

intercede



MyID MFA and PSM

Version 5.0.8

Palo Alto Integration Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | [@intercedemyid](https://twitter.com/intercedemyid) | +44 (0)1455 558111

Copyright

© 2001-2025 Intercede Limited. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished exclusively under a restricted license or non-disclosure agreement. Copies of software supplied by Intercede Limited may not be used resold or disclosed to third parties or used for any commercial purpose without written authorization from Intercede Limited and will perpetually remain the property of Intercede Limited. They may not be transferred to any computer without both a service contract for the use of the software on that computer being in existence and written authorization from Intercede Limited.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Intercede Limited.

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

Licenses and Trademarks

The Intercede® and MyID® word marks and the MyID® logo are registered trademarks of Intercede in the UK, US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such. All other trademarks acknowledged.

Apache log4net

Apache License Version 2.0, January 2004 <http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

© You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. ---

Conventions used in this document

- Lists:
 - Numbered lists are used to show the steps involved in completing a task when the order is important.
 - Bulleted lists are used when the order is unimportant or to show alternatives.
- **Bold** is used for menu items and for labels.
For example:
 - Record a valid email address in '**From**' email address.
 - Select **Save** from the **File** menu.
- *Italic* is used for emphasis:
For example:
 - Copy the file *before* starting the installation.
 - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks are used to identify the titles of other documents.
For example: "See the ***Release Notes*** for further information."
Unless otherwise explicitly stated, all referenced documentation is available on the product installation media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.
For example:
Note: This issue only occurs if updating from a previous version.
- **Warnings** are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.
For example:
Warning: You must take a backup of your database before making any changes to it.

Contents

Palo Alto Integration Guide	1
Copyright	2
Conventions used in this document	6
Contents	7
1 Introduction	8
1.1 Considerations	8
1.1.1 Prerequisites	8
1.1.2 Language	8
1.2 Change history	8
2 MyID Authentication Server configuration	9
2.1 Adding a RADIUS client on the MyID Authentication Server	9
2.2 Palo Alto device configuration	12
2.2.1 Configuring the RADIUS server	12
2.2.2 Configuring the GlobalProtect Portal	14
2.2.3 Configuring GlobalProtect Gateway	15
3 Testing your authentication profile	16

1 Introduction

Note: MyID MFA and MyID PSM were previously known as Authlogics products. Authlogics is now an Intercede Group company and the products have been rebranded accordingly. The term 'Authlogics' may still appear in certain areas of the product.

MyID Authentication Server is a multi-factor authentication system which is pre-integrated with a RADIUS server that 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 MyID with Palo Alto servers using RADIUS.

For step-by-step setup instructions, see the *Adding a RADIUS client* section of the [MyID Authentication Server Installation and Configuration Guide](#).

1.1 Considerations

1.1.1 Prerequisites

You must deploy and configure the Palo Alto device *and* deploy and configure the MyID Authentication Server using the standard username and password authentication mechanism before you configure integration through RADIUS.

1.1.2 Language

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

1.2 Change history

Version	Description
IMP2050-01	Reformatted and released with MyID MFA and PSM version 5.0.7.
IMP2050-5.0.8	Released with MyID MFA and PSM version 5.0.8.

2 MyID Authentication Server configuration

You must configure the MyID Authentication Server for use with the Palo Alto device. The Palo Alto device sends authentication requests to the MyID Authentication Server through RADIUS; you must therefore configure the MyID Authentication Server to accept RADIUS requests from the Palo Alto device.

You must:

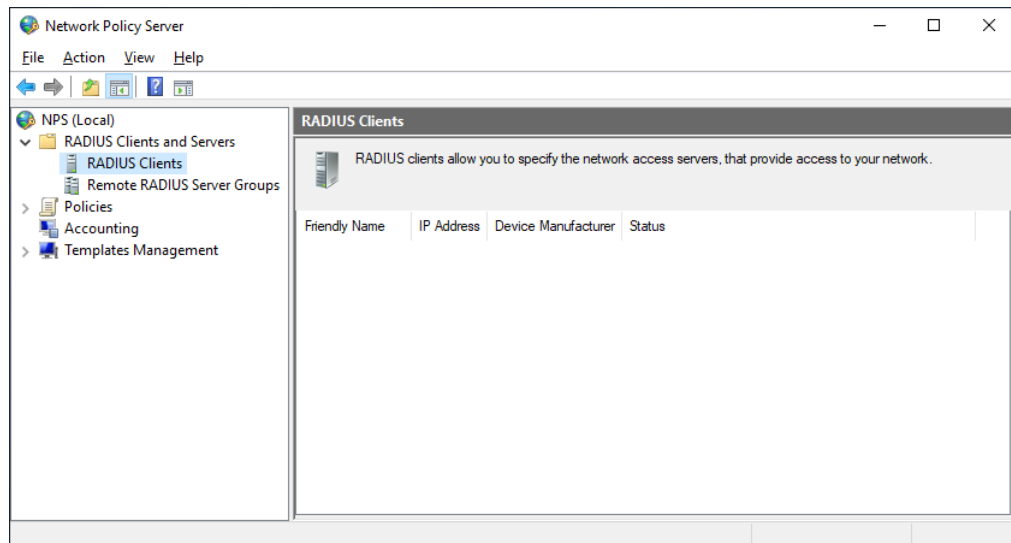
- Add the Palo Alto device as a RADIUS client to the MyID Authentication Server.
See section [2.1, Adding a RADIUS client on the MyID Authentication Server](#).
- Configure the Palo Alto device for the MyID Authentication Server.
See section [2.2, Palo Alto device configuration](#).

