lenovo

Lenovo ConstantConnect and Protect 2.0 User Guide

Lenovo ConstantConnect and Protect 2.0 User Guide

Note

Before reading this book and using the product it supports, be sure to read the warranty information in Appendix F, "Notices," on page 61.

Contents

PDF created with pdfFactory trial version www.pdffactory.com

About this book

This book provides information about installing, configuring, and troubleshooting Lenovo ConstantConnect and Protect.

How this book is organized

Chapter 1, "Introducing ConstantConnect and Protect," on page 1: This chapter presents an overview of ConstantConnect and Protect and its system requirements.

Chapter 2, "Installing and uninstalling ConstantConnect and Protect," on page 9: This chapter presents instructions for installing and uninstalling ConstantConnect and Protect.

Chapter 3, "Working with Windows Firewall and AT&T VPN Client," on page 11: This chapter describes how to work with Windows Firewall and AT&T VPN Client after you install ConstantConnect.

Chapter 4, "Configuration scenarios," on page 13: This chapter describes how to configure the BlackBerry smartphone, BlackBerry Enterprise Server, Microsoft Exchange Server, Microsoft Office Outlook, and ConstantConnect.

Chapter 5, "Sending and receiving e-mails," on page 19: This chapter presents information on how ConstantConnect synchronizes e-mails in different conditions.

Chapter 6, "Configuring ConstantProtect security," on page 23: This chapter describes how to configure ConstantProtect security through your Web browser.

Appendix A, "Troubleshooting," on page 37: This appendix presents troubleshooting hints and tips if you encounter any problems with ConstantConnect.

Appendix B, "Service and Support," on page 43: This appendix describes the technical support that is available for the Lenovo ConstantConnect and Protect.

Appendix C, "Lenovo Limited Warranty," on page 49: This appendix contains warranty information.

Appendix D, "Electronic emission notices," on page 55: This appendix contains the Federal Communications Commission Emission Notice.

Appendix E, "Important information for the European Directive 2002/96/EC," on page 59: This appendix contains information about the Waste Electrical and Electronic Equipment (WEEE) Directive.

Appendix F, "Notices," on page 61: This appendix contains legal and recycling information.

Appendix G, "Hardware specifications," on page 63: This appendix contains the ConstantConnect and Protect hardware information.

Notices used in this book

This book contains the following notices designed to highlight key information:

v **Notes:** These notices provide important tips, guidance, or advice.

v **Attention:** These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation that might lead to damage.

v

Syntax conventions that are used in this book

The syntax in this book adheres to the following convention:

v GUI elements are shown in **bold**.

v Commands are shown in monospace.

Accessibility

ConstantConnect is designed to be accessible to users with physical challenges, such as restricted mobility or limited vision. All operating system accessibility features are supported.

v **High contrast**: When the operating system is set to high contrast mode, the ConstantConnect interface displays objects larger than normal. If the contents of the help window appear clipped or if objects overlap, simply maximize the window.

v **Screen-reading**: ConstantConnect supports screen-reading or text-to-speech technology for visually impaired users. To enable text-to-speech support, you must download and install a screen reader application such as Microsoft Narrator.

v **Keyboard navigation**: This feature enables you to navigate through the ConstantConnect screens using the keyboard.

You can use function key combinations to perform the following tasks.

Command	Shortcut
Next	Alt+N
Back	Alt+B
OK	Alt+O
Cancel	Esc
Close	Alt+F4
Help	F1
About	F6
Minimize	Alt+Spacebar+N

Online resources for ConstantConnect

The following Web page provide resources for understanding and using ConstantConnect:

ConstantConnect home page

http://www.lenovo.com/constantconnect

Go to this Web page to download the latest ConstantConnect software and documentation.

Chapter 1. Introducing ConstantConnect and Protect

This chapter presents an overview of the Lenovo®ConstantConnect and Protect solution (hereinafter referred to as ConstantConnect and Protect) and its system requirements.

How ConstantConnect works

ConstantConnect uses Bluetooth technology to synchronize data between your ThinkPad®computer mail client and BlackBerry®smartphone. The card that came with the solution provides the communication support to send and receive complete e-mails and attachments.

The card uses the Freescale i.MX31L processor, which is a high-performance, low-power processor up to 532MHz based on the ARM1136JF-S microprocessor core. Also, the card uses the Linux operating system as the software platform, and provides additional features.

ConstantConnect enables you to select BlackBerry smartphones and mail accounts to synchronize. It also enables you to set e-mail size restrictions, e-mail prioritization, and power settings. After you have successfully configured these settings, ConstantConnect keeps your system current. Using core technologies that include low-power processing, rugged storage, and constant connectivity, the solution extends the functionality of your ThinkPad computer, and makes your devices work more closely together.

