SafeNet Authentication Client

Integration Guide

Using SAC CBA for Check Point Endpoint Security – FDE

Document Information

Document Part Number	007-012821-001, Rev. A
Release Date	April 2015

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

This document is intended to help users of SafeNet products when working with third-party software, such as Check Point Endpoint Security – FDE.

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

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. SAC enables the implementation of strong two-factor authentication using standard certificates, as well as encryption and digital signing of data. 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 security for web access, network logon, email, and data. 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 Endpoint Security – FDE encryption provides superior encryption across a variety of endpoints, such as desktops and laptops. The Check Point Endpoint Security – FDE solution uses strong access control with pre-boot authentication (PBA). Encryption and decryption are completely transparent to the end user and are performed without hindering system performance.

An effective strong authentication solution must be able to address data breaches on the rise for companies to protect their information assets and comply with privacy regulations. Data encryption is a common technique used by enterprises today, but to be most effective, it must be accompanied by strong two factor user authentication to desktop, mobile, and laptop computer applications. Working together, encryption and authentication reduce risk and stop unauthorized access to sensitive data.

SafeNet smart card certificate-based tokens and secure USB certificate-based tokens are interoperable with Third-Party Product, providing a solution for encryption and strong access control that prevents unauthorized access to sensitive data and stops information loss and exposure. The integrated solution delivers greater security, reduced operational costs, and improved compliance by adding smart card-based strong user authentication to Check Point Endpoint Security – FDE.

SafeNet's X.509 certificate-based USB tokens and smart cards have been integrated with Check Point Endpoint Security – FDE, providing two-factor authentication at both pre-boot and Microsoft Windows levels.

The SafeNet's X.509 certificate-based USB tokens and smart cards provide secure storage for the certificates needed for endpoint encryption for Check Point Endpoint Security – FDE functionality to boot up. If SafeNet's X.509 certificate-based USB token or smart card is not inserted in the client machine, or if the certificates are deleted, revoked, or expired, the Check Point Endpoint Security – FDE software will not boot up and the data on the laptop will stay encrypted and secure.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Check Point Endpoint Security – FDE using SafeNet tokens.

It is assumed that the Check Point Endpoint Security – FDE environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

Check Point Endpoint Security – FDE 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 Endpoint Security – FDE**

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 Endpoint Security – FDE**—Version 6.3.1

Audience

This document is targeted to system administrators who are familiar with Check Point Endpoint Security – FDE, and are interested in adding multi-factor authentication capabilities during pre-boot using SafeNet tokens.

Pre-Boot Authentication Flow

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

NOTE: On successful validation, if single sign-on is configured in the Check Point Endpoint Security – FDE policies, the user is logged in to the system. If single sign-on is not configured in the Check Point Endpoint Security – FDE policies, the Windows login screen is displayed after pre-boot authentication.

Prerequisites

To enable users to perform pre-boot authentication with Check Point Endpoint Security – FDE using SafeNet tokens, ensure the following:

- Users can authenticate through pre-boot from the Check Point Endpoint Security – FDE environment with a static password before configuring the Check Point Endpoint Security – FDE to use SafeNet tokens.
- If SAM is used to manage the tokens, 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 have a SafeNet token with valid certificate enrolled on it.
- 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.

Supported Tokens in SAC

SAC supports a number of tokens that can be used as second authentication factor for users who are authenticating at pre-boot through Check Point Endpoint Security – FDE.

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)

Before Installing Check Point Endpoint Security – FDE

Before installing Check Point Endpoint Security – FDE, ensure the following activities are performed:

- Editing the prd.inf File, page 8
- Creating a Certificate, page 9
- Exporting a Certificate, page 11
- Importing a Certificate, page 12

Editing the prd.inf File

To include SafeNet eToken 7300 and SafeNet eToken 5100 tokens for pre-boot authentication, edit the **prd.inf** file.

1. Open the **prd.inf** file for editing. This file is located in the installation folder; for example, **C:\1_Pointsec for PC\Modules\prd.inf**.
2. Add the following information for 7300 and 5100 tokens:

   [eToken 7300]

   VendorID = VID_0529

   ProductIDList = PID_0602

   Version = 4

   DriverChksum = 9393322743

   DriverBinary = prd_ccid.bin

   DriverChksumUEFI = 3561675170

   DriverBinaryUEFI = etok_prd.efz

   [eToken 5100]

   VendorID = VID_0529

   ProductIDList = PID_0600

   Version = 4

   DriverChksum = 9393322743

   DriverBinary = prd_ccid.bin

   DriverChksumUEFI = 3561675170

   DriverBinaryUEFI = etok_prd.efz
3. Save the **prd.inf** file.