2.1 Adding a RADIUS client on the MyID Authentication Server

Carry out this procedure on the MyID Authentication Server.

Note: This section of the installation process requires Local Administrator rights on the server. You do not require domain rights at this stage.

1. From the Administrative Tools start menu group, open the **Network Policy Server**.
2. Select **RADIUS Clients and Servers**, then **RADIUS Clients**.



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

New RADIUS Client

Settings Advanced

Enable this RADIUS client

Select an existing template:

Name and Address

Friendly name:
VPN Server

Address (IP or DNS):
vpn.authlogicsdemo.com

Shared Secret

Select an existing Shared Secrets template:
None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual Generate

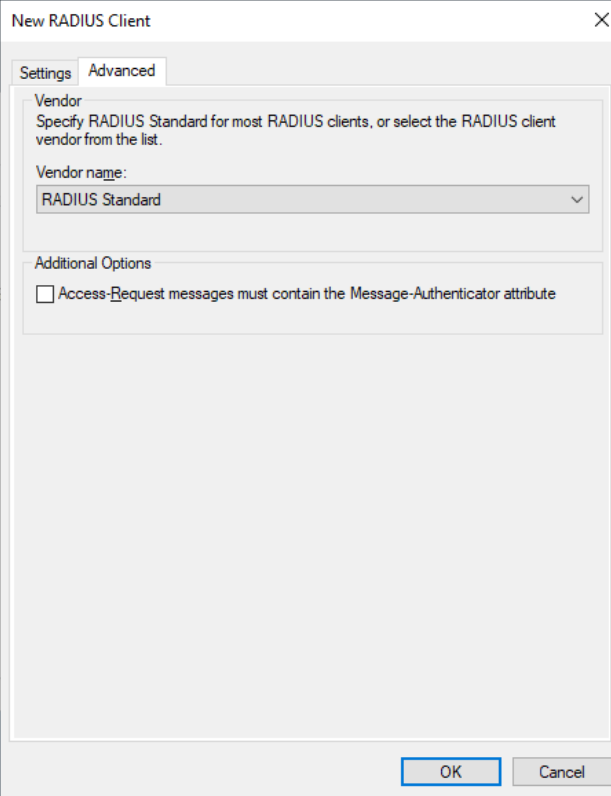
Shared secret:
.....

Confirm shared secret:
.....

4. On the **Settings** tab, enter values for:
 - **Friendly name** – type the friendly name of the Palo Alto device.
 - **Address (IP address or DNS)** – type the IP address or DNS of the Palo Alto device. Click **Verify** to ensure that entered IP address or DNS name is valid.
 - **Shared Secret** – select a template, then either provide a **Manual** shared secret or use the **Generate** option to generate a highly secure random secret.

Note: Make sure that the shared secret matches the secret you enter later on the Palo Alto device.
5. Ensure that the **Enable this RADIUS client** option is selected.

6. Click the **Advanced** tab.



The screenshot shows a dialog box titled "New RADIUS Client" with a close button (X) in the top right corner. It has two tabs: "Settings" and "Advanced", with "Advanced" selected. The "Vendor" section contains the text "Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list." Below this is a "Vendor name:" label and a dropdown menu currently showing "RADIUS Standard". The "Additional Options" section contains a checkbox labeled "Access-Request messages must contain the Message-Authenticator attribute", which is currently unchecked. At the bottom of the dialog are "OK" and "Cancel" buttons.

7. Set the following:

- **Vendor name** – make sure this is set to `RADIUS Standard`.
- **Access-Request messages must contain the Message-Authenticator attribute** – this is optional, but you must make sure it is the same as on the RADIUS client device.

8. Click **OK**.

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

2.2 Palo Alto device configuration

You must configure the Palo Alto device for use with MyID Authentication Server. Follow the instructions in this section after you have fully configured and tested the MyID Authentication Server.

2.2.1 Configuring the RADIUS server

On the Palo Alto device, carry out the following.

