Product Guide

Revision A

McAfee Next Generation Firewall 5.9.0

McAfee VPN Client for Windows

COPYRIGHT

Copyright © 2015 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

TRADEMARK ATTRIBUTIONS

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface 5

About this guide . . . 5

Audience . . . 5

Conventions . . . 5

Find product documentation . . . 6

1 Introduction 7

How the VPN Client works . . . 7

VPN Client configuration and updates . . . 7

Virtual IP addressing . . . 8

How connection settings work . . . 8

2 Deployment 9

Deployment options . . . 9

VPN Client types . . . 9

Installation types . . . 9

User authentication . . . 10

Deployment checklist . . . 11

3 Installing and upgrading the VPN Client 13

Installation overview . . . 13

Download the installation file . . . 14

Install with the wizard . . . 14

Install using a custom installation package . . . 15

Save the gateway contact information to a file . . . 15

Install with a transform file . . . 16

Upgrade the VPN Client . . . 17

4 Configuring certificates 19

Authenticating with client certificates . . . 19

Supported certificate authentication schemes . . . 19

User identities . . . 20

Authenticating with internal certificates . . . 20

Create a basic certificate request . . . 21

Create an advanced certificate request . . . 21

Obtain signed certificates . . . 22

Import a signed certificate . . . 22

Authenticating with external certificates . . . 23

Import a PKCS #12 file . . . 23

Import separate certificate and private key files . . . 24

Change the certificate passphrase . . . 24

View user certificate details . . . 25

Change the certificate user ID type . . . 25

Enable CRL checks . . . 26

Certificate expiration . . . 26

Delete certificates 26

5 Troubleshooting VPN connections 29

Logs and diagnostics 29

Access logs and diagnostics 29

Collect diagnostic information 29

Reading logs 30

Capture network traffic 31

Accessing and customizing traffic dump files 31

Solving connectivity issues 32

Using different connection settings 32

Activate or deactivate random local VPN ports 32

The Connectivity Problems dialog box 32

Change the VPN Client MTU 33

Change the VPN Client MAC address 33

A Custom installation scenario 35

Export gateway contact information 35

Create a transform file 36

Open the installation file 36

Add rows to the transform 37

Save the transform 38

Install with the completed transform file 39

B Using the VPN Client in automated mode 41

How automated mode works 41

How automated mode affects the user interface 41

Preparing files for installation 42

Create a script to install the VPN Client in silent mode 42

Install the VPN Client in silent mode 44

Connection retry times in automated mode 44

Error handling in automated mode 45

Unrecoverable errors 45

Recoverable errors 45

Index 47

Preface

This guide provides the information you need to work with your McAfee product.

Contents

- *About this guide*
- *Find product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
ℹ	**Note:** Additional information, like an alternate method of accessing an option.
💡	**Tip:** Suggestions and recommendations.
❗	**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.
⚠	**Warning:** Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task

1. Go to the **Knowledge Center** tab of the McAfee ServicePortal at http://support.mcafee.com.
2. In the **Knowledge Base** pane, click a content source:
   - **Product Documentation** to find user documentation
   - **Technical Articles** to find KnowledgeBase articles
3. Select **Do not clear my filters**.
4. Enter a product, select a version, then click **Search** to display a list of documents.

1 Introduction

The McAfee® VPN Client (VPN Client) provides a secure virtual private network (VPN) connection to a McAfee Firewall/VPN gateway for end-user computers running on Microsoft Windows platforms.

The VPN Client protects private information transferring over the Internet and allows verification of the end user's identity. Remote end users are able to connect to internal networks securely. The VPN Client mainly runs in the background, automatically prompting the end user to authenticate when a VPN is required.

You can find information about installation, configuration, troubleshooting, and use scenarios in this guide. Additional information about the VPN Client is covered in the following documents:

- **Configuring VPN access for the VPN Client end users** — See the *McAfee Next Generation Firewall Product Guide* and the Management Client online Help.
- **Using the VPN Client** — See the *McAfee VPN Client User Guide*.
- **Windows platform requirements** — See the *McAfee VPN Client Release Notes*.

Contents

- *How the VPN Client works*
- *VPN Client configuration and updates*
- *Virtual IP addressing*
- *How connection settings work*

How the VPN Client works

In the Management Client, VPN and Gateway elements and settings are configured into a VPN profile. The profile is assigned to end users, then firewall policy is edited to allow incoming connections from the VPN Client. During installation, the VPN Client connects back to the firewall.

There might be a limit on the gateway of how many end users can connect at the same time; however, there is no license or serial code enforcement in the VPN Client. The VPN Clients are licensed as part of the Firewall/VPN gateway — you can freely install it on any number of hosts.

VPN Client configuration and updates

The VPN Client settings are mostly configured through Security Management Center (SMC).

The VPN Clients download a configuration file from the Firewall/VPN gateways to set the correct options for establishing a mobile VPN with that gateway. These include options for encryption, authentication, endpoints to contact, and the IP addresses that are accessible through the VPN. When changes are made on the gateway, each VPN Client updates the configuration the next time the VPN Client starts a new VPN connection. Due to the centralized configuration method, the McAfee VPN Client can connect to McAfee Firewall/VPN gateways only.

Virtual IP addressing

The primary access method for production use is the Virtual Adapter feature. This feature allows the VPN Clients to have a second, virtual IP address that is independent of the end-user computer address in the local network.

The virtual IP address is only used in communications through the VPN tunnels. The VPN gateway gets the IP address and network settings of the VPN Client from the configured DHCP server and forwards the information to the VPN Client. For one-way access without DNS resolving, the VPN gateway can alternatively be set up to apply NAT to translate the VPN Client connections. This method is meant for testing purposes.

The VPN gateway specifies the destination IP addresses for traffic that the VPN Clients send into the VPN tunnel. The IP addresses are configured as Site elements for each gateway in the Management Client. When the Sites contain specific internal networks, the VPN Clients receive a configuration for *split tunneling*. Split tunneling means that only the specified portion of traffic uses the VPN tunnel, and other connections use the local network as usual.

By default, when the VPN Client virtual adapter requests an IP address, it uses the MAC address of the physical interface used in the VPN connection.

To configure the IP address distribution on the gateway, see the Management Client Online Help and the *McAfee Next Generation Firewall Product Guide*, in the *Virtual Private Networks* section.

