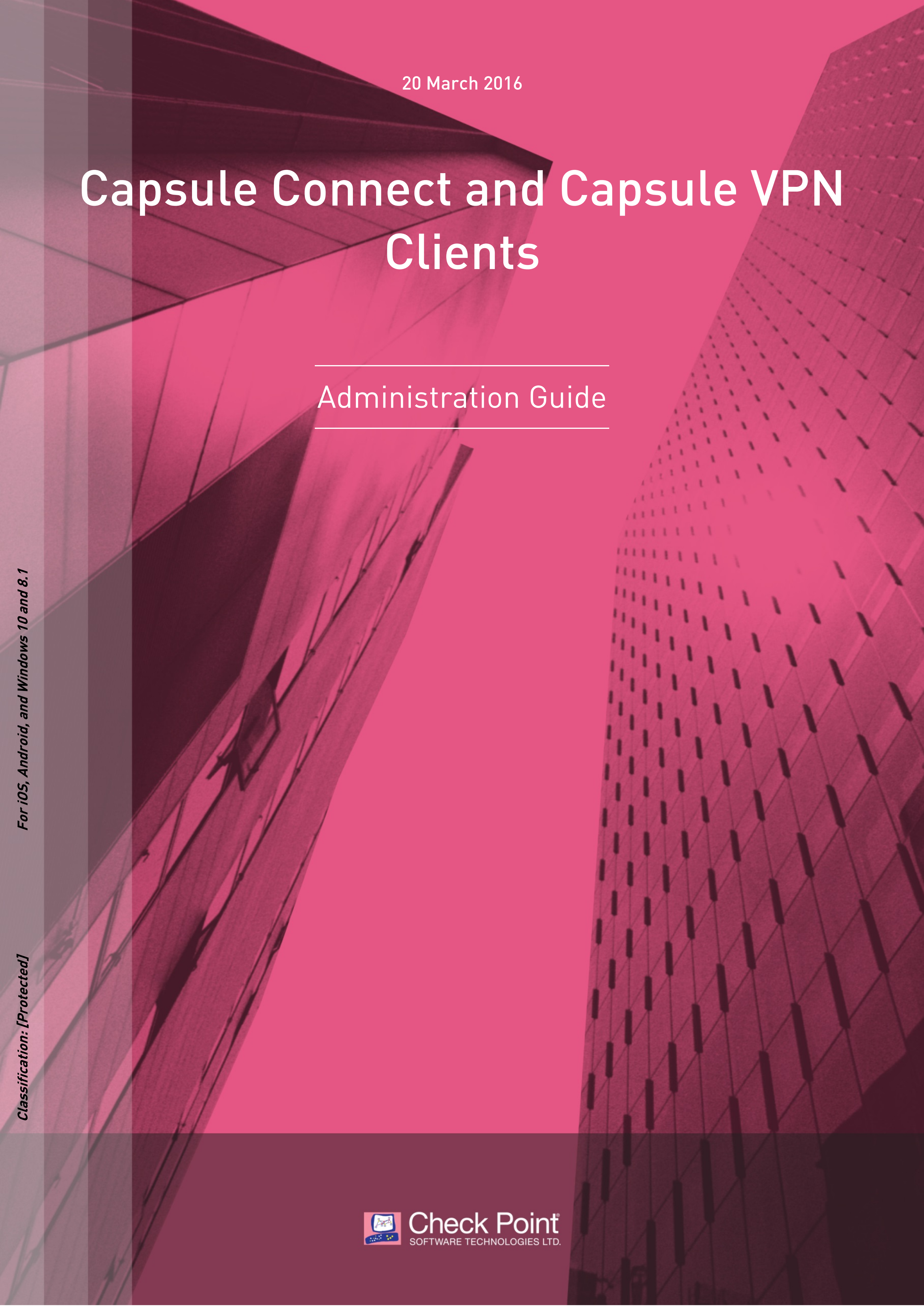

20 March 2016

Capsule Connect and Capsule VPN Clients

Administration Guide

For iOS, Android, and Windows 10 and 8.1

Classification: [Protected]

Check Point
SOFTWARE TECHNOLOGIES LTD.

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=20361

To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

Revision History

Date	Description
20 March 2016	Updated Using the API for a VPN Site (on page 17)
11 October 2015	Updated for Windows 10
31 March 2015	Changed document name and contents to reflect new client names: Capsule VPN and Capsule Connect Added Configuring Per-App VPN in iOS ("Configuring Per App VPN in iOS" on page 13) Added Configuring VPN Sites through an MDM (on page 23) Updated Creating a QR Code
24 July 2014	Added section for Windows Phone 8.1. It applies to Windows Phone 8.1 Preview or GA with the Mobile VPN App ("Capsule VPN for Windows Phone 10 and 8.1" on page 30). Removed note from API sections.
17 October 2013	First release of this document

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Capsule Connect and Capsule VPN Clients Administration Guide.

Contents

Configuring the Security Gateway

In This Section:

Licensing the Client

To connect a mobile device to the VPN, you must have a license for the IPsec VPN Software Blade and a license for the Mobile Access Software Blade. These Software Blades come with introductory licenses that can be used by up to 10 users for 30 days from the time of installation. You can go to the Support Center and extend each 30 day introductory license to let up to 50 users connect to the Security Gateway.

To get a license:

1. Go to the Check Point Support Center and log into your account.
2. Open the **My Products** page.
3. Select the **Mobile Access** license.
4. Click **License**.
5. Install the license on the Mobile Access Security Gateway manually or with SmartUpdate.
6. Do the above steps again for the IPsec VPN license.

