SafeNet Authentication Client Integration Guide

Using SAC CBA with Palo Alto GlobalProtect



THE DATA PROTECTION COMPANY

Document Information

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

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

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 certificatebased 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.

Import Certificate		0
Certificate Name	Root-CA	
Certificate File	C:\fakepath\certnew.cer	Browse
File Format	Base64 Encoded Certificate (PEM)	
	Import private key	
Key File		Browse
Passphrase		
Confirm Passphrase		
	ок	Cancel

(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**.

paloalto	Dashboard ACC Monitor Policies Objects Network Device	de Carrot 🔗 😝 Son			
		S () Hộ			
Config Audit	Management Operations Services Content-ID WildFire Session				
Admin Roles	General Settings	Panorama Settings			
Administrators	Hostname PA	Panorama Servers			
User Identification	Domain	Receive Timeout for Connection to Device (sec) 240			
VM Information Sources	Login Banner	Send Timeout for Connection to Device (sec) 240			
High Availability	Time Zone Asia/Jerusalem	Retry Count for SSL Send to Device 25			
Certificate Management	Locale en				
Certificate Profile	Time Sun Nov 23 17:28:08 IST 2014	Management Interface Settings			
CCSP Responder	Geo Location	12 Address			
Response Pages	Automatically Acquire Commit Lock	Netmask			
▼ 🔁 Log Settings	Certificate Dipiration Check	Default Gateway			
System .		IPv6 Address/Prefix Length			
Leo Contig	Authentication Settings	Default IPv6 Gateway			

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

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.

🕡 palo <mark>alto</mark>	Dashboard	ACC Mo	nitor Policies	Objects	Network Device								á	Commit 💣 🗃 Save
	_					_								C Ottala
Contract Con	4													1 item (+) (*)
Config Audit														
Password Profiles	🔲 Name	Location	Username Field	Domain	Name	Default OCSP URL	OCSP Verify CA	Use CRL	Use OCSP	CRL Receive Timeout	OCSP Receive Timeout	Certificate Status Timeout	Block Unknown Certificate	Block Timeout Certificate
Burger Lander Lander Hard March March Hard March March Hard March March Hard March March Hard March March Hard March H	[] [16, 500]		någet		haro.					8	5	5		
	+Add - Delete 💿 🕻													
	admin Logout													Tasks Language

(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.

Certificate Profi	le			0							
Name	PA-200										
Username Field	J Subject common-name										
Domain											
CA Certificates	Name	Default OCSP	JRL	OCSP Verify CA							
	Root-CA										
	+ Add - Delete										
	Default OCSP URL (must start with http:// or https:/	/)									
	Use CRL C	RL Receive Timeout (s	ec) 5	Block session if certificate status is							
	Use OCSP OC	SP Receive Timeout (s	ec) 5	unknown							
	OCSP takes precedence over CRL Certifi	cate Status Timeout (s	ec) 5	Block session if certificate status cannot							
				be retrieved within timeout							
				OK Cancel							

(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.

Certificate Profi	le				0
Name	PA-200				
Username Field	Subject		common-name		
Domain					
CA Certificates	Name		Default OCSP URL	OCSP Verify C	Ą
	Root-C4 Cert	tificate Profile		0	
		CA Certificate	Root-CA		
		Default OCSP URL			
	+ Add -	OCSP Verify CA Certificate	None		_
	Default OCSP UI			OK Cancel	if certificate status is
	Use OCSP OCSP takes precedence	OCSP R e over CRL Certificate	eceive Timeout (sec) 5 Status Timeout (sec) 5	unknown Block session be retrieved	if certificate status cannot within timeout
					OK Cancel

(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.

	paloalto	Dashboard Al	CC Monito	r Policies	Obje	ects Network	Device						🛓 Commit 💰 🗟 Save
													S (0)Hdp
and in	terfaces	Ttherest WAR Couplest Tunnel											
ST VI	ANs tool Wires	•											4 korras 🖝 🕷
⊕ vi	tual Routers Ser Tunnels	Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual- Wire	Security Zone	Features	Comment	
ź D	CP	ethernet1/1	Layer3			test	default	Untagged	none	13-untrust	6.6		
2 D	IS Proxy	and ethernet1/2	Layer3			local	default	Untagged	none	13- trust	ź		
	Portals	ethernet1/3				none	none	Untagged	none	none			
	Gateways	and ethernet1/4				none	none	Untagged	none	none			

