# SafeNet Authentication Client Integration Guide

Using SafeNet Authentication Client CBA for Check Point Security Gateway



All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016-2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013950-001, Rev. B Release Date: October 2017

## Contents

Third-Party Software Acknowledgement4
Description4
Applicability5
Environment5
Audience5
CBA Flow using SafeNet Authentication Client5
Prerequisites
Supported Tokens in SafeNet Authentication Client6
Configuring Check Point Security Gateway7
Creating a User and Issuing a Registration Key7
Creating a User Group12
Enabling Authentication for the VPN Client14
Configuring a Firewall Rule for the VPN Client16
Installing a Policy19
Enrolling a Certificate21
Enabling Smart card removal detection25
Running the Solution
Support Contacts

## **Third-Party Software Acknowledgement**

This document is intended to help users of Gemalto products when working with third-party software, such as Check Point Security Gateway.

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

Customers today are looking to desktop virtualization to transform static desktops into dynamic mobile workspaces that can be centrally and securely managed from the datacenter, and accessed across a wide range of devices and locations. Deploying desktop virtualization without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat. A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

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. SafeNet's certificate-based tokens provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

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). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

SafeNet Authentication Manager (SAM) provides your organization with a comprehensive platform to manage all of your authentication requirements, across the enterprise and the cloud, in a single, integrated system. SAM enables management of the complete user authentication life cycle. SAM links tokens with users, organizational rules, and security applications to allow streamlined handling of your organization's authentication infrastructure with a flexible, extensible, and scalable management platform.

SAM is a comprehensive token management system. It is an out-of-the-box solution for Public Certificate Authorities (CA) and enterprises to ease the administration of SafeNet's hardware or software tokens devices. SAM is designed and developed based on the best practices of managing PKI devices in common PKI implementations. It offers robust yet easy to customize frameworks that meets different organizations' PKI devices management workflows and policies. Using SAM to manage tokens is not mandatory, but it is recommended for enterprise organizations.

For more information, refer to the SafeNet Authentication Manager Administrator Guide.

Check Point Security Gateway protects dynamic virtualized environments and external networks (such as private and public clouds) from internal and external threats, by securing virtual machines and applications with a full range of Check Point Software Blades.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Check Point Security Gateway using SafeNet tokens. It is assumed that the Check Point Security Gateway environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication. Check Point Security Gateway can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with SafeNet products.

## Applicability

The information in this document applies to:

- SafeNet Authentication Client (SAC)
- Check Point Security Gateway

## Environment

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

- SafeNet Authentication Client (SAC) 10.4
- Check Point Security Gateway R80.10
- Check Point VPN Client endpoint security VPN E80.70 (Standalone)

### **Audience**

This document is targeted to system administrators who are familiar with Check Point Security Gateway, and are interested in adding certificate-based authentication capabilities using SafeNet tokens.

## **CBA Flow using SafeNet Authentication Client**

The diagram below illustrates the flow of certificate-based authentication:



- 1. A user attempts to connect to the Check Point Security Gateway server using the Check Point Security Gateway client application. The user inserts the SafeNet token on which his certificate resides, and, when prompted, enters the token password.
- 2. After successful authentication, the user is allowed access to the internal resource.

## Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificatebased authentication for Check Point Security Gateway using SafeNet tokens:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Check Point GW internal CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) should be configured with MS CA Connector. For further details, refer to the section "Connector for Microsoft CA" in the SafeNet Authentication Manager Administrator's Guide.
- Users must have a SafeNet token with an appropriate certificate enrolled on it.
- SafeNet Authentication Client (10.4) should be installed on all client machines.

### **Supported Tokens in SafeNet Authentication Client**

SafeNet Authentication Client (10.4) supports the following tokens and smart cards:

### Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

#### **Smart Cards**

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

For all supported devices please refer to SafeNet Authentication Client Customer Release Notes.

## **Configuring Check Point Security Gateway**

The Check Point Smart Dashboard application can be used to configure the Check Point Remote Access VPN.

