

INTEGRATION GUIDE

How to Configure Palo Alto (GlobalProtect) to secure VPN access with Portnox CLEAR

Introduction

This document guides you step by step how to configure your VPN environment using Portnox CLEAR to enable secure and trusted cloud-based RADIUS access with an optional push-to-access MFA.

Preliminary Actions

Before configuring VPN authentication, you need to verify the following:

- 1) Verify your organization is registered on Portnox CLEAR Cloud Services: <https://clear.portnox.com/>
- 2) In the CLEAR portal, go to **Settings > Services** and expand **CLEAR RADIUS Service**. Then:
 - a. If the **Enable Cloud RADIUS** checkbox is not checked, click **Edit** and check the **Enable Cloud RADIUS** checkbox.
 - b. Note the RADIUS server details which you will need when configuring VPN access:
 - **Cloud RADIUS IP** – this is the IP address of the CLEAR RADIUS server
 - **Authentication port**
 - **Accounting port**
 - **Shared Secret** – this is the RADIUS client shared secret
- 3) In the CLEAR portal, go to **Settings > Groups** and create a group for VPN users, or edit an existing one. In the **group settings > VPN Access** select the following:
 - Allowed authentication type = credentials.
 - (optional) Multi-Factor Authentication = push-to-access on mobile only.
Note, MFA on mobile devices require AgentP to be enrolled on the mobile device.
 - For implementation with AgentP, check the: validate risk score for all managed devices.

Configuring Palo Alto SSL VPN

In the following steps, we configure the VPN authentication to be secured and protected based on RADIUS authentication. The following steps should be performed in the Palo Alto web interface.

- 1) Create a RADIUS server profile by navigating to **Device > Server Profiles > RADIUS** and clicking **Add**.

In the RADIUS Server Profile window that appears:

- a. Specify a **Name** for the RADIUS server profile.
- b. In **Server Settings**, set **Timeout (sec)** to **40**.
- c. Enter the following CLEAR RADIUS server details, which you noted in [Preliminary Actions](#), step (**Error! Reference source not found**):
 - In **RADIUS Server**, enter the Cloud RADIUS IP.
 - In **Port**, enter the Authentication port.
 - In **Secret**, enter the Shared Secret.

RADIUS Server Profile

Profile Name: CLEAR-RADIUS

Administrator Use Only

Server Settings

Timeout (sec): 40

Retries: 3

Servers

Name	RADIUS Server	Secret	Port
PortnoxCLEAR	[REDACTED]	*****	10000

+ Add - Delete

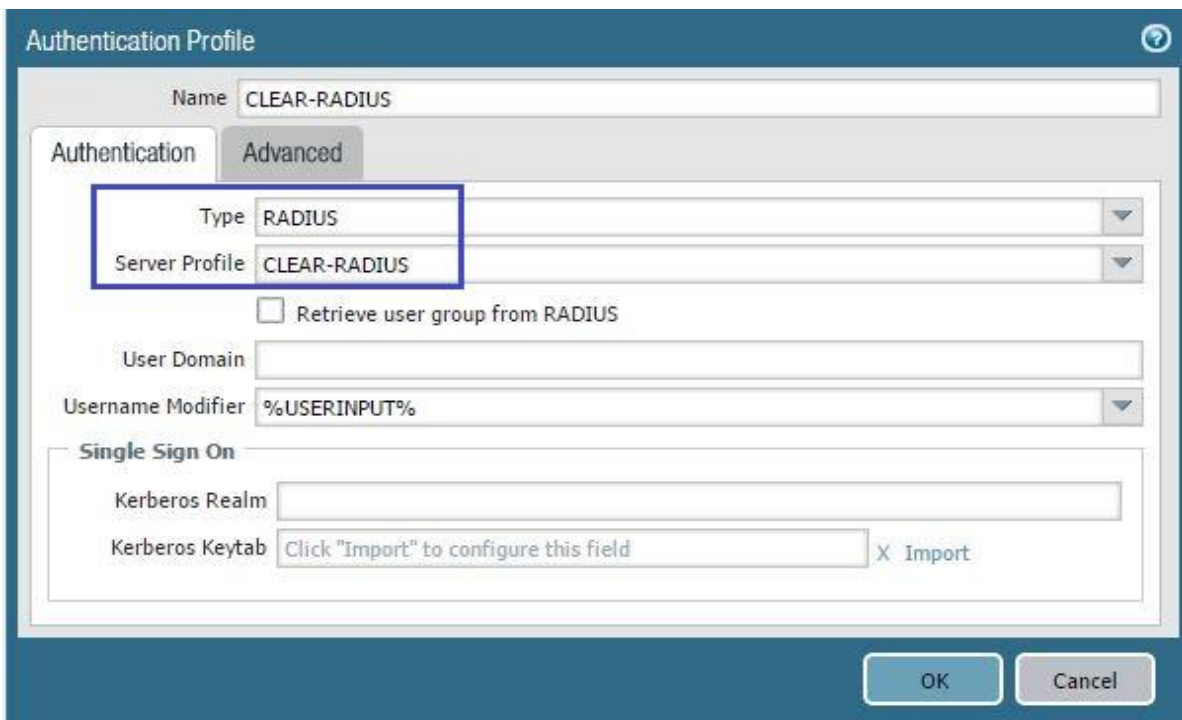
Enter the IP address or FQDN of the RADIUS server

