Alcatel·Lucent

IPSec Client User's Guide

Security Statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of access features.

Additional Product information and Training

The most up-to-date product information is available online at https://service.esd.alcatel-lucent.com/ and https://support.alcatel-lucent.com/portal/olcsHome.do.

The most up-to-date computer-based training is available online at https://training.alcatel-lucent.com/Saba/Web/Main.

IPSec Client User's Guide

Contents

Introducing Alcatel-Lucent IPSec Client

1

Welcome to Alcatel-Lucent IPSec Client Release 10

Alcatel-Lucent IPSec Client enables secure communications between your computer and a remote network. IPSec Client can authenticate you to the remote network and encrypt the information you send to and decrypt the information you receive from the remote network, which enables you to use the Internet for secure communications. The encrypted pathway is called a tunnel and the end-to-end connection is called a virtual private network (VPN).

For information about new features and known issues in this software release, refer to the release notes provided with the software.

VPNs, Tunnels, and Secure Networking

A VPN is simply a path through a network, for example, between a laptop computer in your home, across the Internet, to a VPN gateway at your corporate home office. Behind the VPN gateway (also called the tunnel endpoint) are the enterprise servers and other computers that you access to transact business. Although the packets of information travel through the unsecured pathways of the Internet, the two tunnel endpoints employ data encryption, which makes the communications secure.

What is IPSec?

IPSec (Internet Protocol Security) is a set of extensions to the IP protocol family. It provides cryptographic security services. These services allow for authentication, integrity, access control, and confidentiality.

IPSec is a developing standard for security at the network or packet processing layer of network communication. It defines how to create secure communications over a publicly accessible network. IPSec provides two types of security:

■ Authentication — A method that allows the two endpoints of a tunnel to verify their identity to each other.

■ Encryption — A method of changing the data portion of a packet so that its contents are unintelligible unless you have the correct key to decrypt the data.

Installing IPSec Client

2

Before You Begin

Before you begin the installation, make sure your computer is equipped with the necessary hardware components and software programs to run IPSec Client properly.

Requirements

You can install *IPSec Client* on a computer that meets any of the following installation environments:

■   Windows XP with Service Pack 2 or above

–   Processor: Pentium II 300 MHz or higher

–   Memory (RAM): 64 MB (minimum); 128 MB (recommended)

–   Free hard drive space: 16 MB

■   Windows Vista Business, Enterprise, or Ultimate Editions with Service Pack 1

–   Processor: 1 GHz 32-bit (x86) or 64-bit (x64)

–   Memory (RAM): 1 GB of system memory

–   Free hard drive space: 40 GB hard drive with at least 15 GB of available space

–   CD-ROM or DVD drive

Check the documentation that comes with your computer if you are not sure if it is properly equipped. You can also double-click on the System icon in the Windows Control Panel.

To see if you have enough disk space available, select the appropriate disk drive in the Windows Explorer. The amount of free disk space is displayed at the bottom of the window.

Note: IPSec Client 10 is no longer supported on Windows platforms prior to Windows XP and any server operating system.

Installing IPSec Client

The procedure below explains how to install Release 10 of IPSec Client on your computer.

Note: IPSec Client 10 cannot be upgraded from earlier versions of IPSec Client. Earlier versions of IPSec Client must be manually uninstalled before installing IPSec Client 10.

Note: Because the Windows Firewall blocks a VPN gateway IKE rekey and other administrative activities messages, IPSec Client adds an application rule to the Windows Firewall exceptions list to allow the VPN gateway Brick to send messages to IPSec Client. During the IPSec Client installation process the user is prompted with the message **IPSec Client installation needs to add a rule to Windows Firewall**. Click the OK button when this prompt is displayed.

1   To install IPSec Client from the CD-ROM, insert the CD-ROM into the computer's CD-ROM drive and close the door. Installation begins automatically.

   To install IPSec Client from a network drive, locate the file **ipsec-10.0.exe** and then double-click it.

   If you are installing IPSec Client from an intranet web interface, click the link and then respond to the prompts on the screen.

2   The first window displayed is the **Choose Destination Location** window, which allows you to select the directory in which the IPSec Client files will be installed. We recommend you accept the default directory.

Once the installation is complete and your computer restarted, you are ready to begin using the IPSec Client.

Starting IPSec Client

The installation program adds an entry to your Windows Start menu. Launch IPSec Client from the Start menu to configure a new tunnel or connect through an existing tunnel.
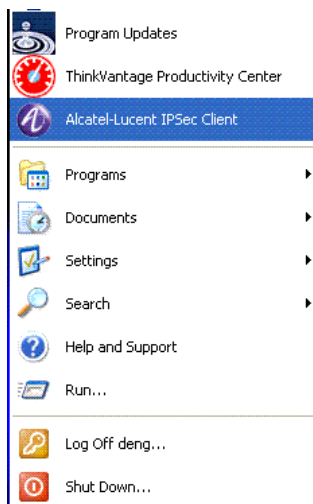
The installation program also puts an icon in the area of the task bar known as the tray, which can be displayed along the bottom or vertically along the right side of your Windows desktop.

