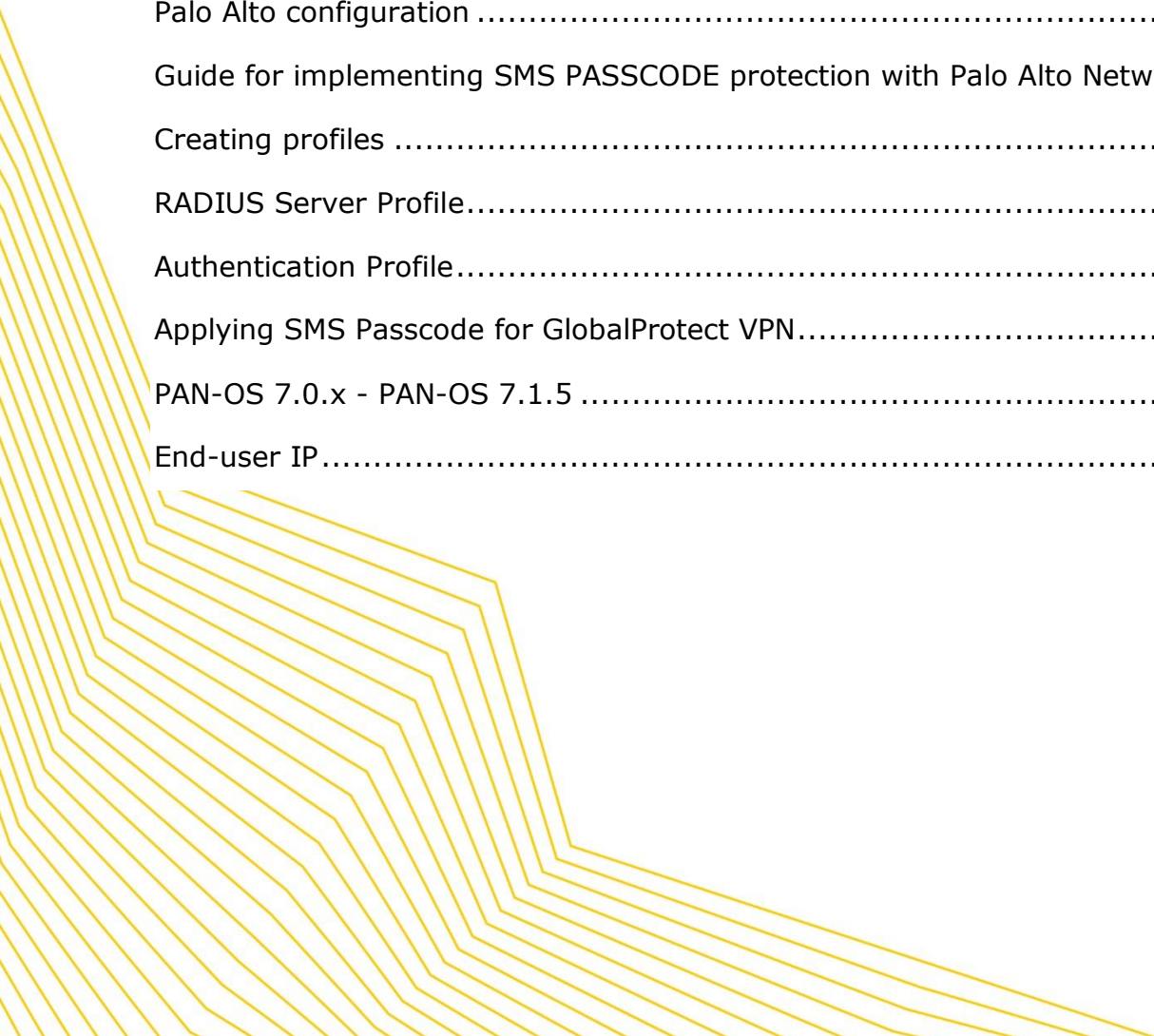


Palo Alto configuration

Contents

- Palo Alto configuration0
- Guide for implementing SMS PASSCODE protection with Palo Alto Networks.1
- Creating profiles1
- RADIUS Server Profile.....2
- Authentication Profile.....3
- Applying SMS Passcode for GlobalProtect VPN.....4
- PAN-OS 7.0.x - PAN-OS 7.1.56
- End-user IP.....7