Using Bluetooth technology, ConstantConnect automatically detects and connects to your BlackBerry smartphone even if your ThinkPad computer is disconnected from the network, suspended, hibernated, or powered off. After pairing your BlackBerry smartphone with your notebook computer and configuring your card, ConstantConnect can receive new data from your BlackBerry smartphone, store it in the card, and notify you when new data has been acquired. The newly acquired data becomes available immediately when you are using your notebook computer. If you are sending an e-mail from your notebook computer that does not have a network connection, the new e-mail is stored in the card, sent to your BlackBerry smartphone through Bluetooth communication, and then sent to the e-mail services. ConstantConnect enables you to send and receive corporate e-mails or personal e-mails depending on the BlackBerry smartphone configuration.

Note: A BlackBerry smartphone configured for corporate e-mails might also be used for personal e-mails.

After pairing your BlackBerry smartphone to your notebook computer, start the ConstantConnect program. When its paired BlackBerry smartphone is in proximity, the Bluetooth modules on both devices start to communicate. When your notebook computer is powered on but disconnected from the network, the mail client on your notebook computer transfers data with your BlackBerry smartphone through Bluetooth communication. When your notebook computer is suspended, hibernated, or powered off, the Bluetooth module on the card will be activated, so that your BlackBerry smartphone communicates with your card. When your notebook computer resumes to the working state, replication occurs between the card and the mail client on your notebook computer. As a result of the communication between these devices, either your ThinkPad computer or BlackBerry smartphone will send and acquire the most recent data.

When the card has been initially configured, it stores information that identifies the notebook computer it has been installed on. The card can be used with only one computer at a time. To start using it with another notebook computer, reconfigure the card.

The card has two LED indicators to show its state, and a **Synch Now** button to enable immediate synchronization. For detailed information on the functionality of the LED indicators and the **Synch Now** button, refer to the *ConstantConnect Help*.

Understanding different scenarios

This section describes different scenarios that occur to the ThinkPad computer that has ConstantConnect, the mail client (Microsoft®Office Outlook®), and the card installed. These scenarios also occur to the mail server and the BlackBerry smartphone that has been correctly configured.

Scenario A

When the ThinkPad computer is working and connected to the Internet, the e-mails are directly sent and received between Outlook and the mail server.
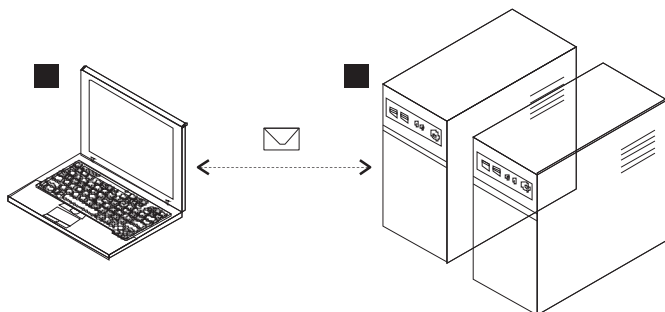
1	ThinkPad computer
2	Mail server

Scenario B

When the ThinkPad computer is working without an Internet connection, and the BlackBerry smartphone is in proximity with a good network connection, the e-mails are replicated from Outlook to the BlackBerry smartphone through Bluetooth communication. Then the e-mails are sent out to the mail server. The ThinkPad computer also initiates synchronization with the card.
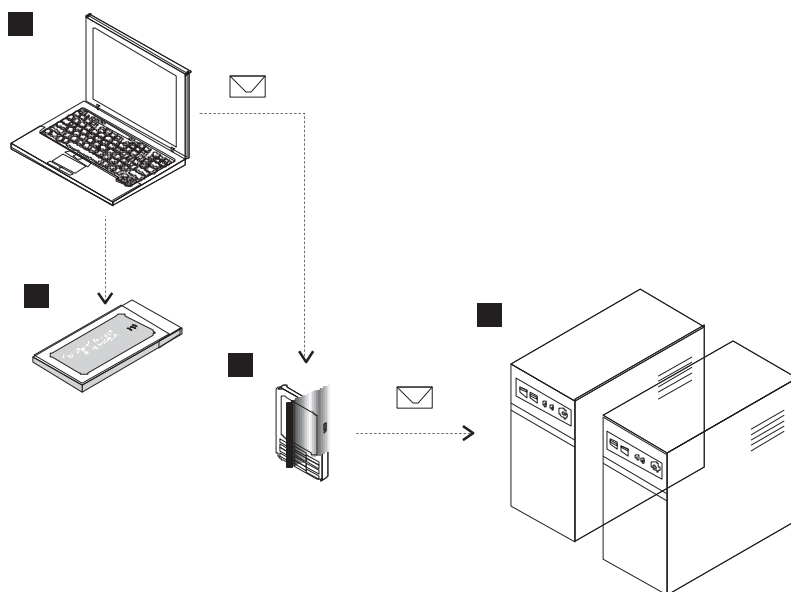
1	ThinkPad computer
2	Mail server
3	BlackBerry smartphone
4	Card