The icon that is displayed depends on several factors:

- **Non-Block All**. If the IPSec Client internal firewall policy is set to **Allow All Traffic** or **Allow Client Initiated Traffic**, the icon is displayed as follows:

- **Block All**. If the IPSec Client internal firewall policy is set to **Block All Clear Text Traffic** a lock icon is displayed as follows:

Note: For Windows Vista x86 and Vista x64, the TrayIcon application will be blocked by Vista's User Account Control (UAC) like other applications, and it is added to the **Blocked Startup Program** list. The **Blocked Startup Program** Taskbar Icon may blink after the machine is rebooted. The application can be launched either by clicking the Taskbar Icon, or from the Windows Startup menu.

Uninstall IPSec Client

To uninstall IPSec Client:

1 On the Windows task bar, click **Start > Settings > Control Panel** to open the Windows Control Panel.

2 In Windows XP, open the **Add/Remove Programs** window, double-click **Add/Remove Program**; in Windows Vista, click **Uninstall a program** under the Programs applet.

3 Locate IPSec Client in the program list and click it to select it. The default name is Alcatel-Lucent IPSec Client.

4 In Windows XP click **Remove**, in Windows Vista double-click, and then click **OK** in the pop-up confirmation box to remove IPSec Client.

5 Reboot your machine.

Using IPSec Client

Once you have installed the required software and restarted your computer you are ready to begin using IPSec Client to enable a VPN tunnel. The following information explains how to set up and enable tunnels and how to configure IPSec Client for your operating environment.

Tunnels

A tunnel establishes secure communications between two points to form a Virtual Private Network (VPN). Your tunnel or network administrator must provide the information that you enter the first time you enable a tunnel. After you have enabled a tunnel for the first time, you can reuse it.

Before you can enable a new tunnel, you need connection information about the network you are connecting to. The information your VPN network administrator must provide depends on whether or not you will be using a digital certificate. For security reasons, you cannot enable a tunnel until your identity has been authenticated. A user ID and a digital certificate is one way to establish your credentials. A digital certificate is an electronic "ticket" issued by a trusted Certificate Authority that establishes that you are who you say you are. If you do not use a digital certificate, you must specify a user ID, a password, and a group key to establish your identity.

Enabling a New Tunnel

To enable a new tunnel, you need the following:

■ The IP address of the tunnel endpoint (the network you want to connect to)

■ A valid user name and password on the destination network

■ A Group Key (an alphanumeric value provided by your network administrator)

Note: The Password and Group Key are case sensitive.

■ Optionally, a digital certificate

If your network policies require a digital certificate (a file that verifies your identity), you must have already obtained the certificate files from your network administrator and installed them on your computer. (See "Obtaining a Digital Certificate" on page 14.)

To enable a new tunnel:

1   On the Windows **Start** menu, click the IPSec Client icon.
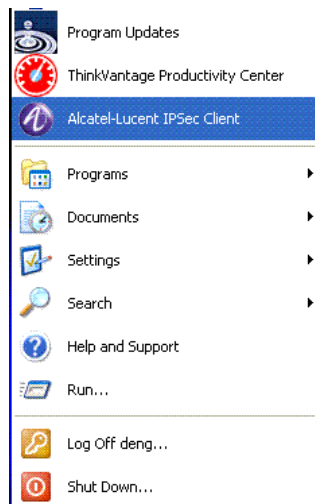
2   On the IPSec Client menu bar, click **Secure Connection > Enable New**, or right-click the client window and then click on **Enable New** to open the Enable Secure Connection dialog.

3   Enter the following information:

Tunnel Name — A name to identify this tunnel, up to 20 characters.

Primary Tunnel End Point — The tunnel endpoint IP address given to you by your VPN network administrator. If your VPN network administrator gave you a backup address, enter that in the **Secondary Tunnel End Point** field.

User Identity — The user ID your VPN network administrator gave you. If you are using a Digital Certificate, enable the Digital Certificate check box to display a Browse button. The User Identity box is then changed to a Certificate File box. Click the Browse button to select your digital certificate.

Password — The password your VPN network administrator gave you. If you are using a SecurID token, enter your PIN followed by the current token number.

Group Key — The group key your VPN network administrator provided. The Group Key box is not used if you are using a Digital Certificate.

4   If the **Save Password** check box is available, you can save your password by enabling the check box.

When enabled, the Save Password feature enables you to activate this tunnel without entering your password each time. If the check box is dimmed, your VPN network administrator has disabled this feature.

Note: If you are using a SecurID token, *do not* enable the Save Password box. Because a SecurID token number changes, you must enter the tunnel password manually each time you enable the tunnel.

