SafeNet Authentication Client

Integration Guide

Using SAC CBA with Palo Alto GlobalProtect

Document Information

Document Part Number	007-012826-001, Rev. A
Release Date	November 2014

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Third-Party Software Acknowledgement 4
Description 4
Applicability 4
Environment 4
Audience 4
Prerequisites 5
Authentication Flow 5
Configuring Palo Alto for Certificate-based Authentication 6
    Adding the Root-CA Certificate 6
    Adding the Server Certificate 7
    Creating a Certificate Profile 8
    Configuring GlobalProtect 10
Running the Solution 12
    CBA Using GlobalProtect Software 12
Support Contacts 13

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Palo Alto GlobalProtect.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Palo Alto using any of SafeNet's certificate-based tokens.

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. It utilizes a system of digital certificates, certificate authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). SafeNet Authentication Client manages SafeNet's extensive portfolio of certificate-based tokens, ensuring full support for all currently deployed eToken and iKey devices.

Palo Alto GlobalProtect is a platform that safely enables applications, users, and content in your enterprise branch offices. Dedicated computing resources for the functional areas of networking, security, content inspection, and management ensure predictable firewall performance.

Applicability

The information in this document applies to:

- SafeNet Authentication Client 8.3 (SAC 8.3)
- Palo Alto PA-200

Environment

The integration environment that was used in this document is based on the following software versions:

- SafeNet Authentication Client 8.3 (SAC)
- Palo Alto PA-200
- Palo Alto GlobalProtect firmware version 2.0.3-5

Audience

This document is targeted to system administrators who are familiar with Palo Alto GlobalProtect and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Client.

Prerequisites

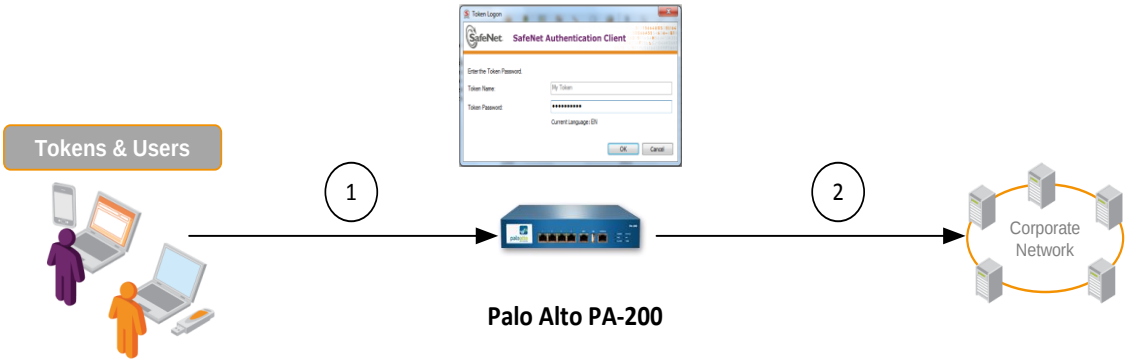
This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for Palo Alto PA using GlobalProtect.

- **Microsoft CA** – In order to use CBA, the Microsoft certificate authority must be installed and configured. In this Integration Guide, a stand-alone Microsoft CA is installed on the domain controller machine.
- **SafeNet Authentication Client 8.3 (SAC)** – Includes all the files and drivers needed to support SafeNet smart card integration. SafeNet Authentication Client must be installed on each computer where the smart card is going to be used.
- **GlobalProtect Software**

> **NOTE:** This document assumes that Palo Alto GlobalProtect is installed, and that the solution is using static passwords or any other user-authentication method.

Authentication Flow

The image below shows the environment required to implement Palo Alto GlobalProtect using SafeNet's certificate-based authentication, and illustrates the dataflow of the authentication request.



1. A user is required to authenticate to Palo Alto PA-200 via the GlobalProtect application using SafeNet's certificate-based token.