Configuring R75.40 and Higher Security Gateways

Use SmartDashboard to configure an R75.40 and higher Security Gateways to support Capsule Connect and Capsule VPN.

To configure a R75.40 Security Gateway:

1. Open SmartDashboard.
2. Open the properties window of the gateway object.
3. Make sure that the **IPsec VPN** Software Blade is selected.
4. Select **IPsec VPN** > **VPN Advanced**.
5. Make sure that **Support NAT traversal** is selected.
6. **R75.40**: Select **IPsec VPN** > **Remote Access**.

R76 and higher: Select **VPN Clients** > **Remote Access**

For all versions: Configure Remote Access settings:

a) Select **Support Visitor Mode**.

b) From **Service**, select **https**.

7. **R75.40**: Select **IPsec VPN** > **Authentication**

   R76 and higher: **VPN Clients** > **Authentication**

   For all versions: Configure the **Authentication Method**.
8. **R75.40**: Select **IPsec VPN** > **Office Mode**

   R76 and higher: **VPN Clients** > **Office Mode**
9. For all versions: Configure Office Mode.

   a) Select **Allow Office Mode to all users** or **a group**.

   b) Click **Optional Parameters**.

   The **IP Pool Optional Parameters** window opens.

   c) Configure these settings,

   - **DNS servers**
   - **DNS suffixes**
   - **IP lease duration**
10. Select VPN Clients to enable:

    R75.40:

    a) Select **IPsec VPN** > **VPN Clients**

    b) Select **SSL Network Extender** and **SecureClient Mobile**.

    R76 and higher:

    c) Select **VPN Clients**

    d) Select **Mobile Devices - iOS and Android client** and make sure **Mobile VPN** is selected
11. Click **OK**.
12. Install the policy on the Security Gateway.

Configuring R71.50 Security Gateways

Use SmartDashboard to configure a R71.50 Security Gateway to support Capsule Connect and Capsule VPN.

To configure a R71.50 Security Gateway:

1. Open SmartDashboard
2. Right-click the Security Gateway and select **Edit**.

   The **Check Point Gateway - General Properties** window opens.
3. Make sure that the **IPsec VPN Software Blade** is selected.
4. Select **IPsec VPN > VPN Advanced**.
5. Make sure that **Support NAT traversal** is selected.

6. Select **IPsec VPN** > **Remote Access** and configure these settings.
   a) Select **Support Visitor Mode**.
   b) From **Service**, select **https**.
7. Select **Authentication** and configure the **Enabled Authentication Schemes**.

   For more about configuring the certificate authentication method, see *Known Limitation 00874317* in the *Capsule Connect and Capsule VPN Release Notes*.
8. Select **IPsec VPN** > **Office Mode** and configure these settings.
   a) Select **Allow Office Mode** to all users or a group.
   b) Click **Optional Parameters**.

   The **IP Pool Optional Parameters** window opens.
9. Install the policy on the Security Gateway.

Optional Configuration

You can configure these authentication and encryption settings for the Security Gateway in the Global Properties settings:

- When users are automatically re-authenticated to the Security Gateway
- User Encryption settings

To configure optional settings:

1. From the menu bar, select **Policy > Global Properties**.

   The **Global Properties** window opens.
2. Select **Remote Access** > **SecureClient Mobile** and configure the value for **Re-authenticate user every**.

   Note -

   - The IP lease duration (available in the IP Pool Optional Parameters) must be equal or larger than the re-authentication time.
   - For more information about Session Timeout see the *R75.40 VPN Administration Guide* http://supportcontent.checkpoint.com/solutions?id=sk67581.
3. **R71.50 and R75.40**: Select **Remote Access** > **VPN - Authentication and Encryption** and click **Advanced**.

   R76 and higher: Select **Remote Access** > **VPN - Authentication and Encryption** and click **Edit**.

   In all versions, the **Encryption Properties** window opens.
   a) Click **IPSEC Security Association (Phase 2)**.
   b) In **User Encryption properties**, configure the settings.

   For more information about encryption algorithms see the *VPN Administration Guide* http://supportcontent.checkpoint.com/solutions?id=sk67581.
4. Click **OK**.
5. Install the policy on the Security Gateway.

Finding the Gateway Fingerprint

In some configurations, when you connect to a site for the first time from the client, you must confirm that the fingerprint shown is valid.

The fingerprint is also necessary if you configure a new site with API or create a QR code.

To find the fingerprint for a site:

1. Open SmartDashboard.
2. From the right side of the Firewall tab, open the **Servers and OPSEC** tree.
3. If the gateway certificate is from the Internal Certificate Authority (ICA):
   a) Select **Trusted CAs** > **internal_ca**.
   b) In the **Local Security Management Server** tab, click **View**.
4. If the gateway certificate is from an external certificate Authority:
   a) Select the folder for the external CA.
   b) In the **OPSEC PKI** tab, click **View.**
5. The **Certificate Authority Properties** window opens.
   The required fingerprint is the string of random words in line 2 under **SHA-1 Fingerprints**.
   For example: BLUE HA GORE FLY MULE SHUT MILT CAKE TAB TINT

Adding Password Policy for Certificate Authentication

On Android, certificates are stored in a protected area, but without a password. For better certificate protection, we recommend adding a password. The password enables:

- Certificate encryption
- Two-factor authentication.

Note - Password protection only applies to Android.