5   If your VPN network administrator indicated that this tunnel uses UDP encapsulation, do the following:

a   Click **Advanced...** button to open the Advanced Connection Options dialog.

       b   In the **Connect via** box, select **UDP-Encapsulate**.

       c   Change the UDP Port if your VPN network administrator has given you a port other than 501. All ports from 1 - 65535 (except 500) are valid.

       d   Click **OK**.

6   Click **Enable** to enable the tunnel.

When the tunnel has been successfully enabled, a window is displayed to verify that the tunnel has been enabled. The entry in the IPSec Client window shows the name of the tunnel, the user ID you entered when enabling the tunnel, and the primary and secondary tunnel endpoints. An asterisk indicates the active endpoint.

The Status column shows that the tunnel is Enabled. If you disable the tunnel, no entry is displayed in the Status column.

In addition, the logo in the task bar changes depending on the firewall policy.

You can leave the IPSec Client window open, minimize it, or close it completely — you do not need to keep the window open to keep the tunnel enabled. If you minimize the IPSec Client window, an icon representing IPSec Client is displayed in the Windows task bar.

Once the tunnel is enabled, you can log into your company's network and transact business securely. You can access network resources through a browser, or by using a non-browser based network utility such as FTP or TELNET.

Enabling an Existing Tunnel

To enable an existing tunnel:

1   Start IPSec Client. On the Windows **Start** menu, click the IPSec Client icon.
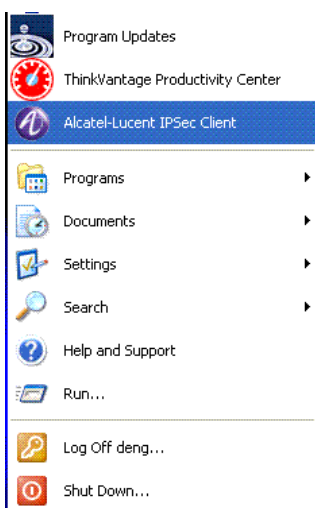
2   Double-click the name of the tunnel you want to enable.

or

Click the tunnel to highlight it. On the menu bar, click **Secure Connection > Enable,** or right-click the highlighted tunnel and then click **Enable** to open the **Enable Secure Connection** dialog.

3   If you clicked the **Save Password** check box when initially enabling this tunnel, your password is displayed in the **Password** field, and you do not have to enter it. If you did not activate the Save Password feature, enter your password in the **Password** field.

4   Click **Enable**.

5   Click **OK** to dismiss the verification window. The tunnel is displayed in the IPSec Client window with **Enabled** in the **Status** column.

Re-enabling a Tunnel

Your VPN network administrator can limit the amount of time that a tunnel can remain enabled. A message is displayed on your screen five minutes before a tunnel is scheduled to expire. You can re-enable the tunnel during this five-minute period.

To re-enable a tunnel prior to timeout:

1   On the Alcatel-Lucent IPSec Client window, click the name of the tunnel once to highlight it.

2   On the menu bar, click **Secure Connection > Enable**, or right-click the highlighted tunnel and then click **Enable**.

3   If you enabled the **Save Password** check box when you initially enabled this tunnel, your password is displayed in the Password box, and you do not have to enter it. If you did not activate the Save Password feature, enter your password in the **Password** box.

4   Click **Enable**.

    A window message is displayed to indicate that the tunnel has been successfully enabled. Note that the tunnel has a new expiration date and time.

Disabling a Tunnel

To disable an active tunnel:

1   On the Alcatel-Lucent IPSec Client window, double-click the name of the active tunnel you want to disable to open the Disable Secure Connection window. Alternatively, single-click the active tunnel you want to disable and select **Secure Connection > Disable** on the menu bar or right-click the highlighted tunnel you want to disable.

2   Click **Disable**. A window is displayed indicating the tunnel has been disabled.

3   Click **OK** to dismiss the pop-up window and complete the disable process.

Deleting a Tunnel

Once a tunnel is enabled, it remains in the IPSec Client window, even if it is inactive. If a particular tunnel is no longer used, you might want to remove it from the IPSec Client window.

To delete a tunnel:

1   On the Alcatel-Lucent IPSec Client window, click the name of the tunnel once to highlight it

2   On the menu bar, click **File > Delete**.

Save and Restore Tunnel Configurations

To save or restore tunnel configurations:

1   Click **File > Tunnel Configuration > Save** to save a tunnel configuration.

2   Click **File > Tunnel Configuration > Restore** to restore a tunnel configuration.

Digital Certificates

A digital certificate provides identification in the electronic world. Issued by trusted third parties called Certification Authorities (CA), digital certificates cannot be forged or tampered with. The Certificate Authorities keep track of the digital certificates to enable users to access network resources in a secure confidential manner. You install the digital certificate on your computer. The digital certificate verifies your identity when you enable a VPN tunnel.

Digital certificate authentication is optional in Alcatel-Lucent IPSec Client. If you do not receive a digital certificate from your VPN network administrator, you must use a Group Key instead.

