SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for Check Point Security Gateway

gemalto
security to be free

Document Part Number: 007-012885-001, Rev. B

Release Date: February 2016

Contents

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

Remote access poses both a security and a compliance challenge to IT organizations. The ability to positively identify users (often remote users) requesting access to resources is a critical consideration in achieving a secure remote access solution. Deploying remote access solution 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.

PKI is and effective strong authentication solution to the functional, security, and compliance requirements.

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)**—SafeNet Authentication Client is the middleware that manages SafeNet's tokens.
- **Check Point Security Gateway**

Environment

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

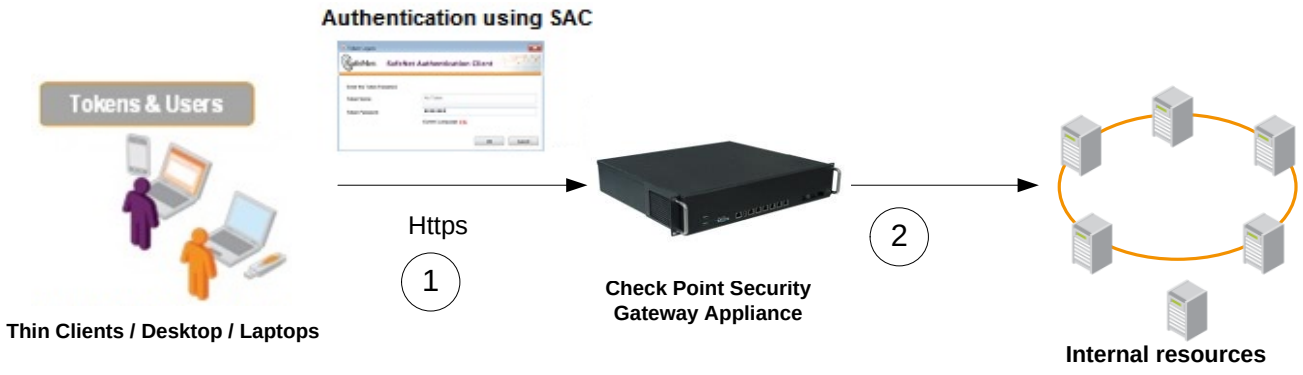
- **SafeNet Authentication Client (SAC)**— Version 9.0
- **Check Point Security Gateway**— Version R77
- **Check Point Endpoint Security Client**—Version E80.41

Audience

This document is targeted to system administrators who are familiar with Check Point Security Gateway, and are interested in adding multi-factor 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 Appliance 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 internal resources.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based 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 Microsoft 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 (9.0) should be installed on all client machines.

Supported Tokens in SafeNet Authentication Client

SafeNet Authentication Client supports a number of tokens that can be used as a second authentication factor for users who authenticate to Check Point Security Gateway.

SafeNet Authentication Client 9.0 (GA) supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID and VSR

Smart Cards

- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

Software Tokens

- SafeNet eToken Virtual
- SafeNet eToken Rescue

Configuring Check Point Security Gateway

The Check Point SmartDashboard application can be used to configure the Check Point SSL VPN or the IPSec VPN.

Configuring Check Point Security Gateway requires:

Creating a User and Issuing a Registration Key

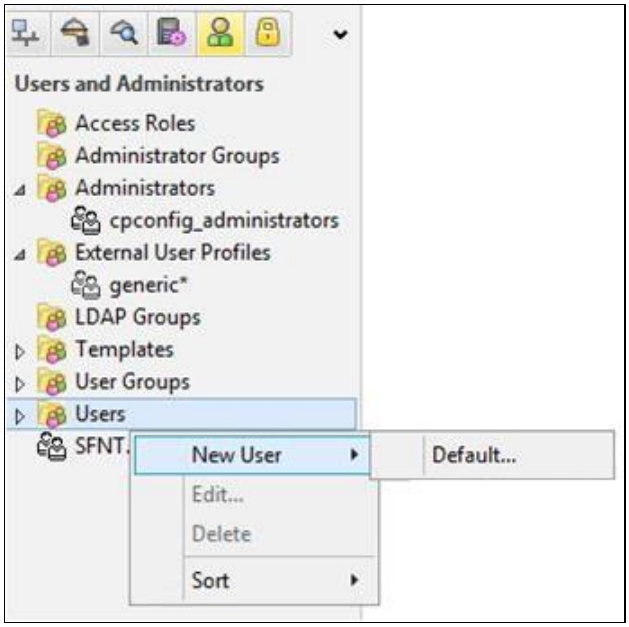
A user is created with a defined authentication scheme to log in to the Check Point Endpoint Security VPN Client and access its applications. Then, the administrator initiates the certificate process on the Security Management server (or ICA management tool), and is given a registration key.