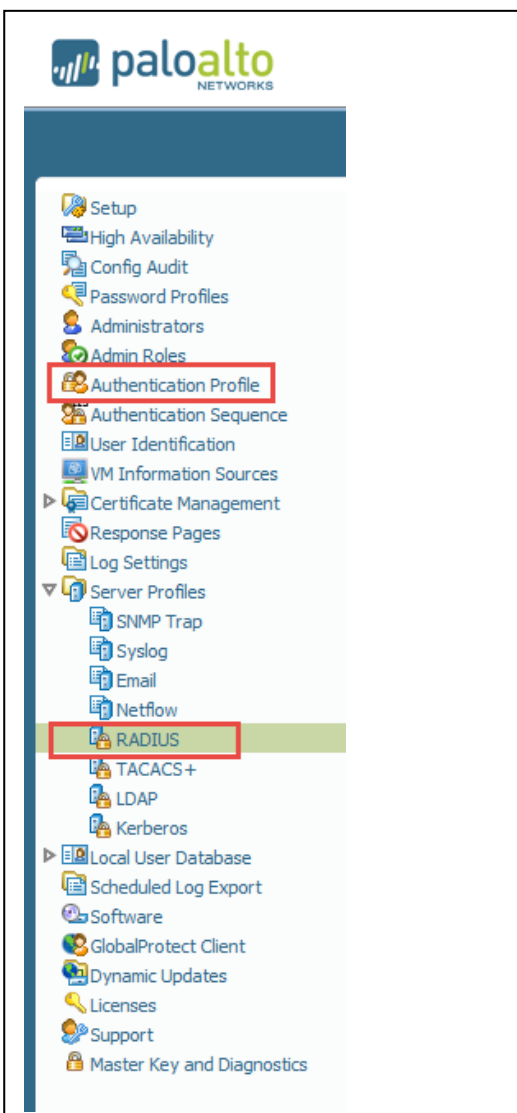




Guide for implementing SMS PASSCODE protection with Palo Alto Networks. This document outlines the process of configuring a Palo Alto Networks GlobalProtect VPN with SMS PASSCODE RADIUS protection.

Creating profiles

Start by creating a RADIUS Server Profile and an Authentication Profile.





RADIUS Server Profile

Navigate to Device → Server Profiles → RADIUS and add a new RADIUS profile

Name is a friendly name of your own choice.

Set RADIUS timeout to 10-20 seconds and retries to 1.

The Authentication port 1812 is the standard RADIUS port (UDP).

Shared secret must match the shared secret entered in the NPS radius client.

When done, click "OK".

RADIUS Server Profile

Name: SMSPasscode_ServerProfile

Administrator Use Only

Domain:

Timeout: 20

Retries: 1

Retrieve user group

Servers

Name	IP Address	Secret	Port
SMSPasscode	10.10.10.10	*****	1812

+ Add - Delete

OK Cancel



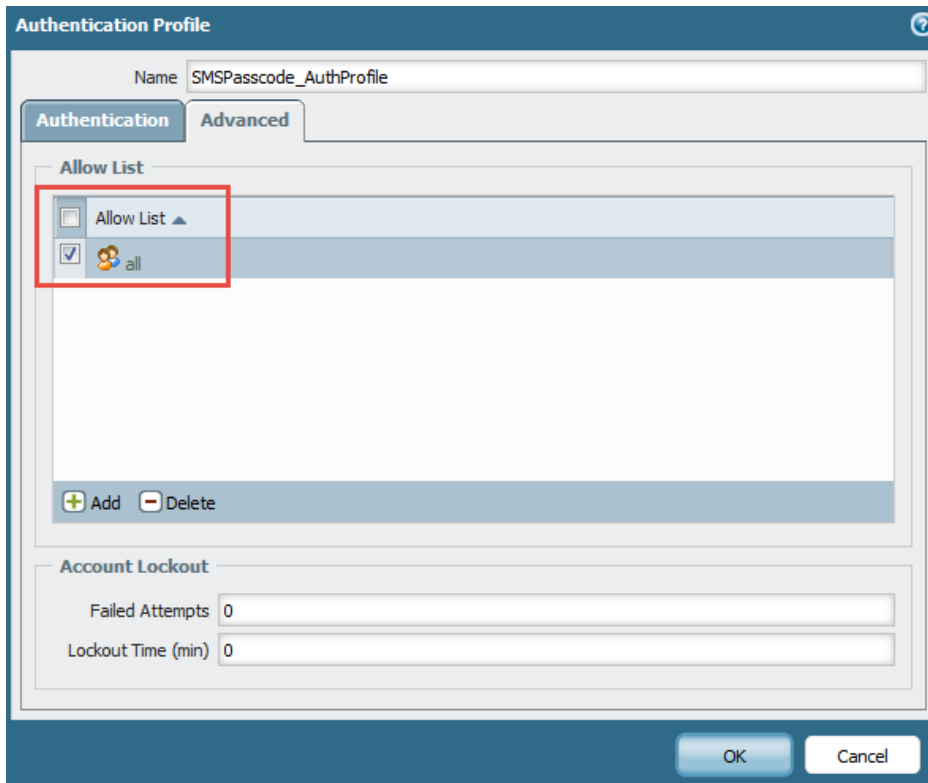
Authentication Profile

Navigate to Device → Authentication Profile and add a new Authentication Profile.

Configure the profile with the RADIUS server profile you just created.