Alcatel-Lucent IPSec Client 10 supports X.509 compatible digital certificates. There are two ways to specify a digital certificate in the current release.

■   Windows CAPI Store-A digital certificate can be saved in the Windows CAPI Store, either in the Current User Store or the Local Machine Store. The preference is the Local Machine Store.

■   PKCS# 12 file-The digital certificate can also be saved as a file. The file is in PKCS# 12 format file (.p12) or in .pfx file.

Note: Cross and subordinate CAs are not supported in the current release.

Note: The PKCS# 12 file should contain the CA certificate.

Note: The certificate should have the Subject Alternative Name (the RFC822 name, or the email) attribute.

Using a Digital Certificate to create a VPN Tunnel

Except the commonly used pre-shared key (Group Key), a digital certificate also can be used for establishing a VPN tunnel. As shown in the below picture, a .p12 (PKCS#12) digital certificate is used. The User Identity and Password fields are automatically updated with the Email and DN attributes of the certificate.

Enable Secure Connection

Tunnel Name: Test_cert_auth
Primary Tunnel End Point: 192.168.1.100
Secondary Tunnel End Point:
User Identity: test-user2@alcatel-lucent.com
Password: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Group Key:

☑ Digital Certificate   Certificate ...
☐ Save Password

Enable   Advanced...   Cancel

Info
Please enter a valid User Identity
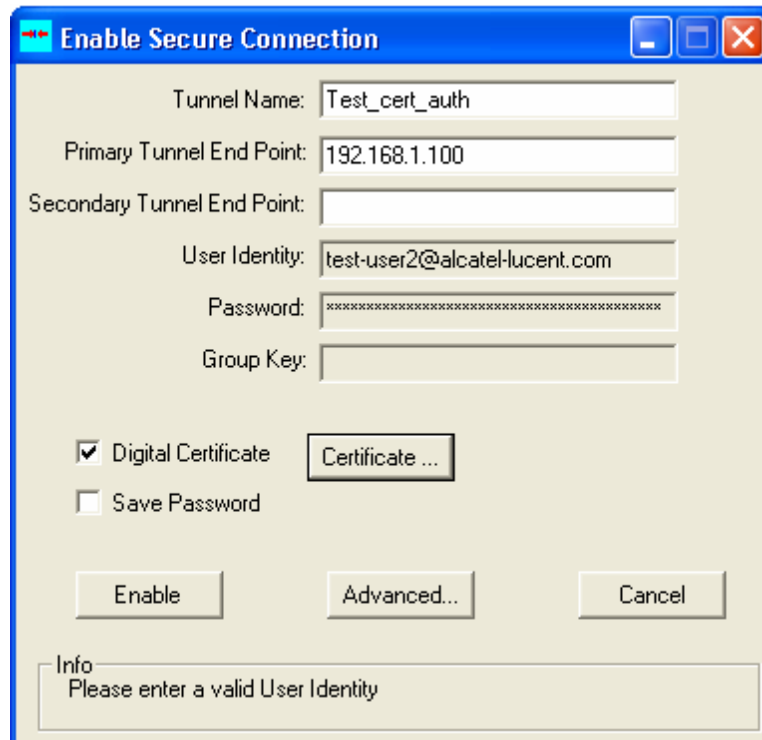
Certificates Store (CAPI Store)

In Alcatel-Lucent IPSec Client, a digital certificate can be saved to and retrieved from the Windows Certificate Store. To browse the contents of the certificate store, use certmgr.msc snap-in. The digital certificate store is also called CAPI Store. There are two ways to save your digital certificate into the CAPI Store:

■ Web based digital certificate enrollment. Details are provided later.

■ Import a PKCS #12 (.p12 or .pfx) certificate file.

Obtaining a Digital Certificate

Generally, there are two ways to obtain a digital certificate:

■ The digital certificate can be provided to you by your VPN network administrator. Your VPN network administrator will provide a file and password for .p12 that must be copied into a directory on your hard drive. It is recommended that you import the certificate by double-clicking the file. You can also use your Internet browser (Microsoft IE) or other tools to import it to the CAPI Store. Launch IE Browser, click menu **Tools->Internet Options->Content**, and then click the **Certificate** button to open the Certificates utility to Import the certificate.

■ Web-based enrollment. If your VPN network administrator provides the certificate enrollment web site URL, get your digital certificate as follows (Using VeriSign as an example):

ENROLL
Choose this option to enroll for a client Digital ID.

• **Click this link to enroll for an IPSec Digital ID for a VPN device**

PICK UP ID (Client certificates)
Choose this option if you enrolled for a Digital ID but did not pick it up.

Step 1: Click the **ENROLL** link to open the VeriSign Enrollment web page, then fill and submit the form.

After you submit the form, you may get a E-mail response from your VPN network administrator confirming your request. Your administrator eventually either approves or rejects your request based on the information you provided in your request form and the policy configured in your organization.

