Palo Alto Integration Guide

RADIUS Configuration

Product Version: 4.2

Publication date: February 2023

Call us on: +44 1344 568 900 (UK/EMEA)
+1 408 706 2866 (US)

Email us: sales@authlogics.com

Table of Contents

Introduction

Authlogics Authentication Server is a multi-factor authentication system which is pre-integrated with a RADIUS server which can process authentication requests from RADIUS aware technologies including PALO ALTO firewall and VPN servers.

This guide outlines the basic prerequisites to complete a successful setup of integrating Authlogics with Palo Alto servers using RADIUS.

Full product documentation, which includes step by step setup, is available here:
https://authlogics.com/download/authentication-server-installation-and-configuration-guide/

Considerations

Requirements

The Palo Alto device AND an Authlogics Authentication Server should already be deployed and functional using the standard username and password authentication mechanism prior to configuring integration via RADIUS.

Language

Authlogics Authentication Server is only available in English. Product support and documentation are only available in English.

Authlogics Authentication Server Configuration

The Authlogics Authentication Server will require configuration for use with Palo Alto device. The Palo Alto device will send authentication requests to the Authlogics Authentication Server via RADIUS. To cater for this, the Authlogics Authentication Server must be configured to accept RADIUS requests from the Palo Alto device.

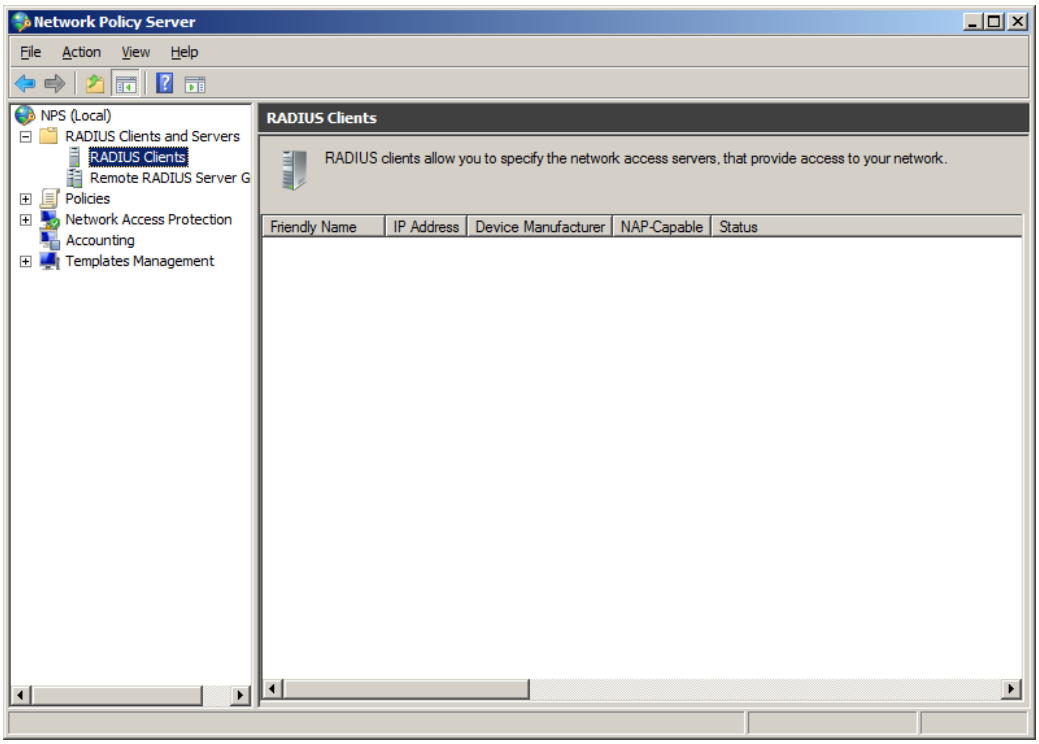
Adding a RADIUS client on the Authentication Server

These steps are performed on the Authlogics Authentication Server.