To change the default password configuration for certificate authentication:

1. Go to `$FWDIR/conf` and edit the `nemo_client_1.ttm file`.
2. Set these parameters using hexadecimal values:

parameter	value
`neo_certificate_password_required` Available values `- 0x0 and 0x1.`	Set to `0x1` to activate the password policy for certificate authentication.
`neo_certificate_password_alphanumeric` Available values `- 0x0 and 0x1.`	Set to `0x1` to require both numbers and letters in a password.
`neo_certificate_password_min_length` Available values `- 1 to 20` (`0x1 to 0x14`).	Set minimum password length. **Note**: the values are in hexadecimal.

parameter	value
`neo_certificate_password_min_complex_length` Available values - `1` to `20` (`0x1` to `0x14`).	Set the minimum number of complex characters that should appear in a password.

3. Save the file after you change it.
4. Install the policy on the Security Gateway.

Here is an example of the `nemo_client_1.ttm` file:

```
(
        :nemo_client_1 (
        :neo_route_all_traffic_through_gateway (
                        :gateway (neo_route_all_traffic_through_gateway
                                :default (client_decide)
                        )
                )
        :neo_certificate_password_required (
                        :gateway (
                                :default (0x1)
                        )
                )
        :neo_certificate_password_alphanumeric (
                        :gateway (
                                :default (0x1)
                        )
                )
        :neo_certificate_password_min_length (
                        :gateway (
                                :default (0x6)
                        )
                )
        :neo_certificate_password_min_complex_length (
                        :gateway (
                                :default (0x0)
                        )
                )
        )
)
```

Adding Support for Back Connections

By default Capsule Connect and Capsule VPN sends traffic only when the VPN tunnel is being used. This lets the application conserve the battery and uses less network data. Some applications must have support for back connections. These applications must be able to send keep alive packets on the route to the Security Gateway to keep the connections alive in the connection tables.

To support back connections:

1. Edit the file `nemo_client_1.ttm`, and enable keep alive. Add these parameters:

```
:keep_alive_enabled (
      :gateway (
      :default (true)
      )
)
:udp_keep_alive_timeout (
      :gateway (
      :default (20)
      )
)
:tcp_keep_alive_timeout (
      :gateway (
      :default (120)
      )
)
```

2. Save the file.
3. Install the policy on the Security Gateway.

Authenticating with an External CA

You can use SmartDashboard to configure the Security Gateway to use an external CA (Certificate Authority) to authenticate Capsule Connect and Capsule VPN.

Make sure that the external CA follows these guidelines:

- Client certificate subject uses a full DN, and not only a CN.
- The certificates must use a user template with the IKE public key property with the LDAP branch.

Note - To learn how to configure an internal CA, see the *VPN Administration Guide* for the Security Gateway version.

Trusting an OPSEC Certified CA

The CA certificate has to be supplied and saved to the disk in advance.

Note - In case of SCEP automatic enrollment, you can skip this stage and fetch the CA certificate automatically after configuring the SCEP parameters.

The CA's Certificate must be retrieved either by downloading it using the CA options on the **Servers and OSPEC Applications** tab, or by obtaining the CA's certificate from the peer administrator in advance.

Then define the CA object according to the following steps:

1. Open **Manage > Servers and OPSEC Applications**.

   The **Servers and OPSEC Application** window opens.
2. Choose **New > CA**.

   Select **Trusted** or **Subordinate**.

   The **Certificate Authority Properties** window opens.
3. Enter a **Name** for the CA object, in the **Certificate Authority Type** drop-down box select the **OPSEC PKI**.
4. On the **OPSEC PKI** tab:
   - For automatic enrollment, select **automatically enroll certificate**.
   - From the **Connect to CA with protocol**, select the protocol used to connect with the certificate authority, either SCEP, CMPV1 or CMPV2.

   Note - For entrust 5.0 and later, use CMPV1

5. Click **Properties**.
   - **If you chose SCEP as** the protocol, in the **Properties for SCEP protocol** window, enter the CA identifier (such as example.com) and the Certification Authority/Registration Authority URL.
   - If you chose cmpV1 as the protocol, in the **Properties for CMP protocol - V1** window, enter the appropriate IP address and port number. (The default port is 829).
   - If you chose cmpV2 as the protocol, in the **Properties for CMP protocol -V2** window, decide whether to use direct TCP or HTTP as the transport layer.

     Note - If Automatic enrollment is not selected, then enrollment will have to be performed manually.
6. Choose a method for retrieving CRLs from this CA.

   If the CA publishes CRLs on HTTP server choose **HTTP Server(s)**. Certificates issued by the CA must contain the CRL location in an URL in the **CRL Distribution Point** extension.

   If the CA publishes CRL on LDAP server, choose **LDAP Server(s)**. In this case, you must define an LDAP Account Unit as well. See the Security Management Server *Administration Guide* for more details about defining an LDAP object.

   Make sure that **CRL retrieval** is checked in the **General** tab of the **LDAP Account Unit Properties** window.

   Certificates issued by the CA must contain the LDAP DN on which the CRL resides in the CRL distribution point extension.
7. Click **Get**.
8. If SCEP is configured, it will try to connect to the CA and retrieve the certificate. If not, browse to where you saved the peer CA certificate and select it.

   VPN reads the certificate and displays its details. Verify the certificate's details. Display and validate the SHA-1 and MD5 fingerprints of the CA certificate.
9. Click **OK**.
10. Install the policy on the Security Gateway.

Configuring an External CA

To configure an external CA:

1. From SmartDashboard, select **Manage > Users and Administrators**.

   The **Users and Administrators** window opens.
2. Select **Standard_User** and click **Edit**.

   The **User Template Properties** window opens.
3. Click **Encryption**.
4. Select **IKE** and click **Edit**.

   The **IKE Phase 2 Properties** window opens.
5. Make sure that **Public Key** is selected.
6. Click **OK**.
7. From the menu bar, select **Manage** > **Servers and OPSEC Applications**.