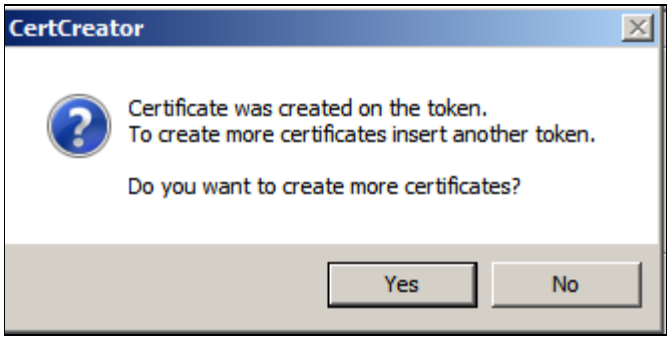
Creating a Certificate

1. Insert the SafeNet eToken 5100 or SafeNet eToken 7300 to the USB slot. Make sure SAC is already installed on the machine.
2. Run the **certCreator.exe** application, which is located in the installation folder; for example, **C:\ 1_Pointsec for PC\Tools\Token Certificate Creator\CertCreator**
3. On the **Full Disk Encryption – Token Certificate Creator** window, in the **Choose CSP** field, select **eToken Base Cryptographic Provider**, and then click **OK**.

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

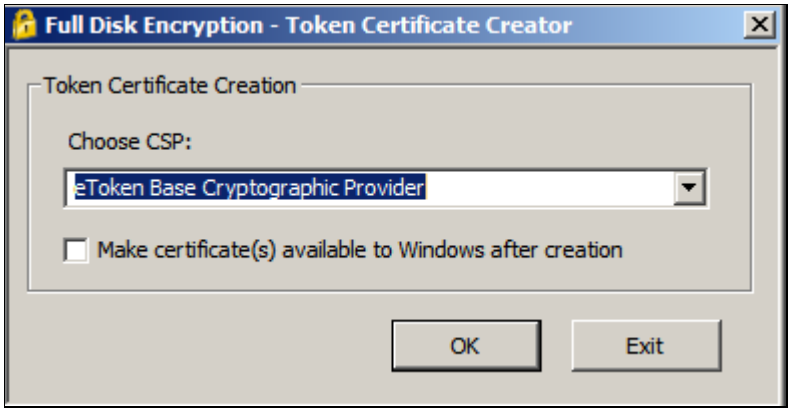
4. On the **Token Logon** window, in the **Token Password** field, enter the token password, and then click **OK**.

5. On the **CertCreator** window, click **No**.



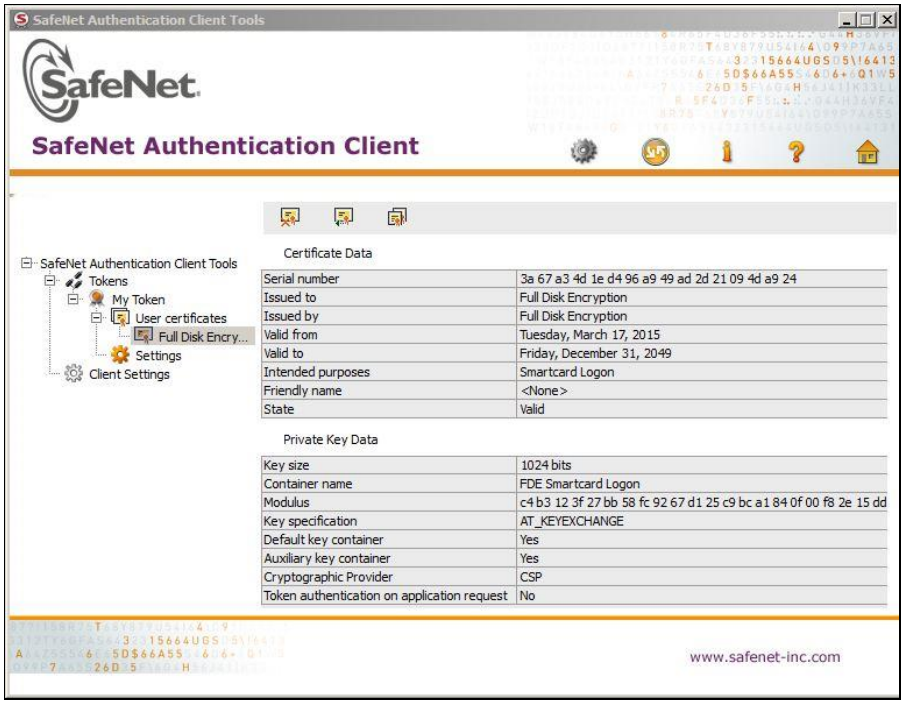
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

6. On the **Full Disk Encryption – Token Certificate Creator** window, click **Exit**.



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

7. The certificate is created. You can see the certificate in SAC tools under **User Certificates > Full Disk Encryption**.



