How to Use the Smart Card Authentication with Check Point GO

Objective

A Smart Card, also known as a chip card, provides strong security authentication for organizations. Check Point GO supports all traditional smart cards, the CAPI- Cryptographic Application Programming Interface, and the Microsoft Windows operating system versions that let developers use secure cryptography-based Windows- applications. Check Point GO also supports public key and private key cryptography. The private key always stays encrypted on the card and the public key is copied from the card to the CAPI.

Check Point GO encrypts and decrypts data and authenticates users using digital certificates.

Supported Software

Check Point GO supports:
- All Security Management Server version, and
- SmartDashboard versions from R70.20

Supported OS

- Windows XP 32-bit, SP3 or higher.
- Windows Vista Home Basic/Premium, Business, Ultimate 32-bit and 64 bit, SP2 or higher.
- Windows 7 Home Premium, Professional, Ultimate 32-bit and 64 bit, Official release or higher.
Configuring Smart Card

Enabling Check Point GO Authentication on the Gateway

1. Open SmartDashboard.
2. Open the Global Properties menu.
   The Global Properties window opens.
3. Click Check Point GO.
4. Select Support certificate based user authentication.
5. Click OK.

Note: You must permit the Certificate Authority (CA) that the Smart Card uses on the gateway.
For internal CA:
1. Select the gateway from Network Objects list.
2. Open the IPSec VPN tab.
3. Make sure that the internal CA is on the list.
Configuring the Client for Check Point GO

Before you configure your desktop, prepare the Smart Card.

Preparing the Smart Card

Working with the Smart Card Requires:
- Driver – Export APIs for accessing the card.
- Dongle – Card reader.
- Smart Card – holds the user credentials.
- GUI – Provides API for uploading certificate on the smart card.

Make sure that the Smart Card reader:
- Is attached to the Host PC.
- Has a certificate to the GW.
- Can identify the certificate. After inserting the card, the reader's graphical interface must show the certificate.

If necessary, import certificate to the Smart Card:
- Generate certificate (P.12 file) for the user .
- Import the certificate file to the Smart Card.
- Connect the dongle to the computer and insert the card.

For external CA configuration, see the documentation.
Notes:
Each Smart Card vendor has its own installation method. If asked to install the CA certificates to Windows, allow the request.

Configuring Computer for VPN

To configure the host computer to connect to VPN:
1. Insert the Check Point GO device in to the host computer.

2. If the VPN site is not configured, configure a new VPN using the Check Point GO Site Wizard:

   Welcome to the Site Wizard

   The wizard will guide you through the configuration of a new site for the VPN client.
a) Enter required server information.

b) Select **Certificate** as the authentication method.
c) Select **Select certificate from Smart Card.**

![Certificate Authentication](image)

- Use P12 certificate
- Select certificate from Smart Card

1. If the VPN is already configured, you only need to change the authentication method for the Smart Card:
   a) Right-click the **VPN** icon and select **Site Properties** from the pop-

![Site created successfully](image)
b) Open the **Settings** tab and change the authentication method to **Certificate – Smart Card**.

c) From the drop-down box select the Smart Card Certificate and click **Connect**.

d) Enter the Smart Card password at the prompt.

e) Click **Connect**.
When the client connects to the site, the “Connection succeeded” message shows.

![Connection succeeded](image)

**Note:** Before you click **Connect**, you can review the certificate properties. Click **Show Certificate Properties**, located next to the **Certificate** drop-down menu.

![Show Certificate Properties](image)
Important Notes:

- Each time the user reconnects the Smart Card, the Smart Card client prompts for the Smart Card password.
- While the Smart Card remains inside the reader, the user can disconnect from the site and reconnect to it without re-entering the Smart Card password.
- If the Smart Card reader disconnects from the USB port of the computer, or the Smart Card is removed from the Smart Card reader, the authentication certificate becomes invalid and the VPN disconnects.
- When the Smart Card is the selected authentication method, the Check Point GO VPN client does not show options for the certificate enrollment or renewal.