How connection settings work

For IPsec connections, the VPN Clients might need to use different settings at different locations due to different port filtering and NAT arrangements.

The VPN Client can work within the allowed settings to automatically try to connect with TCP tunneling enabled/disabled or using different port combinations if the automatic IKE retry option is active in the VPN Client installation. The VPN Client tries the settings one by one in the following order until the connection succeeds or all options are exhausted:

1. Enable/disable TCP tunneling, if allowed for the endpoint on the gateway.
2. Enable/disable the option to use random local source ports on the client.
3. Use only destination port UDP/4500 (NAT-T port) for the gateway, instead of both port UDP/500 and UDP/4500.
4. Use a combination of a random local source port and destination port UDP/4500 for the gateway.

Also, the VPN Client can automatically react if a connection to port UDP/500 succeeds, but port UDP/4500 (NAT-T) is unavailable. In this situation, the VPN Client tries the connection with TCP tunneling enabled/disabled, if allowed for the endpoint on the gateway. If changing the TCP tunneling option does not help, the VPN Client defaults to using destination port UDP/500 only.

The end user is notified if the VPN Client is unable to use one of the two necessary ports.

2 Deployment

To allow end users to access company networks through the VPN Client, plan your deployment carefully.

Contents

- *Deployment options*
- *Deployment checklist*

Deployment options

Consider the available options for deployment.

VPN Client types

SMC supports both types of VPN Clients; select the one that is right for your environment.

IPsec — IPsec VPNs allow any IP traffic to be transported in the VPN regardless of which higher-level protocol the traffic uses on top of the IP protocol. Hosts can communicate through the VPN as if it was a normal link without the need for application-specific configurations on the gateway device.

SSL — SSL VPNs allow authenticated end users to establish secure connections to internal HTTP-based services through a portal on a web browser or through a client application that allows direct network access. SSL VPN Portals provide access by using the SSL encryption features included in web browsers. End users log on to a portal to access those resources that you have configured. You can use SSL VPN Portals to provide remote access to specific resources from various types of devices and platforms.

> The SSL VPN tunnel and portal cannot be on the same IP address and port pair simultaneously. If both are needed, McAfee recommends configuring the SSL VPN tunnel to port 443 and adding the port number to the URI when accessing the portal.

Installation types

The VPN Client can be installed in interactive mode by manually starting the installer, or in silent mode through a remote software deployment service.

- **Standard** — Uses the downloaded VPN Client files
    - **Wizard** — Uses a guided installation and configuration process
    - **Silent batch file** — Uses a script to install the VPN Client without end-user interaction
- **Custom** — Uses a third-party program to make a custom installation package that includes the gateway information.

Installation file types

Several files are available to use for installing the VPN Client.

- McAfee-VPN-Client-<version>.exe
- McAfee-VPN-Client-<version>-x64.msi
- McAfee-VPN-Client-<version>-x86.msi

The variable, <version>, is the exact version number that changes each time an update is released. The x64 .msi package is meant for a 64-bit operating system and the x86 .msi for a 32-bit operating system installation. The executable package uses the correct package for the operating system automatically.

The VPN Client can be installed locally with the .exe installer. The .msi packages allow remote installation or customized installations that remove the need for some end-user actions:

- With a standard installation package, the end-users type the gateway IP address manually, authenticate themselves to the gateway, and verify the certificate fingerprint of the gateway. Alternatively, you can export the contact details of the gateway to a file and instruct the end users to copy the file to the correct location.
- If you generate a customized installation package, the gateway information can be included in the installation package, requiring no end-user intervention.

See also

Download the installation file on page 14

Standard installation

End users either install the VPN Client following the instructions in the installation wizard, or you can provide a batch file for silent installation.

Use the following commands for silent installation, replacing `<version>` with the exact version number in the file you are using:

- **.exe file** — `McAfee_VPN_<version>.exe /quiet`
- **.msi file** — `msiexec /i McAfee-VPN-Client-<version>-x64.msi /quiet.` or `msiexec /i McAfee-VPN-Client-<version>-x86.msi /quiet.`

Custom installation

The VPN Client installation package can be customized by creating a Microsoft Installer (MSI) transform file from the McAfee-VPN-Client-<version>-x64.msi or McAfee-VPN-Client-<version>-x86.msi file.

The contact information of the security gateways is added to the transform file. To customize the installation package, you must have a basic knowledge of MSI transforms and know how transforms can be applied to installation packages.

User authentication

End users must authenticate before they can connect to a gateway.

You can select different authentication methods for each gateway. If several authentication methods are allowed for an end user, the end user can select between the methods in the VPN Client.

Two basic authentication schemes are available:

- **User name and password** — The gateway can be integrated with external authentication servers.
- **Certificate** — Various certificate authentication options are available for the VPN Client.

  Certificate authentication is only supported with IPsec connections.

Different methods can be used on the same gateway simultaneously.

The user name and password method supports integration with external RADIUS or TACACS+ authentication servers. This integration allows various authentication schemes such as RSA SecurID cards or Active Directory/Network Policy Server (NPS) authentication.

The VPN Client always sends the user name and password using the UTF-8 character encoding. When using external authentication servers, make sure that they support UTF-8 encoding if the user names or passwords contain letters outside the US-ASCII character set.

For a detailed overview to user authentication and step-by-step configuration instructions, see the *McAfee Next Generation Firewall Product Guide* or the Management Client online Help.

See also
Authenticating with client certificates on page 19

Deployment checklist

Determine how you want to deploy the VPN Client in your environment.

Table 2-1 Deployment checklist

Determine...	Verified
VPN Client type: • IPsec • SSL	
Installation type: • Standard • Wizard • Silent batch file • Custom	
Method of user authentication: • User name and password • Certificate	
VPN Client mode: • User-controlled — Whenever the VPN Client connects, it requires authentication. • Automated mode — The VPN Client connects automatically.	

3 Installing and upgrading the VPN Client

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

Contents

- *Installation overview*
- *Download the installation file*
- *Install with the wizard*
- *Install using a custom installation package*
- *Upgrade the VPN Client*

Installation overview

The installation process requires changes in the Management Client and in the end user computer.