OK Cancel

- 2) Create a RADIUS authentication profile by navigating to **Device > Authentication Profiles** and clicking **Add**.

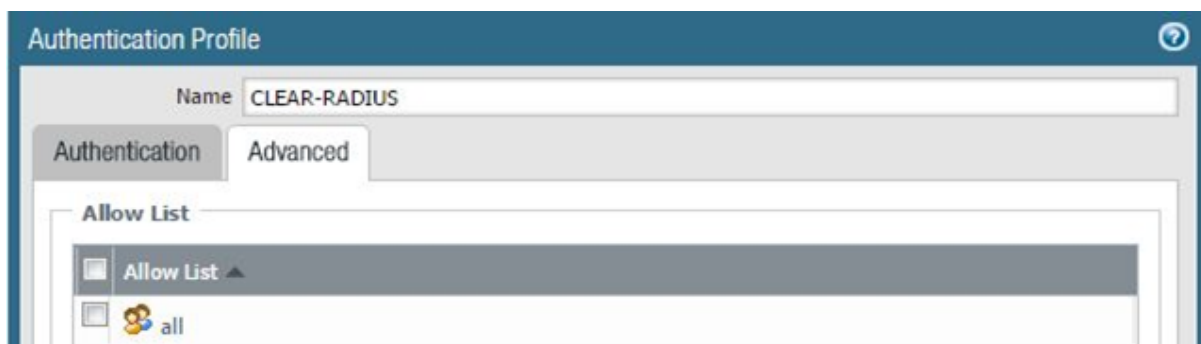
In the Authentication Profile window that appears:

- a. Specify a **Name** for the authentication profile.
- b. In the **Authentication** tab:
 - In **Type**, select **RADIUS**.
 - In **Server Profile**, specify the RADIUS server profile you created in step (1) of this section.



The screenshot shows the 'Authentication Profile' configuration window with the 'Authentication' tab selected. The 'Name' field is set to 'CLEAR-RADIUS'. The 'Type' dropdown is set to 'RADIUS' and the 'Server Profile' dropdown is set to 'CLEAR-RADIUS'. A blue box highlights these two dropdowns. Below them is a checkbox for 'Retrieve user group from RADIUS' which is unchecked. The 'User Domain' field is empty. The 'Username Modifier' dropdown is set to '%USERINPUT%'. The 'Single Sign On' section contains a 'Kerberos Realm' field and a 'Kerberos Keytab' field with a button that says 'Click "Import" to configure this field' and an 'X Import' button. At the bottom right are 'OK' and 'Cancel' buttons.

- c. In the **Advanced** tab, add **All** to the **Allow List**.



The screenshot shows the 'Authentication Profile' configuration window with the 'Advanced' tab selected. The 'Name' field is set to 'CLEAR-RADIUS'. The 'Allow List' section is visible, showing a list with two items: 'Allow List' (with a dropdown arrow) and 'all' (with a user icon).

- 3) Add the new RADIUS authentication profile to the GlobalProtect gateway, as follows:
 - a. Navigate to **Network > GlobalProtect > Gateways**.
 - b. Select the relevant gateway, that is, the gateway that will be communicating with Portnox CLEAR.
 - c. In the **Authentication** tab, select **Add**.
 - d. Specify the RADIUS authentication profile you created in step (2) of this section.

The screenshot shows the 'GlobalProtect Gateway Configuration' window with the 'Authentication' tab selected. The 'Server Authentication' section has an 'SSL/TLS Service Profile' dropdown menu. The 'Client Authentication' section contains a table with one entry: 'CLEAR-RADIUS' with OS 'Any' and Authentication Profile 'CLEAR-RADIUS'. Below the table are buttons for '+ Add', '- Delete', 'Clone', 'Move Up', and 'Move Down'. At the bottom, there is a 'Certificate Profile' dropdown menu set to 'None'. 'OK' and 'Cancel' buttons are at the bottom right.