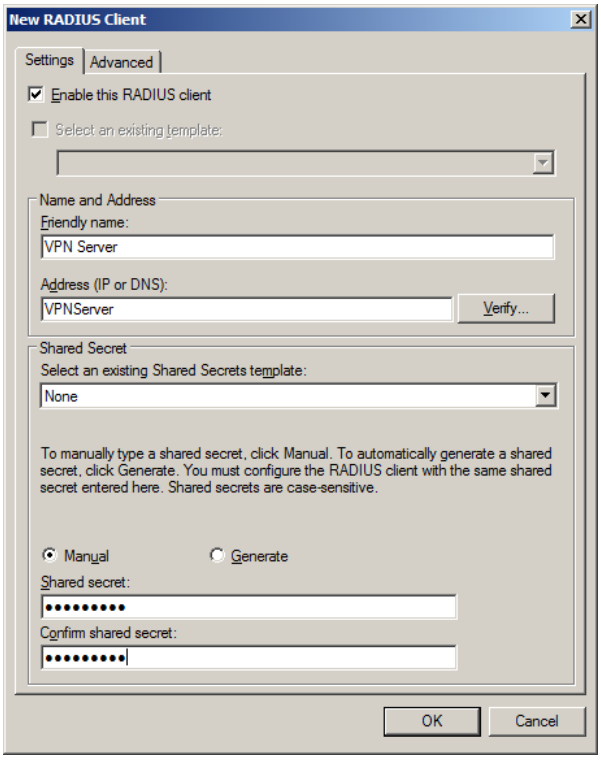
> **Note**
> This section of the installation process requires Local Administrator rights on the server. Domain rights are not required at this stage.

(1) Open the *Network Policy Server* from the Administrative Tools start menu group.

(2) Select *RADIUS Clients and Servers*, then *RADIUS Clients*.



(3) Right-click *RADIUS Clients* and select *New*.

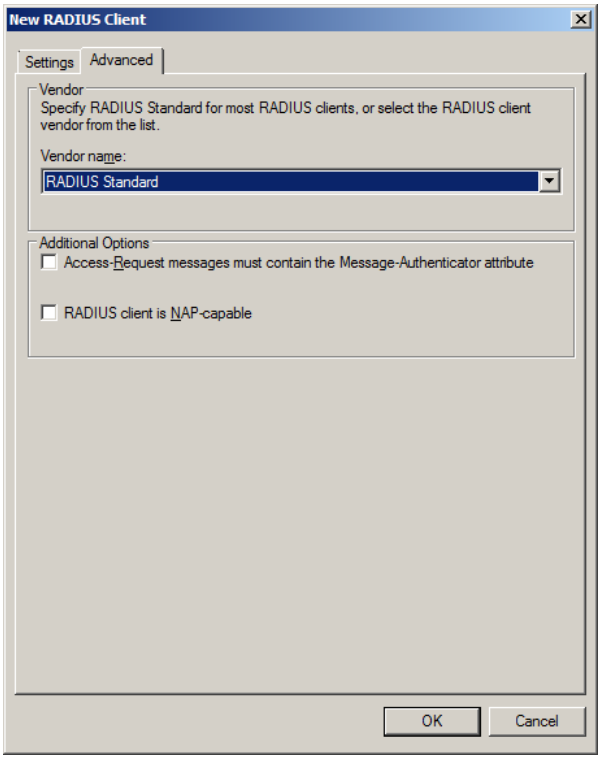


(4) On the *Settings* tab, enter values for:

- "Friendly name" of the Palo Alto device;
- Address (IP address or DNS) of the Palo Alto device. Use the Verify option to ensure that entered IP Address or DNS name is valid;
- Enter and Confirm your Shared Secret. Ensure that the shared secret matches the secret entered later on the Palo Alto device. You can also use the *Generate* option to generate a highly secure random secret.

Ensure that the *Enable this RADIUS client* checkbox is ticked.

(5) Select the *Advanced* tab.



(6) Ensure that the:

- Vendor name is set to *RADIUS Standard*.
- The *Access-Request messages must contain the Message-Authenticator attribute* is optional but must be set the same as on the RADIUS client device.
- Ensure that *RADIUS client is NAP-capable* is NOT selected

Click *OK*

You may add as many Palo Alto RADIUS clients as required.

