



User Guide
Revision A

McAfee Next Generation Firewall 5.9.0

McAfee VPN Client for Windows

Contents

- ▶ *Introduction*
- ▶ *Installing and upgrading*
- ▶ *Using the right-click menu*
- ▶ *Connecting to a new gateway*
- ▶ *Connecting and authenticating*
- ▶ *Managing certificates*
- ▶ *Monitoring VPN connections*
- ▶ *Change VPN Client settings*
- ▶ *Close the VPN connection*
- ▶ *Disable the VPN Client*
- ▶ *Troubleshooting VPN connections*

Introduction

This guide provides end-user instructions for installing and using McAfee® VPN Client (VPN Client). VPN Client is a software application that runs on your computer. The client allows you to connect to your organization's network from anywhere. Using a virtual private network (VPN) establishes a secure, encrypted connection that protects the information you transfer.

Installing and upgrading

The VPN Client can be added as a new installation or as an upgrade.

Tasks

- [Install the VPN Client on page 2](#)
Your administrator provides the installation file.
- [Upgrade the VPN Client on page 2](#)
You can upgrade an existing VPN Client installation.

Install the VPN Client

Your administrator provides the installation file.

Before you begin

Check with your administrator about the installation process. Your administrator might be using a standard installation file or a preconfigured file.

Task

- 1 Double-click the installation executable file.
The **McAfee VPN Client Setup** window opens.
- 2 Click **Install**.
The **McAfee VPN Client Setup** wizard opens.
- 3 Click **Next** and follow the on-screen prompts.



You might see one or more confirmation requests during the installation. Allow the installation of all drivers and components.

When the installation is complete, connect to a new gateway to start using the VPN Client.

See also

[Connecting to a new gateway on page 3](#)

Upgrade the VPN Client

You can upgrade an existing VPN Client installation.

Task

- 1 Double-click the executable file.



Your network administrator supplies this file.

A confirmation message appears.

- 2 Click **Yes**.
The **Welcome** screen for the installation wizard opens.
- 3 Click **Next** to start the upgrade.
During the upgrade process, the earlier version of the VPN Client is removed and replaced with the current version using the same settings.
- 4 Accept the License Agreement and click **Next** to continue.
- 5 When the upgrade is finished, click **Finish** to close the wizard.

Using the right-click menu

You have access to several commands and properties in the right-click menu of the McAfee VPN Client icon.

The color of the VPN Client icon changes according to the status of the VPN Client. The available menu commands change with the status of the VPN connection.



View the status as text by holding the cursor over the VPN Client icon.

Table 3-1 VPN Client right-click menu

Option	Definition
Properties	More actions and status information.
Connect to New Gateway	Adds a gateway.
Select Gateway	Select where you want to connect.
Connect	Use Connect/Disconnect to open and close a VPN.
Connect to End-Point	Select endpoint if the gateway has several endpoints.
Reauthenticate	Reauthenticate when convenient (instead of waiting for the authentication timeout).
Disable VPN	Disconnect the VPN and turn off the automatic VPN connection trigger.
Exit	Exit the VPN Client.

More information and commands are available in the **McAfee VPN Client Properties** dialog box that opens through the right-click menu or by double-clicking the VPN Client icon.

See also

[Monitoring VPN connections on page 16](#)

Connecting to a new gateway

VPN Client connects to a *gateway*, a device within your organization's network that is integrated with the rest of the network. Connecting to a gateway for the first time requires a different process than subsequent connections.

Before you begin

If the gateway requires certificate authentication, you cannot connect to the gateway until you have a valid certificate. Your administrator should inform you if you must obtain a certificate.

The VPN connection requires identity verification in two directions, known as *mutual authentication*.

- **Certificate fingerprint** — The first time the VPN Client connects to a gateway, the identity of the gateway is verified to the VPN Client with the certificate fingerprint.
- **User authentication** — User identity is authenticated each time you connect to a gateway.



Your administrator will advise what to use in your environment.

After the installation, you cannot connect to gateways and endpoints until they are configured in the VPN Client. The administrator might have preconfigured the gateways for you so that you can connect to them by selecting them in a list. Alternatively, the administrator might have you manually connect

with the gateway, either in a file or as an address that you can contact. If the VPN Client is configured to allow domain logon through the Windows logon screen, only gateways you have connected to at least once are available.

Depending on your situation, select the correct starting point:

- If you are unsure that the gateway that you want to connect to is configured, see *Check the list of available gateways*.
- If you know the gateway that you want to connect to is configured, see *Connect to a preconfigured gateway*.
- If you know that the gateway information is not yet configured, see *Add a gateway manually*.