- Before installing the VPN Client, you must configure the VPN-related elements and settings in the Management Client.
  - Create a VPN, or add the Client Gateway element to an existing VPN and configure the Client settings in the internal Gateway and VPN Profile elements.
  - Create the user accounts, or integrate an existing LDAP database or an external authentication service with the SMC.
  - Edit the firewall policy so that the policy allows incoming connections from the VPN Clients.
- The installation of the VPN Client can be done by the administrator or the end user. You can use the standard VPN Client installation package or create a custom installation package. Either installation option requires that you download the installation files.
  - A standard installation package allows the end user to install the VPN Client through the installation wizard.
  - In a custom installation package, you can include the contact information for the gateway so that the end users do not need to add it manually.
- During the upgrade process, the earlier version of the VPN Client is removed and replaced with the current version with the same settings.

> Instructions for tasks performed in the Management Client can be found in the Management Client online Help and *McAfee Next Generation Firewall Product Guide*, in the *Virtual Private Networks* section.

Download the installation file

The VPN Client installation files are available on the McAfee NGFW download page.

Before you begin

You must have a grant number to access product downloads.

Windows does not have MD5 or SHA-1 checksum programs by default, but there are several third-party programs available.

Task

1. Go to www.mcafee.com/us/downloads/downloads.aspx, enter your grant number, then select the appropriate product and version.
2. Download the installation files.

   These packages are available:

   - **.exe** — Standard installations
   - **.msi** — Custom installation package creation
3. Change to the directory that contains the files to be checked.
4. Generate a checksum of the file using the command `md5sum filename` or `sha1sum filename`, where `filename` is the name of the installation file.

   Example:

   ```
   sha1sum McAfee-VPN-Client-5.9.0.0000.exe
   ```

   ```
   1334641d17859e7f2585a744a993be75473c6930 McAfee-VPN-Client-5.9.0.0000.exe
   ```
5. Verify the checksums.
   a. Compare the displayed output to the checksum on the website.
   b. Proceed according to the result of the comparison:
      - If the values match, the files are safe to use.
      - If there is a difference in the values, try downloading the files again.

   Do not use files that have invalid checksums. If downloading the files again does not help, contact McAfee technical support to resolve the issue.

Install with the wizard

You can use the VPN Client .exe file to install the VPN Client with a wizard.

Before you begin

You must have downloaded the installation .exe file.

Task

1. Right-click the installation executable file and select **Run as Administrator**.

   The **McAfee VPN Client Setup** window opens.

2 Click **Install**.

The **McAfee VPN Client Setup** wizard opens.

3 Click **Next**.

4 Accept the License Agreement and click **Next** to continue.

5 Click **Install**.

If you see one or more confirmation messages from Windows during the installation, accept them. The installation of all drivers and components must be allowed for the VPN Client to work correctly.

6 When the installation is complete, click **Finish**.

The **McAfee VPN Client Setup** window shows a confirmation message.

7 Click **Close**.

Install using a custom installation package

Customizing the installation allows you to add information into the installation package and to install and update the VPN Clients remotely.

Tasks

- *Save the gateway contact information to a file* on page 15
  You can save the contact information for security gateways to a file. The file can then be added into a customized installation package or copied to the end-user computers that already have a VPN Client installed.
- *Install with a transform file* on page 16
  Use an .mst transform file that you created with the .msi file to install the VPN Client either remotely or locally on the command line of the client computer.

Save the gateway contact information to a file

You can save the contact information for security gateways to a file. The file can then be added into a customized installation package or copied to the end-user computers that already have a VPN Client installed.

The gateway contact information allows end users to connect to new gateways without needing to add the security gateway address manually and without verifying the gateway certificate fingerprint.

Tasks

- *Export gateway contact information* on page 15
  You must first use the Management Client to export the contact information of each security gateway that the end users connect to.
- *Copy gateway contact information files manually* on page 16
  You can add new gateways to existing VPN Clients by copying the exported gateway contact information files to the client computers.

Export gateway contact information

You must first use the Management Client to export the contact information of each security gateway that the end users connect to.

Exporting the gateway contact information allows you to distribute the contact information files to end users. You can add the files to a customized installation package or send them to end users so that they can copy the files manually to their computer.

The contact information is always gateway-specific.

Task

1. From the Management Client, select **Configuration** | **Configuration** | **VPN**.
2. In the element tree, select **Gateways**.
3. For each contact you want to export:
   a. Right-click the internal Gateway element for which you want to save the configuration and select **Tools** | **Save Gateway Contact Information**.
   b. Browse to the folder where you want to save the contact information file.
   c. Enter a file name and click **Save**.

      The contact information of the selected security gateway is saved in an `.xml` file.

Copy gateway contact information files manually

You can add new gateways to existing VPN Clients by copying the exported gateway contact information files to the client computers.

Provide the files to the VPN Client end users and instruct them to copy the files to the correct location.

Task

1. Place the exported gateway contact information file in a location that is accessible to the client computer.
2. Copy the security gateway contact information .xml file to the <system_drive>\ProgramData \McAfee\McAfee VPN Client\gateway_info directory on the client computer.

Install with a transform file

Use an .mst transform file that you created with the .msi file to install the VPN Client either remotely or locally on the command line of the client computer.

> **Before you begin**
>
> You can create a customized installation package from the .msi file with any Windows installation package editor, for example, with Orca.
>
> See *Installing with a custom installation package* for an example.

If you want the end users to install the VPN Client on the command line, provide them the transform file, the gateway contact information files, and installation instructions.

Task

1. Copy the transform file to the same directory as the .msi file.
2. Create the path in the directory where you have the installation files:

   All Users\Application Data\McAfee\McAfee VPN Client\ gateway_info
3. Copy the exported gateway contact information files to the gateway_info directory.

4. Start the installation:
   - **Remote installation** — Run the .msi file with the transform .mst file following the instructions of the software solution you are using.
   - **Command-line installation**
     - If an earlier version of the McAfee VPN Client is already installed on the computer, run one of these commands:

       ```
       msiexec /i McAfee-VPN-Client-<version>-x64.msi REINSTALLMODE=vomus REINSTALL=ALL
       TRANSFORMS=<transform_file>
       ```

       ```
       msiexec /i McAfee-VPN-Client-<version>-x86.msi REINSTALLMODE=vomus REINSTALL=ALL
       TRANSFORMS=<transform_file>
       ```

     - If an earlier version of the McAfee VPN Client is not installed on the computer, run one of these commands:

       ```
       msiexec /i McAfee-VPN-Client-<version>-x64.msi TRANSFORMS=<transform_file>
       ```

       ```
       msiexec /i McAfee-VPN-Client-<version>-x86.msi TRANSFORMS=<transform_file>
       ```

     `<version>` is the exact version number that changes each time an update is released.