1. Open the **Check Point SmartDashboard R77**.
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.

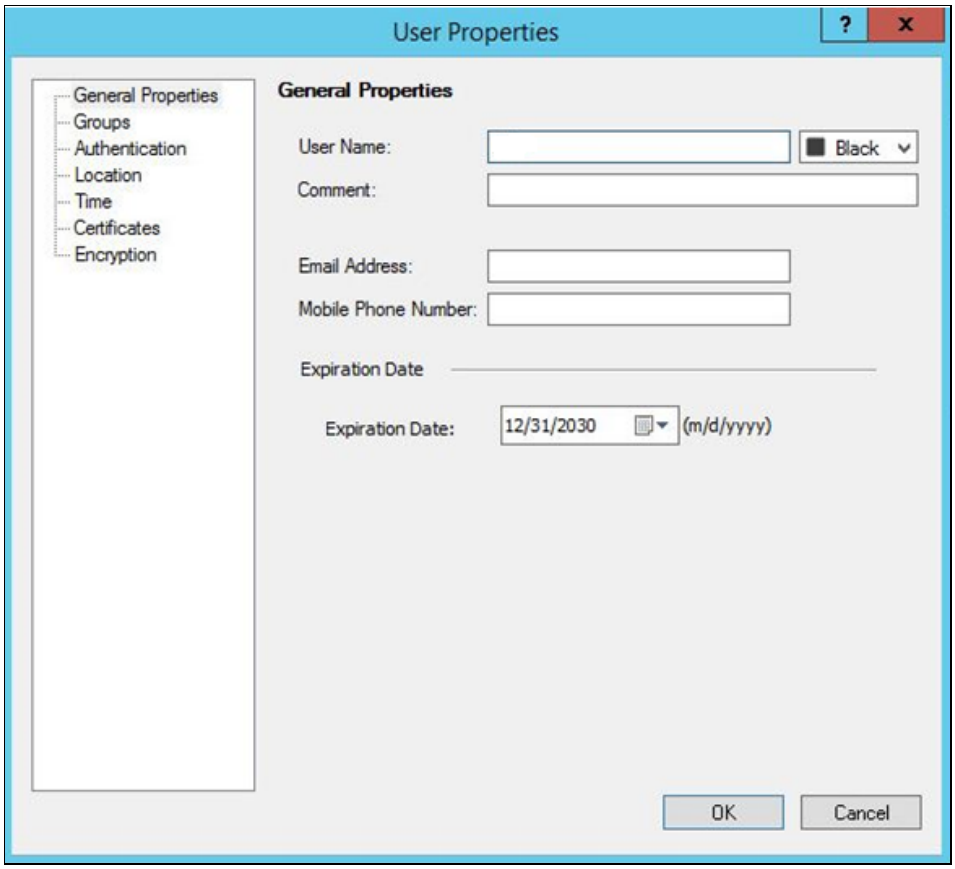
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

3. On the **Check Point SmartDashboard** main window, under **Users and Administrators**, right-click **Users** and then click **New User > Default**.



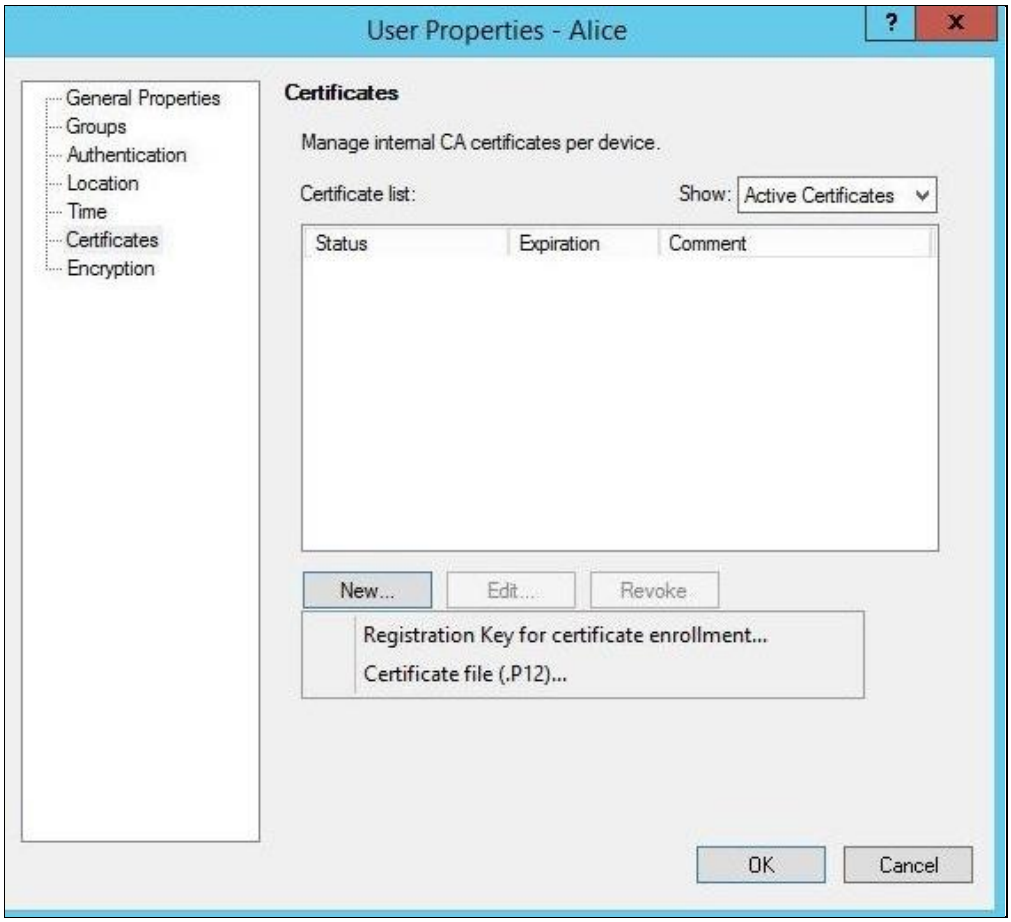
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