Tasks

- *Check the list of available gateways on page 4*
View the gateways that are already configured.
- *Connect to a preconfigured gateway on page 4*
The administrator might have configured a gateway for you in the installation package.
- *Add a gateway manually on page 5*
If you have not previously connected to the gateway and it has not been preconfigured for you, you can add it manually.
- *Check the gateway certificate fingerprint on page 7*
When you connect to a new gateway for the first time, you must verify its identity.

See also

Managing certificates on page 10

Check the list of available gateways

View the gateways that are already configured.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Gateways** tab. All configured gateways are listed in the table.

Connect to a preconfigured gateway

The administrator might have configured a gateway for you in the installation package.



The administrator should inform you if you need a certificate. If the gateway requires certificate authentication, you must have a valid certificate to connect to the gateway.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box and select one of the following from the menu:
 - **No preconfigured gateways yet** — Select **Connect to New Gateway** directly at the main level.
 - **Preconfigured gateway available** — Select **Select Gateway | Connect to New Gateway**.
- 2 Make sure that **Preconfigured Gateway** is selected.



If the setting is disabled, add any new gateways manually.

- 3 Select the preconfigured gateway.

4 (Optional) Select the endpoint to connect to.



Endpoints usually correspond to different Internet connections at the office.

5 Select whether authentication is based on a manually entered user name and password or on the user certificate.

Your administrator informs you what to select.

6 For IPsec connections, click **Advanced** to define the settings.



Do not change the Advanced settings unless your network administrator specifically instructs you to.

Option	Definition
Use TCP Tunneling to Port	If TCP tunneling is enabled for the selected endpoint and the initial connection to the gateway is through a TCP tunnel, use these settings: <ul style="list-style-type: none">• Use TCP Tunneling to Port• Enter the number of the port defined for TCP tunneling on the endpoint.
Use Limited Cryptography	Select this option only if your organization prohibits the use of strong cryptographic methods.
Trust CAs in Microsoft Certificate Store	Select this option to use the Microsoft Certificate Store on the client computer. The certificate sent by the VPN gateway is verified against the certificate authority (CA) certificates in the Microsoft Certificate Store. The client connects to the VPN gateway only if a matching certificate is found in the store.
Gateway Authentication (User Name Authentication only)	Select the signature type that matches the gateway certificate.

7 Click **OK**. The **User Authentication** dialog box opens.

See also

[Check the gateway certificate fingerprint on page 7](#)

[Managing certificates on page 10](#)

[Select the authentication method on page 9](#)

Add a gateway manually

If you have not previously connected to the gateway and it has not been preconfigured for you, you can add it manually.

Before you begin

To manually connect to a gateway, you need the following information from your network administrator:

- An address for each gateway that you connect to
- Information about which credentials to use for authentication


- The gateway certificate fingerprint that allows you to verify the gateway identity
- A valid certificate to connect to the gateway (provided by the administrator if certificate authentication is required)

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box and select one of the following from the menu:
 - **No preconfigured gateways yet** — Select **Connect to New Gateway** directly at the main level.
 - **Preconfigured gateway available** — Select **Select Gateway | Connect to New Gateway**.
- 2 Select **New Gateway**.
If there are no preconfigured gateways that have not been contacted, the new gateway setting is selected by default.
- 3 In the **Host Name** field, enter the gateway address.
- 4 *For SSL connections*, click **SSL port** and enter the port number.
Your administrator informs you what to select.
- 5 Select whether authentication is based on a manually entered user name and password or on the user certificate.
Your administrator informs you what to select.
- 6 *For IPsec connections*, click **Advanced** to define the settings.



Do not change the Advanced settings unless your network administrator specifically instructs you to.

Option	Definition
Use TCP Tunneling to Port	If TCP tunneling is enabled for the selected endpoint and the initial connection to the gateway is through a TCP tunnel, use these settings: <ul style="list-style-type: none"> • Use TCP Tunneling to Port • Enter the number of the port defined for TCP tunneling on the endpoint
Use Limited Cryptography	 Select this option only if your organization prohibits the use of strong cryptographic methods.
Trust CAs in Microsoft Certificate Store	Select this option to use the Microsoft Certificate Store on the client computer. The certificate sent by the VPN gateway is verified against the CA certificates in the Microsoft Certificate Store. The client connects to the VPN gateway only if a matching certificate is found in the store.
Gateway Authentication <i>(User Name Authentication only)</i>	Select the signature type that matches the gateway certificate.

- 7 Click **OK**.
- 8 *For certificate authentication*, enter the passphrase defined for the certificate. The **New Gateway** dialog box opens. You are prompted to verify the identity of the gateway by checking its certificate fingerprint.

See also

[Managing certificates on page 10](#)

Check the gateway certificate fingerprint

When you connect to a new gateway for the first time, you must verify its identity.

The certificate fingerprint is an important security feature that ensures confidential communication. A fingerprint that does not match might indicate a malicious attempt to spy on your communications.

Task

- 1 Check the entries in the **Subject Name** and the **Certificate Fingerprint** fields against the information the administrator has provided.