Name	OS	Authentication Profile	Authentication Message
CLEAR-RADIUS	Any	CLEAR-RADIUS	Enter login credentials

- 4) Add the new RADIUS authentication profile to the GlobalProtect portal, as follows:
 - a. Navigate to **Network > GlobalProtect > Portals**.
 - b. Select the relevant portal, that is, the portal that will be communicating with Portnox CLEAR.
 - c. In the **Authentication** tab, select **Add**.
 - d. Specify the RADIUS authentication profile you created in step (2) of this section.

The screenshot shows the 'GlobalProtect Portal Configuration' window with the 'Authentication' tab selected. The 'Server Authentication' section has a dropdown menu for 'SSL/TLS Service Profile'. The 'Client Authentication' section contains a table with one entry: 'CLEAR-RADIUS' with OS 'Any' and Authentication Profile 'CLEAR-RADIUS'. Below the table are buttons for 'Add', 'Delete', 'Clone', 'Move Up', and 'Move Down'. At the bottom, there is a 'Certificate Profile' dropdown set to 'None'. 'OK' and 'Cancel' buttons are at the bottom right.

Name	OS	Authentication Profile	Authentication Message
CLEAR-RADIUS	Any	CLEAR-RADIUS	Enter login credentials

- 5) Update the Portal connection timeout, as follows:
 - a. Navigate to **Network > GlobalProtect > Portals**.
 - b. Select the relevant portal, that is, the portal that will be communicating with Portnox CLEAR.
 - c. In the **Agent** tab, select the VPN gateway.
 - d. Select the **App** tab.
 - e. Set the **Portal Connection Timeout** to **60** seconds.

The screenshot shows the 'App Configurations' window in the Palo Alto Networks configuration interface. The 'App' tab is selected, and the 'Portal Connection Timeout (sec)' is set to 60. The 'Disable GlobalProtect App' section includes fields for 'Passcode', 'Confirm Passcode', 'Max Times User Can Disable' (0), and 'Disable Timeout (min)' (0). The 'Mobile Security Manager Settings' section includes a 'Mobile Security Manager' field and an 'Enrollment Port' dropdown set to 443. The 'Welcome Page' is set to 'None'. The 'App Configurations' table is as follows:

App Configurations	
Show System Tray Notifications	Yes
Custom Password Expiration Message (LDAP Authentication Only)	
Maximum Internal Gateway Connection Attempts	5
Portal Connection Timeout (sec)	60
TCP Connection Timeout (sec)	5 [1 - 600]
TCP Receive Timeout (sec)	30 [1 - 600]
Update DNS Settings at Connect (Windows Only)	No
Detect Proxy for Each Connection (Windows only)	No
Restart GlobalProtect Agent After Timing Out (Windows Only)	No
Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Windows Only)	Yes

- 6) Add additional information to RADIUS attributes, by logging in to the Palo Alto CLI and running the following commands:

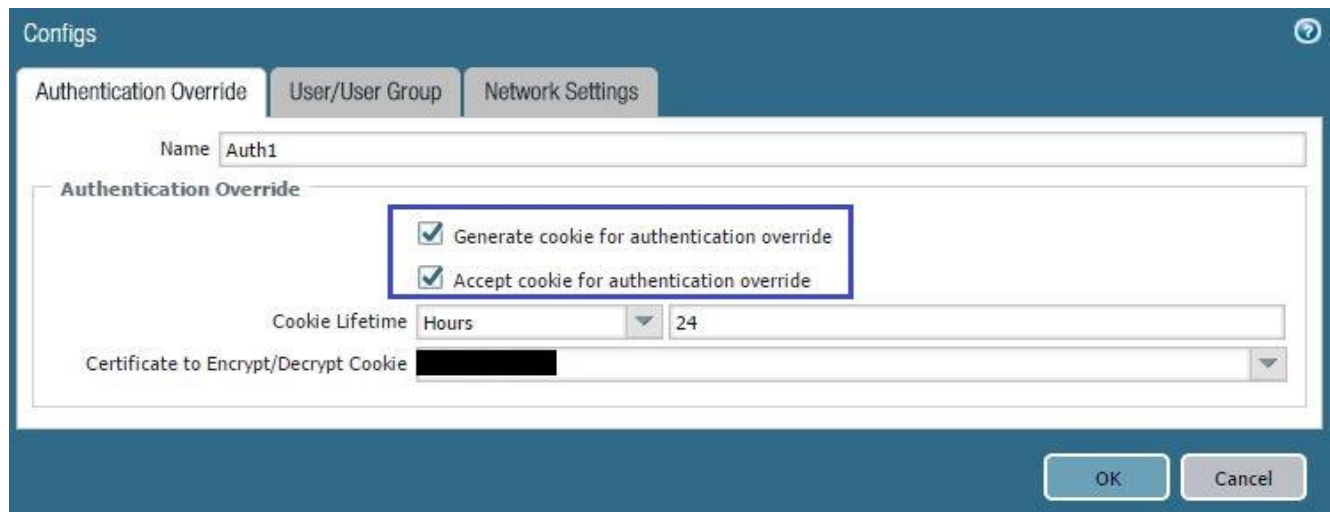
```
username@hostname> set authentication radius-vsa-on client-source-ip
username@hostname> set authentication radius-vsa-on client-osu
username@hostname> set authentication radius-vsa-on client-hostname
username@hostname> set authentication radius-vsa-on user-domain
username@hostname> set authentication radius-vsa-on client-gp-version
```