See also
Custom installation scenario on page 4

Upgrade the VPN Client

You can upgrade an existing VPN Client installation.

Task

1. Download the installation .exe file.
2. Double-click the executable file.

   A confirmation message appears.
3. Click **Yes**.

   The **Welcome** screen for the installation wizard opens.
4. Click **Next** to start the upgrade.
5. Accept the License Agreement and click **Next** to continue.
6. When the upgrade is finished, click **Finish** to close the wizard.

See also
Download the installation file on page 14
Install using a custom installation package on page 15

4 Configuring certificates

The VPN Client can authenticate using internal or external certificates. Certificates can be used only with IPsec-based McAfee VPN Client connections.

Contents

- *Authenticating with client certificates*
- *Authenticating with internal certificates*
- *Authenticating with external certificates*
- *Change the certificate passphrase*
- *View user certificate details*
- *Change the certificate user ID type*
- *Enable CRL checks*
- *Certificate expiration*
- *Delete certificates*

Authenticating with client certificates

McAfee VPN Client IPsec connections support using certificates to authenticate end users.

In certificate-based authentication, you or the end user must first create a certificate request. The request process also generates a private key for the certificate. The certificate cannot be used without the private key, which should always be protected by a passphrase to prevent unauthorized use of the certificate. The certificate request must be signed by a valid certificate authority (CA) to produce a valid certificate. For a gateway to accept the client certificate as proof of identity, it must be configured to trust the CA that has signed the VPN Client certificate.

Supported certificate authentication schemes

There are four general options for setting up certificates required for authentication.

- **Create certificates using the Management Server internal tools** — Create a certificate request in the VPN Client. Then sign the request through the Management Client using the Management Server internal VPN CA.
- **Create certificates externally** — Import certificates with their associated private key into the VPN Client.
- **Certificate and private key stored on a smart card** — The VPN Client calls the external smart card software on the computer and there is no need for any configuration steps on the VPN Client. The smart card is ready to use and is available when inserted if the smart card reader is correctly configured in Windows.
- **Locally stored certificates in the Microsoft Certificates Store** — Certificates are stored in the Microsoft Certificates Store on the end-user computer and are automatically available for use with the VPN Client.

When the certificate request is generated in the VPN Client, the resulting certificate is called an *Internal Certificate* in the VPN Client. When the certificate request is created using other tools, the certificate is called an *External Certificate* in the VPN Client.

User identities

Certificates are a proof of the certificate holder identity. The exact form of the identity used can vary.

Two fields in internal certificates can be used for authentication in mobile VPNs:

- **Subject Name** — Contains a *Distinguished Name* (DN) that can consist of multiple items such as *Common Name* (CN), *Organization* (O), *Country* (C), and *Email Address* (E).
- **Subject Alternative Name** — Usually contains the user's email address. Some client certificates do not have a Subject Alternative Name. This field is used in authentication if it is available in the client certificate.

Depending on the certificate, an end user can authenticate to a gateway either with an email address, a subject name, a DNS name, or an IP address. The end user can change their user ID type in the VPN Client, except for certificates stored on smart cards or in the Microsoft Certificates Store. The certificate information is matched against details defined in the User elements in the Management Client or in an external LDAP database. For more information, see the *McAfee VPN Client User Guide*.

Authenticating with internal certificates

The VPN Client has tools for creating a certificate request and the associated private key.

When the certificate request is ready, the end user must deliver the certificate request to a trusted CA for signing. The request can be signed using the SMC internal VPN CA or some other certificate authority. The signed certificate is sent back to the end user, who must import it in the VPN Client. To use the certificate for authentication, the end user must enter the passphrase that protects the private key each time they connect. (The passphrase was selected by the end user when creating a certificate request or when they decide to change the key)

Tasks

- *Create a basic certificate request* on page 21
  You can create a basic certificate request for an internal certificate in the VPN Client.
- *Create an advanced certificate request* on page 21
  An advanced certificate request offers more options than a basic certificate request for defining the properties of the certificate request and the private key. The exact options to use depend on the capabilities of the CA and the requirements and preferences of your organization.
- *Obtain signed certificates* on page 22
  Certificate requests generated in the VPN Client are signed by the Management Server internal VPN CA or by a third-party CA.
- *Import a signed certificate* on page 22
  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.

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.
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*.

Create an advanced certificate request

An advanced certificate request offers more options than a basic certificate request for defining the properties of the certificate request and the private key. The exact options to use depend on the capabilities of the CA and the requirements and preferences of your organization.

Task

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

4 Select **Advanced Mode** and click **Next**.

5 Enter the information according to your environment as described in the table.

Table 4-1 Create certificate request options

Setting	Description
Subject Name	Distinguished name that identifies the end user on the gateway.
Alternative Subject Type	Type of attribute to use as the Subject Alternative name.
Alternative Subject Value	Value of the attribute that is used as the Subject Alternative name.
Private Key Type	Algorithm for generating the private key.
Private Key Length	Length of the private key.
Passphrase	Passphrase you want the end user to enter and confirm when the user authenticates using the certificate. 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.

6 Click **Next**.

7 (Optional) Select additional options for Key Usage and Extended Key Usage according to your environment.

8 Click **Create**. The certificate request is created and saved as a .csr file.

If you configured internal certificates as a gateway authentication method, you must:

- Inform end users that they must create a certificate request in the VPN Client.
- Provide end users with the information they must enter.
- Inform end users which options they must select when they create the certificate request.

Obtain signed certificates

Certificate requests generated in the VPN Client are signed by the Management Server internal VPN CA or by a third-party CA.

The CA that signs the VPN Client certificate must be defined as a trusted VPN certificate authority in the SMC. To sign a certificate request internally, use the certificate signing tool in the VPN Configuration view in the Management Client. See the *McAfee Next Generation Firewall Product Guide*, in the *Virtual Private Networks* section, or the Management Client online Help for more information.