Exporting a Certificate

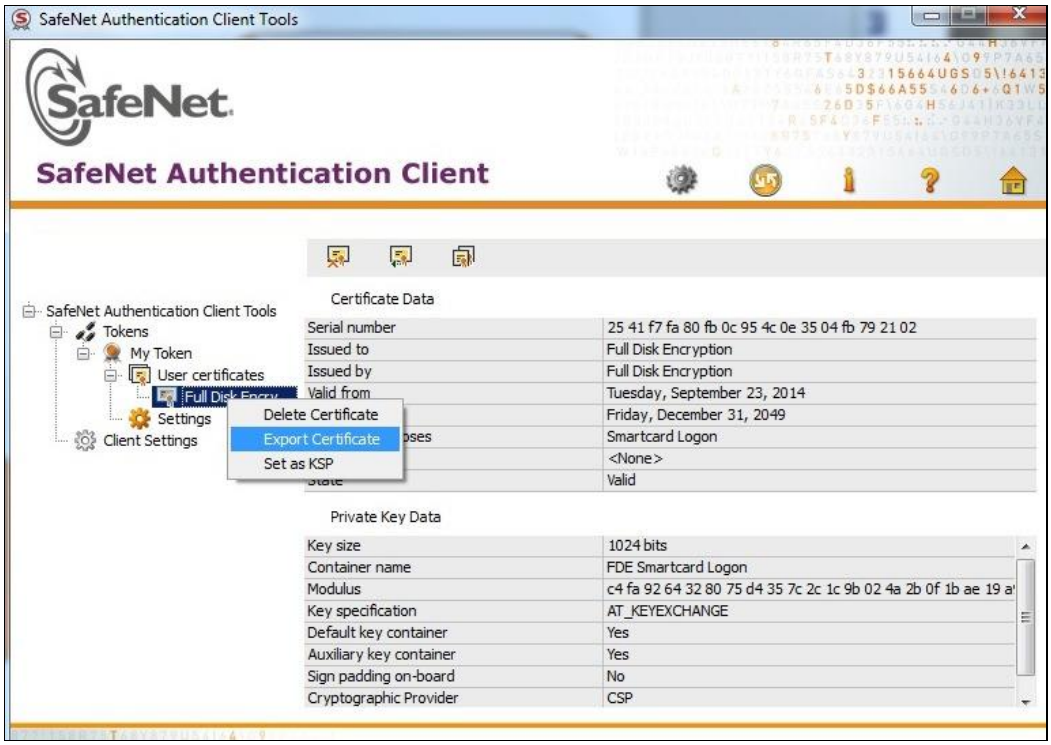
Export the certificate from SAC Tools to your machine. This certificate is later imported to the Windows machine you want to protect with pre-boot authentication.

1. Right-click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **Tools**.

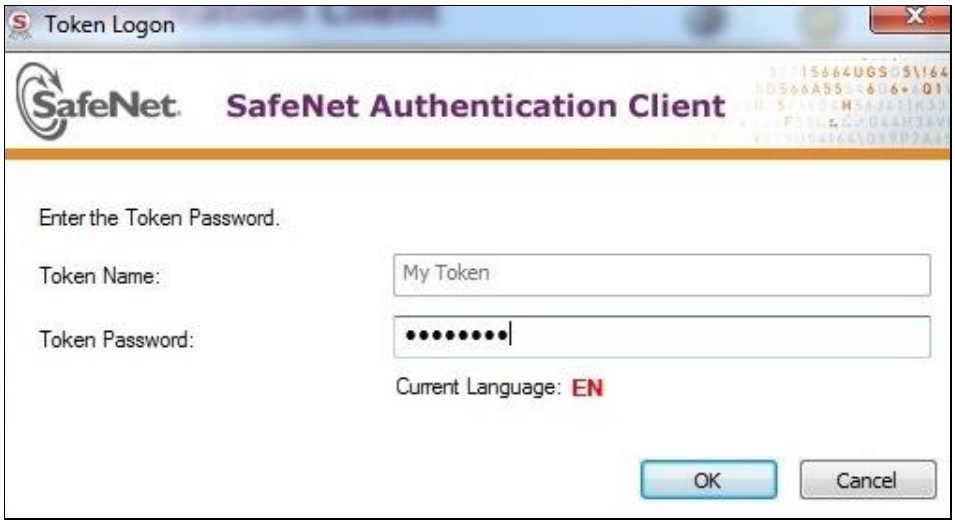
   Or

   From the Windows taskbar, click **Start > Programs > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client Tools**.

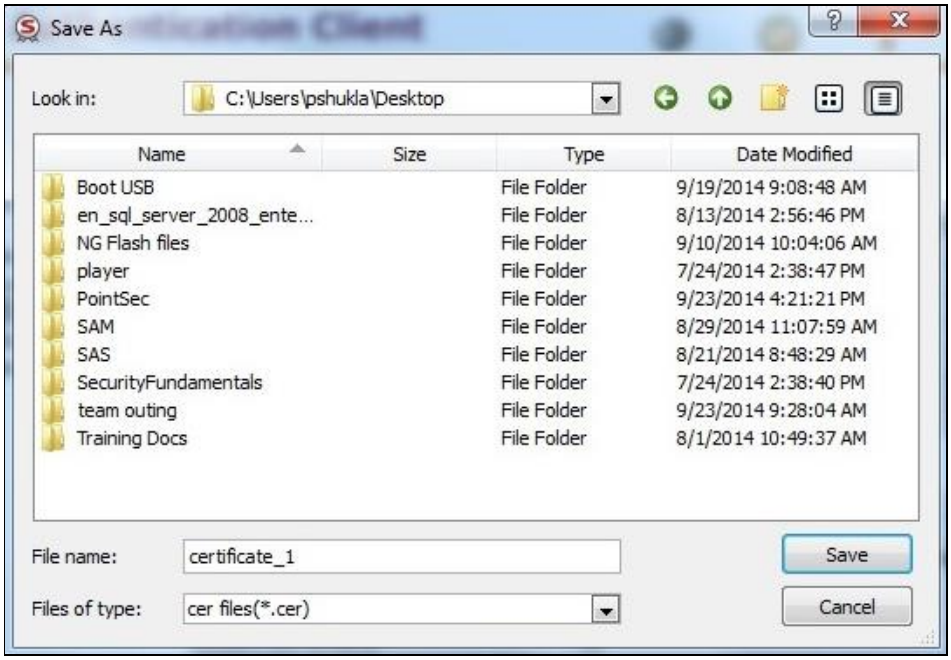
2. Expand **User Certificates**, right-click **Full Disk Encryption**, and then click **Export Certificate**.