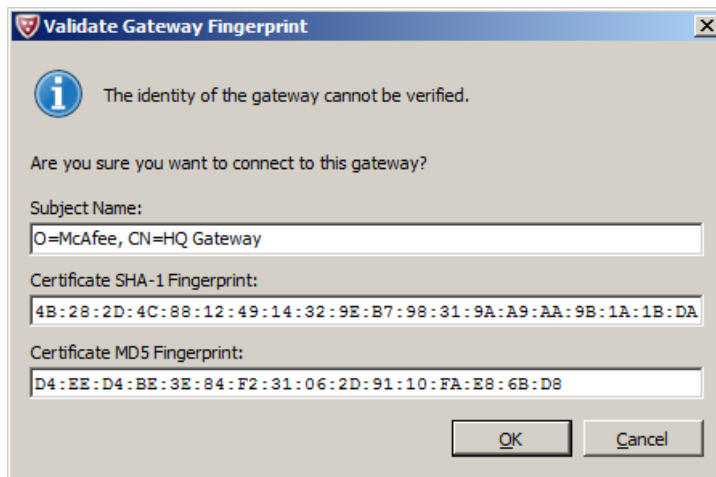


Figure 4-1 Validate Gateway Fingerprint dialog box

- 2 Proceed according to the result of the comparison:
 - **Values do not match** — Click **Cancel** and contact the administrator.
 - **Values match** — Click **OK**.



If the gateway certificate changes, you might have to recheck the certificate fingerprint. If a recheck is necessary, your administrator will inform you and provide you with the information for checking the new certificate fingerprint.

See also

[Select the authentication method on page 9](#)

Connecting and authenticating

There are several ways to establish a VPN connection and authenticate to a gateway.

- **Connection methods**
 - **Domain logon** — You might be able to log on to the VPN on the Windows logon screen. This way, the computer can connect all internal network resources, such as network drives, immediately when it starts.
 - **Manual connection** — You can manually connect your VPN Client to a gateway.
 - **Change endpoint** — You can select which endpoint connection the gateway uses.

- **Authentication methods** — However you connect, when you are outside the office, the VPN Client automatically prompts you to authenticate when you access a service or application that requires a VPN. You can authenticate yourself with either user name and password, a certificate, or a smart card. Usually, the administrator selects a single method that you can use. In some cases, you can select from alternative methods. As a further security measure, your authentication is valid for a specific period; after that, you must reauthenticate. Reauthentication might also be required if the VPN connection is lost due to network problems.

Tasks

- [Connect to a gateway from a Windows logon on page 8](#)
If domain logon is enabled, you can open the VPN connection at the Windows logon screen.
- [Connect to a gateway manually on page 9](#)
You can select the gateway that the VPN Client connects to.
- [Switch to an alternative endpoint on page 9](#)
Some gateways can be reached through several endpoints. These endpoints usually correspond to different Internet connections at the office you are connecting to.
- [Select the authentication method on page 9](#)
A gateway might allow you to select how you want to authenticate.

Connect to a gateway from a Windows logon

If domain logon is enabled, you can open the VPN connection at the Windows logon screen.

Using the domain logon gives you automatic connections to network drives and other resources in your organization. The domain logon is helpful to avoid error messages and delays that can sometimes occur if resources are not available.

- You can use the logon screen to access gateways that you have used previously.
- This feature is not available in Windows XP.

Task

- 1 On the Windows logon screen, select **Switch User**.
Icons are displayed for all configured user accounts and previously contacted VPN gateways.
- 2 Select the gateway that you want to connect to.
The logon screen for that gateway is displayed.
 - If you do not see any VPN gateways even though you have successfully connected to a gateway previously, this feature is most likely deactivated in your installation.
 - If a VPN connection is already active, you can deactivate it here.
- 3 For user name and password authentication, make a selection for the **Use same credentials to log on to** setting:
 - Credentials valid for both Windows and VPN Client — Select the option.
 - Different credentials — Deselect the option to avoid a Windows logon failure.
- 4 Enter your credentials for the VPN connection.
The VPN is established.
Depending on the authentication method and the options selected, you either need to log on to Windows or you are automatically logged in.

After logging on to Windows, the VPN connection is active. When the Windows desktop loads, you can use resources through the VPN.

See also

[Connecting to a new gateway on page 3](#)

[Select the authentication method on page 9](#)

[Activate or deactivate domain logon on page 18](#)

[Close the VPN connection on page 19](#)

[Monitoring VPN connections on page 16](#)

Connect to a gateway manually

You can select the gateway that the VPN Client connects to.