   The **Servers and OPSEC Applications** window opens.
8. Edit the LDAP account settings.

   The **LDAP Account Unit** window opens.
9. Click **Authentication**.

10. Select **Use user template** and **Standard_User**.
11. Click **OK** and then **Close**.
12. Install the policy on the Security Gateway.

Configuring Route All Traffic

When the Route All Traffic feature is enabled, the gateway agrees to act as a VPN router for the client. All connections the client opens, either to the internal network or to other parts of the Internet, pass through the gateway.

To configure the Route All Traffic settings:

1. Open SmartDashboard
2. Right-click the Security Gateway and select **Edit**.

   The **Check Point Gateway - General Properties** window opens.
3. **R71.50 and R75.40**: Select **IPsec VPN > Remote Access**.

   R76 and higher: Select **VPN Clients** > **Remote Access**
4. Select **Allow VPN clients to route traffic through this gateway**.
5. Click **OK**.
6. From the menu bar, select **Policy > Global Properties**.
7. Select **Remote Access** > **SecureClient Mobile**.
8. From **Route all traffic to gateway**, select **Yes**.
9. Click **OK**.
10. Install the policy on the Security Gateway.

Configuring Per App VPN in iOS

In iOS 7 and higher, you can configure a Per App VPN site to allow only selected applications to send their traffic (TCP only) through a VPN tunnel. Other applications on the device are not affected and do not send traffic through the VPN. Per App VPN is in contrast to the device-wide VPN, which allows traffic from the entire device to go through the Layer 3, VPN tunnel.

In iOS 7, only one connection can be active at one time.

In iOS 8, multiple Per App connections can be connected at the same time. This can be in addition to the device-wide Layer 3, VPN tunnel. This lets devices connect to Capsule Cloud in parallel to a connection with the on-premises Security Gateway.

Configure Per App VPN sites through a third-party MDM (Mobile Device Management) that you use to manage the device and applications. See your MDM vendor documentation on Per App VPN to configure this. No other configuration is necessary on the Security Gateway.

Alternatively, if your organization does not use an MDM, you can configure Per App VPN sites through the Security Gateway. See sk105462 http://supportcontent.checkpoint.com/solutions?id=sk105462 for details.

iOS and Android Clients

In This Section:

Downloading the Application

Download the **Check Point** application for:

- **Android Capsule VPN** from Google Play (https://play.google.com/store/apps/details?id=com.checkpoint.VPN).
- **iOS Capsule Connect** from the AppStore (http://itunes.apple.com/app/check-point-mobile-vpn/id506669652?mt=8).

Creating and Configuring the VPN Site

Capsule Connect and Capsule VPN supports different procedures to create and configure the VPN site. Use the procedure that is the most convenient for your users:

- **Manual Configuration -** Use the application to manually configure the VPN site settings.
- **VPN Site API -** Create a URL that configures the settings for the VPN site.
- **QR Code -** The application scans a QR code. The code embeds a URL for site configuration.
- **iPhone Configuration Utility** - Use the iPhone configuration utility to send the VPN site settings to all the users. (iOS only).
- **MDM** - Use your MDM vendor's dashboard to push VPN site settings to your managed devices (iOS only).

Manually configuring the VPN Site in Android

1. If necessary, open the window for creating new sites.
   a) Tap the **wrench** icon.
   b) Tap **+**.
2. Configure these settings for the VPN site:
   - **Name** - name of VPN site.
   - **Server** - IP address or host name

3. Tap **Create**.

   The **Verify Server** message opens.
4. Tap **Yes** to accept the certificate and fingerprint.

   The **Authentication** screen opens.
5. Select the **Authentication Method**.
6. Close the settings window.

VPN Site Settings

These are the VPN site settings that users can manually configure in the application.

To configure the VPN site settings:

1. From the login screen, tap the **wrench** icon.

   The **Site List** screen opens.
2. Press and hold the VPN site to edit.

   The settings for that VPN site are shown.

Authentication Methods

- **Username and password** – Check Point or LDAP password.
- **Certificate** – Authenticate using an x509 certificate. Certificates can be enrolled from the client.
- **RSA SecurID token** – Authenticate using an RSA SecurID.
- **Challenge response** – Authenticate using the challenge and response procedure.

Importing an external certificate

An external certificate can be imported from a file.

1. Copy the p12 or pfx file to the device.
2. In the Capsule VPN application go to **Sites > Edit Site > Authentication method > Certificate**
3. Tap **Import**.
4. Select the p12 or pfx file.

VPN Tunnel Type

You can set the VPN tunnel type to IPsec or SSL for the client:

To set the VPN tunnel type:

In the site settings screen, select **IPsec** or **SSL**.

Always Connect

When this option is enabled, the client automatically opens a VPN connection to the site.

Sending Logs

To send logs to Check Point technical support:

1. Open the application.
2. Tap the **i** icon.
3. Tap on the **Menu** button or the **Action Sheet**.
4. Tap **Send Logs**.

Manually Configuring the VPN site in iOS

This section covers manually configuring the VPN site in iOS.

VPN Site Settings

These are the VPN site settings that users can manually configure in the application.

To configure the VPN site settings:

1. From the main Site List screen, tap **Sites**.
2. Tap the arrow for the VPN site.

   The settings for that VPN site are shown.

Authentication Method

- Username and password – Check Point or LDAP password.
- Certificate – Authenticate using an x509 certificate. Certificates can be:
- Enrolled
- Installed by email
- Installed from the Internet
- Installed using iPhone configuration utility
- RSA SecurID token – Authenticate using an RSA SecurID.
- Challenge response – Authenticate using the challenge and response procedure.