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



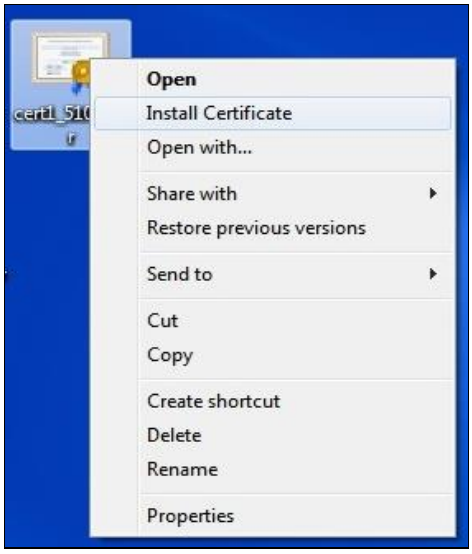
4. Select the location where you want to save the certificate, and then click **Save**.



Importing a Certificate

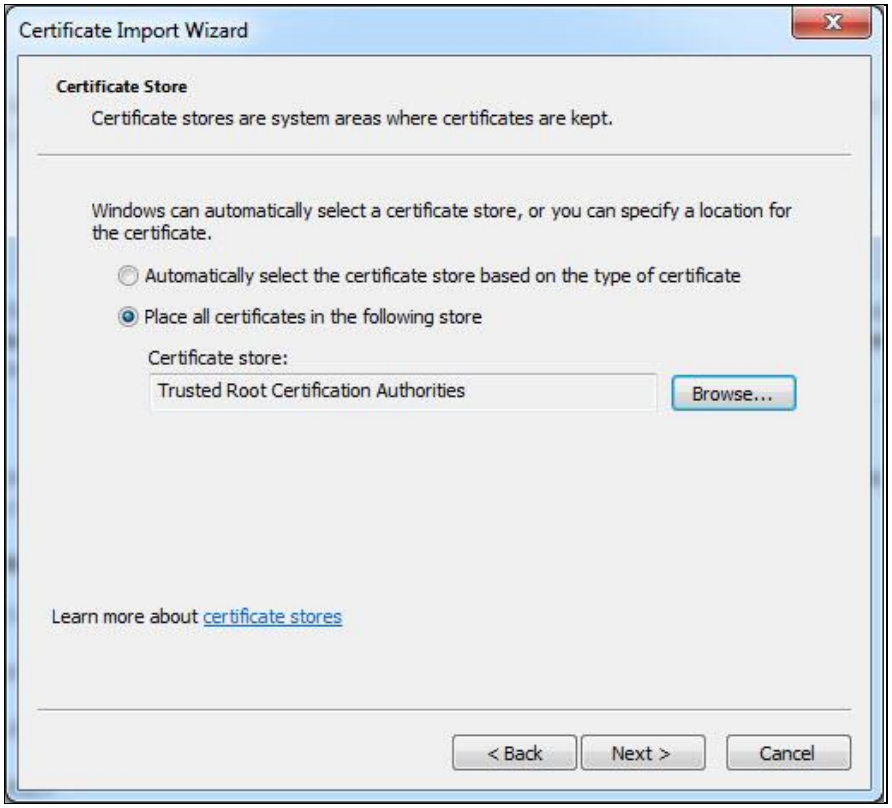
Import the certificate to the machine you want to protect with pre-boot authentication.

1. Locate the certificate you have exported in the section “Exporting a Certificate” on page 11.
2. Right-click the certificate and then click **Install Certificate**.



3. On the **Certificate Import Wizard** window, click **Next**.

4. Select **Place all certificates in the following store**, click **Browse**, select **Trusted Root Certification Authorities** from the Certificate Store, and then click **Next**.