Import a signed certificate

A signed certificate must be imported 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**.

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.

Authenticating with external certificates

You might prefer to use external tools to create the certificate request instead of having it created in the VPN Client. This method is useful if the end users already have suitable signed certificates and private keys that can be used.

There are of three ways of using 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

Locally stored certificates used for the Microsoft Certificates Store on the end-user computer are automatically available for use with the VPN Client. In all other cases, the end users must import both the certificate and the private key in the VPN Client. The certificates and the private keys can be imported either as a single PKCS # 12 file or as two separate files. You must inform the end users which options they must select when importing the external certificates.

Only certificates signed by the Management Server internal VPN certificate authority are trusted by default. Other certificate signers must be configured as trusted on the gateway to allow the end users to authenticate. See the *McAfee Next Generation Firewall Product Guide*, in the *Virtual Private Networks* section, or the Management Client online Help for more information.

Tasks

- *Import a PKCS #12 file* on page 23
  Import the file containing the certificate and the private key.
- *Import separate certificate and private key files* on page 24
  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.

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.**

Enable CRL checks

For IPsec connections, you can optionally enable Certificate Revocation List (CRL) checks to verify the validity of gateway certificates.

Enabling CRL checks is required in GOST environments, and optional in other environments.

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 **Check Gateway Certificate Validity on Certificate-Specified CRLs**.

4 Click **Apply**.

5 Click **Close**.

Certificate expiration

For added security, certificates have an expiration date. Certificates signed by the Management Server internal VPN CA are valid for three years from their creation.

It is not possible to extend the validity of the certificates. To continue using certificate authentication for more than three years on the same installation, you must create a new certificate.

The CA also has an expiration date. The Management Server internal VPN CA is valid for 10 years. A new CA is automatically created six months before the expiration, and you must create new certificates for the clients and sign them with the new CA.

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.

5 Troubleshooting VPN connections

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

Contents

- *Logs and diagnostics*
- *Solving connectivity issues*

Logs and diagnostics

The VPN Client has a **Diagnostics** tab where you can access logs and diagnostics information to analyze VPN connections.

Access logs and diagnostics

Logs and diagnostics are a useful resource for administrators and McAfee technical support when troubleshooting VPNs.

There are two ways to gather the diagnostics and log files. The most convenient way to gather information from end-user computers is to instruct end users to collect a diagnostics file that also includes the logs. You can also view the logs separately when you are troubleshooting a VPN Client locally.

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.

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.

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.

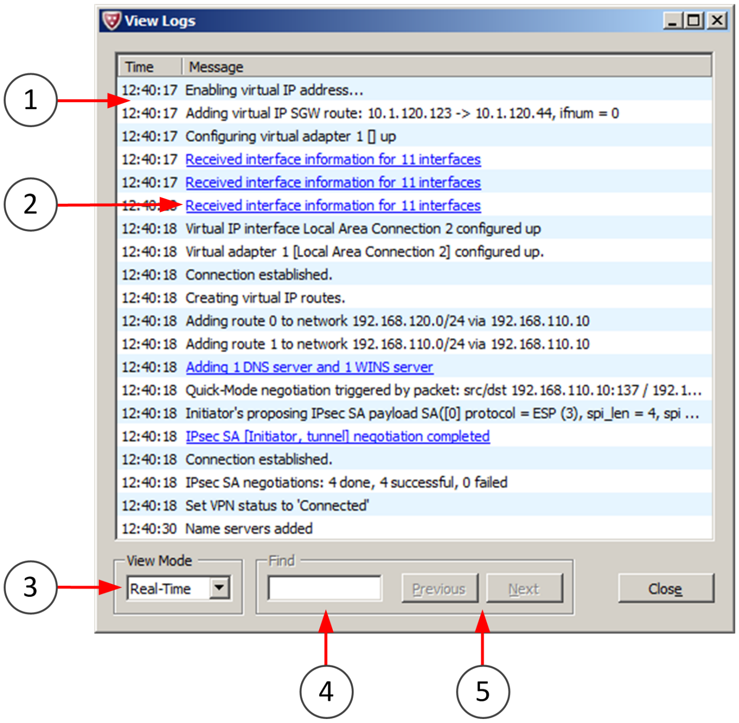
4 When the data collection finishes, click **Save Diagnostics**.

5 Browse to the location where you want to save the file, enter a file name, and click **Save**.

Reading logs

The VPN Client maintains its own log of events related to its operation. You can view this log directly in the VPN Client.

This log is also included in the diagnostics file. Depending on the issue you are troubleshooting, there might be additional relevant logs in the Windows logs.



```
Time      Message
12:40:17  Enabling virtual IP address...
12:40:17  Adding virtual IP SGW route: 10.1.120.123 -> 10.1.120.44, ifnum = 0
12:40:17  Configuring virtual adapter 1 [] up
12:40:17  Received interface information for 11 interfaces
12:40:17  Received interface information for 11 interfaces
12:40:[illegible]  Received interface information for 11 interfaces
12:40:18  Virtual IP interface Local Area Connection 2 configured up
12:40:18  Virtual adapter 1 [Local Area Connection 2] configured up.
12:40:18  Connection established.
12:40:18  Creating virtual IP routes.
12:40:18  Adding route 0 to network 192.168.120.0/24 via 192.168.110.10
12:40:18  Adding route 1 to network 192.168.110.0/24 via 192.168.110.10
12:40:18  Adding 1 DNS server and 1 WINS server
12:40:18  Quick-Mode negotiation triggered by packet: src/dst 192.168.110.10:137 / 192.1...
12:40:18  Initiator's proposing IPsec SA payload SA([0] protocol = ESP (3), spi_len = 4, spi ...
12:40:18  IPsec SA [Initiator, tunnel] negotiation completed
12:40:18  Connection established.
12:40:18  IPsec SA negotiations: 4 done, 4 successful, 0 failed
12:40:18  Set VPN status to 'Connected'
12:40:30  Name servers added
```

Figure 5-1 View Logs dialog box

1 Log entries

2 Links to view more detailed information

3 Modes to view logs in real time, from a certain time period, all stored logs, or the most recent logs with detailed information

4 Keyword search to look for specific log entries

> This option is not available in all view modes.