Automatic Reconnect

- **On** – When connectivity is broken, the application tries to reconnect as long as there is network available.
- **Off** – When connectivity is broken, the application tries to reconnect for 120 seconds. After this time, the application disconnects from the VPN site.

  You can select the **Off** setting to use less battery on the device.

Connect On-Demand

This feature configures the VPN site to automatically create a VPN tunnel for specified domain names. Connect On-demand is only available when Certificate Authentication is enabled.

- Select **Connect On-demand** to enable this feature.

VPN Tunnel Type

You can set the VPN tunnel type to IPsec or SSL for the client:

To set the VPN tunnel type:

1. In the site settings screen, swipe up.

   The VPN tunnel types are shown.
2. Select **IPsec** or **SSL**.
3. Swipe down.

Sending Logs

To send logs to Check Point technical support:

1. Open the application.
2. Tap the **About** button.
3. Make sure that **Collect Logs** is enabled.
4. Tap **Send Logs**.

Using the API for a VPN Site

The VPN API lets you control the application to:

- Create a VPN site
- Connect to and disconnect from a VPN site

To use the VPN API, create a URL that can be integrated into web sites, configuration emails and 3rd party applications.

Sample URL that creates a VPN site using the VPN site API

Tap this URL in a mobile device with Capsule Connect and Capsule VPN. The application creates a new VPN site with these settings:

```
cpvpn:///?V1&name=demo&host=demo.example.com&user=John+Doe
```

- VPN site name - demo
- Host - idemo.checkpoint.com
- User name - John Doe

Configuring the URL

The API URL is made of these segments:

- Mandatory segment- The app identifier: `cpvpn:///?V1`
- Fields paired with values, each two pairs are separated by the **&** character.
- Do not use spaces, use the **+** character. Example: `John+Doe`
- Assign a value to the field with the = character. Example: `name=idemo`

Creating a New VPN Site with API

Use these parameters to configure the settings for the VPN site.

Mandatory Parameters

Parameter	Description
`name`	The name of the site that is shown to the user.
`host`	The address of the host. Example: `idemo.checkpoint.com`
`fingerprint`	Fingerprint that is used for server validation. If you set the value to the server fingerprint, and the certificate is valid and signed by a trusted CA, users will not be prompted to decide if they trust the server.

Optional Parameters

Parameter	Description	Default Value
`user`	Login name for the user.	No value
`tun`	Possible values: `kmp` (IPsec tunnel) or `snx` (SSL tunnel)	`kmp`
`auth`	Authentication method. The valid values are: • `username` (user name and password method) • `RSA` (RSA SecureID) • `Certificate` • `PinPad` (Keypad for PIN code) • `KeyFob` (Security token key fob) • `Challenge` (Challenge and response method)	`username`
`port`	Port to use	`443`
`url`	After each connection to the VPN site, this URL is opened.	No value
`remoteActions`	Enables using the VPN site API. Valid values: `yes` or `no`	`No`

Parameters for Certificate Authentication

These parameters can be used for VPN sites that use certificate authentication.

Parameter	Description	Default Value
`regKey`	Activation key that enrolls a certificate	No value
`onDemand`	Valid values: • `yes` • `no` • `askUser`	No
`domainAlways`	An array of hosts to which the iOS connects only using a VPN tunnel. Example: `domainAlways="example1.com+example2.com+idemo.com"`	
`domainNever`	Hosts that are exceptions to the `domainAlways` parameters. The iOS never tries to connect to these hosts using a VPN tunnel. Example: `domainNever="help.example1.com+products.example1.com"`	
`domainIfNeeded`	An array of hosts that the iOS first tries to connect without using a VPN tunnel. If the first connection fails, iOS tries to connect using a regular connection. Example: `domainIfNeeded="example1.com+example.com"`	

Connecting to a VPN Site

The connect action attempts to connect to the site. If more authentication is necessary, the login screen for the site is shown.

Important - This action is only enabled if the `remoteActions` field was set to `yes` when site was created.

- Example:
  `cpvpn://?connect&siteName=MySite&url=www.URLToLaunchAfterConnect.com`

The connect action is identified by the field `connect`. This field is not assigned a value.

Parameters for the connect action:

- `siteName` - (Mandatory) The name of the site that is in the **Sites** list in the VPN Client.
- `url` - (Optional) A one-time response URL that is launched when the application connects to the site.

Disconnecting from a VPN Site

This action is only enabled if the `remoteActions` field was set to `yes` when the site was created.

The disconnect action disconnects the device from the site.

Important - This action is only enabled if the `remoteActions` field was set to `yes` when site was created.

- Example:
  `cpvpn://?disconnect&siteName=MySite&url=www.URLToLaunchAfterDisconnect.com`

The disconnect action is identified by the field `disconnect`. This field is not assigned a value.

Parameters for the connect action:

- `siteName` - (Mandatory) The name of the site that is in the **Sites** list in the VPN Client.
- `url` - (Optional) A one-time response URL that is launched when the application disconnects to the site.

Creating a QR Code

A QR code is a URL that is encoded in a QR image. The application has a built-in QR scanner that can read the URL and create a VPN site. You can create a QR code that creates VPN sites on handheld devices.

To create a QR code using the QR Code Tool:

1. Download the QR Code Tool http://supportcontent.checkpoint.com/solutions?id=sk69540.

From the CLI, run the command CPQRCodeGenerator.

These are the mandatory parameters for the command:

`name="<name>" host="host" fingerprint= "fingerprint" file='file'`.

This is a sample script that creates a QR code PNG file.

```
CPQRCodeGenerator name="demo" host="demo.example.com" fingerprint = "DEMO FING ERP
RINT FOR CODE" user='John Doe' file=demoQR.png
```

To create a QR code using a QR code generator:

1. Create a URL for the VPN site.
2. Use a QR code generator to create a QR image of the URL. Use the QR Code URL Parameters.