5. If a security warning such as the one shown below is displayed, click **Yes**.

6. The certificate is imported successfully. Click **OK**.

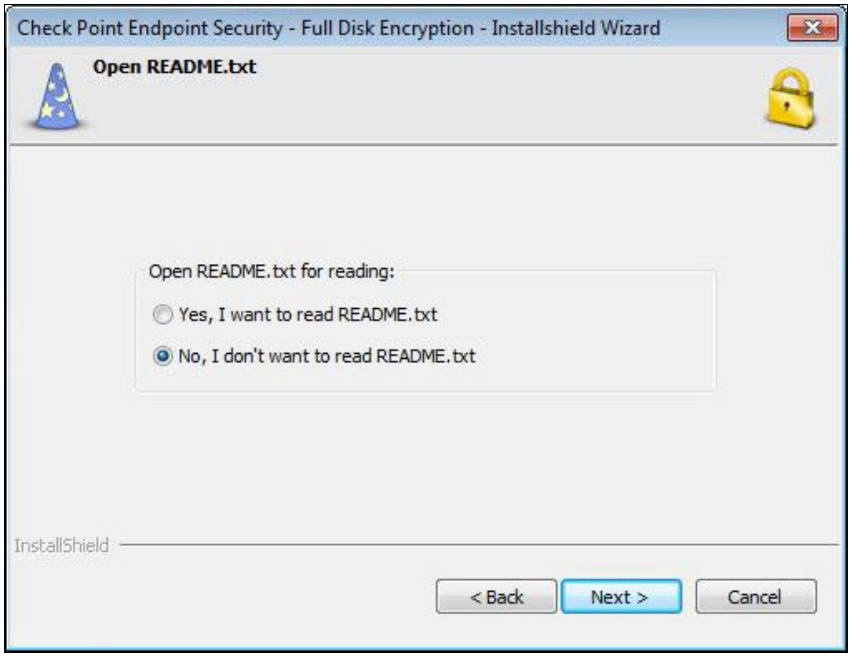
Installing Check Point Endpoint Security – FDE

Install Check Point Endpoint Security – FDE and configure the settings for smart card authentication using the certificate and eToken.

1. Start the Check Point Endpoint Security – FDE installer **Pointsec for PC.msi** from **C:\1_Pointsec for PC**.
2. Click **Accept**.

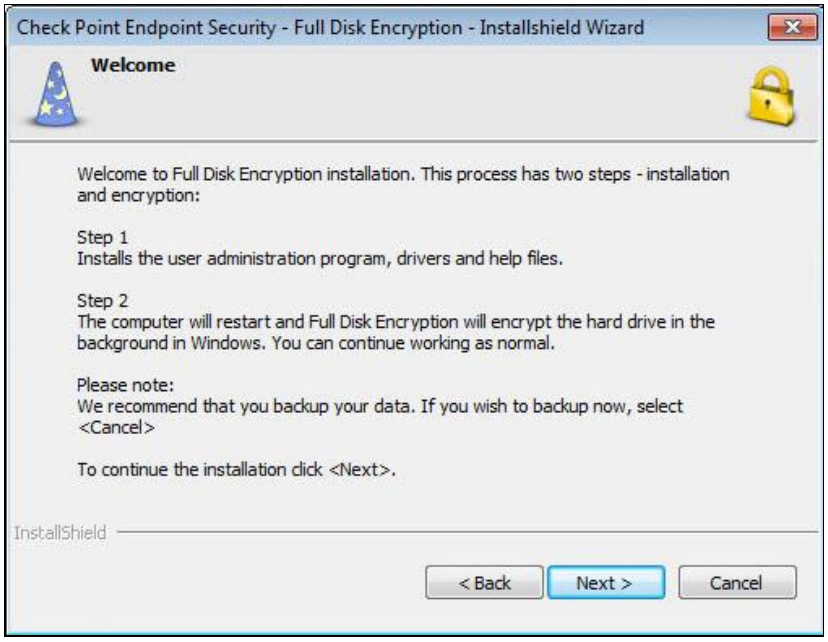
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

3. Select **No, I don't want to read README.txt**, and then click **Next**.



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

4. On the **Welcome** window, click **Next**.



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

5. Complete the following fields, and then click **Next**.

Name	Enter your name.
Company	Enter the name of your organization.
Serial Number	Click **Insert** and select the Full Disk Encryption serial number.

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

6. Add a user account that uses **Password** as the authentication method. Complete the following fields, and then click **Next**.

Username	Enter a name for this user account.
Authentication Method	Select **Password**.
Password	Enter a password for this user account.
Confirm Password	Enter the password again.

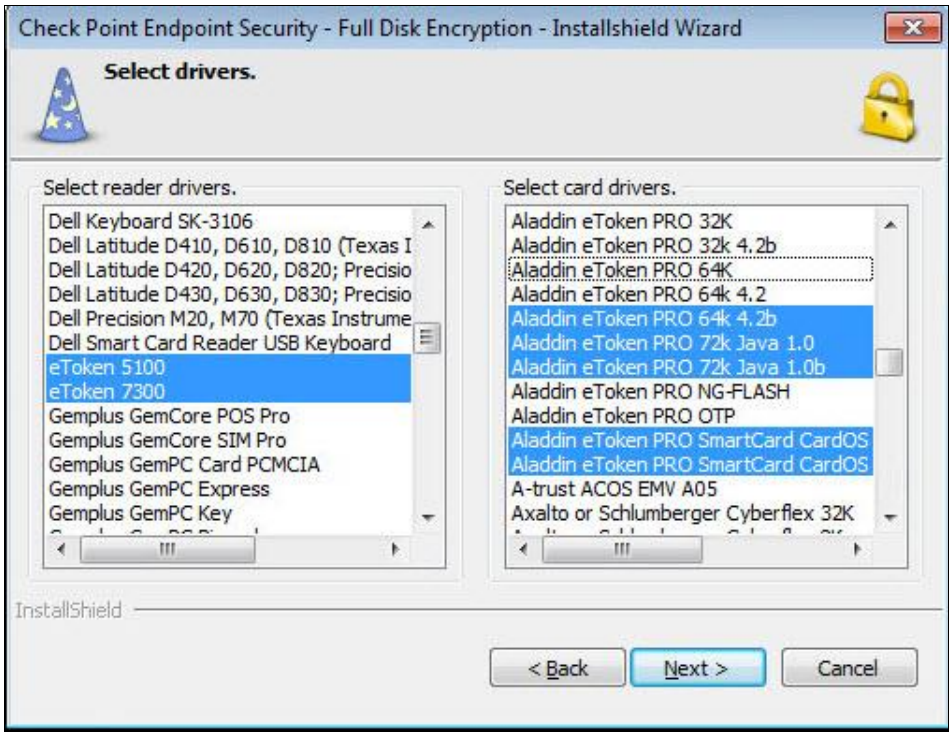
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