- **Connect to a gateway that is not listed** — If you want to connect to a gateway that is not yet listed, you must add the gateway as described in *Add a new gateway*.
- **Connect to the gateway the VPN Client contacted** — From the VPN Client right-click menu, select **Connect** and enter your credentials.
- **Connect to a different gateway than the last gateway used** — From the VPN Client right-click menu, select **Select Gateway** and then select the gateway from the submenu. Enter your credentials to connect. The gateway is stored as your default connection.

See also

[Connecting to a new gateway on page 3](#)

[Select the authentication method on page 9](#)

Switch to an alternative endpoint

Some gateways can be reached through several endpoints. These endpoints usually correspond to different Internet connections at the office you are connecting to.

Selecting a different endpoint might be useful when one of the Internet connections at the office you are connecting to is experiencing technical difficulties.

Task

- 1 In the Windows taskbar, right-click the VPN Client icon and select the correct endpoint from the **Connect to End-Point** submenu.
- 2 Enter your credentials for the VPN connection.

The VPN is established and the endpoint you selected is stored as your default connection.

Select the authentication method

A gateway might allow you to select how you want to authenticate.

If you authenticate to a gateway with a user name and a password, the VPN Client prompts you to reauthenticate periodically. If a certificate or a smart card is used, reauthentication is automatic.




All gateways might not accept all authentication methods.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Gateways** tab. All configured gateways are listed in the table.
- 3 Right-click the gateway for which you want to select the authentication method and select **Authentication | Username** or **Authentication | Certificate | <name used in certificate>**.

Table 5-1 Authentication methods

Method	Explanation
User name and password	<p>The user name and password authentication dialog box appears for any method that requires you to enter your user name manually.</p> <p>The password you enter can be fixed or, for example, a code generated by a physical security token that you carry with you. The network administrator provides you the necessary details for logging on.</p> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px;"> You cannot change your password through the VPN Client. Contact the network administrator if you need information for changing the password.</div>
Certificate	<p>Certificates electronically identify a user or device, proving that they are who or what they claim to be. This verification is completed using public/private key pairs and digital signatures. A CA grants and verifies digital certificates.</p> <p>The certificate is protected with a passphrase that you or your administrator defined.</p> <p>If you have certificates that can be used for authentication in the Microsoft Certificates Store on your local computer, those certificates are also listed.</p>
Smart card	<p>If you have a smart card, the VPN Client uses the smart card software installed on your computer to prompt you for your passphrase when authentication is needed.</p> <p>The dialog box you see depends on the smart card software installed on your computer. The certificates stored on smart cards are included on the list of available certificates when you select the method for authenticating to a gateway.</p>

The selected authentication method is used the next time you authenticate yourself.

Managing certificates

If you use certificates imported through the VPN Client, you can manage the imported certificates directly in the VPN Client.

- The signed certificates that you have imported are listed on the **Certificates** tab.
- Certificates stored on smart cards or in the Microsoft Certificates Store on the local computer are not listed on the **Certificates** tab. They are included on the list of available certificates when you select the authentication method for connecting to a gateway. You cannot otherwise manage these certificates in the VPN Client.

Tasks

- [Use internal certificates on page 11](#)
The administrator might require that VPN connections use a client certificate.
- [Use external certificates on page 13](#)
There are three ways to use previously generated external certificates with the VPN Client.
- [Change the certificate passphrase on page 14](#)
You must enter a passphrase every time the VPN Client asks you to authenticate yourself using this certificate. You can change the passphrase of a certificate that you have imported through the VPN Client.
- [View user certificate details on page 15](#)
To learn more about a user certificate, you can access the Microsoft Certificates Store on your computer and the issuer certificate in the Trusted Root Certification Store.
- [Change the certificate user ID type on page 15](#)
Several user IDs can be available for each imported certificate. The options available depend on which types of information are included in the certificate.
- [Delete certificates on page 15](#)
Sometimes, an imported certificate might become unnecessary. In such cases, you can delete the obsolete certificate through the VPN Client.

See also

[Select the authentication method on page 9](#)

Use internal certificates

The administrator might require that VPN connections use a client certificate.

There are two stages to the internal certificate process. You create a certificate request and send it to your network administrator to be signed. After being signed by the CA, the certificate must be imported into the VPN Client.

If the client certificate on your computer or the CA that signed the client certificate has expired, repeat the same process to renew the certificate.

Tasks

- [Create a basic certificate request on page 11](#)
You can create a basic certificate request for an internal certificate in the VPN Client.
- [Import a signed certificate on page 12](#)
A signed certificate must be imported into the VPN Client.

Create a basic certificate request

You can create a basic certificate request for an internal certificate in the VPN Client.

If the administrator informs you that you must create an advanced certificate request for an internal certificate, see the *McAfee VPN Client Product Guide* for instructions.

Task

- 1 Start the **Certificate Request Wizard**.
 - a In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
 - b Click the **Certificates** tab.
 - c Click **Create Certificate Request**.