QR Code URL Parameters

Mandatory Parameters

Parameter	Description
`name`	The name of the site that is shown to the user.
`host`	The address of the host. Example: `androdemo.checkpoint.com`
`fingerprint`	Fingerprint that is used for server validation. If you set the value to the server fingerprint, and the certificate is valid and signed by a trusted CA, users will not be prompted to decide if they trust the server.
`file`	The PNG file name of the QR Code image that is created. Example: **mySite.png**

Optional Parameters

Parameter	Description	Default Value
`user`	Login name for the user.	No value
`tun`	Possible values: `kmp` (IPsec tunnel) or `snx` (SSL tunnel)	`kmp`
`auth`	Authentication method. The valid values are: • `username` (user name and password method) • `RSA` (RSA SecureID) • `Certificate` • `PinPad` (Keypad for PIN code) • `KeyFob` (Security token key fob) • `Challenge` (Challenge and response method)	`username`
`port`	Port to use	`443`
`url`	After each connection to the VPN site, this URL is opened.	No value
`remoteActions`	Enables using the VPN site API. Valid values: `yes` or `no`	`No`

Parameters for Certificate Authentication

These parameters can be used for VPN sites that use certificate authentication.

Parameter	Description	Default Value
`regKey`	Activation key that enrolls a certificate	No value
`onDemand`	Valid values: • `yes` • `no` • `askUser`	`No`
`domainAlways`	An array of hosts to which the client always tries to connect. Example: `domainAlways = "example1.com example2.com checkpoint.com"`	
`domainNever`	An array of hosts to which the client never tries to connect. Example: `domainNever = "example1.com example2.com checkpoint.com"`	
`domainIfNeeded`	An array of hosts to which the client tries to connect when necessary. Example: `domainIfNeeded = "example1.com example2.com checkpoint.com"`	

Using the iPhone Configuration Utility

This section covers using the iPhone Configuration Utility.

Configuring the VPN Profile

You can configure the VPN site using the iPhone configuration utility. You can download this utility from Apple iPhone Support Enterprise.

When configuring a VPN Profile, use the **Configuration Profile** section and select the **VPN** tab.

Configure these parameters:

- **Connection Name** - Name of the site
- **Connection Type** - Set to custom SSL
- **Identifier** - Set to: `com.checkpoint.CheckPoint-VPN.vpnplugin`
- **Server** - Hostname or IP address for the server.
- **Account** - User name or account for authenticating
- **Custom Data** - A list of fields and values are available here. See Custom Data Fields (on page 22).
- **User Authentication** - Choose certificate or password.
  - If a certificate was chosen for User Authentication you must also select a valid certificate in the Credential field.

    When using certificate as User Authentication you can enable **VPN On Demand** - select **Enable VPN On Demand**.

    Add Domains or hosts and select an action: **Always establish**, **Never establish**, **Establish if needed**.
  - If password credentials are used, it is necessary to fill in the password field to authenticate the connection.

Custom Data Fields

These are the keys that can be used in the Custom Data screen:

- **tuntype** - possible values: `kmp` (IPsec tunnel) or `snx` (SSL tunnel)
- **AuthMethod**

  Possible values:
  - Username and Password
  - Certificate
  - PinPad
  - KeyFob
  - Challenge Response

  Note - The `authMethod` field should match the value selected in the User Authentication field. For certificate authentication, select certificate in the User Authentication field. For other forms of authentication, select: password.
- **password** - Password to connect to host, if password was chosen for User Authentication.

- **fingerprint** - The fingerprint expected from the server.

  Note -

  - To complete the fingerprint verification, this parameter must be configured along with the CN field.
  - To prevent the user from seeing the fingerprint and deciding if the site can be trusted, set the value to the server fingerprint.
- **user** - default user name that is used to authenticate the connection. The same value that is set in the **Account** field.
- **regKey** - Activation key required to enroll a certificate. (Only when authentication method is by certificate)
- **port** - Port that the VPN connection uses
- **url** - A url to launch after each connection to the site
- **remoteActions** - Lets the VPN API to interact with this site. Possible values: yes and no

Configuring VPN Sites through an MDM

To configure a new VPN site with an MDM (iOS only):

1. In your MDM dashboard, add a VPN profile and choose the **Custom SSL** type.
2. Set **com.checkpoint.CheckPoint-VPN.vpnplugin** as the identifier.
3. To configure trust between the Capsule Connect client and the Security Gateway, add these key-value pairs in the **Custom Data**:
   - authMethod
   - cn
   - fingerprint.

   It is not required to add these keys but we recommend that you do. If you do not add these keys, end-users must approve the gateway authenticity before the first connection.

   For more details on these and other optional parameters, see Custom Data Fields (on page 22).

Windows 10 Capsule VPN for PC

In This Section:

Creating and Configuring the VPN Site

You can configure a VPN site for the Windows 10 Plugin in these ways:

- **PowerShell Script**

  Use the PowerShell script to push site configuration to users. See sk107535 http://supportcontent.checkpoint.com/solutions?id=sk107535.

- **Manual Configuration**

  Manually configure a site on each Windows 10 device.

- **Mobile Device Management**

  Use a Mobile Device Management Tool, such as Microsoft Intune to push site configuration to users.

These authentication methods are supported:

- Username and Password (Check Point or LDAP password defined on the gateway)
- Certificate (Use a certificate that is defined on the gateway)
- Smart Card
- RSA SecurID PinPad
- RSA SecurID KeyFob
- Challenge Response

Using the Client in Windows 10

This section contains detailed instructions for using the Check Point VPN Plugin on Windows 10.