7. Add a user account that uses **Smart card** as the authentication method. Complete the following fields, and then click **Next**.

User account name	Enter a name for this user account.
Authentication method	Select **Smart card**.
Settings	Select the certificate. If the Check Point Endpoint Security – FDE certificate is not displayed in the right pane, check that the token with the certificate is inserted, and click **Refresh** to update the display.

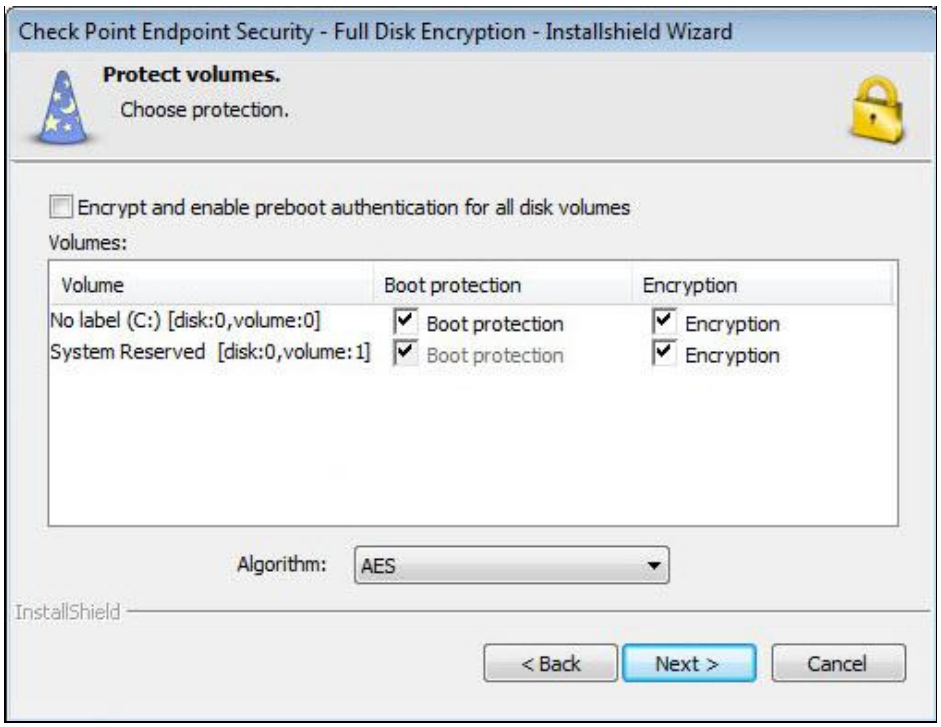
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

8. In the left pane, select the relevant reader drivers (for example, eToken 7300 and eToken 5100). Similarly, in the right pane, select the relevant card drivers. Click **Next**.



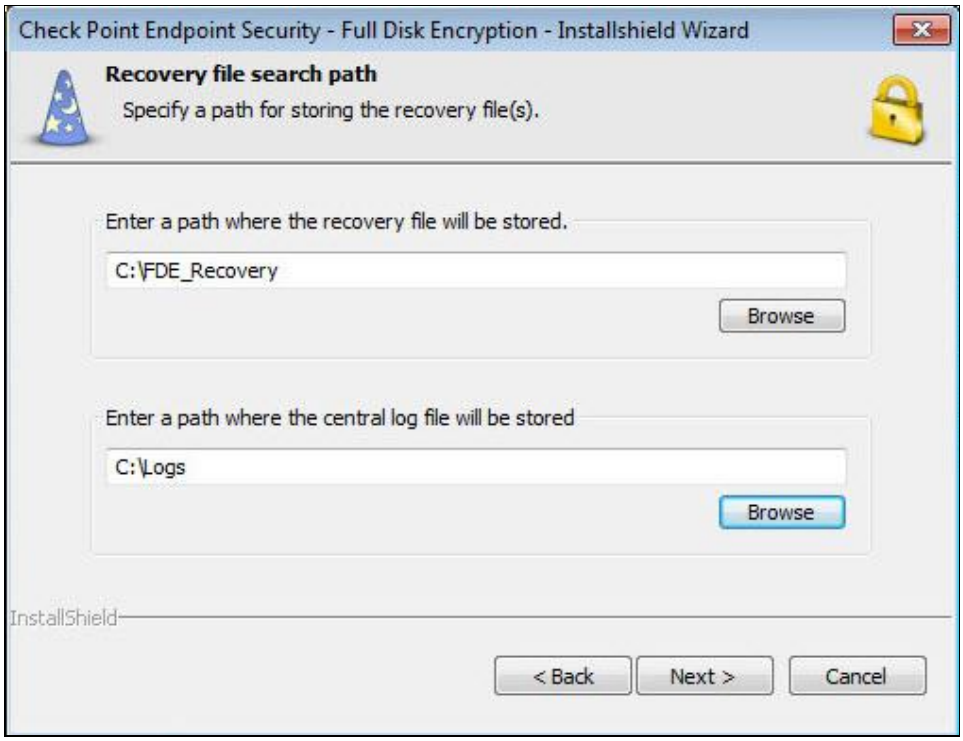
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

9. Select **Boot protection** and/or **Encryption** for each file system as required. Next, select the required **Algorithm** type, and then click **Next**.