2 Verify that **Basic Mode** is selected and click **Next**.

3 In the **User Name** field, enter the user name.

The user name must correspond to what is defined on the gateway.



Contact the administrator if you are unsure what to enter as the user name.

4 In the **Passphrase** field, enter and confirm a passphrase to use whenever you authenticate yourself using the certificate.

You can select this passphrase yourself. It must meet these requirements:

- Be at least eight characters long
- Contain a combination of numbers, letters, and special characters



Secure passphrases are never based on personal information such as names, birthdays, ID numbers, or phone numbers.

5 Click **Create**. You are prompted to save the certificate request.

6 Click **Save**. A file save dialog box opens.

7 Save and send the file to your administrator.

- a Browse to the correct folder, enter a file name, and click **Save**. Make sure that **Certificate Requests (*.csr)** is selected as the file type.
- b (Optional) Click **Launch Default Windows E-Mail Application** to create a message in your default email application.
- c Send the certificate request .csr file that you saved to your network administrator for signing.

8 Click **Finish** to close the wizard.

When you receive the signed internal certificate, import it as described in *Import a signed certificate*.

Import a signed certificate

A signed certificate must be imported into the VPN Client.



The administrator signs your certificate request for an internal certificate and sends it back to you.

Task

1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.

2 Click the **Certificates** tab.

3 Click **Import Certificate**.

4 Verify that **Internal Certificate** is selected and click **Next**.

5 Click **Select**.

A Windows file browser opens.

6 Browse to the correct folder, select the signed certificate, and click **Open**.

7 Click **Finish** to close the wizard.

The certificate is now listed on the **Certificates** tab. The **Certificates** tab displays, among other information, the expiration date of the certificate.

Use external certificates

There are three ways to use previously generated external certificates with the VPN Client.

You can use:

- An external certificate stored on a smart card
- A certificate stored in the Microsoft Certificates Store on your local computer
- An imported certificate in the VPN Client

You can either import the external certificate and its private key as a single PKCS # 12 file or as two separate files. Follow the instructions if the administrator informs you that you must import an external certificate in the VPN Client.

Tasks

- [Import a PKCS #12 file on page 13](#)
Import the file containing the certificate and the private key.
- [Import separate certificate and private key files on page 14](#)
If there is an existing external certificate and private key files that you want to use for authentication, you can import them into the VPN Client.

Import a PKCS #12 file

Import the file containing the certificate and the private key.

Task

- 1 Open the **Import Certificate Wizard**.
 - a In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
 - b Click the **Certificates** tab.
 - c Click **Import Certificate**.
- 2 Select **External Certificate**.
- 3 Select **PKCS # 12 File** and click **Next**.
- 4 Click **Browse** and select the PKCS #12 file to import.
- 5 In the **PKCS #12 Password** field, enter the PKCS #12 password for the certificate file.
- 6 In the **Passphrase** field, enter and confirm a passphrase to use whenever you authenticate yourself using the certificate.

You can select this passphrase yourself. It must meet these requirements:

 - Be at least eight characters long
 - Contain a combination of numbers, letters, and special characters



Secure passphrases are never based on personal information such as names, birthdays, ID numbers, or phone numbers.

- 7 Click **Next | Finish**.

The signed certificate is now listed on the **Certificates** tab. The **Certificates** tab displays, among other information, the expiration date of the certificate.

Import separate certificate and private key files

If there is an existing external certificate and private key files that you want to use for authentication, you can import them into the VPN Client.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Certificates** tab.
- 3 Click **Import Certificate**. The **Import Certificate Wizard** opens.
- 4 Select **External Certificate**.
- 5 Select **Separate Certificate and Private Key Files** and click **Next**.
- 6 Click **Browse** to select the certificate file and private key file to import.
- 7 Click **Next | Finish**.

The certificate is now listed on the **Certificates** tab. The **Certificates** tab displays, among other information, the expiration date of the certificate.

Change the certificate passphrase

You must enter a passphrase every time the VPN Client asks you to authenticate yourself using this certificate. You can change the passphrase of a certificate that you have imported through the VPN Client.

You can select this passphrase yourself. It must meet these requirements:

- Be at least eight characters long
- Contain a combination of numbers, letters, and special characters



Secure passphrases are never based on personal information such as names, birthdays, ID numbers, or phone numbers.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Certificates** tab.
- 3 Right-click the certificate and select **Change Key Passphrase**.
The **Change Key Passphrase** dialog box opens.
- 4 Enter the current passphrase and the new passphrase in both fields provided, and click **OK**.



If you leave the new passphrase fields empty, the private key of the certificate is not encrypted. For security reasons, it is highly recommended that you enter a passphrase.

View user certificate details

To learn more about a user certificate, you can access the Microsoft Certificates Store on your computer and the issuer certificate in the Trusted Root Certification Store.

Although the **Windows Certificate** dialog box provides tools for installing the user certificate, installing the user certificate is not necessary for the operation of the VPN Client.