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



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

5. Click **Certificates**.

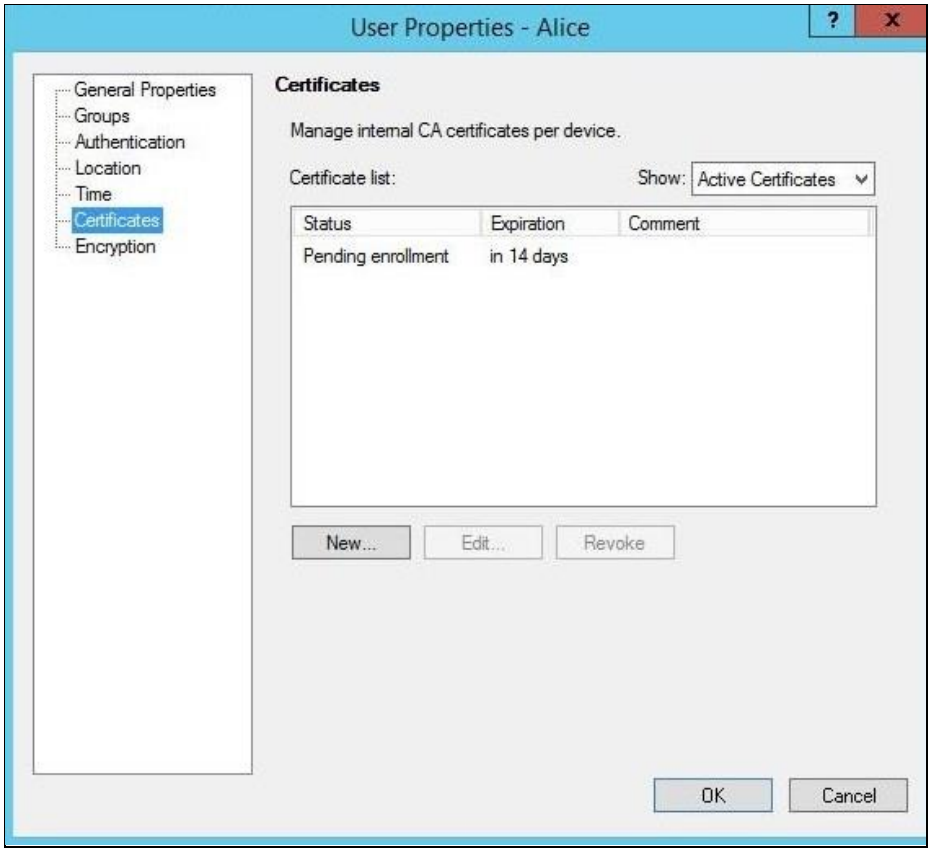


(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

6. Click **New**, and then select **Registration Key for certificate enrollment**.
7. On 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**.

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

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



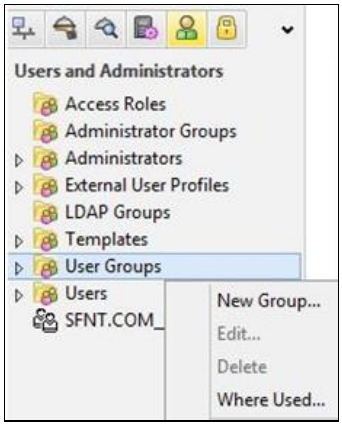
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

Creating a User Group

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.

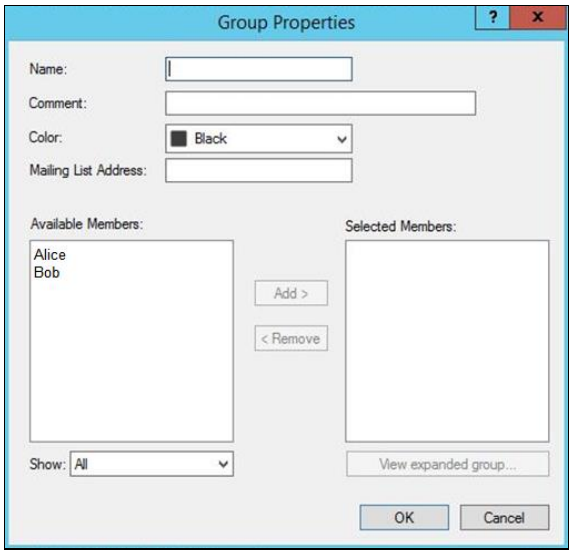
1. On the **Check Point SmartDashboard** main window, under **Users and Administrators**, right-click **User Groups**, and then click **New Group**.