Configuring Check Point Security Gateway requires:

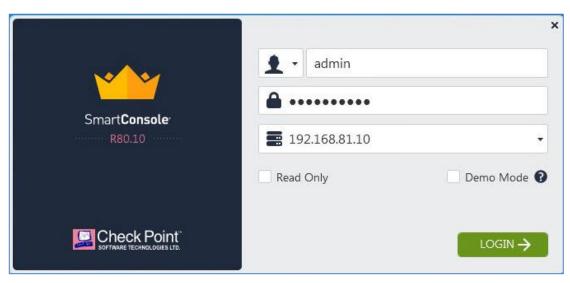
- Creating a User and Issuing a Registration Key, page 7
- Creating a User Group, page 12
- Enabling Authentication for the VPN Client, page 14
- Configuring a Firewall Rule for the VPN Client, page 16
- Installing a Policy, page 19
- Enrolling a Certificate, page 21
- Enabling Smart card removal detection, page 25

### Creating a User and Issuing a Registration Key

A user is created with a defined authentication scheme to log in to the Check Point Endpoint Security VPN Client and access its applications. Then, the administrator initiates the certificate process on the Security Management server (or ICA management tool), and is given a registration key.

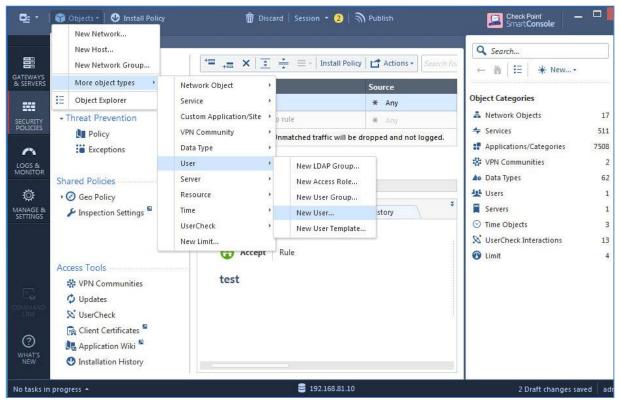
- 1. Open the Check Point SmartConsole R80.10.
- 2. On the login window, complete the following fields, and then click Login.

Username	Enter your user name.
Password	Enter your password.
Server Name or Server IP Address	Select the name or IP address of the server where Check Point Security Gateway is hosted.
Read only	Clear this option.



(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

3. On the Check Point SmartConsole main window, under Objects, select More Object types > User and then click New User.



(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

#### 4. Choose Default and click OK.

lew User			>
Choose template:	1 Defa	ult	•
	1	ОК	Cancel

5. On the User Properties window, in the User Name field, enter the name of the user (for example, Alice).

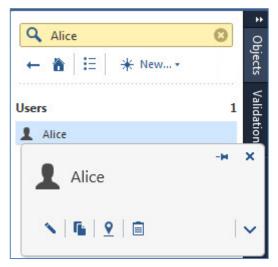
User		Q, 😨   X
Alice Enter C	Dbject Comment	
General Authentication Location Time Certificates Encryption	General properties         Email address:         Mobile phone number:         Expiration         Expire at:       12/31/2030         Image: Add Tag	
	0	K Cancel

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

6. Click OK.

The user is created.

7. On Search Bar find the user created and click the user name



(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

8. In the User window, click Certificates.

General	Manage internal CA	certificates per devid	e	
Authentication	🛞 🔨 💥 Revo	ke Only Active 👻		
Location	Status	Expiration	Comment	
Time				
Certificates				
Encryption				
		No items foun	d	

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

9. Click New, and then select Registration Key for certificate enrollment.

General Authentication	Manage internal CA certificates per device	
Location	Registration Key for certificate enrollment	Comment
Time	Certificate file (.P12)	
Certificates		
Encryption	No items found	

10. In the **Registration Key for Certificate Enrollment** window, a registration key is displayed. Copy this registration key, save it (where you can retrieve it later for certificate enrollment), and then click **OK**.

Alice     Enter Object Comment	
egistration Key For Certificate Enrollment	<b>⊘</b>   ×
Send this registration key to the user: $47774$ -uxg The user must enroll within: $14$ $\xrightarrow{+}$ days (31-Jul Comment:	

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

In the **User Properties** window, in the **Certificate list**, a **Pending enrollment** certificate status is added. 11. Click **OK**.