5 Navigation to find more occurrences of the keyword

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.

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.

Accessing and customizing traffic dump files

Traffic captures record the network traffic of the local computer to help with troubleshooting when network problems are suspected.

The recorded traffic is saved on the local computer in the traffic dump files adapter.pcap and protocol.pcap. These files can be opened with any program that can display .pcap files.

You can customize how traffic is captured by changing the values for the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\sgravpn\Parameters on the local computer.

Table 5-1 Registry values for customizing traffic captures

Name	Type	Description
CaptureMaxSize	REG_DWORD	The maximum traffic capture file size in MB. If not defined, the maximum size is 10 MB.
CaptureDirectory	REG_SZ	The default directory in which traffic capture files are stored.
CaptureSnapLength	REG_DWORD	The number of bytes captured from each network packet. If not defined, the whole packet is captured.
CaptureSystemStartup	REG_DWORD	If set to 1, the traffic capture is started immediately when the operating system starts.

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.

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.

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.

If these default ports cannot be used for VPN connections, enable a random selection of ports from the 1025–65535 range every time a VPN connection is made.

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**.

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 5-2 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.

Change the VPN Client MTU

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

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.

> The VPN Client MAC address can also be changed through the command line or with a script by running the sgvmac.exe command.
>
> *Example:* To change the MAC address to 06:05:04:03:02:01, enter:
>
> ```
> sgvmac.exe 06:05:04:03:02:01
> ```

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

A Custom installation scenario

This installation scenario shows an example of how you can customize the McAfee VPN Client installation package using a third-party installer program.

A customized installation package includes the gateway information that the VPN Client end users need for connecting to security gateways. When the VPN Client is installed from the customized installation package, the gateways are automatically added to the VPN Clients. End users do not need to add the gateways manually after the installation.

The scenario tasks must be completed in order.

Contents

- *Export gateway contact information*
- *Create a transform file*
- *Install with the completed transform file*

Export gateway contact information

You must export the contact information from the Management Client into a file to add the gateway contact information to the installation package.

Task

1. Select **Configuration** | **Configuration**.
2. Navigate to **Virtual Private Networks** | **Gateways** in the **All Elements** tree.
3. For each contact you want to export:
   - a Right-click the Internal Security Gateway element for which you want to save the configuration and select **Tools** | **Save Gateway Contact Information**.
   - b Browse to the folder where you want to save the contact information file.
   - c Enter a file name and click **Save**.

     The contact information of the selected security gateway is saved in an .xml file.

See also

Copy gateway contact information files manually on page 16

Create a transform file

Customize the VPN Client installation package, and add the gateway information to it. The installation package is customized by creating an MSI (Microsoft Installer) transform file from the McAfee-VPN-Client-<version>-x64.msi or McAfee-VPN-Client-<version>-x86.msi file.

The following workflow assumes that you have a basic knowledge of MSI transforms and know how they can be applied to installation packages.

You can create a customized installation package with any Windows installation package editor. This example describes how you can customize the installation package using Orca version 5.0.9600.0. Orca is a Windows Installer package editor provided as part of the Microsoft Windows software development kit (SDK).

In the following tables, some of the values are predefined values that you must use in specific columns. The predefined values are shown in ***bold italic.*** You can select the other values as needed.

Tasks

- *Open the installation file* on page 36
  Open the McAfee VPN .msi file in the third-party installer program.
- *Add rows to the transform* on page 37
  The transform values must be updated to include the VPN Client information.
- *Save the transform* on page 38
  The completed transform file must be saved so that it can be used for installation.

Open the installation file

Open the McAfee VPN .msi file in the third-party installer program.

Task

1. Start Orca.
2. Select **File** | **Open** and navigate to the McAfee VPN .msi file.
3. Click **Open**.
4. Select **Transform** | **New Transform**.

   A new transform of the file opens.

Add rows to the transform

The transform values must be updated to include the VPN Client information.

Task

1 In the transform, add a component.

   a Browse to **Component** in the left pane.

   b Select **Tables** | **Add Row**.

   c In the **Add Row** dialog box, enter the following values in the columns.

Table A-1 Information for a new component

Column	Value
Component	Enter a unique name for the component.
ComponentID	Enter a unique ID for the component. Select **Edit** | **Paste New GUID** to add an ID.
Directory_	***GATEWAY_INFO***
Attributes	***16*** (msidbComponentAttributesPermanent)
KeyPath	Enter a unique name for the gateway contact information file. Do not use the actual name of the file. Both the actual name of the file and this additional unique name are used later in step 4.

2 Add a feature.

   a Browse to **Feature** in the left pane.

   b Select **Tables** | **Add Row**.

   c In the **Add Row** dialog box, enter the following values in the columns.

Table A-2 Information for a new feature

Column	Value
Feature	Enter a unique name for the feature.
Display	***0***
Level	***1***
Attributes	***24*** (msidbFeatureAttributesDisallowAdvertise and msidbFeatureAttributesUIDisallowAbsent)

3 Map the new component and the new feature.

   a Browse to **Feature Components** in the left pane.

   b Select **Tables** | **Add Row**.

   c In the **Add Row** dialog box, enter the following values in the columns.

Table A-3 Information for mapping the new component and the new feature

Column	Value
Feature_	Enter a name of the new feature.
Component_	Enter a name of the new component.

4 Add gateway contact information to the file table.

The contact information must be added for each security gateway into the **File** table. If there are several security gateways, add the contact information of each gateway on a separate row in the table.

a Browse to **File** in the left panel.

b Select **Tables** | **Add Row**.

c In the **Add Row** dialog box, enter the following values in the columns.

Table A-4 Adding gateway contact information

Column	Value
File	The same unique file name used in the **KeyPath** column in the **Component** table in step 1.
Component_	Enter the name of the component.
FileName	Actual name of the gateway contact information file.
FileSize	Enter the size of the gateway contact information file in bytes.
Attributes	***8192*** (msidbFileAttributesNoncompressed)
Sequence	Enter the next available number after the highest number in the **Sequence** column. For example, if the highest number is 28, enter 29 as the value.

5 Add new media.

a Browse to **Media** in the left panel.

b Select **Tables** | **Add Row**.

c In the **Add Row** dialog box, enter the following values in the columns.