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

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

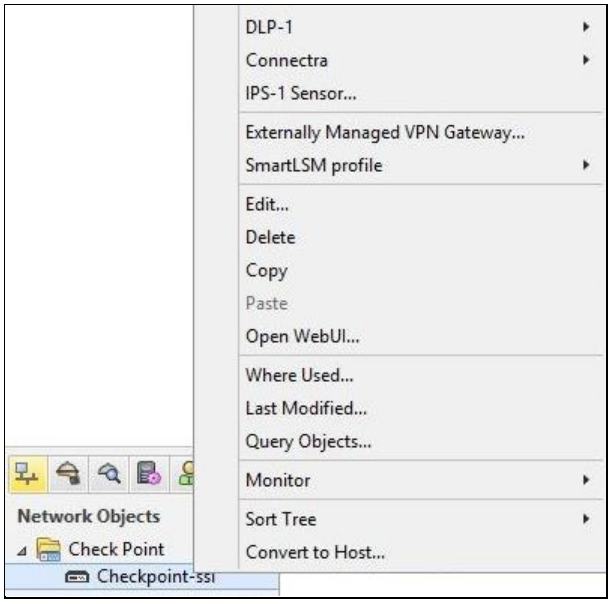
Name	Enter the name of the group (for example, **Remote_access_group)**.
Available Members/Selected Members	In the **Available Members** list, select the members to add to the group, and then click **Add**. These members are moved to the **Selected Members** list.



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

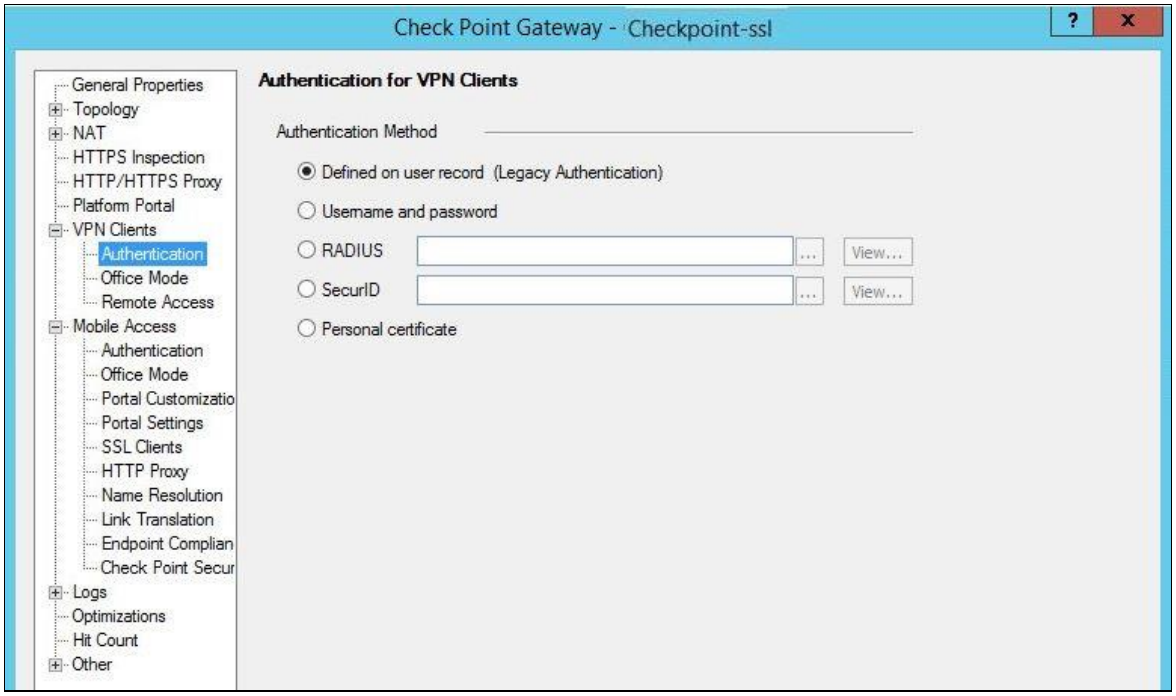
Enabling Authentication for the VPN Client

1. On the **Check Point SmartDashboard** main window, under **Network Objects**, expand **Check Point**, right-click your device (for example, **Checkpoint-ssl**), and then click **Edit**.



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

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



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

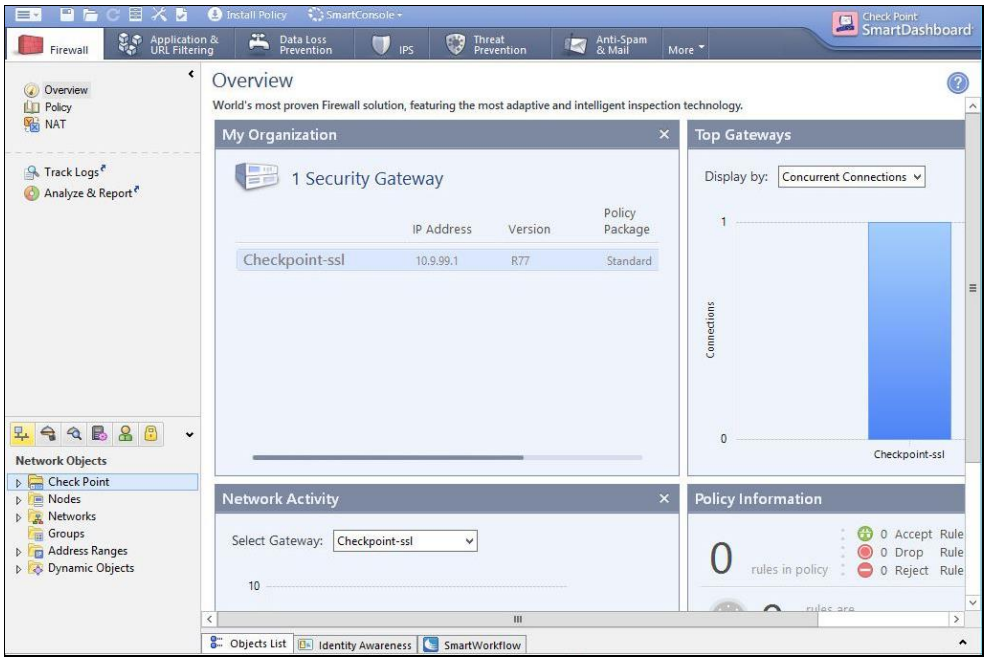
3. Under **Authentication Method**, select **Defined on user record (Legacy Authentication)**, and then click **OK**.