General Authentication	Manage internal CA o		ice	
Location	Status	Expiration	Comment	
Time	Pending enrollment	In 14 days		
Certificates				
	Add Tag			

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

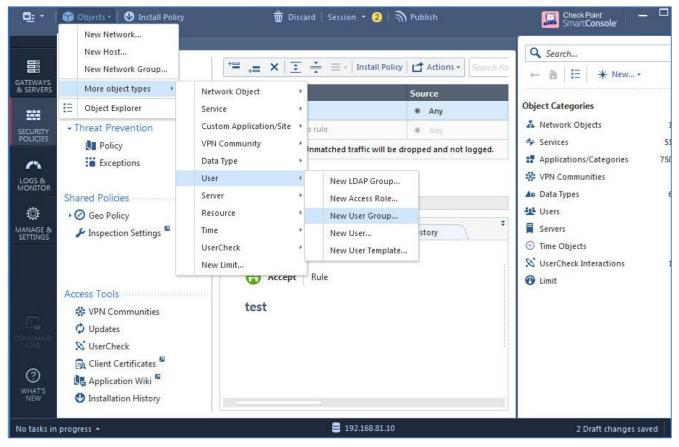
### **Creating a User Group**

B

A user group is a set of users who have related responsibilities or perform related tasks. Similar to individual users, user groups can be specified in policy rules.

**NOTE:** Creating a group enables you to allow some of your users to perform some tasks, but not others. Firewalls do not allow you to define rules for individual users, but you can define rules for groups.

1. On the Check Point SmartConsole main window, under Objects, select More Object types > User and then click New User Group.



2. On the Group Properties window, complete the following fields, and then click OK.

Name	Enter the name of the group (for example,
	Remote_access_group).
Available Members/Selected Members	In the All list, select the members to add to the group, and then
	click Add (+ sign). These members are in the Members list.

ing List Address:		
×	Q Search	
* All • Q		
Name	Comments	
Recently Used (1)		^
🕂 🤹 Alice		
Ali (2)		^
🚊 admin		

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

3. The user is added. Click OK.

ailing List Address:		
+   ×	Q Search	
Name	* Comments	

SafeNet Authentication Client: Integration Guide
Using SafeNet Authentication Client CBA for Check Point Security Gateway
Document PN: 007-013950-001, Rev. B

### **Enabling Authentication for the VPN Client**

1. On the **Check Point SmartConsole** in **Gateways & Servers** left tab, expand **Check Point**, right-click your device (for example, **GWR80.10**), and then click **Edit**.

===	Columns: 💿 G	eneral	• *•	× ×	S • C • O Q Search	Y	]	1 😋
	Status Nam	e '	r IP	Version	Active Blades	Hardware	CPU Usage	Recomme
ERVERS	o 🖷 📀	WR80.10	192.168.81.10	R80.10	₩☆■◇★国	Open server	<b>a</b> 1%	N/A
		5	Scripts					
IRITY		L.	Actions					
CLES		0	Monitor					
•		0	View					
S & ITOR		~	Edit					
4.		<b>F</b>	Clone					
<b>≱</b>		×	Delete					
AGE & INGS		9	Where Used					
	. XC:		Copy To Clipboa	ird				
			Copy As Image					

<sup>(</sup>The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

2. In the Check Point Gateway – Checkpoint-ssl window, expand VPN Clients, and then click Authentication.

Check Point Gateway - GWR	30.10	? 🗙
General Properties Network Management NAT HTTPS Inspection HTTP/HTTPS Proxy Platform Portal FISec VPN VPN Clients Authentication	Compatibility with Older clients  For a list of clients supporting single authentication option only, please see sk111583  Allow older clients to connect to this gateway Authentication Method: Defined On User Record (Legacy)  Multiple Authentication Clients Settings  For a list of newer clients that support Multiple Login Options, see sk111583	Settings
Office Mode Remote Access	+ Add > Edit × Remove  Up Down	
Mobile Access     Logs     Optimizations     Ht Count     Other	Display Order Display Name Authentication Factors	
	Edit	Cancel