This operating system dialog box is not part of the McAfee VPN Client. If you want more instructions for it, press **F1** to view the context-specific Windows help for this dialog box.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Certificates** tab.
- 3 Right-click the certificate and select **Details of User Certificate** or **Details of Issuer Certificate**.
The **Windows Certificate** dialog box opens.

The **General**, **Details**, and **Certification Path** tabs provide detailed information about the certificate.

Change the certificate user ID type

Several user IDs can be available for each imported certificate. The options available depend on which types of information are included in the certificate.



The administrator has defined your user ID and its type. Do not change the user ID type unless the network administrator specifically instructs you to do so.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Certificates** tab.
- 3 Right-click the certificate that you want to change and select one of these options:
 - **Certificate ID to Use | E-mail**
 - **Certificate ID to Use | Subject Name**
 - **Certificate ID to Use | DNS Name**
 - **Certificate ID to Use | IP Address.**

Delete certificates

Sometimes, an imported certificate might become unnecessary. In such cases, you can delete the obsolete certificate through the VPN Client.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Certificates** tab.

- 3 Right-click the certificate and select **Delete Certificate**.
A confirmation dialog box appears.
- 4 Click **Yes** to permanently delete the certificate.






Monitoring VPN connections

You can manage and monitor active VPN connections.

VPN connection status

The color of the VPN Client icon shows the connection status. More details are available in the **McAfee VPN Client Properties** dialog box.

Table 7-1 VPN Client status icons

Icon	Status
	VPN is disabled
	No VPN connection
	VPN established
	Connectivity problems
	VPN error

You can manage and monitor the VPN connections on the **Status** tab.

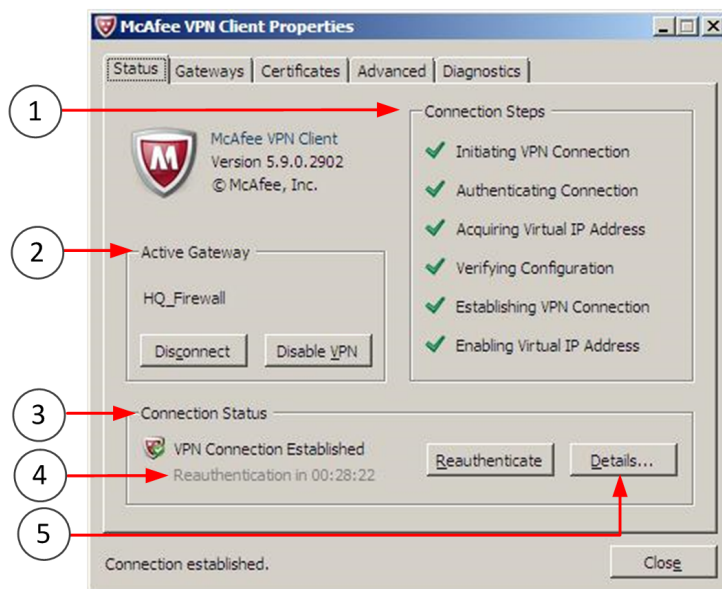


Figure 7-1 VPN Client Properties dialog box

- 1 Progress of establishing a VPN connection.
- 2 Name of the currently selected gateway.
- 3 Status information.
- 4 Reauthentication is required at regular intervals. The timer shows how long it takes until the authentication dialog box automatically opens again.
- 5 Details of the active VPN connection.

View active VPN connection details

Detailed information on the established VPN connection is available. This information is useful for advanced users and administrators. Interpreting the details requires knowledge about IPsec standards.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click **Details**. The **VPN Details** dialog box opens.
- 3 Check the settings used in the currently active VPN connection.
IPsec-related terms are used as follows:
 - **IKE** — Settings for negotiation phase 1
 - **IPsec** — Settings for negotiation phase 2
- 4 Click **Close** when you are finished.

View the configuration downloaded from a gateway

When you connect to a gateway, the VPN Client checks if there are previously downloaded settings from the gateway in question, and whether such settings are up to date. If necessary, a new configuration is downloaded, replacing the old configuration.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Gateways** tab.
- 3 Right-click a gateway to which you have previously connected and select **View Gateway Configuration**. The settings that the client has downloaded from that gateway are displayed in a new dialog box.
- 4 Click **Close** when you are finished.

Change VPN Client settings

Your administrator might advise you to make some changes to your VPN Client to improve performance.

Tasks

- [Activate or deactivate user name memory on page 18](#)
By default, the VPN Client remembers up to five most recently used user names. These stored user names prevent the need to type frequently used user names each time you authenticate.
- [Activate or deactivate domain logon on page 18](#)
Domain logon allows you to open the VPN connection directly on the Windows logon screen before you log on to Windows
- [Activate or deactivate random local VPN ports on page 19](#)
For IPsec connections, you can configure the VPN Client to select random local VPN ports when opening a VPN connection.
- [Activate or deactivate retry options on page 19](#)
Some locations might require different connection settings than you used previously.