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.

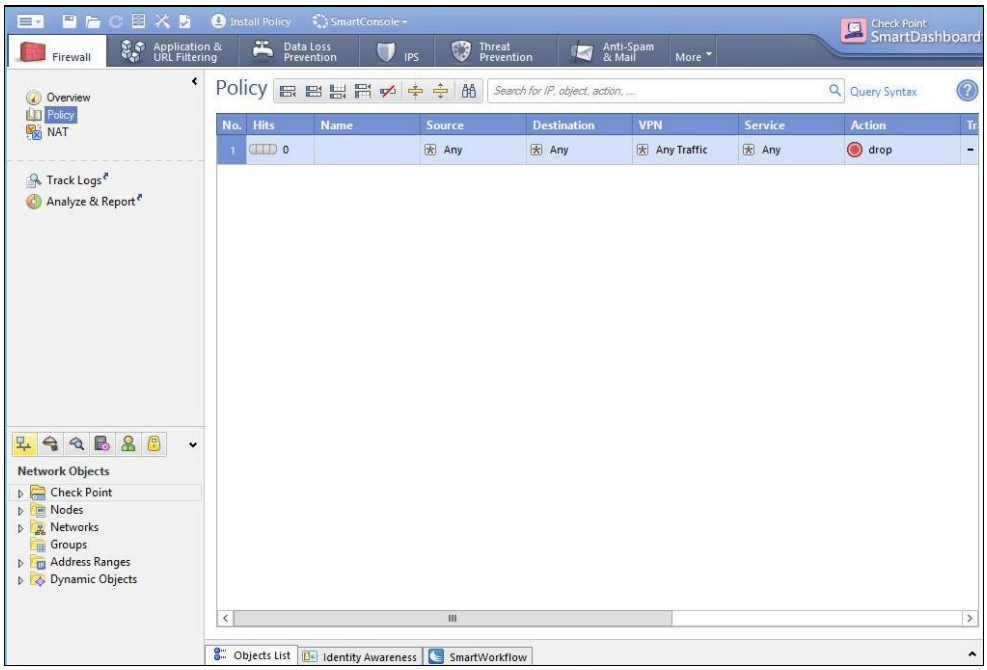
The firewall rule is a policy definition of what is allowed and what is blocked by the firewall. Rules are based on the concept of objects. For example, networks objects can be used in the source and destination of rules.

1. On the **Check Point SmartDashboard** main window, click the **Firewall** tab.



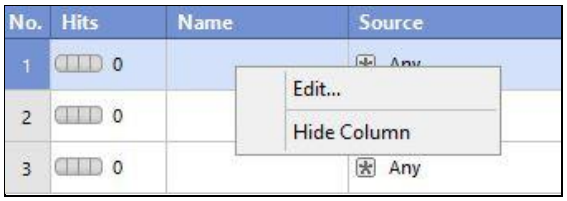
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