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

10. Select the path for the locations where the **recovery file** and the **central log file** will be stored, and then click **Next**.

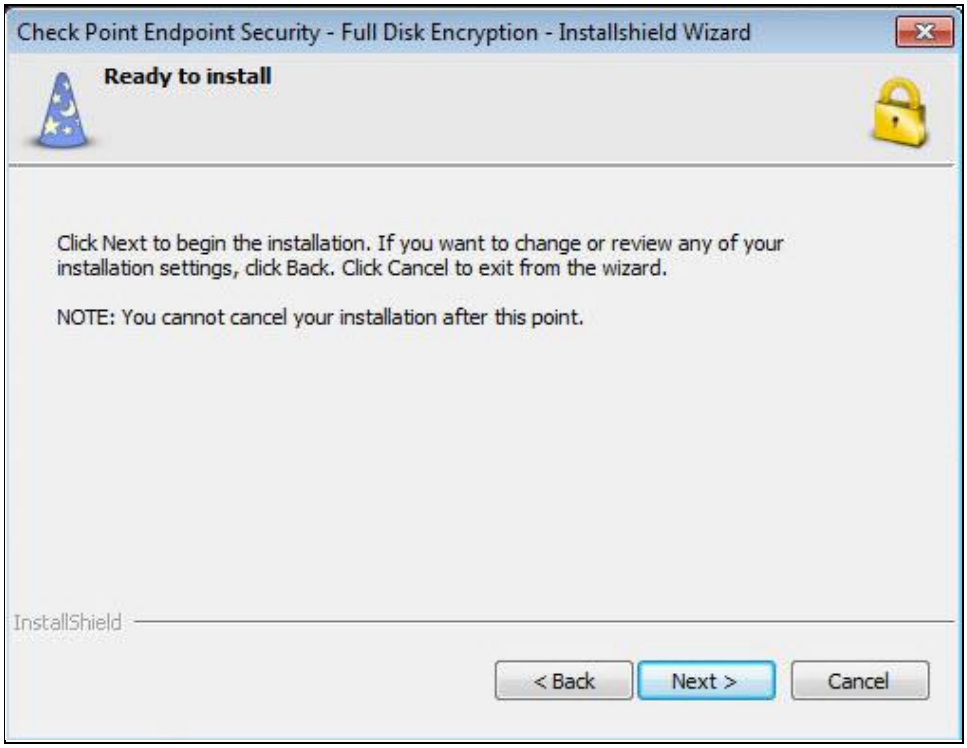


(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

11. On the **Access to network paths** window, click **Next**

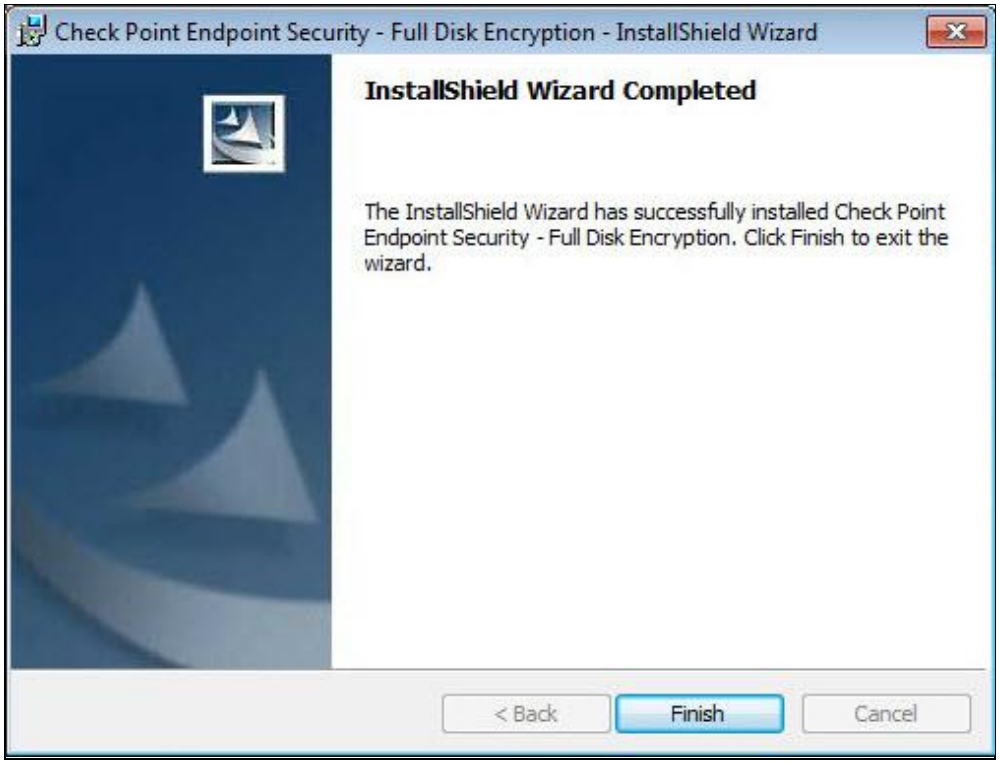
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