Following approval, your administrator will send you a E-mail containing a PIN number and a URL from where to Pick up your digital certificate.
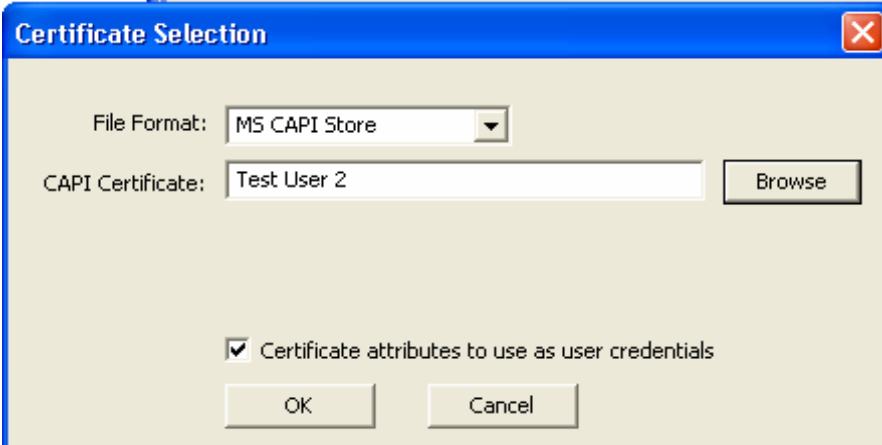
Step 2: On the PICK UP ID web page, type in the PIN number and submit the form. The digital certificate will then be automatically installed into your CAPI Store.

Note: Your VeriSign digital certificate must be exportable and must be installed on your machine (CAPI Store).
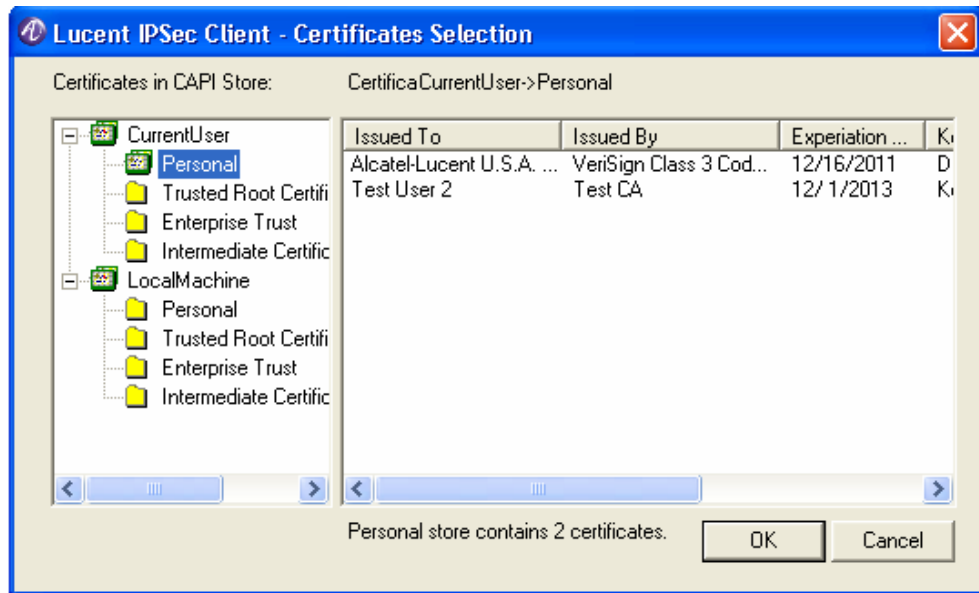
Using a Digital Certificate from CAPI Store

In order to select a certificate in the Windows CAPI Store, you must check the **Digital Certificate** check box, and then click the **Certificate** button on the **Enable Secure Connection** dialog box shown above to display the **Certificate Selection** dialog box as displayed below.
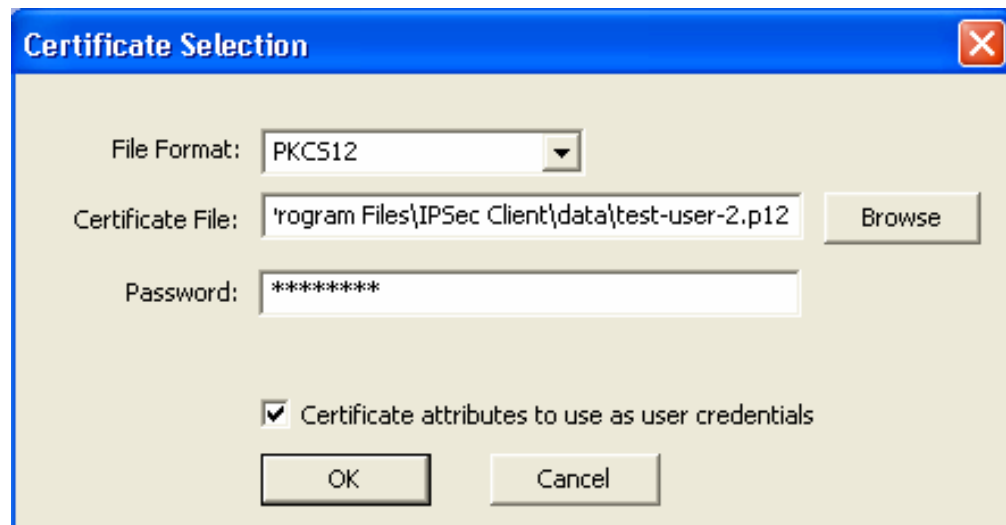
Use the Browse button to select a digital certificate from CAPI Store:

Using a Digital Certificate File

You can use the certificate file .p12 (.pfx), like using a digital certificate in the CAPI Store, by selecting **PKCS12** file format in the **Certificate Selection** dialog box as shown:

IPSec Client Personal Firewall

IPSec Client includes an internally built-in firewall. A firewall can help protect your computer from unwanted intrusion when it is sending and receiving traffic **outside** a tunnel. If you enable the firewall when no tunnel is enabled, the firewall filters all traffic to and from your computer.

When no tunnel is enabled, all traffic to and from your computer is in clear text form, that is, unencrypted, and susceptible to interception or attack.

If you enable the firewall when a tunnel is enabled, the firewall filters only the traffic that does not go through the tunnel. There is, of course, no need to filter traffic through the tunnel, since the tunnel traffic is encrypted, and therefore secure.

You can set the type of filtering for the IPSec Client firewall:

■ **Block All Clear Text Traffic** — The firewall drops all traffic to and from your computer that does not go through a tunnel. Traffic within the tunnel is allowed. This means that if no tunnel is enabled, your computer cannot communicate with any other device.

 When you select this option, the tray icon becomes:

■ **Allow All Traffic —** The firewall allows all inbound and outbound sessions to reach your computer, and, therefore, offers no protection.

 When you select this option, the tray icon becomes:

■ **Allow Client Initiated Traffic —** The firewall allows all outgoing sessions and any return sessions that are generated, but it blocks all unsolicited inbound sessions. This means you could, for example, surf the Web and still be protected from external attack.

 When you select this option, the tray icon becomes:

Note: Your VPN network administrator can specify different setting which take effect when you enable the tunnel. The Firewall policy setting in your tunnel policy override your local Firewall settings.

Note: For Windows Vista x86 and Vista x64, the TrayIcon application will be blocked by Vista's User Account Control (UAC) like other applications, and it is added to the **Blocked Startup Program** list. The **Blocked Startup Program** Taskbar Icon may blink after the machine is rebooted. The application can be launched either by clicking the Taskbar Icon, or from the Windows Startup menu.

Setting Built-in Firewall Filtering

The IPSec Client includes a built-in firewall with basic features. To set IPSec Client firewall filtering:

1   Start IPSec Client. On the Windows **Start** menu, click the IPSec Client icon to open the IPSec Client window:
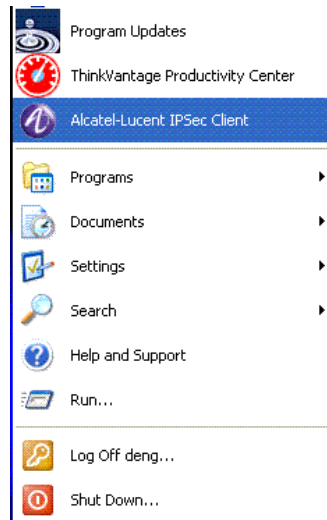
2   On the menu bar, click **Firewall**, and then click one of the following menu items:

■   **Block All Clear Text Traffic** — The firewall drops all traffic to and from your computer that does not go through a tunnel. Traffic within the tunnel is allowed.

When you select this option, the tray icon becomes:

■   **Allow All Traffic —** The firewall allows all inbound and outbound sessions to reach your computer, and, therefore, offers no protection.

When you select this option, the tray icon is becomes:

■   **Allow Client Initiated Traffic —** The firewall allows all outgoing sessions and any return sessions that are generated, but it blocks all unsolicited inbound sessions. This means you could for, example, surf the Web and still be protected from external attack.

When you select this option, the tray icon becomes:

IPSec Client Logging

IPSec Client logs tunnel activity to a file on the local drive. You can customize the type of information that is logged to the file and view, search, and save the contents of the log file. You can also activate a firewall log file to track the activity monitored by the firewall.

The IPSec Client log viewer window can act as a stand-alone application, that is, you do not need to have the IPSec Client window open to display the log file.

The log file, logipsec.log, is allowed to reach a defined size or age (1 Mb or seven days) before it is saved to a backup file (replacing the previous backup file) and a new empty file is created.

Saving, Printing Log Files

The log file viewer enables you to save log information to a new file and to print the log.