2. Click **Policy**, and then click the **Add rule at bottom**  icon. A row is added below the **Policy** icon bar.



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

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

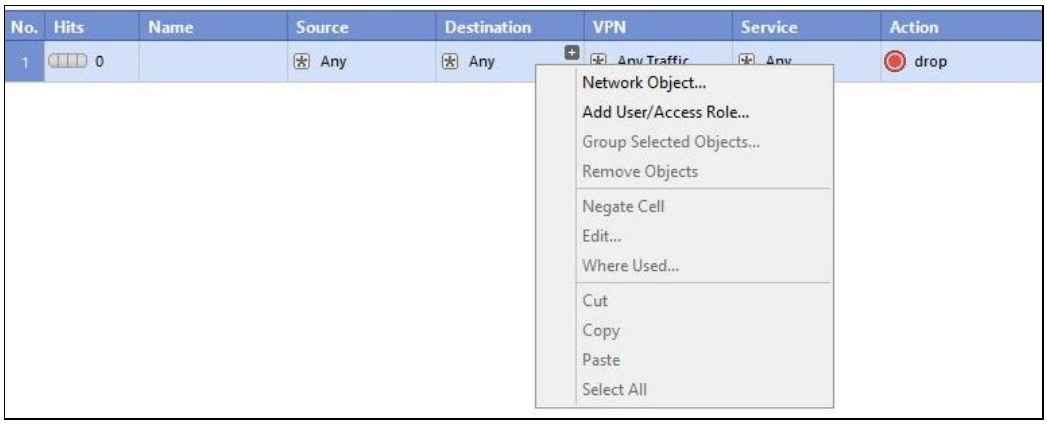


(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

4. On the **Rule Name** window, in the **Rule Name** field, add a name for the firewall rule, and then click **OK**.

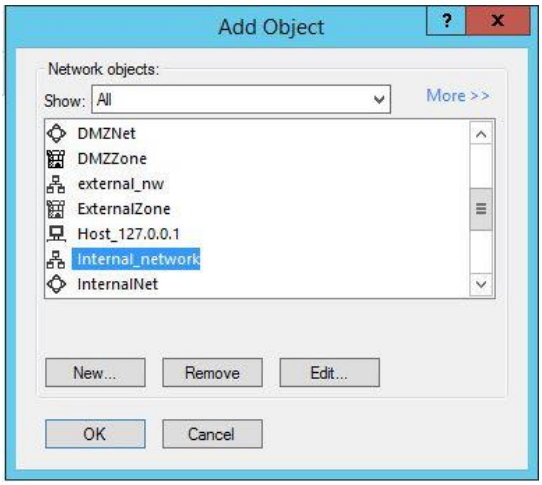
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

5. In the **Destination** column, right-click the new row, and then click **Network Object**.



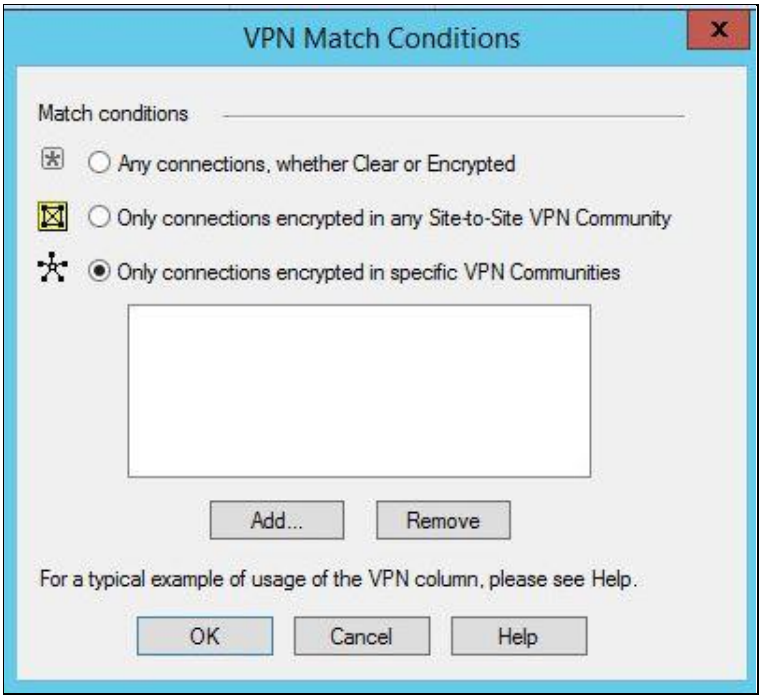
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

6. On the **Add Object** window, select **Internal_network**, and then click **OK**. **Internal_network** is an alias for the corporate network in an organization.



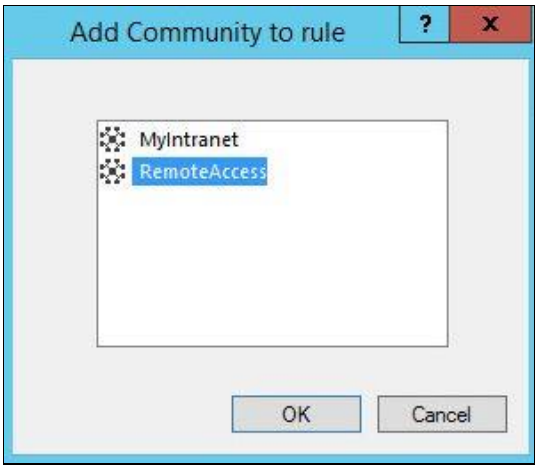
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

7. In the **VPN** column, right-click the new row, and then click **Edit Cell**.
8. On the **VPN Match Conditions** window, perform the following steps, and then click **OK**:
   a. Select **Only connections encrypted in specific VPN communities**, and then click **Add**.



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

   b. In the **Add Community to rule** window, select **RemoteAccess**, and then click **OK**.



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

The new policy is created.

Installing a Policy

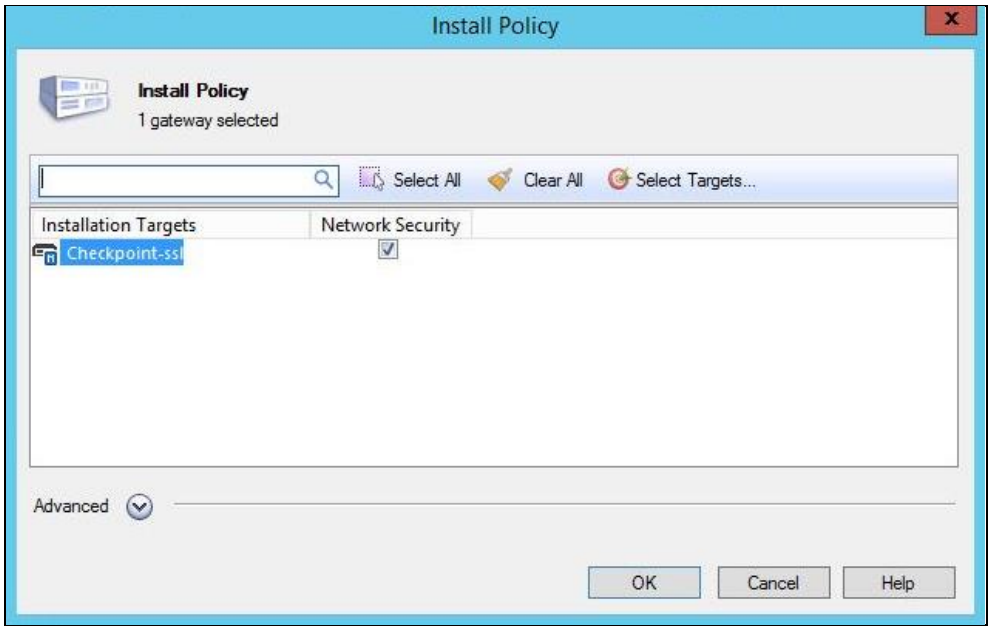
The policy installation process does the following:

- 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. On the **Check Point SmartDashboard** main window, in the icon bar at the top, click **Install Policy**.

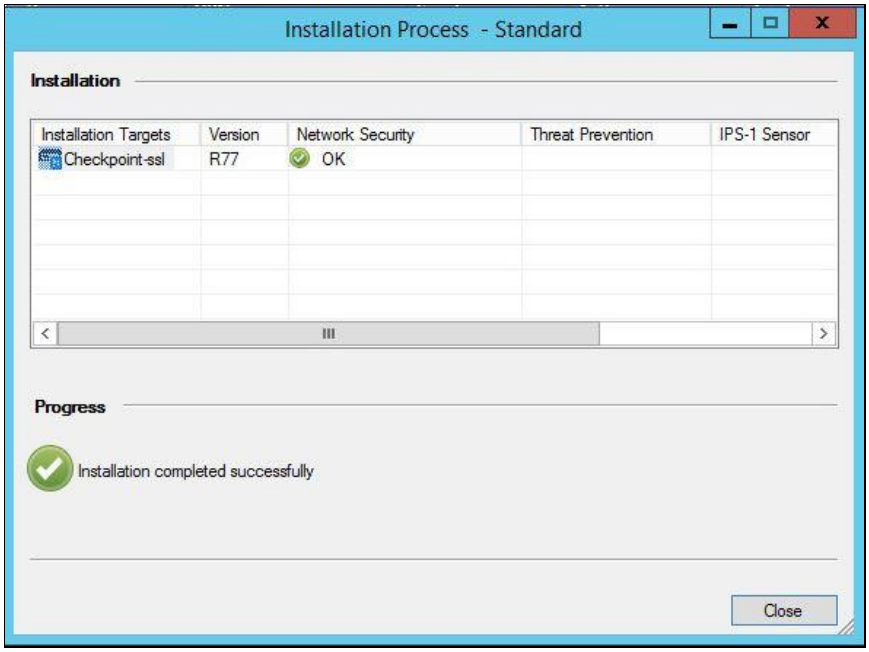
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

2. On the **Install Policy** window, in the **Network Security** column, select the option for your device (for example, **Checkpoint-ssl**), and then click **OK**.



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

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



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

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 eToken first into your USB slot, and then open the **Check Point Endpoint Security** application.
2. 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. Click the **Click here if you don't have a certificate for this site** link.

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

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

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

4. In the **Registration Key** field, enter the registration key that you saved in step 7 of "Creating a User" on page 7, and then click **Enroll**.

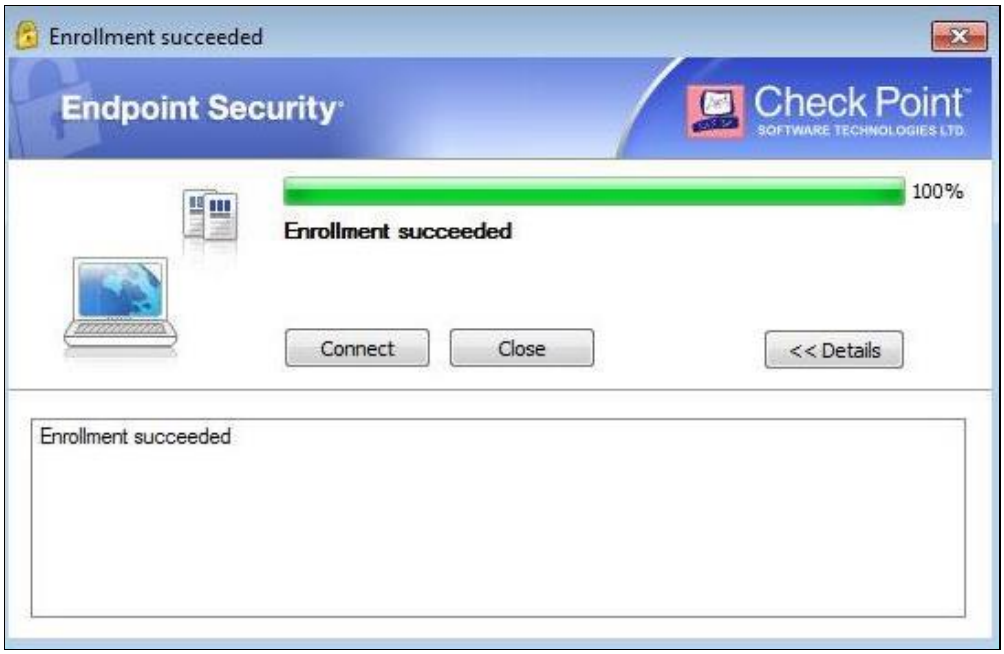
5. On the **Token Logon** window, in the **Token Password** field, enter your SafeNet eToken password, and then click **OK**.