We recommend that you give your users the information that applies to them.

Make sure that all users have:

- The credentials and/or devices necessary to authenticate
- The fingerprint of the site

In addition, if users will configure a site manually, make sure that they:

- Have the site name or IP address
- Know which authentication method to select

Downloading the Windows 10 Application

The Check Point VPN client in Windows 10 is called Check Point Capsule VPN and it is necessary to download the app from the Microsoft store https://www.microsoft.com/en-us/store/apps/check-point-capsule-vpn/9wzdncrdjxtj.

Manually Configuring a VPN Site

Create a VPN site on each Windows 10 device. This is the site that your device connects to access organizational resources.

To create a VPN site:

1. Open the Start menu and type **VPN**.
2. Tap **Change Virtual Private Network (VPN)**.
3. Tap **Add a VPN connection**.
4. Enter the required information:
   a) **VPN provider** - Select **Check Point VPN**

   b) **Connection name** - Enter a display name for the connection. This is the name that shows on your device. For example, "Work."

   c) **Server name or address** - Enter the name or IP address of the site. For example, company_vpn.company.com or 192.0.2.1. Contact your administrator if you do not have this information.

   d) Optional: Select **Remember my sign-in information**. If selected, re-authentication is enabled and the password is cached for later logins.
5. Tap **Save**.

Connecting to a Site for the First Time

The first time that you connect to a site, you select the authentication method that you will use to sign in to the site. After you select the authentication method for a site, you cannot change it.

You are also asked to verify the fingerprint of the gateway. This means that the site you are connecting to is valid. The fingerprint is a string of random words. Compare the fingerprint that you see to the fingerprint that your administrator supplies. If they are the same, you know that the site is valid.

To connect to a VPN site for the first time:

1. Tap the Network icon in the taskbar notification area.

   The **Networks** menu opens.
2. Tap **Connections.**
3. Tap your site.

   If you created the site manually, the name of the site is the **Connection name** that you entered.
4. Tap **Connect**. If you do not see a Connect button, check your internet connection.
5. Select an **Authentication method**.

   If you do not know which method to select, contact your administrator.
6. Click **Next**.
7. Enter the required credentials.

8. A message says: **Check Point is connecting to site: xxx Which has this fingerprint:xxx. Click Next to continue.**

   Confirm that the fingerprint is correct and click **Next**.
9. Wait while your computer connects to the VPN for the first time.

Connecting with a Certificate for the First Time

If you connect with a certificate that you have not registered, you must enter a **Registration Key**. If you do not have the registration key, contact your administrator. If multiple certificates are registered for you, select one from the list.

For subsequent log-ins, you are automatically connected with the same certificate.

Connecting to the VPN

To connect to the VPN after you have connected successfully before:

1. Open the **Networks** menu.
2. Tap your site.
3. Click **Connect**.
4. Enter your credentials, as prompted.

Troubleshooting

For Users

If you cannot connect to the site or do not have the required authentication device or credentials, contact your administrator.

For administrators

Client logs contain the technical information related to user authentication and VPN connection.

To see logs on a client computer:

1. Search for **View Event Logs**.

   The **Event Viewer** opens.
2. Select **Applications and Services Logs** > **Microsoft** > **Windows** > **VPN Plugin Platform** > **Operational Verbose**.
3. Press and hold **Operational Verbose** to and select **Enable Logging**.

   The client logs open.

Windows 8.1 VPN Plugin for PC

In This Section:

Creating and Configuring the VPN Site

You can configure a VPN site for the Windows 8.1 Plugin in these ways:

- **PowerShell Script**

  Use the PowerShell script to push site configuration to users. See sk93638 https://supportcontent.checkpoint.com/solutions?id=sk93638.

- **Manual Configuration**

  Manually configure a site on each Windows 8.1 device.

- **Mobile Device Management**

  Use a Mobile Device Management Tool, such as Microsoft Intune to push site configuration to users.

These authentication methods are supported:

- Username and Password (Check Point or LDAP password defined on the gateway)
- Certificate (Use a certificate that is defined on the gateway)
- Smart Card
- RSA SecurID PinPad
- RSA SecurID KeyFob
- Challenge Response

Using the Plugin in Windows 8.1

This section contains detailed instructions for using the Check Point VPN Plugin on Windows 8.1.

We recommend that you give your users the information that applies to them.

Make sure that all users have:

- The credentials and/or devices necessary to authenticate
- The fingerprint of the site

In addition, if users will configure a site manually, make sure that they:

- Have the site name or IP address
- Know which authentication method to select

Downloading the Windows 8.1 Application

The Check Point VPN client in Windows 8.1 is called Check Point VPN Plugin and it is pre-installed in the operating system. No installation is necessary.

Manually Configuring a VPN Site

Create a VPN site on each Windows 8.1 device. This is the site that your device connects to access organizational resources.

To create a VPN site:

1. Open the Start menu and type **VPN**.
2. Tap **Manage Virtual Private Networks**.
3. Tap **Add a VPN connection**.
4. Enter the required information:
   a) **VPN provider** - Select **Check Point VPN**

   b) **Connection name** - Enter a display name for the connection. This is the name that shows on your device. For example, "Work."

   c) **Server name or address** - Enter the name or IP address of the site. For example, company_vpn.company.com or 192.0.2.1. Contact your administrator if you do not have this information.

   d) Optional: Select **Remember my sign-in information**. If selected, re-authentication is enabled and the password is cached for later logins.
5. Tap **Save**.

Connecting to a Site for the First Time

The first time that you connect to a site, you select the authentication method that you will use to sign in to the site. After you select the authentication method for a site, you cannot change it.