12. Click **Next**.



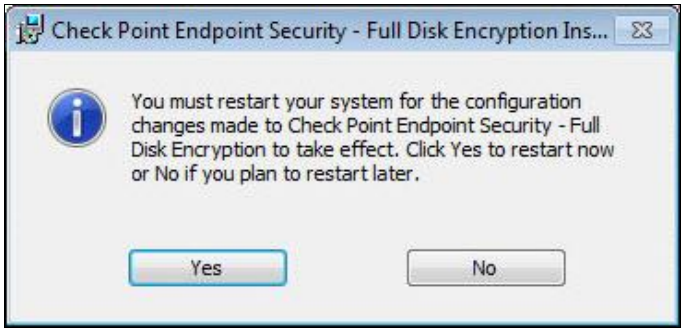
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

13. Click **Finish**. The installation is complete.



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

14. Click **Yes**. The PC restarts. You can now log on using eToken.



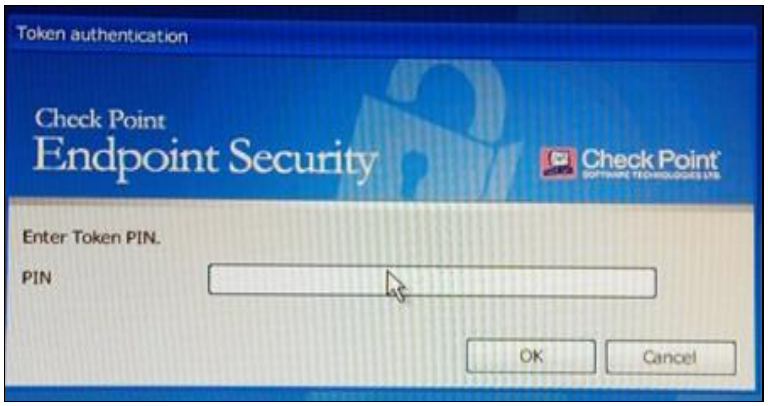
(The screen image above is from Check Point® software. Trademarks are the property of their respective owners.)

Running the Solution

Pre-boot can successfully unlock your system when you present the appropriate smart card (containing the certificate specified while installing Check Point Endpoint Security – FDE and the correct token password.

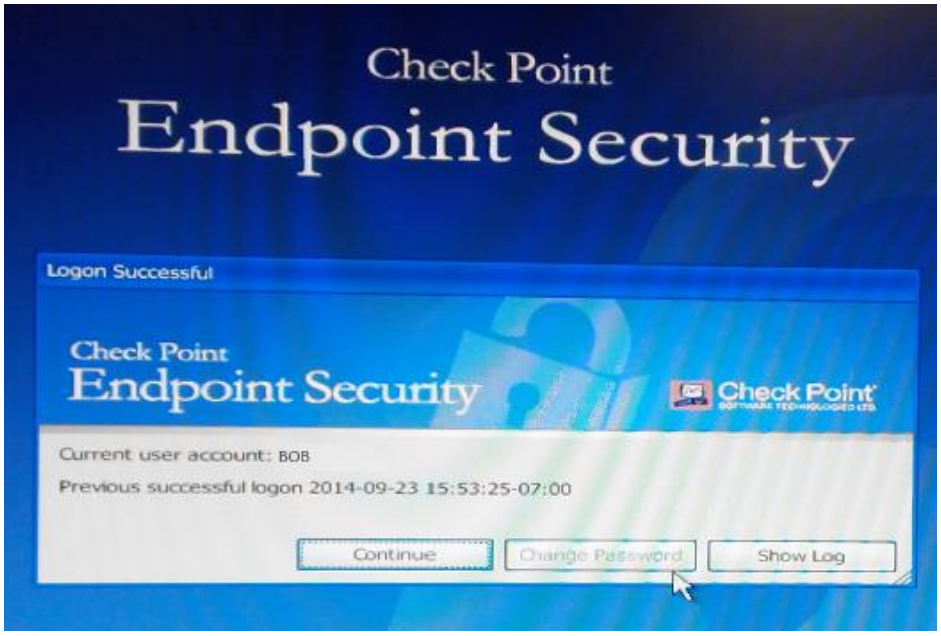
Ensure that you insert the token (containing the certificate of the user) either before starting the system or before attempting to authenticate.

1. Start the protected system.
2. In the **PIN** field, enter your **token password** and then click **OK**.



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

3. If the PIN is correct, the user is authenticated. Click **Continue**.



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

4. On the Windows login window, enter your Windows credentials, and then press the **Enter** key.

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

If the Windows credentials are validated, you will be logged in to the protected system.

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.	