6. A security warning message is displayed. Click **Yes**.

   This is the certificate offered by Check Point's Internal Certificate Authority (ICA).

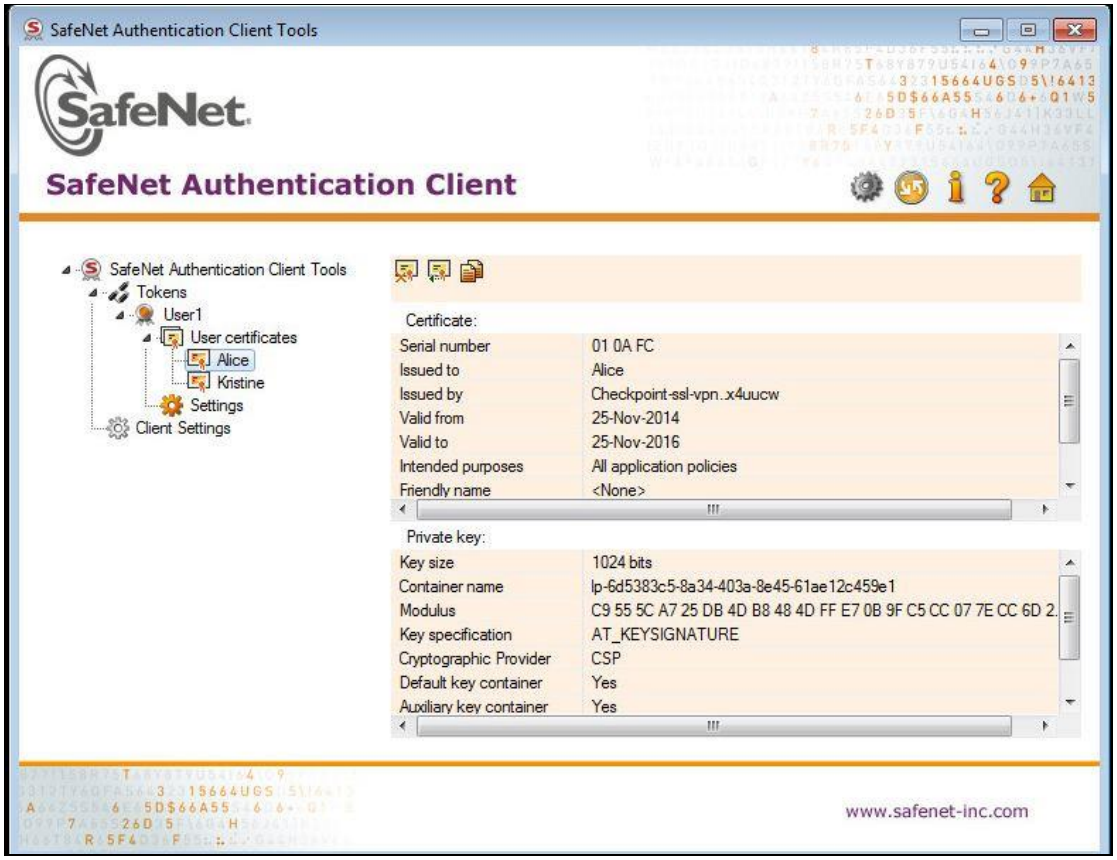
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

7. When enrollment is complete, click **Close**.



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

8. Open the **SafeNet Authentication Client** tools application and verify that the certificate is issued to the user you specified (for example, **Alice**).



Enabling Smart card removal detection

1. On 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)

)

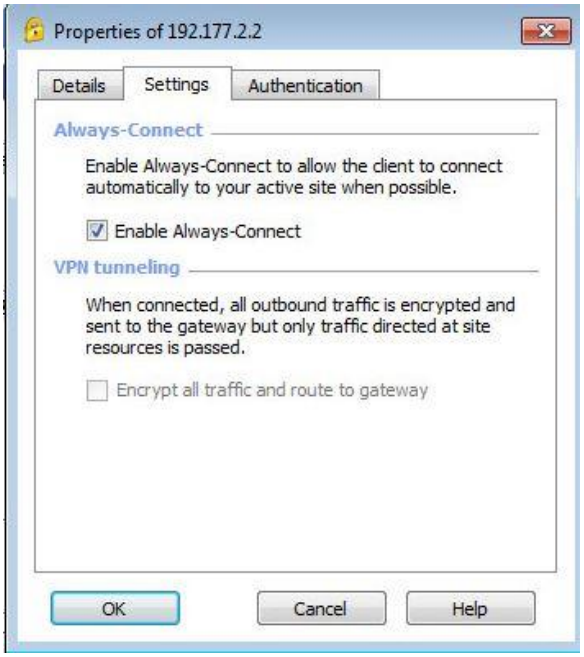
)*
3. Change the default property as follows :

   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 Check Point® software. 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**.

(The screen image above is from Check Point® software. 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**.

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**.

(The screen image above is from Check Point® software. 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 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, 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 Gemalto Knowledge Base.	