1. Start the Palo Alto Networks Administration console.
2. On the **Device** tab, select **Server Profiles > RADIUS**.
3. Click **Add**.

RADIUS Server Profile

Name: PINGRID

Administrator Use Only

Domain:

Timeout: 3

Retries: 3

Retrieve user group

Servers

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

+ Add - Delete

OK Cancel

4. Set the following options:

- **Name** – Provide a descriptive name for the MyID Authentication Server.

For example:

PINGrid

- **Domain** – Optionally, provide a domain name to be appended to the authentication server.

- **IP Address or hostname** – Provide the IP Address or FQDN of the MyID Authentication Server.

For example:

192.168.0.254

- **Shared secret** – Enter the shared secret as specified in the RADIUS Client.

For example:

Thisisasecret

- **Port** – Provide the port number on which RADIUS is operating.

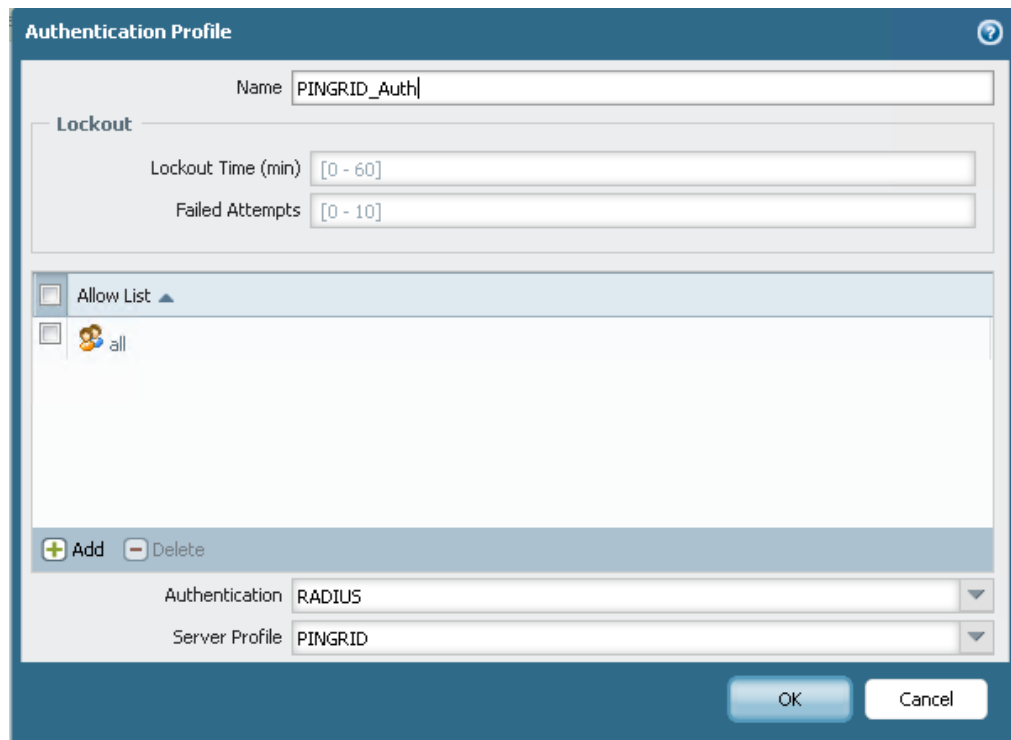
For example:

1812

5. Click **OK**.

6. Create an Authentication Profile.

In the Palo Alto Networks Administration console, select **Device > Authentication Profiles**, then click **New**.



The screenshot shows the 'Authentication Profile' configuration window. The 'Name' field is set to 'PINGRID_Auth'. The 'Lockout' section has 'Lockout Time (min)' set to '[0 - 60]' and 'Failed Attempts' set to '[0 - 10]'. The 'Allow List' section shows a list with one entry: 'all'. Below the list are '+ Add' and '- Delete' buttons. The 'Authentication' dropdown is set to 'RADIUS' and the 'Server Profile' dropdown is set to 'PINGRID'. At the bottom right are 'OK' and 'Cancel' buttons.

7. Set the following options:

- **Name** – Provide a descriptive name for the MyID Authentication Server Profile.

For example:

PINGrid_Auth

- **Authentication** – Select the authentication type.

For example:

RADIUS

- **Server Profile** – Select the MyID Authentication Server Profile created above.

For example:

PINGrid

8. Click **OK**.

2.2.2 Configuring the GlobalProtect Portal

To configure the Palo Alto Networks Administration console to use the above created MyID Authentication Server Authentication Profile for authentication, carry out the following:

1. Start the Palo Alto Networks Administration console.
2. On the **Network** tab, select **Global Protect**.
3. Either select an existing GlobalProtect Portal, or click **New** to create a new one.