   SafeNet's token is deployed with a user-unique client certificate for authentication. When the user is authenticated, they must provide a PIN to access the token. The credentials are passed to the Palo Alto gateway, which will accept or reject the authentication request.

2. After successful authentication, the user receives VPN/SSL access to the network.

Configuring Palo Alto for Certificate-based Authentication

The configuration of Palo Alto PA-200 with certificate-based authentication (CBA) requires the following:

- Adding the Root-CA Certificate
- Adding the Server Certificate
- Creating a Certificate Profile
- Configuring GlobalProtect

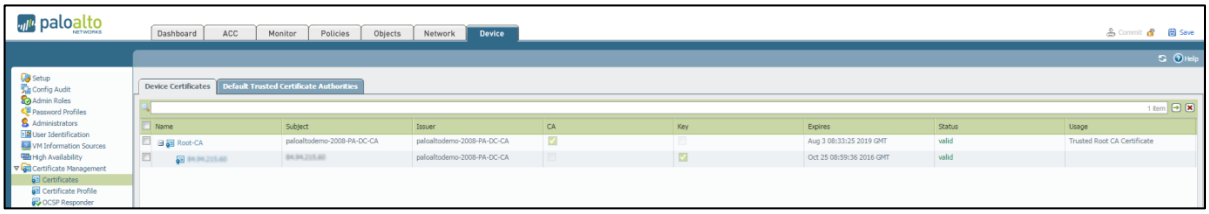
Adding the Root-CA Certificate

This section explains how the Root-CA certificate is added to the Palo Alto gateway. The root CA certificate is used to authenticate users with a valid user certificate.

To add the root CA Certificate to the Palo Alto gateway:

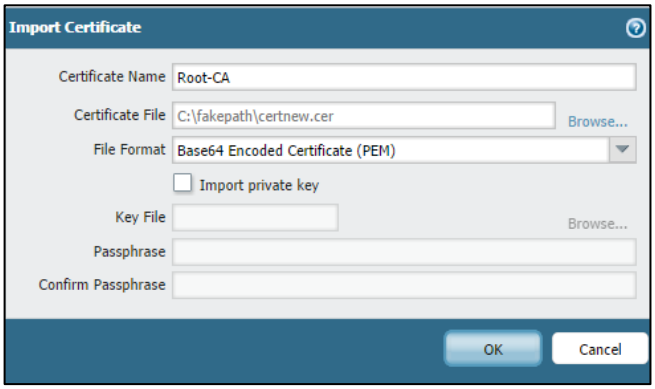
1. Connect to the Palo Alto PA-200 web console.
2. Click the **Device** tab. In the left pane, click **Certificate Management > Certificates**.

(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)



(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

3. Click **Import** at the bottom of the page to import the Root-CA certificate. The **Import Certificate** window is displayed.



(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

4. On the **Import Certificate** window, enter the following:

Certificate Name	Enter the certificate name
Certificate File	Click **Browse**, and then select the Root-CA certificate file
File Format	Use the default file format, **Base64**.

5. Click **OK**.

Adding the Server Certificate

This section explains how to add a server certificate to the Palo Alto PA-200 in order to accept SSL connections.

To add a server certificate to the Palo Alto PA-200:

1. Connect to the Palo Alto web console.
2. Click the **Device** tab. In the left pane, click **Certificate Management > Certificates**.

(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

3. Click **Import** at the bottom of the page to import the server certificate. The **Import Certificate** window is displayed.