To access log file functions:

1   Open the log viewer.

    On the IPSec Client menu, click **File > IPSec Client Log**

2   On the log viewer menu bar, click the **File** menu, and then click the appropriate item.

Setting the Logging Level

To set the log file logging level:

1   Open the log viewer.

    On the IPSec Client menu, click **File > IPSec Client Log**

2   Click **Options > Configure** to open the **Log Event Level** dialog.

3   Choose a new logging level:

    Low: Reports fatal and critical error conditions

    Medium: Reports fatal and critical error conditions, warnings and information messages, and enables firewall logging

    High: Reports fatal and critical error conditions, warnings and information messages, enables firewall logging, and trace and debug messages

Note: Logging level changes are dynamic. They take effect immediately.

Viewing a Log File

To view the log file, on the IPSec Client menu, click **File > IPSec Client Log.**

To view the most recent logging information, **IPSec Log Viewer** provides two menu items within the **File** menu; **Clear** and **Refresh**. The **Clear** command clears the **Log Viewer** window, and the **Refresh** command reads the **IPSec Log** file again and displays the logging information. The **Highlight Error Messages** command highlights all error logging messages in the view window.

Searching a Log File

To search the log file:

1   Open the log viewer.

    On the IPSec Client menu, click **File > IPSec Client Log.**

2   On the on the menu bar, click **Search**.

IPSec Client Advanced Configuration

Your networking environment might require some special configuration. Before using any of the following IPSec Client features, see your VPN network administrator.

Logging onto a Windows Domain

If your computer environment makes use of Windows network domains, and you are working from home, or hotel, and you want to login to a domain, you must follow a special procedure to log onto your Windows domain.

Note: IPSec Client does not support Windows Domain logon using Windows XP Home Edition.

To logon to a Windows domain:

1   Start your computer and log in locally. Enter your local User ID and password, and then logon to your computer.

2   Enable a tunnel, using the standard procedure.

3   Log off.

4   Using your domain credentials, including the domain name, logon again.

Using the Command Line Interface

The command line interface (CLI) enables you to create and configure tunnels by using a script or a Command Prompt window instead of the using the IPSec Client graphical interface. The CLI includes just one command that can take a number of arguments.

Command format:

lucentipsecclient -arg1 -arg2 -arg3 ...

The usage of the CLI help dialog is displayed when the dos command *lucentipsecclient.exe -h* command is run.
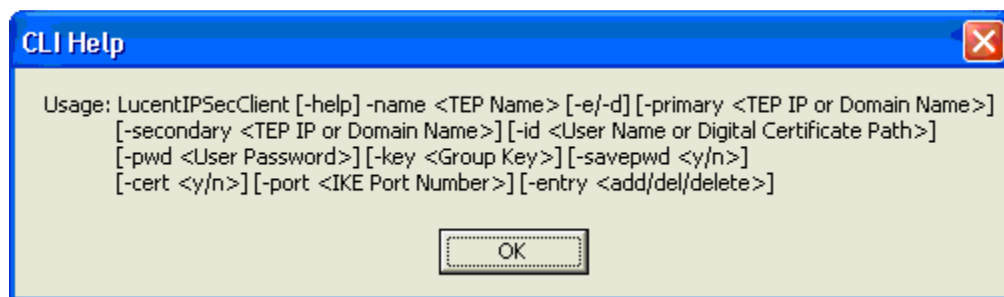
The command arguments are explained in the table below. Remember to enter a space after each argument.

Table 1   CLI Command Arguments

Argument	Description
-e	Enable the specified tunnel
-d	Disable the specified tunnel
-name	The name of the tunnel. For example: lucentipsecclient -name my_tunnel
-primary	The IP address of the primary tunnel endpoint. For example: lucentipsecclient -primary 192.168.123.32 If you are using a fully qualified domain name, enter that instead. For example: lucentipsecclient -primary tunnels.lucent.com
-secondary	The IP address of the secondary tunnel endpoint, if the tunnel has one. For example: lucentipsecclient -secondary 192.168.123.33 If you are using a fully qualified domain name, enter that instead. For example: lucentipsecclient -secondary tunnels2.lucent.com
-id	The User ID. For example: lucentipsecclient -id diane_weber If you are using a digital certificate, enter the full path to the folder containing the .ini file you used to obtain the certificate. For example: lucentipsecclient -id c:\Program Files\IPSec Client\Data **Note:** If you are using a digital certificate, you must also use the -cert argument (see below).
-pwd	The account password. For example: lucentipsecclient -pwd my_password-135
-key	The group key. For example: lucentipsecclient -key our_group_key-790

