



Palo Alto Integration Guide

With PINgrid, PINphrase and PINpass technology

Product Version: 3.3.x

Publication date: March 2019

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organisations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organisation, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

Authlogics may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written licence agreement from Authlogics, the furnishing of this document does not give you any licence to these patents, trademarks, copyrights, or other intellectual property.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

The information contained in this document represents the current view of Authlogics on the issues discussed as of the date of publication. Because Authlogics must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Authlogics, and Authlogics cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. AUTHLOGICS LTD MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS Document.

Copyright © 2019 Authlogics Ltd. All rights reserved.



Table of Contents

Introduction	3
Considerations	3
Requirements.....	3
Language Requirements	3
Authlogics Authentication Server Configuration	4
Adding a RADIUS client on the Authlogics Authentication Server.....	4
Palo Alto Device Configuration	7
Configuring the RADIUS server	7
Configuring GlobalProtect Portal to use Authlogics Authentication Server	9
Configuring GlobalProtect Gateway to use Authlogics Authentication Server	10



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/authlogics-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 Requirements

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 Authlogics Authentication Server

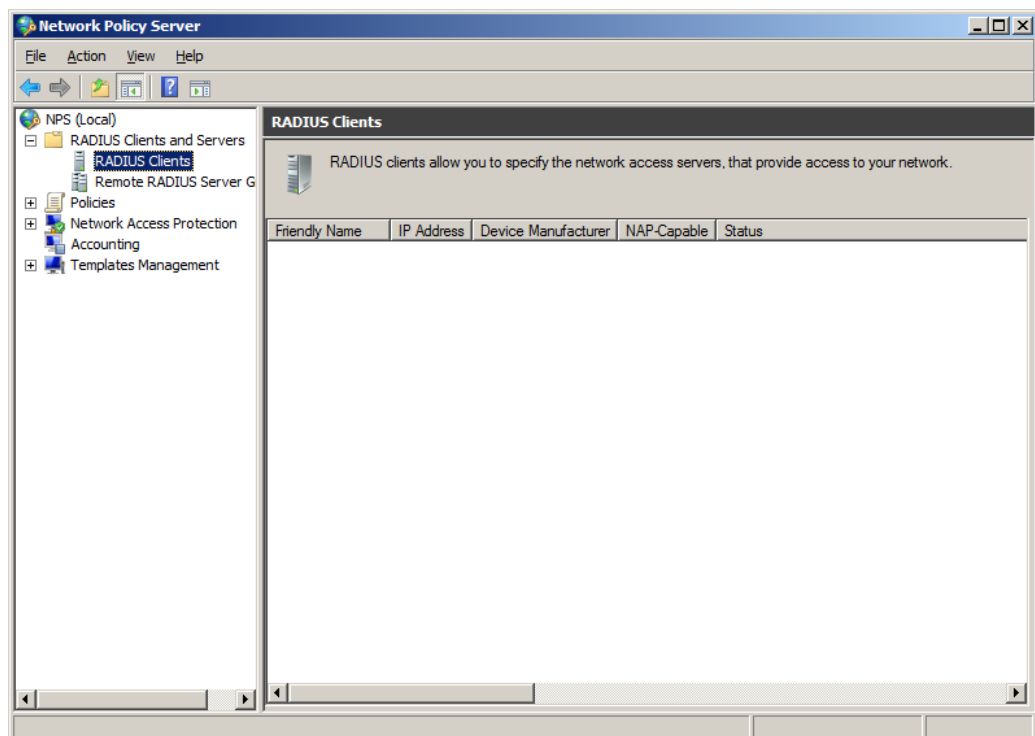
These steps are performed on the Authlogics Authentication Server.



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*.