4. On the **Import Certificate** window, enter the following:

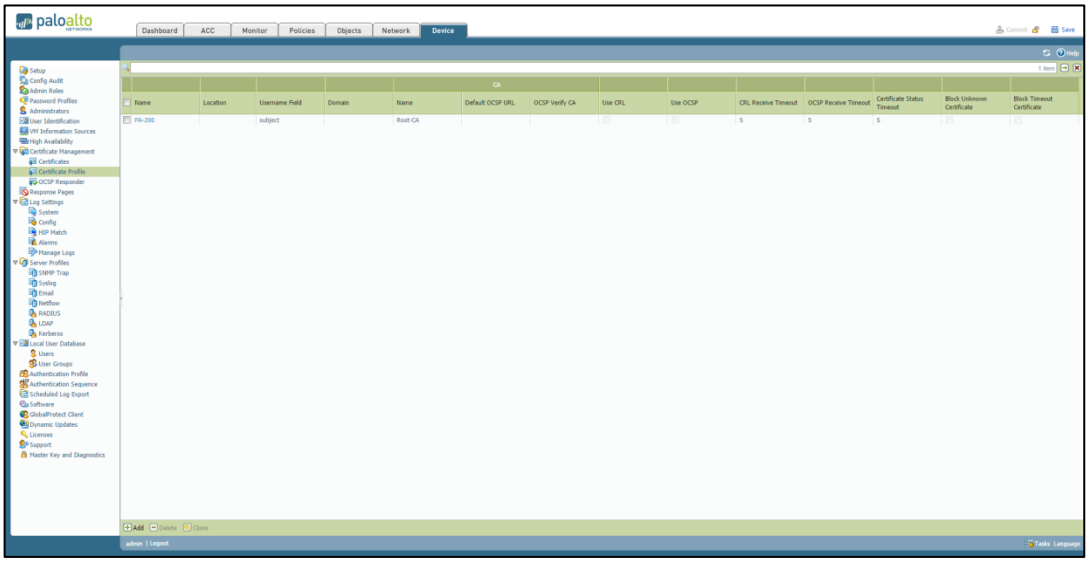
Certificate Name	Enter the certificate name.
Certificate File	Click **Browse**, and then select the Root-CA certificate file.
File Format	Use the default file format, **Base64**.

5. Click **OK**.

Creating a Certificate Profile

The following section describes how to create a certificate profile that will be used to define the CBA authentication.

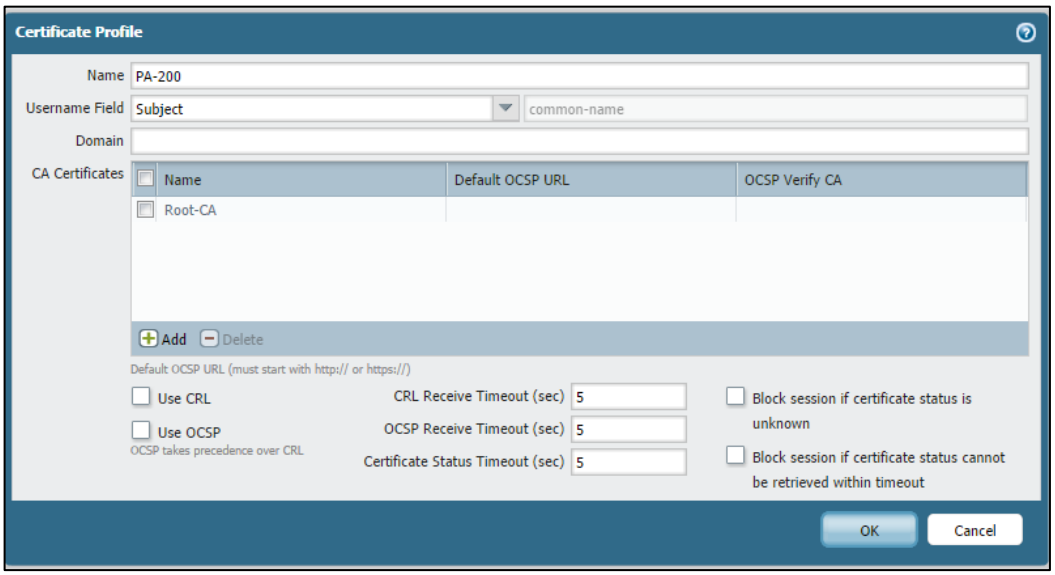
1. Connect to the Palo Alto web console.