Table A-5 Information for adding new media

Column	Value
DiskId	Enter the next available number after the highest number in the **DiskId** column. For example, if the highest number is 2, enter 3 as the value.
LastSequence	Enter the last sequence value used in the **File** table; see step 4 for more information.

Save the transform

The completed transform file must be saved so that it can be used for installation.

Task

1 Select **Transform** | **Generate Transform**.

A **File Save** dialog box opens.

2 Select a suitable folder, enter a name for the file, and click **Save**.

3 Select **Transform** | **Close Transform**.

You have now saved the transform file, so you can close Orca.

Install with the completed transform file

The transform file you created is a new .mst file. You can use the .mst file together with the McAfee VPN .msi file to install the VPN Client remotely or locally on the command line.

If you want end users to install the VPN Client locally on the command line, send the transform file and the gateway contact information files to them with instructions on how to proceed with the installation.

See also

Install with a transform file on page 16

B Using the VPN Client in automated mode

You can configure the McAfee VPN Client to establish and maintain VPN connections automatically. This mode is useful for situations where there is no user present every time to start the VPN connection, such as for automated teller machines.

See also

Install using a custom installation package on page 15

Contents

- *How automated mode works*
- *How automated mode affects the user interface*
- *Preparing files for installation*
- *Create a script to install the VPN Client in silent mode*
- *Install the VPN Client in silent mode*
- *Connection retry times in automated mode*
- *Error handling in automated mode*

How automated mode works

If the VPN Client is started in automated mode, it automatically creates a VPN connection to the VPN gateway specified in the VPN Client configuration. It also automatically creates a VPN when the computer on which the VPN Client has been installed is started.

The VPN Client user is authenticated either with a certificate or with a password. The first certificate found in the VPN Client Certificate directory is used with certificate authentication.

> If you want to use the VPN Client in automated mode on a computer that already has the VPN Client installed, you must first uninstall the existing VPN Client. Then reinstall it according to the instructions in this document.

How automated mode affects the user interface

The VPN Client user interface is not started automatically when the VPN Client has been installed in automated mode. If necessary, you can start the user interface from the Programs folder in the Start menu. In automated mode, the user interface can only be used for monitoring the connection status. All commands from the user interface are ignored.

Preparing files for installation

Several files are always needed for installing and authenticating the VPN Client for use in automated mode.

- VPN Client installation file
- Gateway contact information file for the VPN Client
- Depending on the authentication method, one of these options:
    - **Password** — You must have the password file for the VPN Client.
    - **Certificate** — You must have a private key file and a certificate file for the IPsec VPN Client.

> ℹ The private key must not be encrypted.

If the VPN Client user is authenticated with a password, you must create a .txt file that defines the user name and the password. Optionally, the signature type that matches the gateway certificate (RSA, DSS, or ECDSA) can also be defined. If the signature type is not specified in the password file, RSA is used.

The user name and the password are defined in the password file using this format:

<user>user name</user>

<pass>password</pass>

The signature type is defined in one of the following ways:

<auth>RSA</auth>

<auth>DSS</auth>

<auth>ECDSA</auth>

The private key file and certificate file or the password file are used to authenticate the user. Only one of the authentication methods can be used at the same time. The gateway contact information file contains the information the VPN Client needs for making an initial connection to a gateway. The installer asks for the gateway contact information and for the authentication files (the private key file and certificate file, or the password file) during the installation. The gateway contact information file is created in the Management Client.

See also

User authentication on page 10
Save the gateway contact information to a file on page 15
Authenticating with client certificates on page 19

Create a script to install the VPN Client in silent mode

Create your own script or use one of the example scripts provided.

Sample script 1 — This script is for certificate authentication.

```
@echo.

@echo * Installing McAfee VPN Client...

%1 /quiet /log install_log.txt SG_INSTALL_MODE=Automated

@echo.
```

```
@echo * Stopping McAfee VPN Client Service...

net stop sgipsecvpn

@echo.

@echo * Copying configuration files...

copy %2 "%ALLUSERSPROFILE%\Application Data\McAfee\McAfee VPN Client\certificates\client.crt"

copy %3 "%ALLUSERSPROFILE%\Application Data\McAfee\McAfee VPN Client\certificates\client.prv"

copy %4 "%ALLUSERSPROFILE%\Application Data\McAfee\McAfee VPN Client\gateway_info
\contact_info_a.xml"

@echo.

@echo * Starting McAfee VPN Client Service...

net start sgipsecvpn
```

Sample script 2 — This script is for username and password authentication.

```
@echo.

@echo * Installing McAfee VPN Client...

%1 /quiet /log install_log.txt SG_INSTALL_MODE=Automated

@echo.

@echo * Stopping McAfee VPN Client Service...

net stop sgipsecvpn

@echo.

@echo * Copying configuration files...

copy %2 "%ALLUSERSPROFILE%\Application Data\McAfee\McAfee VPN Client\passwd.txt"

copy %3 "%ALLUSERSPROFILE%\Application Data\McAfee\McAfee VPN Client\gateway_info
\contact_info_a.xml"

@echo.

@echo * Starting McAfee VPN Client Service...

net start sgipsecvpn
```

Each sample script works in this order:

1. It starts the installer with the following arguments: `/quiet /log install_log.txt SG_INSTALL_MODE=Automated`. It also creates a log file `install_log.txt` from the installation process.
2. It then starts the VPN Client. The VPN Client service is still shut down because the files used in authentication and the gateway contact information file are still missing.
3. Next the script copies the missing files to the directory `%ALLUSERSPROFILE%\Application Data\McAfee\McAfee VPN Client`.
4. Finally, the script starts the VPN Client service.

To use the script, put all relevant files in the same directory:

- Script file
- VPN Client installation file
- Gateway contact information file for the VPN Client
- (If a certificate is used as the authentication method) Certificate file and private key file for the IPsec VPN Client
- (If a password is used as the authentication method) Password file for the VPN Client

> If you use your own script, use the same destination file names for the certificate and the private key as in the example script — client.crt and client.prv.

Install the VPN Client in silent mode

You can install the VPN Client silently with a command-line script.