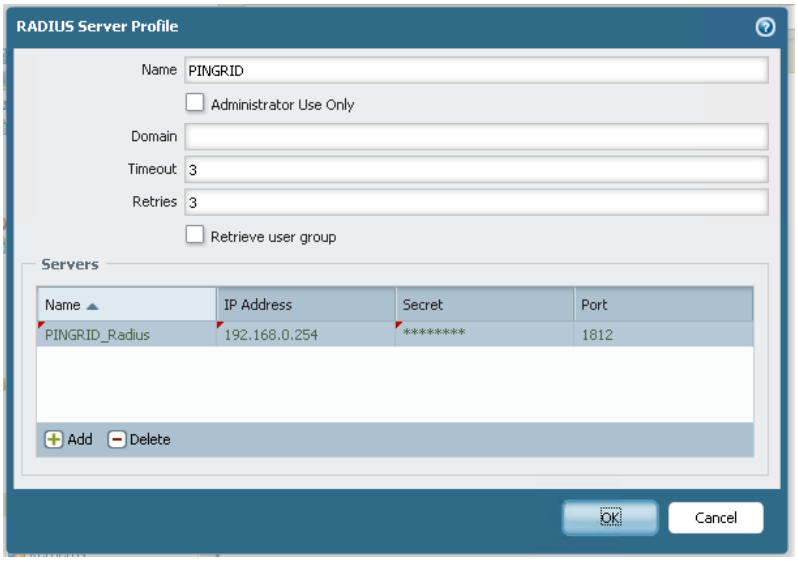
Palo Alto Device Configuration

The Palo Alto device will require configuration for use with Authlogics Authentication Server. This section should only be followed after Authlogics Authentication Server has been fully configured and tested.

Configuring the RADIUS server

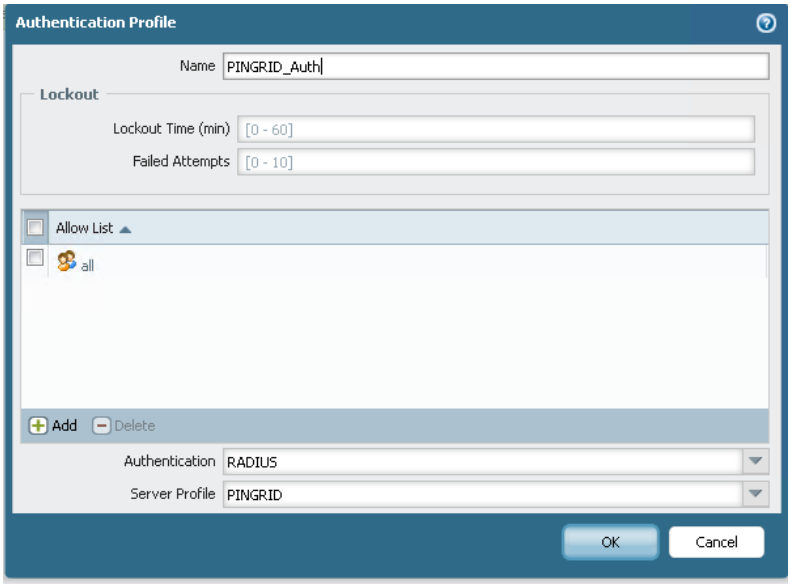
These steps are performed on the Palo Alto device.

(1) Start the Palo Alto Networks Administration console.
(2) Select the *Device* tab -> *Server Profiles->RADIUS*. Click *Add*.



Parameter	Description	Sample Value
Name	Provide a descriptive name for the Authlogics Authentication Server.	PINgrid
Domain	Optional domain name appended to the authentication server.	{Blank}
IP Address or hostname	Provide the IP Address or FQDN of the Authlogics Authentication Server	192.168.0.254
Shared secret	Enter the shared secret as specified in the RADIUS Client	Thisisasecret
Port	Provide the port number that RADIUS is operating on	1812

(3) Click *OK*.
(4) Create an Authentication Profile. In the Palo Alto Networks Administration console, select *Device -> Authentication Profiles*. Click *New*.