(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

2. Click the **Device** tab. In the left pane, click **Certificate Management > Certificate Profile**.

3. Click **Add**. The **Certificate Profile** window is displayed.

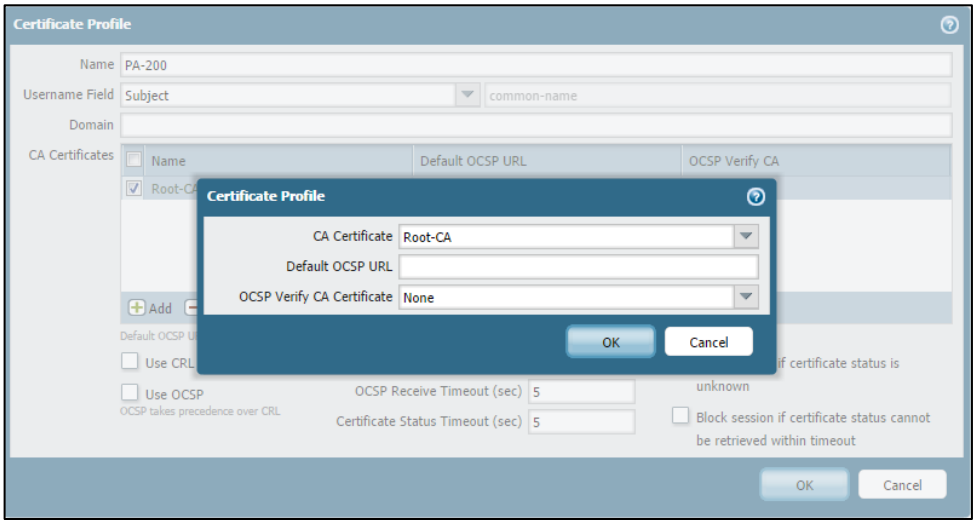


(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

4. On the **Certificate Profile** window, enter the following:

Name	Enter the profile name.
Username Field	Select **Subject**.

5. Click **Add.** The **Certificate Profile** window is displayed.



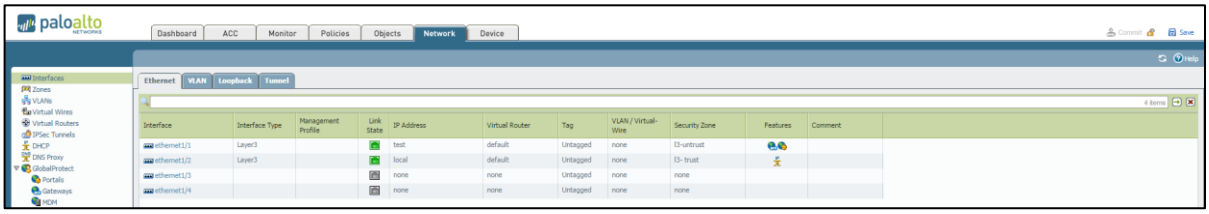
(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

6. In the **CA Certificate** field, select the Root-CA certificate that was added under "Adding the Root-CA Certificate" on page 6. Click **OK** to continue.
7. Click **OK** again to add the certificate profile.
8. Click **Commit** to commit the changes.

Configuring GlobalProtect

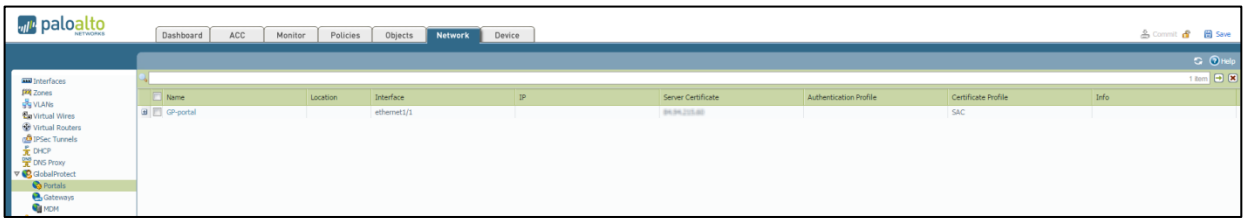
To configure GlobalProtect to use CBA:

1. Connect to the Palo Alto web console.
2. Click the **Network** tab.



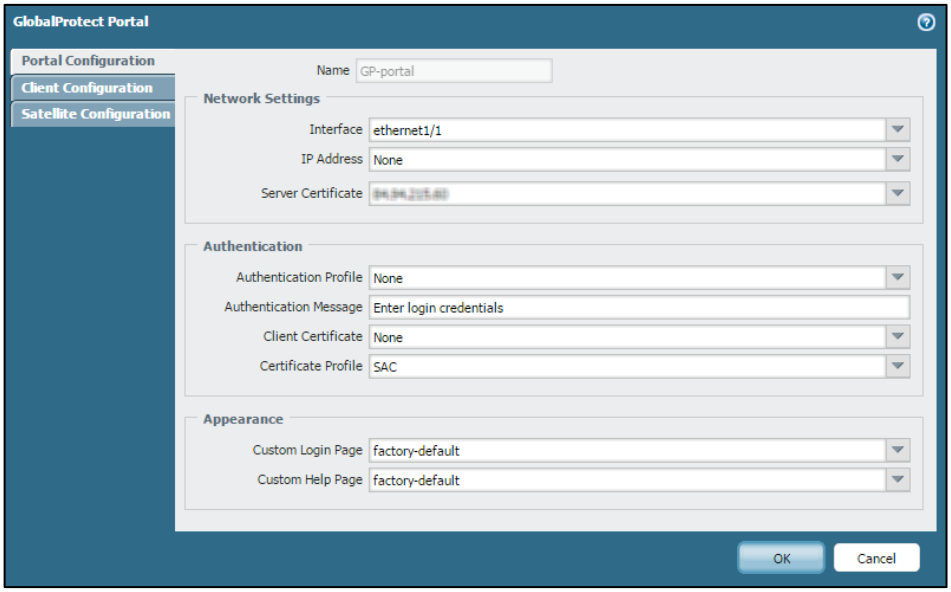
(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

3. In the left pane, click **GlobalProtect > Portals.**



(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

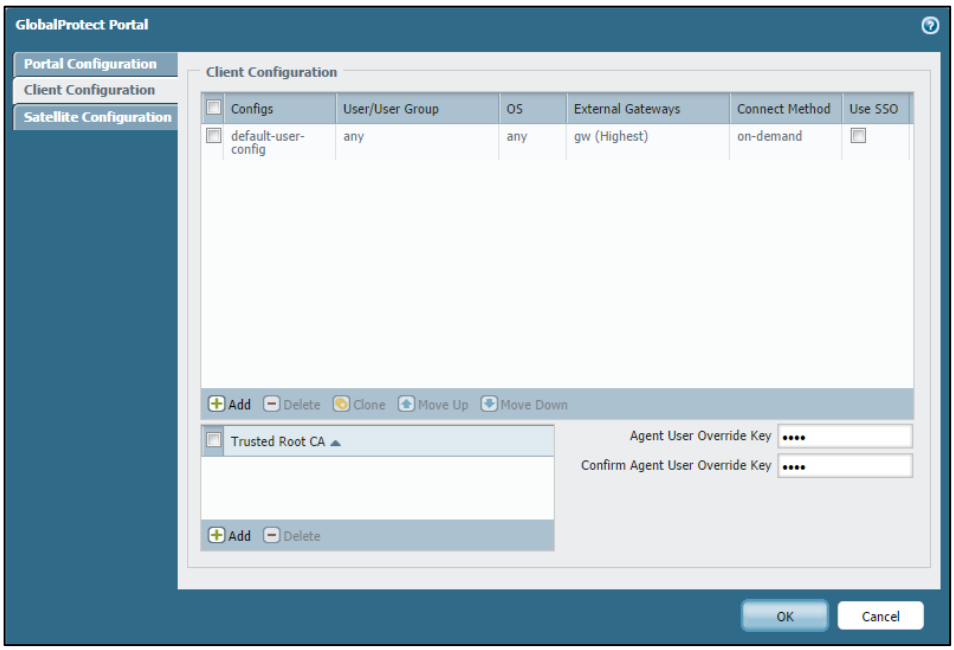
4. Select the portal created previously (it is assumed that you have a portal configured with username/password authentication). The **GlobalProtect Portal** window is displayed.
5. Under **Authentication**, in the **Authentication Profile** field, select **None**.