Task

1. Open a command prompt as an administrator.
2. Run the script and enter the parameters according to the selected authentication method:
   - If you use a certificate (Example Script 1), enter:

     ```
     script.bat <INSTALLER.EXE> <CERTIFICATE> <PRIVATE_KEY> <GW_CONTACT_INFO_FILE>
     ```

   - If you use a password (Example Script 2), enter:

     ```
     script.bat <INSTALLER.EXE> <PASSWORD> <GW_CONTACT_INFO_FILE>
     ```

When the installation is finished, VPN Client has been configured for use in automated mode. It starts automatically and tries to establish a VPN to the gateway.

If the number of VPN Clients is large, it might be necessary to adjust the default connection retry times.

See also

Connection retry times in automated mode on page 44
Error handling in automated mode on page 45
How automated mode affects the user interface on page 41

Connection retry times in automated mode

If the VPN Client is used in automated mode, it automatically tries to reconnect to the VPN gateway if the VPN connection is lost.

The default connection retry times for the automated VPN Client are:

- Minimum connection retry time: 3 seconds
- Maximum connection retry time: 192 seconds.

In installations that have many automated VPN Clients, it might be necessary to adjust the default connection retry times. Changing the connection retry times might be useful to ensure connectivity after network outages, for example. To adjust the default connection retry times, edit the retryconf.txt file and save it to the directory ALLUSERSPROFILES\Application Data\McAfee\McAfee VPN Client \retryconf.txt. The VPN Client must be installed before you can save the retryconf.txt file to the directory.

The syntax for adjusting the connection retry times using the retryconf.txt file is the following:

<min>minimum connection retry time in seconds</min>

<max>maximum connection retry time in seconds</max>

<rnd>percentage of randomness in connection retry time</rnd>

The default connection retry time is an increasing multiple of the minimum connection retry time, but it does not exceed the maximum connection retry value. The randomness percentage adds time*rnd(-1.0 .. 1.0)*percentage/100 to the connection retry time during each attempt. However, the connection retry time never exceeds the maximum connection retry time or goes below the minimum connection retry time.

Unless specified in the configuration file, the randomness percentage is not used. If the retryconf.txt file does not exist in the directory, the default connection retry times are used.

Error handling in automated mode

If errors occur in VPN connections, the VPN Client automatically attempts to recover. There are two types of errors — unrecoverable and recoverable.

Unrecoverable errors

Unrecoverable errors cannot be resolved automatically and require user interaction.

If the VPN Client encounters an unrecoverable error, it shuts down and does not attempt a restart. Unrecoverable errors include:

- A required certificate, private key, or gateway information file is missing or contains invalid information.
- The private key is encrypted and requires entering a passphrase.
- The password file is incorrectly formatted or contains incorrect information (for example, there is a typo in the user name or password).

Recoverable errors

Certain types of errors are recoverable and do not require user interaction.

When the VPN Client encounters a recoverable error, it automatically tries to establish a new VPN connection to the gateway. Depending on the error, the next connection attempt is either a normal connection to the next gateway endpoint or an initial connection.

The VPN Client tries to make a normal connection when the following errors occur:

- Any connection state fails due to a recoverable error.
- Gateway connectivity problems have been detected (dead peer detection).

The VPN Client tries to make an initial connection when the following errors are encountered:

- Configuration load fails. A failure can happen if the VPN Client receives an invalid configuration file from the gateway.
- The VPN Client has already attempted to connect to all gateway endpoints to solve the error.

When an error that does not require an initial connection occurs, the VPN Client always tries to connect to the next gateway endpoint. When an initial connection is required, the VPN Client starts the connection attempts from the first gateway endpoint specified in the gateway information file. If the configuration file is not retrieved from the gateway, the VPN Client attempts to connect to the next gateway endpoint.

If an initial connection is required to recover from an error, the VPN Client usually waits for 3 seconds before initiating the connection. If the initial connection fails, the delay before the next connection attempt increases exponentially — 3 s, 6 s, 12 s, up to a maximum of one hour.

If the number of VPN Clients is large, it might be necessary to adjust the default connection retry times.

See also

Connection retry times in automated mode on page 44

Index

A

about this guide 5
addressing, virtual IP 8
authenticating
- certificates 19
- method 10

automated mode 41

C

certificate request
- advanced 21
- basic 21
- passphrase 21
- signed 22

certificates
- authenticating 19
- configuring 19
- CRL checks 26
- deleting 26
- details 25
- expiration 26
- external 23
- import 22, 23
- internal 20
- options 19
- passphrase 24
- signed 22

checksum 14
client MAC, troubleshooting 33
client MTU, troubleshooting 33
client, VPN
- upgrade 17

connections
- retry times 44
- settings 8
- troubleshooting 32

contact information, gateway
- export 15
- save 15

conventions and icons used in this guide 5
CRL checks 26

D

delete certificates 26
diagnostics 29
documentation
- audience for this guide 5
- product-specific, finding 6
- typographical conventions and icons 5

dump files 31

E

errors, automated mode
- recoverable 45
- unrecoverable 45

expiration, certificates 26
export, contact information 15
external certificates 23

G

gateway
- client 9
- contact information 15

I

identities, user 20
import
- certificate 22, 24
- PKCS #12 file 23
- private key files 24

installation
- checksum 14
- command line 16, 39
- custom 10, 15
- custom scenario 35
- executable 10
- file types 10
- files 14
- interactive vs. silent 9
- options 9
- remote 10
- scripts 42
- silent 44
- standard 10
- transform file 16, 39

installation *(continued)*
- using the wizard 14

internal certificates 20

L

logs
- accessing 29
- collecting 29
- reading 30

M

McAfee ServicePortal, accessing 6

Microsoft Installer file
- edit 36
- silent installation 10
- VPN Client file name 10

MTU 33

P

passphrase, change 24

PKCS #12 file 23

R

retry settings 32, 44

S

ServicePortal, finding product documentation 6

settings
- retry 32, 44
- VPN 8

split tunneling 8

T

technical support, finding product information 6

traffic, network
- capture 31
- customize 31
- dump files 31

transform files
- create 36
- edit 37
- install 16, 39
- save 38

troubleshooting
- connections 32
- logs and diagnostics 29
- MAC address 33
- MTU 33

U

upgrade 17

user identities 20

V

Virtual Adapter 8

virtual IP addressing 8

VPN
- automated 9, 41
- client configuration 7
- gateway 7, 9

VPN ports 32