Table 1   CLI Command Arguments

Argument	Description
-savepwd	The answer to the 'Save password?' prompt. Enter y to save the password so that it does not have to be entered each time the tunnel is enabled. Enter n (or omit this option) and the password will have to be entered each time. For example: lucentipsecclient -savepwd y
-cert	Indicates the presence of a digital certificate. If you indicated a digital certificate when entering the -id argument, you must also use -cert. For example: lucentipsecclient -cert y
-port	Indicates the use of UDP encapsulation. For example: lucentipsecclient -port 63123 All ports from 1 - 65535 (except 500) are valid.
-entry	Add a tunnel configuration without enabling the tunnel, or remove a (or all) tunnel configurations if the tunnel is not enabled. For example: -- Add an entry lucentipsecclient -entry add -primary 192.168.123.32 -name my_tunnel -- Delete an entry lucentipsecclient -entry del -name my_tunnel -- Delete all entries lucentipsecclient -entry del -name *

Downloading a New Release

When a new release of the IPSec Client is available, you may be notified automatically. Depending on how your VPN network administrator sets up the notification system, you receive notification either when you enable a tunnel or immediately after disabling a tunnel.

■   Inside a Tunnel — If your VPN network administrator wants you to download the new software while you have a tunnel enabled, you receive a message immediately after you enable a tunnel. The message prompts you to download the new version immediately or download it later. If you click **Yes** to download the software immediately, a browser is displayed with instructions to guide you through the download process. If you click **No**, the **Download** option on the **File** menu becomes active. When you are ready to download the new release, select that option and follow the on-screen instructions.

■   Outside a Tunnel — If your VPN network administrator wants you to download the new software outside a tunnel, you receive a message immediately after you disable a tunnel. A message prompts you to download the new version immediately, or download it later.

Click **OK** to download the software immediately. If you click **No**, the **Download** option on the **File** menu becomes active. When you are ready to download the new release, select that option and follow the on-screen instructions.

Troubleshooting IPSec Client   4

IPSec Client can generate error messages to help you troubleshoot problems. The log viewer can also help you track issues within IPSec Client. The log viewer can display messages that are received from outside of IPSec Client. For example, a RADIUS server can include a message when it rejects a login attempt.

Error Messages

Another secure connection is currently active

IPSec Client does not allow you to enable two tunnels at the same time, even to different endpoints. If you attempt to enable a second tunnel while a first is still enabled, the following error message is displayed:
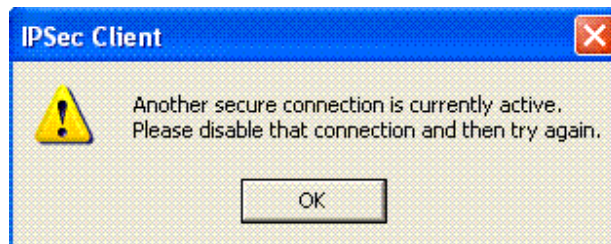
Authentication will time out in 5 minutes for tunnel <tunnel_ name>

This message is displayed five minutes before the tunnel expiration time. To keep the tunnel enabled, re-enable it within the five-minute period.

Secured tunnel time elapsed for tunnel <tunnel_name>, Please re-enable later

This message is displayed when the tunnel timeout period expires. If you still need the tunnel, you must re-enable it.

Lost connectivity to tunnel <tunnel_name>, Please re-enable later

This message is displayed if connectivity to the tunnel endpoint is lost. Once the problem that caused the lost connectivity is solved, you can re-enable the tunnel.

Secured session for tunnel <tunnel_name> ended due to inactivity

Your VPN network administrator can set a time limit on tunnel inactivity. If you do not send or receive data through the tunnel for that period of time, the tunnel expires.

This message is displayed after a tunnel has expired for that reason. To find out the inactivity time period, contact your VPN network administrator.

Could not signal LucentIKE or load security policy

If this error is displayed when enabling a tunnel, it usually means one of the IPSec Client services is not running. Restart your computer and re-enable the tunnel. If the problem persists, contact your VPN network administrator.

Error communicating with LucentIKE

If this error is displayed when enabling a tunnel, it usually means one of the IPSec Client services is not running. Restart the computer and re-enable the tunnel. If the problem persists, contact your VPN network administrator.

Driver is not Installed. Try re-installation.

If this message is displayed, uninstall and reinstall the IPSec Client program. If the message repeats, call your VPN network administrator.

Invalid internal IP for local presence received from Gateway

If this message is displayed, the internal IP address is invalid because:

It is not part of the Host Access List. Contact your VPN network administrator to correct the tunnel configuration.

or

It is on the same subnet as one of the physical adapters in you machine. You can disable the adapter in conflict either permanently or temporarily (create separate hardware profile) from the current hardware profile. If the problem persists, contact your VPN network administrator to change the local presence IP address pool.

Unable to update local network configuration

IPSec Client could not determine the IP address configuration of your PC. For example, the combination of IP Address and subnet mask is invalid. All of the bits in the host address portion of the IP address are set to 0 or 1. Contact your VPN network administrator to correct the tunnel configuration.

Index

U

UDP encapsulation 10
User Identity 10

V

VPN
    defined 3

W

Windows CAPI Store 13