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

3. Next to Authentication Method, click on Settings.

heck Point Gateway - GWR	30.10	? <mark>×</mark>
General Properties  Network Management  NAT  HTTPS Inspection  HTTP/HTTPS Proxy Platform Portal  FIPSec VPN  VPN Clients  Authentication  Office Mode  Remote Access  Cuss  Optimizations Hit Count  Other	Compatibility with Older clients  For a list of clients supporting single authentication option only, please see sk 111583  Allow older clients to connect to this gateway Authentication Method: Defined On User Record (Legacy)  Multiple Authentication Clients Settings  For a list of newer clients that support Multiple Login Options, see sk 111583  Add Edit × Remove  Up  Down  Display Order Display Name Authentication Factors	Settings

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

4. Under Authentication Methods, select Defined On User record (Legacy), and then click OK twice

Single Authentication Clients	Settings	? 💌
General Properties		
Allow newer clients that	t support Multiple Login Options to use this authentication method	
Display Name:	Standard	
Authentication Methods		
Authentication method:	Defined On User Record (Legacy)	-
Client Display:	Customize	
	ОК	Cancel

### **Configuring a Firewall Rule for the VPN Client**

A security gateway object has at least one firewall blade installed that serves as an entry point to the corporate network.

The firewall rule is a policy definition of what is allowed and what is blocked by the firewall. Rules are based on the concept of objects. For example, networks objects can be used in the source and destination of rules.

1. In the Check Point SmartConsole, in the main window in the left tab , click Security Policies

<b>Q:</b> -	😚 Objects 🔹 🛛 😍 Install Poli				🗑 Discard   Session 👻 3	n Publish		Check Point Smart Console	
m	Standard + " • Access Control		+=	.≡ ×   Ξ ÷	= • Install Policy	for IP, object, action,	Q .	~   ^   <b>T</b>	
SATEWAYS & SERVERS	Policy	No.		Source	Destination	VPN	Services & Applications	Action	
	K NAT	1	٩e	* Any	* Any	* Any	* Any	🔘 Drop	
SECURITY	Threat Prevention								
LOGS & MONITOR	Exceptions								
	Shared Policies								
Ö	🗢 Mobile Access								
ANAGE & ETTINGS	🕨 🕜 Geo Policy								
	🖌 Inspection Settings 🖗								

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

2. Click **Policy**, and then click **Add rule below**.

+=	+=	×	-
e	Add r	ule a	bove

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

#### A row is added below the Policy icon bar.

≌ -	🎲 Objects +   🔮 Install P	olicy		🛱 Discard   Session 🕤	🗧 🌀   🖣 Publish	Ľ
	Standard +					
GATEWAYS	** * Access Control	+= +=	$\mathbf{X} \mid \overline{\underline{:}} \stackrel{*}{\underline{:}} \equiv \cdot \mid \text{Install}$	Policy Actions - Search for I	P, object, action,	9. V 1 ~ 1 T
& SERVERS	Policy	No.	Source	Destination	VPN	Services & Applications
	NAT	1	* Any	* Any	* Any	* Any
SECURITY	Threat Prevention	2	* Any	* Any	* Any	* Any

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

#### 3. In the **Name** column, right-click the new row, and then click **Edit**.

Q: •	📬 Objects 🕶   🕑 Install Po	olicy		觉 Discard	Session 🝷 🤞   🖣 Publish		E
	Standard +						
GATEWAYS	Access Control	+= +=	×⊡ ÷≡	Install Policy C Actions •	earch for IP, object, action,	٩	~   ^   <b>Y</b>
& SERVERS	Policy	No.	Name	Source	Destination	VPN	Si
	NAT	1			* Any	* Any	+
SECURITY		2		Edit	* Any	* Any	

<sup>(</sup>The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

4. In the Rule Name window, in the Rule Name field, add a name for the firewall rule.

<b>C</b> : -	🗊 Objects 🔹   🔮 Install Polic	cy	🌐 Discard   Session 👻 🙃   🔊 Publish					
	Standard +							
	** • Access Control	*= ,= ;	<b>×</b>   <u>:</u> = -   Inst	all Policy Actions •	r IP, object, action,	Q v   ^		
GATEWAYS & SERVERS	Policy	No.	Name	Source	Destination	VPN		
	NAT	1		* Any	* Any	* Any		

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

5. In the **Destination** column, right-click the new row, and then click **add new item**.

Q: •	😭 Objects 🔹   🔮 Install Po			💼 Discard	Session + 🙆   🕥 Publish		
	Standard +						
GATEWAYS	* Access Control	+= +	∎ × I ± ÷ ≡·	Install Policy	arch for IP, object, action,		9
& SERVERS	Policy	No.	Name	Source	Destination		VPN
	NAT	1	N	* Any	* Any	۵	* Any
SECURITY POLICIES	<ul> <li>Threat Prevention</li> <li>Policy</li> </ul>	2		* Any	* Any	[	Add new items

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

6. In the **Search Object** window, select **InternalNet** which is an alias for the internal network in an organization.