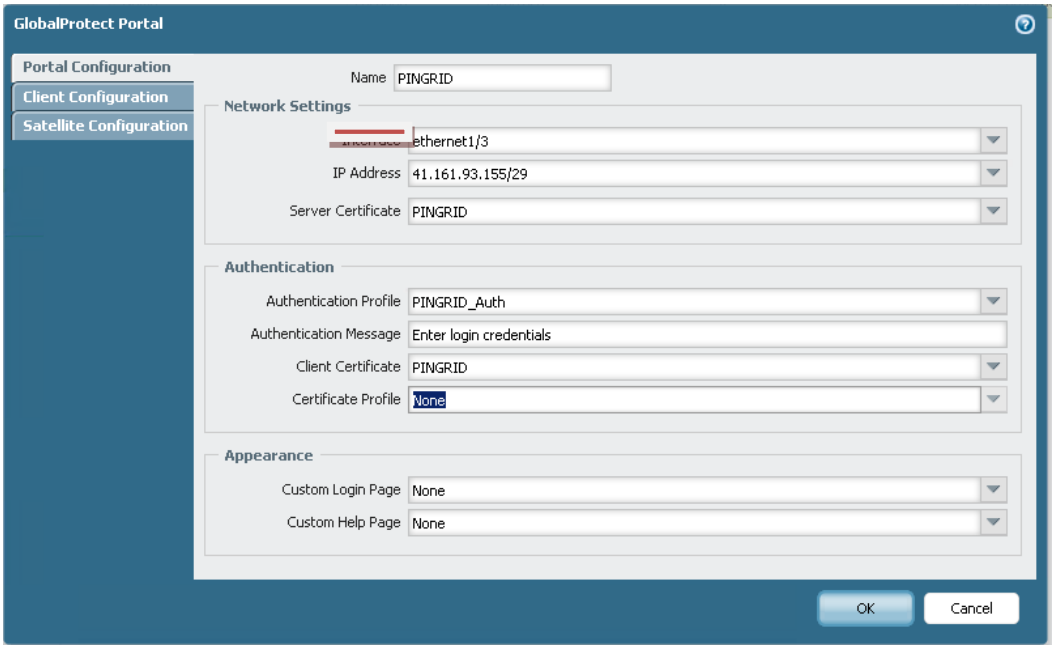
Parameter	Description	Sample Value
Name	Provide a descriptive name for the Authlogics Authentication Server Profile	PINgrid_Auth
Authentication	Select the authentication type.	RADIUS
Server Profile	Select the Authlogics Authentication Server Profile created above.	PINgrid

(5) Click *OK*.

Configuring GlobalProtect Portal

To configure the Palo Alto GlobalProtect Portal to use the above created Authlogics Authentication Server Authentication Profile for authentication, perform the following steps:

(1) Start the Palo Alto Networks Administration console.
(2) Select the *Network* tab -> *Global Protect*
(3) Select either an existing GlobalProtect Portal or a new one by clicking *New*.

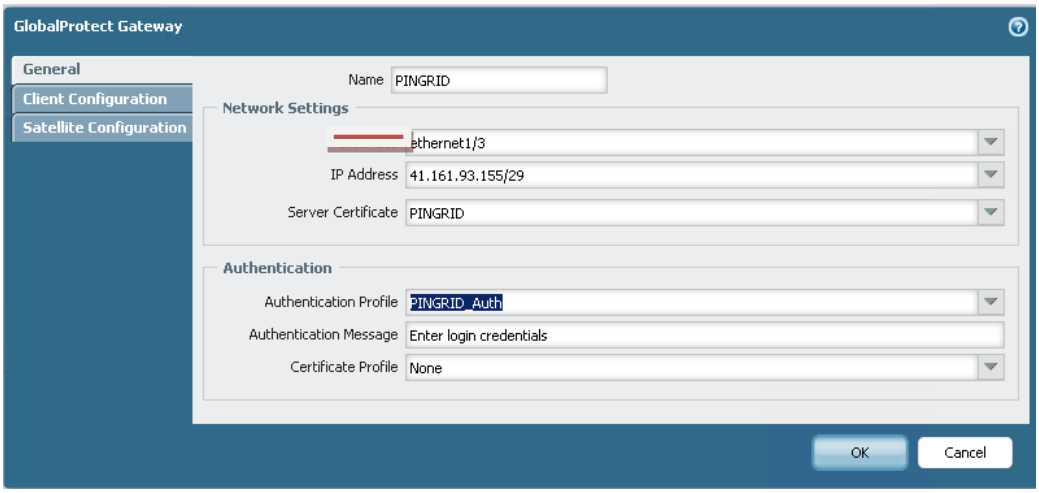


(4) Using the *Authentication Profile*, select the Authlogics Authentication Server Authentication Profile created in the steps above.
(5) Click *OK*.

Configuring GlobalProtect Gateway

To configure the Palo Alto GlobalProtect Gateway to use the above created Authlogics Authentication Server Authentication Profile for authentication, perform the following steps:

(1) Start the Palo Alto Networks Administration console.
(2) Select the *Network* tab -> *Global Protect*
(3) Select either an existing GlobalProtect Gateway or a new one by clicking *New*.



(4) Using the *Authentication Profile*, select the Authlogics Authentication Server Authentication Profile created in the steps above.
(5) Click *OK*.