Activate or deactivate user name memory

By default, the VPN Client remembers up to five most recently used user names. These stored user names prevent the need to type frequently used user names each time you authenticate.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Advanced** tab.
- 3 Select or deselect **Remember User Names**.
- 4 Click **Apply**.
- 5 Click **Close**.

Activate or deactivate domain logon

Domain logon allows you to open the VPN connection directly on the Windows logon screen before you log on to Windows

Using the domain logon allows network drives and other resources to be connected when you log on to Windows. The domain logon is helpful to avoid error messages and delays that can sometimes occur if resources are not available.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Advanced** tab.
- 3 Select or deselect **Enable Secure Domain Logon**.
- 4 Click **Apply**.
- 5 Click **Close**.

By default, all Gateways you have contacted at least once are listed at Windows Logon when the domain logon feature is enabled. You can remove gateways from the logon screen by manually disabling the secure domain logon feature. Disable it through each gateway right-click menu on the **Gateways** tab of the **McAfee VPN Client Properties** dialog box.

See also

[Connect to a gateway from a Windows logon on page 8](#)

Activate or deactivate random local VPN ports

For IPsec connections, you can configure the VPN Client to select random local VPN ports when opening a VPN connection.



By default, the VPN Client uses local ports 500 and 4500 for VPN connections.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Advanced** tab.
- 3 Select or deselect **Use Random Local VPN Connection Ports**.
- 4 Click **Apply**.
- 5 Click **Close**.

Activate or deactivate retry options

Some locations might require different connection settings than you used previously.

By default, the VPN Client has an automatic retry setting to help with some connection issues.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Advanced** tab.
- 3 Select or deselect **Reconnect using different options after timeout**.
- 4 Click **Apply**.
- 5 Click **Close**.

Close the VPN connection

There is usually no need to close the VPN connection when you stop using it. An unused connection automatically times out after a while.

You can disconnect an active VPN connection manually at any time in the following ways:

- **Windows taskbar** — Select **Disconnect** from the right-click menu for the VPN Client icon in the Windows taskbar.
- **McAfee VPN Client Properties dialog box** — Click **Disconnect** on the **Status** tab.
- **Active gateway selection** — Right-click the active gateway on the **Gateways** tab and select **Disconnect** from the menu that opens.
- **Windows user switch screen** — Click **Disconnect** in the Windows user switch screen.

Selecting one of the methods changes the VPN status to **No VPN connection**. With any request that requires a VPN, an authentication prompt appears; to avoid the prompt, turn off the VPN Client.

See also

Connect to a gateway from a Windows logon on page 8

Disable the VPN Client

If necessary, you can disable the VPN Client so that it does not prompt you for authentication automatically.

Task

- Turning off the prompt can be done in one of the following ways:
 - Right-click the VPN Client icon in the Windows taskbar and select **Disable VPN**.
 - Click **Disable VPN** on the **Status** tab in the **McAfee VPN Client Properties** dialog box.
 - When the authentication prompt is automatically displayed, click the gray icon in the **User Authentication** dialog box to disable the VPN.

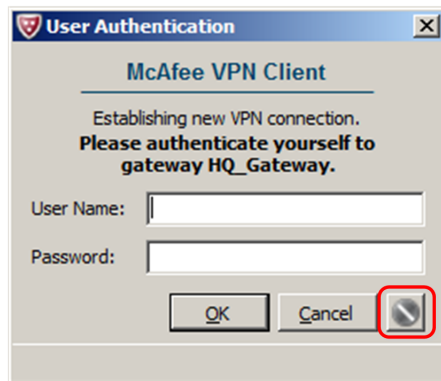


Figure 10-1 VPN Client disable button

When you disable the VPN Client, the status of the VPN changes to **No VPN connection (VPN Disabled)**. You can connect the VPN manually following the usual procedure without specifically re-enabling the VPN Client. You are not able to use any resource through the VPN before you connect manually.

See also

Connecting and authenticating on page 7

Troubleshooting VPN connections

If you are having problems with your VPN connections, consider these options for resolving the issue.

Solving connectivity issues

You can resolve some connectivity issues by adjusting different VPN settings.

Using different connection settings

Some connectivity problems can be solved by configuring the VPN Client to automatically try different combinations of retry settings.

The automatic retry setting is useful in dealing with network connections that severely restrict the allowed communications. In such situations, you can browse the Internet outside the VPN connection, but the VPN Client is unable to connect to the VPN gateway. The retry option is on the **Advanced** tab in **McAfee VPN Client Properties** dialog box.