The screenshot shows the 'Authentication Profile' configuration window. The 'Name' field is 'SMSPasscode_AuthProfile'. The 'Advanced' tab is active. The 'Type' dropdown is set to 'RADIUS' and the 'Server Profile' dropdown is set to 'SMSPasscode_ServerProfile'. A red box highlights these two dropdowns. Below them is a checkbox for 'Retrieve user group from RADIUS'. The 'User Domain' field is empty. The 'Username Modifier' dropdown is set to '%USERINPUT%'. The 'Single Sign On' section has 'Kerberos Realm' empty and 'Kerberos Keytab' with the text 'Click "Import" to configure this field' and an 'Import' button. At the bottom are 'OK' and 'Cancel' buttons.

Under 'Advanced' – select 'all' in the Allow List (user filtering will be handled by SMS PASSCODE).



Applying SMS Passcode for GlobalProtect VPN

Navigate to the Network → GlobalProtect → Gateway



Configure the GlobalProtect Gateway to use the Authentication Profile you created earlier.



GlobalProtect Gateway

General Name GP-Gateway

Client Configuration

Satellite Configuration

Network Settings

Interface ethernet1/1

IP Address 10.35.100.99/16

SSL/TLS Service Profile SSL-TLS-Profile

Authentication

Authentication Profile SMSPasscode_AuthProfile

Authentication Message Enter login credentials

Certificate Profile None

OK Cancel

To avoid duplicate login prompts, it is recommended to configure the GlobalProtect Portal with an LDAP or Kerberos Authentication Profile.



PAN-OS 7.0.x - PAN-OS 7.1.5

For devices running PAN-OS version between 7.0.x and 7.1.5 (PAN-54196) add the following DWORD in the registry on the RADIUS server. For devices running PAN-OS 7.1.5 or newer, they should not make this registry key.:

For SMS PASSCODE 7.2 and earlier:


HKLM\Software\SMS PASSCODE\RADIUS\RetransmissionEnableFiltering

For SMS PASSCODE 8.0

HKLM\Software\SMS PASSCODE\RADIUS\Connection Request

Policies\RetransmissionEnableFiltering

The DWORD must have a value of "0"

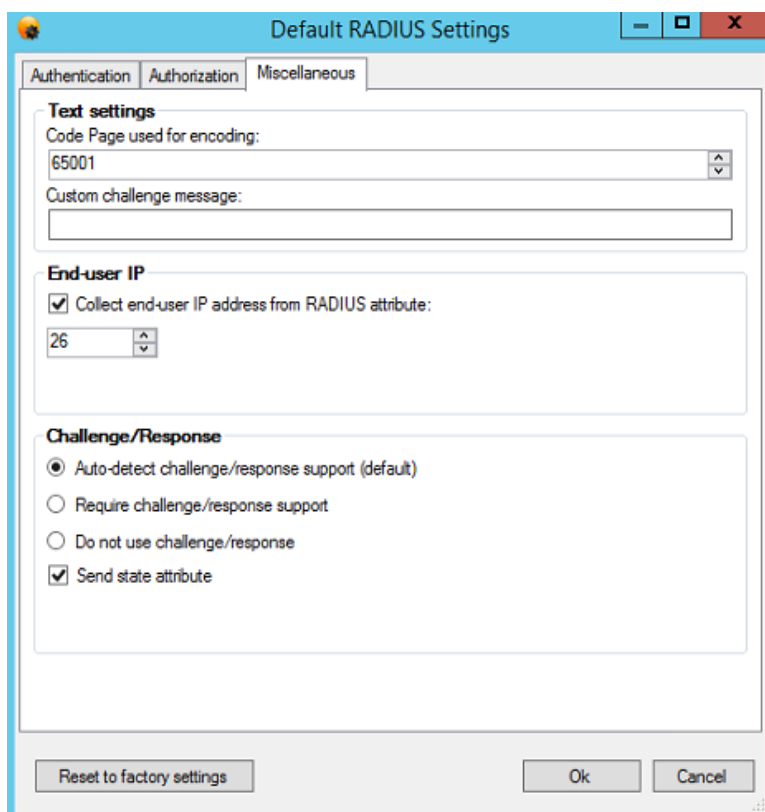
 RetransmissionEnableFiltering	REG_DWORD	0x00000000 (0)
---	-----------	----------------



End-user IP

With PAN-OS 7.0 and SMS PASSCODE version 8.0 you can retrieve the end-user IP address from GlobalProtect VPN logins and log them to the SMS PASSCODE Authentication Monitoring. This can also be used for location- and behavior aware authentication.

From the SMS PASSCODE Configuration Tool, under RADIUS settings, navigate to the 'Miscellaneous' tab and set the End-user IP attribute to 26.



On the firewall, enter the following CLI command:

```
set authentication radius-vsa-on client-source-ip
```

For more information on end-user IP, please refer to the SMS PASSCODE Administrator's Guide.