Note: these commands may be removed after Palo Alto reboot, in which case they will need to be run again.

Eliminating Multiple Logins and OTPs

You can optionally configure your settings so that end users will not be required to log in to both the portal and the gateway in succession, nor enter multiple OTPs for authenticating to each. To do so:

- 7) Set the Authentication Override settings for the gateway, as follows:
 - a. Navigate to **Network > GlobalProtect > Gateways**.
 - b. Select the relevant gateway, that is, the gateway that will be communicating with Portnox CLEAR.
 - c. In the **Agent** tab, select **Client Settings**.
 - d. Select the relevant Config, and in the **Authentication Override** tab, select:
 - **Generate cookie for authentication override**
 - **Accept cookie for authentication override**



The screenshot shows a configuration window titled 'Auth1' with three tabs: 'Authentication Override', 'User/User Group', and 'Network Settings'. The 'Authentication Override' tab is active. The 'Name' field contains 'Auth1'. Below the 'Authentication Override' section, there are two checked checkboxes: 'Generate cookie for authentication override' and 'Accept cookie for authentication override'. The 'Cookie Lifetime' is set to 'Hours' with a value of '24'. The 'Certificate to Encrypt/Decrypt Cookie' field is redacted with a black box. At the bottom right, there are 'OK' and 'Cancel' buttons.

- 8) Set the Authentication Override settings for the portal, as follows:
- Navigate to **Network > GlobalProtect > Portals**.
 - Select the relevant portal, that is, the portal that will be communicating with Portnox CLEAR.
 - In the **Agent** tab, select the relevant Config.
 - In the **Authentication** tab, select:
 - Generate cookie for authentication override**
 - Accept cookie for authentication override**

The screenshot shows the 'Configs' window with the 'Authentication' tab selected. The configuration is for a portal named 'VPN-GW'. The 'Client Certificate' is set to 'None'. The 'Save User Credentials' option is set to 'Yes'. In the 'Authentication Override' section, both 'Generate cookie for authentication override' and 'Accept cookie for authentication override' are checked. The 'Cookie Lifetime' is set to 'Hours' with a value of '24'. The 'Certificate to Encrypt/Decrypt Cookie' field is redacted. The 'Components that Require Dynamic Passwords (Two-Factor Authentication)' section is also visible, with options for 'Portal', 'Internal gateways-all', 'External gateways-manual only', and 'External gateways-auto discovery'.

Authentication | User/User Group | Gateways | App | Data Collection

Name: VPN-GW

Client Certificate: None

The selected client certificate including its private key will be installed on client machines.

Save User Credentials: Yes

Authentication Override

- Generate cookie for authentication override
- Accept cookie for authentication override

Cookie Lifetime: Hours | 24

Certificate to Encrypt/Decrypt Cookie: [REDACTED]

Components that Require Dynamic Passwords (Two-Factor Authentication)

- Portal
- Internal gateways-all
- External gateways-manual only
- External gateways-auto discovery

Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.

OK Cancel

Instructions for Supplying VPN Credentials

Supplying VPN Credentials without MFA

For successful VPN authentication using Portnox CLEAR RADIUS, users are required to provide their username + password:

Supplying VPN Credentials with push-to-access MFA

For successful VPN authentication using Portnox CLEAR RADIUS and push-to-access MFA, users are required to provide their username + password and allow the push notification on their mobile device:



portnox™

NEW SIGN IN

Your device attempted to access the corporate network. Please confirm.

portnox2

Aug 14, 2020 | 3:27 PM

✕
DENY

✔
ALLOW