	Name	IP Address	Comments
Rec	cently Used (1)		
+	😪 GWR80.10	192.168.81.10	
AII	(7)		
	All_Internet	0.0.0.0 - 255.255.255.255	All Internet Addresses
	👗 CP_default_Office_Mode_add	172.16.10.0	Used as a default for Office Mode
	😪 GWR80.10	192.168.81.10	
+			

7. In the VPN column, right-click the new row, and then click Specific VPN Communities.

<b>C</b> : -	🎁 Objects 🕶   🔮 Install Po	licy		觉 Discar	d   Session - 15   🗟	Publish	<u> </u>	Check Point Smart <b>Console</b>
GATEWAYS	Standard + + + + - Access Control	+= +=	×   <u>:</u> ÷ ≡ +   In	stall Policy 🛛 🚰 Actions -	Search for IP, object, a	ction,	Q \_ \ \ T	Q Search ← 🏠 🗄
& SERVERS	Policy	No.	Name	Source	Destination	VPN	Services & Applicat Action	
	NAT	1	Remote_Access	* Any		* Any	Accept	Users
SECURITY POLICIES	Threat Prevention     Policy	2		* Any	* Any	* Any	All Connections (Clear or Encrypted) All Site-To-Site VPN Communities	1 Alice
0	Exceptions						Specific VPN Communities	
LOGS & MONITOR							Directional Match Condition	

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

#### 8. In the search window, select RemoteAccess.

<u>©:</u> •	👕 Objects 🔹 🛛 🕁 Install Poli	cy		觉 Discard	Session + 15   🕄	h Publish		🔄 Check Point 🛛 🗕 🗗 🔜
	Standard +	+= .=	× 🗟 ≛ ⊒- Ir	nstall Policy 📑 Actions •	Search for IP, object, a	iction		Q. Search
GATEWAYS & SERVERS	Access Control     Policy	No.	Name	Source	Destination	VPN	Services & Applicat Action	= ← 🏠      ★ New • 65
	NAT	1	Remote_Access	* Any	InternalNet	* Any	Q	▼- *- ×
SECURITY POLICIES	Threat Prevention	2		* Any	* Any	* Any	Name	Comments
100	Policy							Comments
~	Exceptions						🗱 MyIntranet	
LOGS & MONITOR							🏶 RemoteAccess	
1977	Shared Policies							
Ö	🗢 Mobile Access						2 items	

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

#### The new policy is created.

<b>Q</b> : •	📬 Objects 🔹   🔮 Install Po			觉 Disc	ard   Session - 16	Publish		Check Point Smart Consol
	Standard +							
GATEWAYS	* Access Control		≡ ÷ Ξ   X ≡, ≡	Install Policy	Actions • Search for IP, ob		٩	~   ^   <b>T</b>
GATEWAYS & SERVERS	Policy	No.	Name	Source	Destination	VPN	Services & Applicat	Action
	NAT	1	Remote_Access	* Any	🔶 InternalNet	🗱 RemoteAccess	\star Any 📢	Accept

### **Installing a Policy**

The policy installation process does the following:

- Performs a heuristic verification on rules to ensure they are consistent, and that no rule is redundant.
- Confirms that each of the Security Gateways on which the rule is enforced (known as Install On object) enforces at least one of the rules.
- Converts the Security Policy into an Inspection Script, and compiles this script into an Inspection Code.
- Distributes Inspection Codes to the selected installation targets.
- 1. In the Check Point SmartConsole main window, in the icon bar at the top, click Install Policy.