The screenshot shows the 'GlobalProtect Portal' configuration window. The 'Name' field is set to 'PINGRID'. Under 'Network Settings', the 'Interface' is 'ethernet1/3', 'IP Address' is '41.111.111.155/29', and 'Server Certificate' is 'PINGRID'. In the 'Authentication' section, the 'Authentication Profile' is 'PINGRID_Auth', the 'Authentication Message' is 'Enter login credentials', the 'Client Certificate' is 'PINGRID', and the 'Certificate Profile' is 'None'. Under 'Appearance', both 'Custom Login Page' and 'Custom Help Page' are set to 'None'. The 'OK' and 'Cancel' buttons are visible at the bottom right.

4. From the **Authentication Profile** drop-down list, select the MyID Authentication Server Authentication Profile that you created.

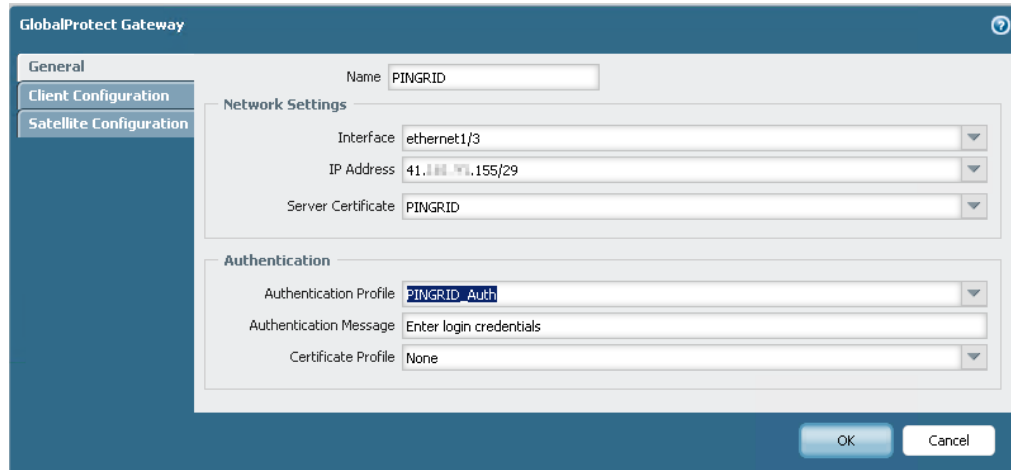
See section [2.2.1, Configuring the RADIUS server](#) for details.

5. Click **OK**.

2.2.3 Configuring GlobalProtect Gateway

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

1. Open the Palo Alto Networks Administration console.
2. Select the **Network** tab, then select **Global Protect**.
3. Either select an existing GlobalProtect Gateway, or click **New** to create a new one.



The screenshot displays the 'GlobalProtect Gateway' configuration window. On the left, a sidebar contains three tabs: 'General' (selected), 'Client Configuration', and 'Satellite Configuration'. The main area is divided into two sections: 'Network Settings' and 'Authentication'. In 'Network Settings', the 'Name' field contains 'PINGRID', 'Interface' is 'ethernet1/3', 'IP Address' is '41.111.111.155/29', and 'Server Certificate' is 'PINGRID'. In the 'Authentication' section, 'Authentication Profile' is set to 'PINGRID Auth', 'Authentication Message' is 'Enter login credentials', and 'Certificate Profile' is 'None'. At the bottom right, there are 'OK' and 'Cancel' buttons.

4. From the **Authentication Profile** drop-down list, select the MyID Authentication Server Authentication Profile that you created.
See section [2.2.1, Configuring the RADIUS server](#) for details.
5. Click **OK**.

3 Testing your authentication profile

To test your Palo Alto Authentication Profile:

1. Log in to the Palo Alto Server and run the following PAN-OS CLI command:

```
test authentication authentication-profile "<RADIUS Profile name>"
username "<username>" password
```

Where:

- <RADIUS Profile name> – the name you set for the RADIUS Server Profile.
- <username> – the username of an MFA user.

2. Enter authentication credentials for the MFA user.

This may be the Active Directory password or an OTP, depending on how you have set up your RADIUS client. MyID MFA and PSM supports the standard RADIUS return Access-Challenge response. For more information, see the *2-step logons (Access-Challenge)* section in the [MyID Authentication Server Installation and Configuration Guide](#).

If you provide valid credentials and you have set up your RADIUS client to take only one form of authentication credential, the return from the `test` CLI command includes:

```
Authentication succeeded for user "<username>"
```

While MyID MFA and PSM supports RADIUS Access-Challenge response, the `test` CLI command does not support this feature. If you have set up your RADIUS client for this, the return from the `test` CLI command includes:

```
Got challenge response, which is regarded as failed auth since "test auth
..." CLI command does not support it.
```

This is a successful test.