(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

6. Under **Authentication**, in the **Certificate Profile** field, select the certificate profile that was created under “Creating a Certificate Profile” on page 8.

7. In the left pane, click **Client Configuration**, and ensure that **Use SSO** is not selected.



(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

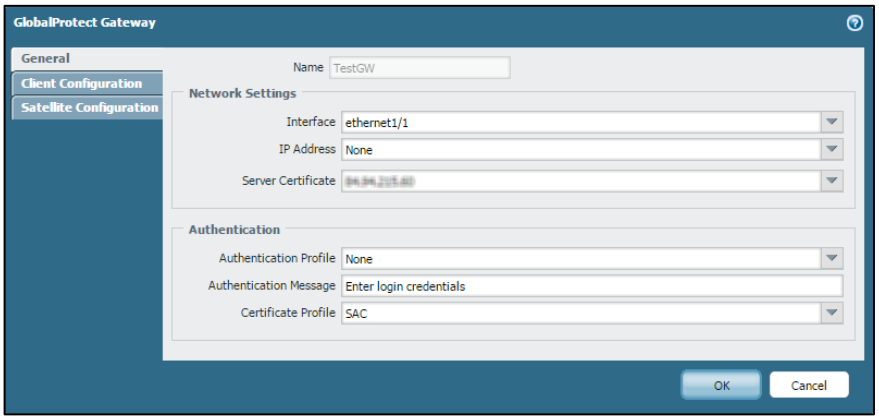
8. Click **OK.**

9. In the left pane, click **GlobalProtect > Gateways**.

(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.

10. Click the gateway created previously (it is assumed that you have a portal configured with username/password authentication).

11. On the **General** tab, under **Authentication**, select **None** in the **Authentication Profile** field. Under **Certificate Profile**, select the certificate profile that was created under “Creating a Certificate Profile” on page 8.



(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

12. Click **OK**.
13. Click **Commit** to commit the changes.

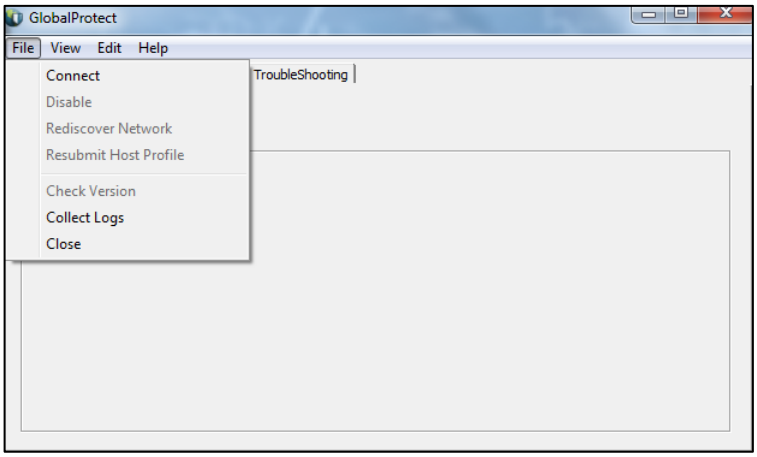
Running the Solution

This section explains how to authenticate to Palo Alto GlobalProtect using the GlobalProtect client and SAC.