🔹 🕴 🗊 Objects • 🛛 🕑 Install Policy			🌐 Discard   Se	ssion 🝷 🛛 🕤 Publish			Check Point SmartCons
Standard * * * Access Control		x   ₹ ₹ = -   1	nstall Policy	• Search for IP, object,	action,	٩	✓   ∧   Y
RVERS Policy	No.	Name	Source	Destination	VPN	Services & Applicat	Action
T NAT	1	Remote_Access	* Any	InternalNet	👯 RemoteAccess	* Any	Accept
Threat Prevention	2	Cleanup rule	* Any	* Any	* Any	* Any	🕀 Accept
Exceptions     Stared Policies     Mobile Access     O Geo Policy     // Inspection Settings						_	

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

#### 2. Click Publish & install

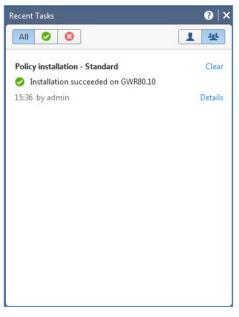
SmartConsol	e		×
9	Do you want to	unpublished changes publish changes before installing the policy?	
	Session name:	admin@7/17/2017	
	Description:	1 change published by admin on 7/17/2017	
		Total draft changes: 1	
🔲 Don't sł	now again	Publish & Install Cance	el 📄

3. In the **Install Policy** window, in **policy Targets** select the option for your device (for example, **GWR80.10**), and then click **Install**.

Install Policy	❷   □ ×
L.	Standard
✓ L Access Control ✓ R, Threat Prevention	Total changes from last installation (7/17/2017): 1 Changes from 1 sessions (by admin) 🔮
	GWR80.10 .10   Version: R80.10 res   & Policy Targets
<ul> <li>Install on each selected gateway independently</li> </ul>	
For gateway clusters, if installation on a cluster member fails, do not install on t Install on all selected gateways. If installation on a gateway fails, do not install on a	
	Install Cancel

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

4. When the installation is complete, click **Close**.



### **Enrolling a Certificate**

The client establishes an SSL connection to the Check Point's Internal Certificate Authority (ICA) and completes the certificate generation process using the registration key. When you enroll a certificate with Endpoint Security for the first time, provide the registration key and enroll a certificate in the token.

1. Insert the SafeNet SmartCard/Token first into your USB slot, and then open the **Check Point Endpoint Security** application.

The IP address in the **Site** field is same one that was configured during the installation. Also during the installation, **Certificate** was the selected **Authentication** option.

2. Click the Click here if you don't have a certificate for this site link.

TrGUI		- • •
Endpoint	Security	SOFTWARE TECHNOLOGIES LTD.
Site:	10.0.80.10	
Authentication	ficate with acceptable DN in the CAPI store	
Please provide creder User name	ntials to authenticate	
<u>Click here if you don't</u>	have a certificate for this site	<u> </u>
Connect	Cancel Help	
elected Login Option: S	Standard	Change Login Option Settings

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

3. In the Provider field, select eToken Base Cryptographic Provider

TrGUI		
Endpoint	Security	Check Point SOFTWARE TECHNOLOGIES LTD.
Site:	10.0.80.10	
Authentication		
No valid certif	ficate with acceptable DN in the CAPI store	$\square$
Provider:	eToken Base Cryptographic Provider 🔹 🔻	2
Registration Key:		
Click here if you alread	dy have a certificate for this site	
Enroll	Cancel Help	

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

- 4. In the **Registration Key** field, enter the registration key that you saved in step "Creating a User and Issuing a Registration Key" on page 7, and then click **Enroll**.
- 5. On the **Token Logon** window, in the **Token Password** field, enter your SafeNet eToken password, and then click **OK**.

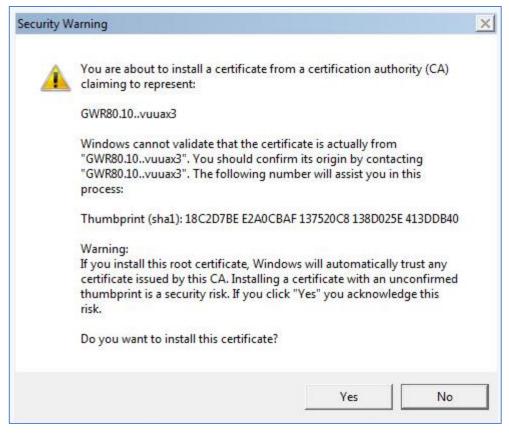
SafeNet Authent	cation Client	gemalto
Enter the Token Password		
Token Name:	Card #16BC972F938EDA7	F
Token Password:	••••	

#### Certificate enrollment proceeds.

Endpoint Se	curity		Check Poin
	Enrolling certificate (tl	his may take a while)	50%
	Cancel Clos	e	<< Details
Enrolling certificate (th	is may take a while)		

A security warning message is displayed. This is the certificate offered by Check Point's Internal Certificate Authority (ICA).