See also

[Activate or deactivate retry options on page 19](#)

Enabling random ports

VPN connections might fail because the default local ports that the VPN Client uses for VPN connections, ports 500 and 4500, cannot be used in your environment.

You can configure the VPN Client to select random local VPN ports when opening a VPN connection.

See also

[Activate or deactivate random local VPN ports on page 19](#)

The Connectivity Problems dialog box

If network connectivity problems occur when the VPN Client has already established a connection to a gateway, the **Connectivity Problems** dialog box might appear.

The table lists the options available.

Table 11-1 Connectivity Troubleshooting options

Option	Definition
Switch to the next endpoint of the gateway	If the gateway has several endpoints, the VPN Client tries to establish a VPN connection by switching to the next endpoint. This action helps if there are several Internet connections at the office you are connecting to and the link you were using is down.
Reconnect to the endpoint	The VPN Client tries to establish a new connection to the currently selected endpoint. This action helps if your connection to the gateway was cut because of a temporary problem at any point along the communications path.
Continue with the current endpoint as usual	The VPN Client waits for the already-established connection to the current endpoint to become available. This action helps particularly with network problems related to your local environment, for example, if the network cable is removed and reinserted.

If the VPN Client fails to establish a connection according to the selected option, wait until network connections become available again, then try to connect to the gateway manually.

See also

[Connecting and authenticating on page 7](#)

Change the VPN Client MTU

If you experience network problems, you can adjust the maximum transmission unit (MTU) size for your VPN Client installation.

Large chunks of data that you send over networks are broken down into several smaller units, called *packets*, for transfer. The MTU defines how large the packets can be. A larger MTU is more efficient, but the packet size might have to be reduced if the packets are sent through a network or device that cannot handle large packets.



Do not change the VPN Client MTU unless your administrator tells you to.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Advanced** tab.
- 3 Select the correct **MTU** from the list or type in the correct value according to the information you have received from the administrator.
- 4 Click **Apply** and **Close**.
- 5 Restart the computer.

Change the VPN Client MAC address

If you experience networking problems, you can adjust the MAC address of your VPN Client. Changing the MAC address requires Windows administrator rights.

A media access control address (MAC address) is a unique identifier assigned to the VPN Client for communications on the network. Changing the MAC address affects the virtual IP address the VPN Client gets when connecting to the gateway.



Do not make this change unless your administrator tells you to.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Advanced** tab.
- 3 Click **Select MAC Address**.
The **MAC Address for Virtual IP Address** dialog box opens.
Windows might display a security dialog box before the **MAC Address for Virtual IP Address** dialog box opens.
- 4 Select the correct value and click **Apply**.



Your administrator provides the information.

- 5 Click **Close**.
- 6 Click **Apply** and **Close** in the **McAfee VPN Client Properties** dialog box.

Collect diagnostic information

Diagnostics collect all the relevant information on how the VPN Client operates, including logs, network interface status, routes, and active connections.

The diagnostics are collected in a single archive for easy transfer. The file does not contain secret information such as passwords, but it does contain information related to the VPN configuration such as internal IP addresses. Depending on your operating environment, the file might need to be handled securely.

If you are experiencing connection problems with the VPN Client, the administrator might ask you to collect and send in a file containing diagnostics information about your installation. Diagnostics information is meant for administrators.

Task

- 1 In the Windows taskbar, double-click the VPN Client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Diagnostics** tab.
- 3 Click **Collect Diagnostics**.
The **Collect Diagnostics** dialog box opens and displays the progress of the data collection. You might see an additional dialog box open when system information is gathered.
- 4 When the data collection finishes, click **Save Diagnostics**.
- 5 Browse to the location where you want to save the file, enter a file name, and click **Save**.

Capture network traffic

From the VPN Client, you can record the network traffic of the local computer during a problem situation to help with troubleshooting.

The administrator might ask for the traffic capture files. Alternatively, the administrator might capture local network traffic through your VPN Client. The traffic recordings are saved on the local computer in the traffic dump files adapter.pcap and protocol.pcap in the specified folder.

Task

- 1 In the Windows taskbar, double-click the VPN client icon to open the **McAfee VPN Client Properties** dialog box.
- 2 Click the **Diagnostics** tab.
- 3 Click **Capture Traffic**.
The **Capture Traffic** dialog box opens.
- 4 (Optional) Click **Browse** and browse to the folder where you want to save the traffic capture files.
- 5 Click **Start Capture**.
The traffic capture begins.
- 6 Click **Stop Capture** when all traffic related to the problem has been recorded.
- 7 Click **Close** to close the **Capture Traffic** dialog box.

Copyright © 2015 McAfee, Inc. www.intelsecurity.com

Intel and the Intel logo are trademarks/registered trademarks of Intel Corporation. McAfee and the McAfee logo are trademarks/registered trademarks of McAfee, Inc. Other names and brands may be claimed as the property of others.

A00