You are also asked to verify the fingerprint of the gateway. This means that the site you are connecting to is valid. The fingerprint is a string of random words. Compare the fingerprint that you see to the fingerprint that your administrator supplies. If they are the same, you know that the site is valid.

To connect to a VPN site for the first time:

1. Tap the Network icon in the taskbar notification area.
   The **Networks** menu opens.
2. Tap **Connections.**
3. Tap your site.
   If you created the site manually, the name of the site is the **Connection name** that you entered.
4. Tap **Connect**. If you do not see a Connect button, check your internet connection.
5. Select an **Authentication method**.
   If you do not know which method to select, contact your administrator.
6. Click **Next**.
7. Enter the required credentials.

8. A message says: **Check Point is connecting to site: xxx Which has this fingerprint:xxx. Click Next to continue.**

   Confirm that the fingerprint is correct and click **Next**.
9. Wait while your computer connects to the VPN for the first time.

Connecting with a Certificate for the First Time

If you connect with a certificate that you have not registered, you must enter a **Registration Key**. If you do not have the registration key, contact your administrator. If multiple certificates are registered for you, select one from the list.

For subsequent log-ins, you are automatically connected with the same certificate.

Connecting to the VPN

To connect to the VPN after you have connected successfully before:

1. Open the **Networks** menu.
2. Tap your site.
3. Click **Connect**.
4. Enter your credentials, as prompted.

Troubleshooting

For Users

If you cannot connect to the site or do not have the required authentication device or credentials, contact your administrator.

For administrators

Client logs contain the technical information related to user authentication and VPN connection.

To see logs on a client computer:

1. Search for **View Event Logs**.

   The **Event Viewer** opens.
2. Select **Applications and Services Logs** > **Microsoft** > **Windows** > **VPN Plugin Platform** > **Operational Verbose**.
3. Press and hold **Operational Verbose** to and select **Enable Logging**.

   The client logs open.

Capsule VPN for Windows Phone 10 and 8.1

In This Section:

Creating and Configuring the VPN Site

You can configure a VPN site for Capsule VPN in Windows 10 and Windows 8.1 in these ways:

- **Manual Configuration**

  Manually configure a site on each Windows 10 and Windows 8.1 device.

- **Mobile Device Management**

  Use a Mobile Device Management Tool, such as Microsoft Intune to push site configuration to users.

These authentication methods are supported:

- Username and Password (Check Point or LDAP password defined on the gateway)
- Certificate (Use a certificate that is defined on the gateway)
- RSA SecurID PinPad
- RSA SecurID KeyFob
- Challenge Response

Using the Client in Windows 10 and 8.1

This section contains detailed instructions for downloading, setting up, and using the Check Point VPN Application on Windows Phone 10 and 8.1.

We recommend that you give your users the information that applies to them.

Make sure that all users have:

- The credentials and/or devices necessary to authenticate
- The fingerprint of the site

In addition, if users will configure a site manually, make sure that they:

- Have the site name or IP address
- Know which authentication method to select

Downloading the Application

To download and install the application:

1. Tap the **Windows Store.**
2. Search the Windows Store for **Check Point Capsule VPN**.
3. Install the application.

Manually Configuring a VPN Site

Create a VPN site on your Windows Phone 10 and 8.1. This is the site that your device connects to access organizational resources.

To create a VPN site:

1. Tap **Settings** >**VPN**.
2. If the status is **Off**, slide the slider to **On**.
3. Tap **+**.
4. Enter the required information:
   a) **Server name or IP address** - Enter the name or IP address of the site. For example, company_vpn.company.com or 192.0.2.1. Contact your administrator if you do not have this information.
   b) **Type** - Select **Check Point Capsule VPN**.
   c) **Profile name** - Enter a display name for the connection. This is the name that shows on your device. For example, "Work."
5. Tap **Save**.

Connecting to a Site for the First Time

The first time that you connect to a site, you select the authentication method that you will use to sign in to the site. After you select the authentication method for a site, you cannot change it. Your administrator gives you the authentication method.

You are also asked to verify the fingerprint of the gateway. This means that the site you are connecting to is valid. The fingerprint is a string of random words. Compare the fingerprint that you see to the fingerprint that your administrator supplies. If they are the same, you know that the site is valid.

To connect to a VPN site for the first time:

1. Tap **Systems Settings** > **VPN**.
2. Tap your site.

   If you created the site manually, the name of the site is the **Profile name** that you entered.
3. Select an **Authentication method**.

   If you do not know which method to select, contact your administrator.
4. Click **Next**.
5. Enter the required credentials.

6. A message says: **Check Point is connecting to site: xxx Which has this fingerprint:xxx. Click Next to continue.**

   Confirm that the fingerprint is correct and click **Next**.
7. Wait while your computer connects to the VPN for the first time.

Connecting with a Certificate for the First Time

If you connect with a certificate that you have not registered, you must enter a **Registration Key**. If you do not have the registration key, contact your administrator. If multiple certificates are registered for you, select one from the list.

For subsequent log-ins, you are automatically connected with the same certificate.

Connecting to the VPN

To connect to the VPN after you have connected successfully before:

1. Tap **System Settings** > **VPN**.
2. Tap your site.
3. Enter your credentials, if prompted.

Setting Up Quick Action to Connect to VPN

Optionally, you can set up a Quick Action to quickly connect to the VPN.

To set up a Quick Action to connect to the VPN:

1. Tap **Settings > notifications + actions.**
2. Below **Choose your quick actions**, tap one of the icons.
3. Tap **VPN**.

You can now connect and disconnect from the VPN from the notifications center.