(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.**

paloalto	Dashboard ACC Monit	or Policies	Objects Network Devi	ce				🍰 Commit 👩 🗒 Save
								S 🔘 Help
and Interfaces	9							1 item 🔿 🗙
20nes	Name Name	Location	Interface	Ib	Server Certificate	Authentication Profile	Certificate Profile	Info
Sa Virtual Wires	😖 📰 GP-portal		ethemet1/1		04.94.215.60		SAC	
Virtual Routers								
2 IPSec Tunnels								
TOHEP								
V ClobalProtect								
Portals								
Gateways								
MDM 💕								

(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.

GlobalProtect Portal			0
Portal Configuration	Name	P-portal	
Client Configuration	Network Settings		
Satellite Configuration	Interface	ethernet1/1	
	IP Address	None	
	Server Certificate	26,26,205,80	
	Authentication		
	Authentication Profile	None	
	Authentication Message	Enter login credentials	
	Client Certificate	None	
	Certificate Profile	SAC 💌	
			-
	Appearance		
	Custom Login Page	factory-default 💌	
	Custom Help Page	factory-default	
		OK Cancel	

(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.

GlobalProtect Portal ()							
Portal Configuration	Client Configuration	n ————					
Satellite Configuration	Configs	User/User Group	os	External Gateways	Connect Method	Use SSO	
	default-user- config	any	any	gw (Highest)	on-demand		
	Add - Delete O Clone Move Up Move Down						
	Trusted Root CA	•		Agent User Overr	ide Key 🚥		
				Confirm Agent User Overr	ide Key		
	🛨 Add 🕒 Delete						
			_		ок	Cancel	

(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**.

paloalto	Dashboard ACC	Monitor P	Policies Objects Network	Device					🍰 Commit 👩 🔞 Save
									С 🔘 нер
Interfaces R Zones	Name	Location	Local Interface	Local IP	IP Pool	Turnel	Max User	Access Route	1 tem 🔁 🗶
Sig Victual Wires	Client Config		ethernet1/1		10.9.17.15-10.9.17.30	tunnel.1			Remote Users
DHCP									
V Clobal Protect									
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.

GlobalProtect Gateway			0
General Client Configuration Satellite Configuration	Name T	estGW	
Succinc comgutation	Interface	ethernet1/1	•
	IP Address	None	-
	Server Certificate	04,04,225,40	•
	Authentication		
	Authentication Profile	None	~
	Authentication Message	Enter login credentials	
	Certificate Profile	SAC	-
		OK Canc	el

(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**.

🚺 G	lobalProtect	
File	View Edit Help	
	Connect Disable Rediscover Network Resubmit Host Profile	TroubleShooting
	Check Version Collect Logs Close	

(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.

SafeNet Authentica	tion Client Tools		10000000000000000000000000000000000000	Control of the second sec
SafeNet A	uthentication	Client	W16F619169121Y60FAS	1 ? 💼
⊖ SafeNet Authenti ⊖ ✔ Tokens □ ₩ ₩ To ⊕ ₩ ₩ ♥ ₩ ⊕ ₩ ♥ ₩ ♥ ₩ ♥ ₩ ♥ ₩ ♥ ₩ ♥ ₩ ♥ ₩ ♥	Token Logon GafeNet: Safe Erter the Token Password. Token Name: Token Password:	Met Authenticati	on Client	
T 4 1 2 2 3 2 1 A 6 50\$66	Supported k Token Passw Token Passw Maximum Maximum A564400515/16410	ey size ord ord retries remaining oben Password retries	2048 Present 15 15 15 15 15 15	12 2014) vw.safenet-inc.com

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

GlobalProtect	
Eile View Edit Help	
Status: Connected	
Warnings/Errors	

(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 Supp manage incidents, get the latest software Base.	bs://serviceportal.safenet-inc.com sting customers with a Technical Support Customer Portal account can log in to nage incidents, get the latest software upgrades, and access the SafeNet Knowledge se.		