This guide assumes that the GlobalProtect application is already installed on the client machine.

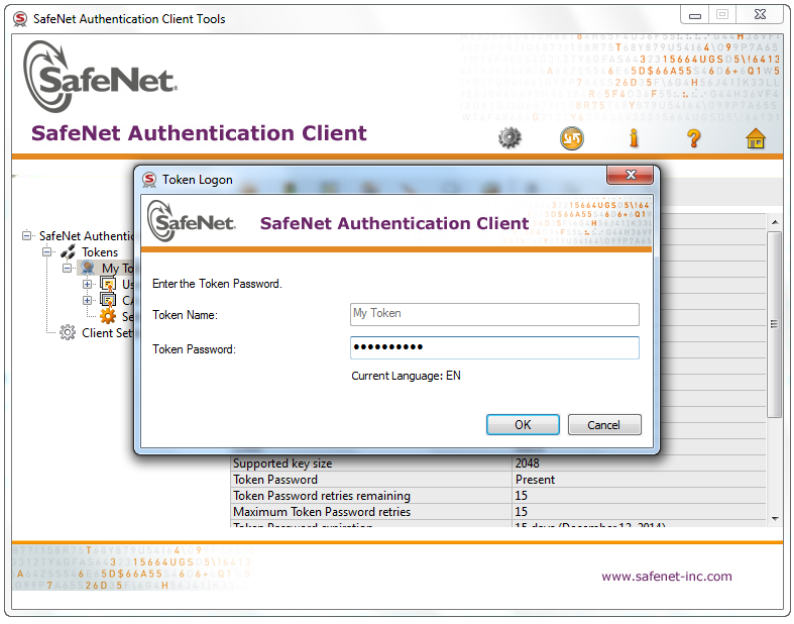
CBA Using GlobalProtect Software

1. Open the GlobalProtect client.
2. Click **File > Connect**.

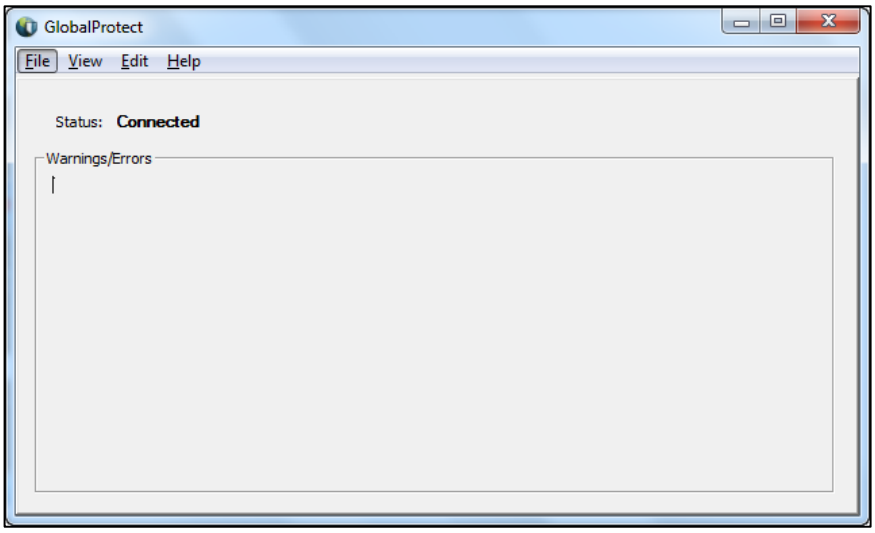


(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

3. On the **SafeNet Authentication Client** login window, enter the Token Password.



4. Click **OK**. The user is connected to the VPN.



(The screen image above is from Palo Alto Networks – GlobalProtect. Trademarks are the property of their respective owners.)

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	