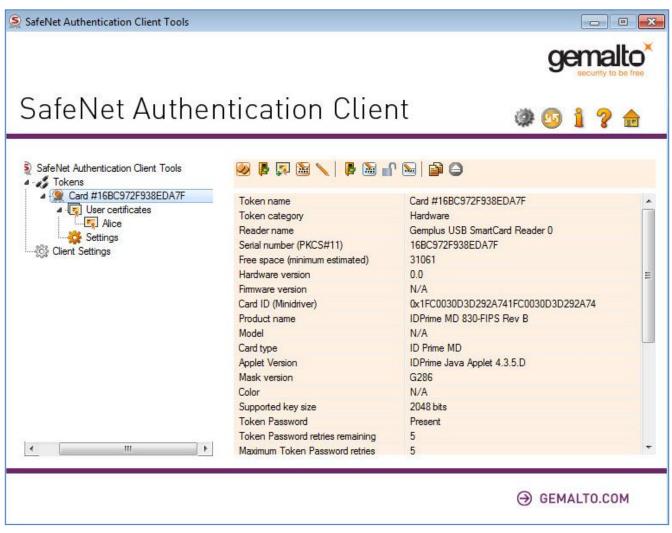
6. Click Yes.



7. When the enrollment has completed, click Close

1009
< Details

8. Open the SafeNet Authentication Client tools application and verify that the certificate is issued to the user



### **Enabling Smart card removal detection**

- 1. In the Check Point Gateway, edit the file \$FWDIR/conf/trac\_client\_1.ttm using VI or any other text editor.
- 2. Locate the disconnect\_on\_smartcard\_removal line:

```
*:disconnect_on_smartcard_removal (
:gateway (
:default (true)
)
)*
```

3. Change the default property as follows:

true - Enables smart card removal detection for all connections to the current gateway
 false - Disable smart card removal detection for all connections to the current gateway
 client\_deside - Enables or disables smart card removal detection individually for each client

- 4. Save the file and exit.
- 5. Install the policy using the Smart Dashboard.
- 6. On the client machine, open the Check Point Endpoint Security properties window and select the Checkbox **Enable always-connect**.



(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

## **Running the Solution**

- 1. Open the Check Point Endpoint Security application.
- 2. Insert the SafeNet eToken into your USB slot. The certificate on the eToken is propagated in the **Certificate** field. Click **Connect**.

👌 TrGUI		
Endpoint	Security <sup>.</sup>	Check Point SOFTWARE TECHNOLOGIES LTD.
Site:	10.0.80.10	•
Authentication		
	intials to authenticate	
User name <u>Click here if you don'</u>	Alice(SerialNum=22670)	
Connect	Cancel He	elp
Selected Login Option:	Standard	Change Login Option Settings

(The screen image above is from Checkpoint®. Trademarks are the property of their respective owners).

3. On the Token Logon window, in the Token Password field, enter your token password, and then click OK.

SafeNet Authent	ication Client	gemalto
Enter the Token Password		
Token Name:	Card #16BC972F938EDA7	7F
Token Password:	••••	

4. On the right side of the task bar, click on the VPN client process to see the VPN connection status. When the authentication succeeds, the VPN connection status is shown as **Connected**.

View	No security policy is configured.				
Status	Active site is 10.0.80.10			💟 Connected	
VPN	UNI				
Compliance	Site:	10.0.80.10			
Firewall	IP Address:	192.168.81.10		Disconnect	
	Duration:	00:00:11		Disconnect	
fools	Expiration:	07:59:36			
Disconnect	Options				
	Manage your VF	VPN Options			
	Advanced				
		Packets	KBs		
	Encrypted	0	0		
			0		

## **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 Gemalto Customer Support. Gemalto 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 Gemalto 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	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA			
Phone	United States International	1-800-545-6608 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 Gemalto Knowledge Base.			