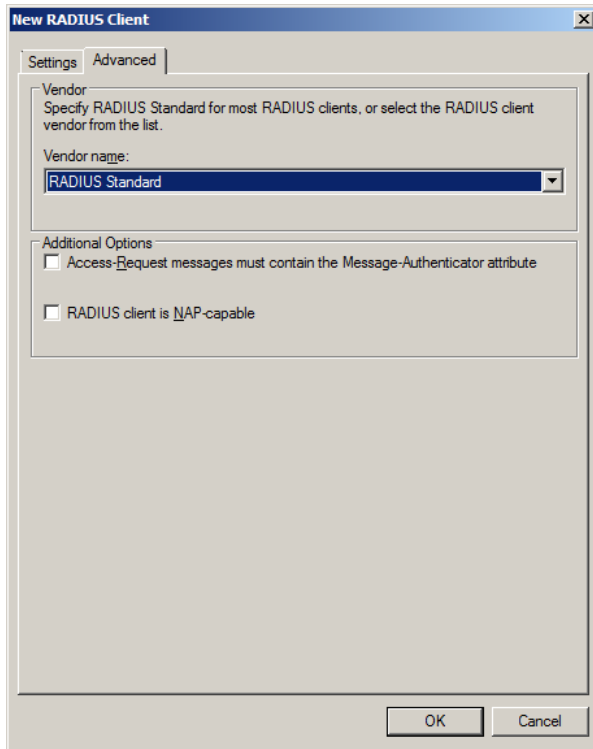
(4) On the *Settings* tab, enter values for:

- “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*.

Name	IP Address	Secret	Port
PINGRID_Radius	192.168.0.254	*****	1812

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 use Authlogics Authentication Server

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*.

The screenshot shows the configuration window for a GlobalProtect Portal named 'PINGRID'. The 'Authentication' section is the focus, where the 'Authentication Profile' is set to 'PINGRID_Auth'. Other settings include the interface 'Ethernet1/3', IP address '41.161.93.155/29', and server certificate 'PINGRID'. The 'Appearance' section shows custom pages set to 'None'.

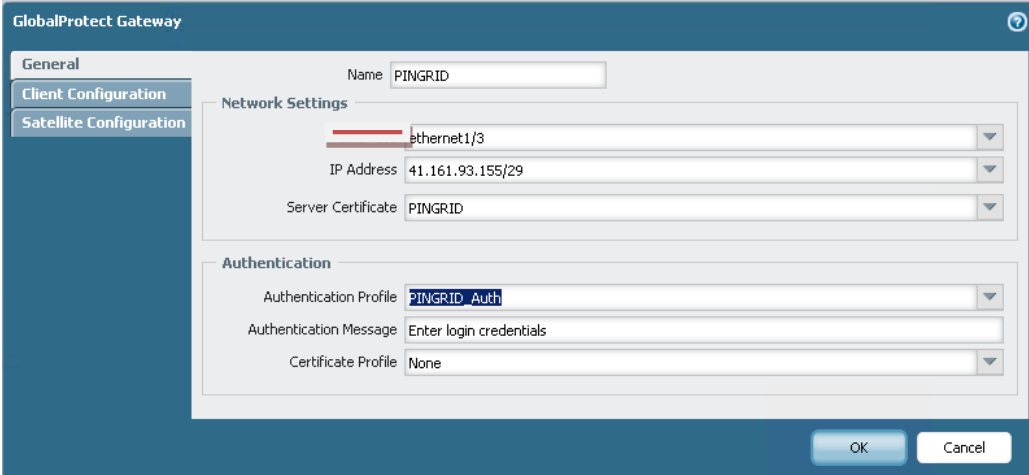
- (4) Using the *Authentication Profile*, select the Authlogics Authentication Server Authentication Profile created in the steps above.
- (5) Click *OK*.



Configuring GlobalProtect Gateway to use Authlogics Authentication Server

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*.



The screenshot displays the 'GlobalProtect Gateway' configuration window. On the left, there is a sidebar with three tabs: 'General' (selected), 'Client Configuration', and 'Satellite Configuration'. The main area is divided into two sections: 'Network Settings' and 'Authentication'. In the 'Network Settings' section, the 'Name' field is 'PINGRID', the interface is 'Ethernet1/3', the 'IP Address' is '41.161.93.155/29', and the 'Server Certificate' is 'PINGRID'. In the 'Authentication' section, the 'Authentication Profile' is 'PINGRID_Auth', the 'Authentication Message' is 'Enter login credentials', and the 'Certificate Profile' is 'None'. At the bottom right, there are 'OK' and 'Cancel' buttons.

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