When new e-mails arrive, they are transferred from the mail server to the BlackBerry smartphone. The BlackBerry smartphone receives the e-mails and replicates the e-mails to Outlook through Bluetooth communication. The ThinkPad computer also initiates synchronization with the card.
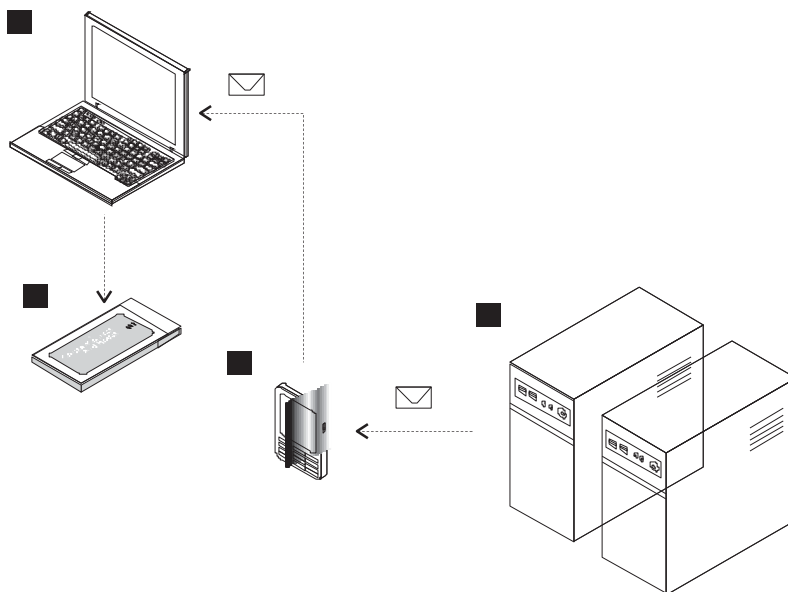
Scenario C

When the ThinkPad computer is working without an Internet connection, and the BlackBerry smartphone is not in proximity with the ThinkPad computer, the ThinkPad computer initiates synchronization with the card.

Notes:

1. Later the synchronized e-mails will be sent to the BlackBerry smartphone when it is in proximity with the ThinkPad computer, even if the ThinkPad computer is suspended, hibernated, or powered off.

2. If the ThinkPad computer is still working, follow **Scenario B**.
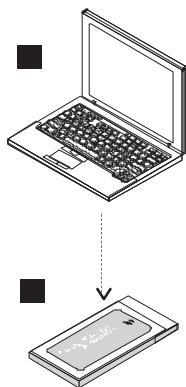
If the BlackBerry smartphone has a good network connection and new e-mails arrive, the e-mails are transferred from the mail server to the BlackBerry smartphone. They are stored on the BlackBerry smartphone for later replication.

Note: When the ThinkPad computer and the BlackBerry smartphone are in proximity, replication will happen to Outlook if the ThinkPad computer is working, or to the card if the ThinkPad computer is suspended, hibernated, or powered off.
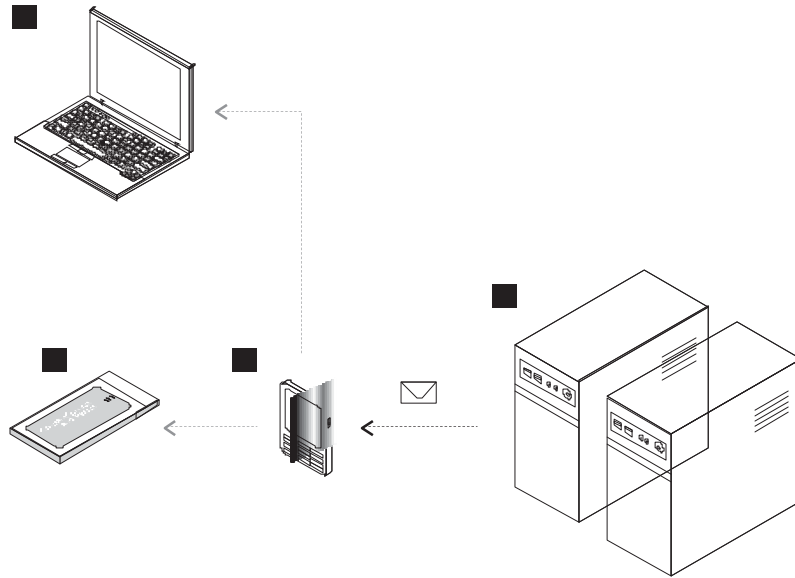
Scenario D

When the ThinkPad computer is suspended, hibernated, or powered off, and the BlackBerry smartphone is available, the card communicates with the BlackBerry smartphone and sends the e-mails, which are transferred to the mail server.

Note: The e-mails were replicated from Outlook to the card before the ThinkPad computer is suspended, hibernated, or powered off.
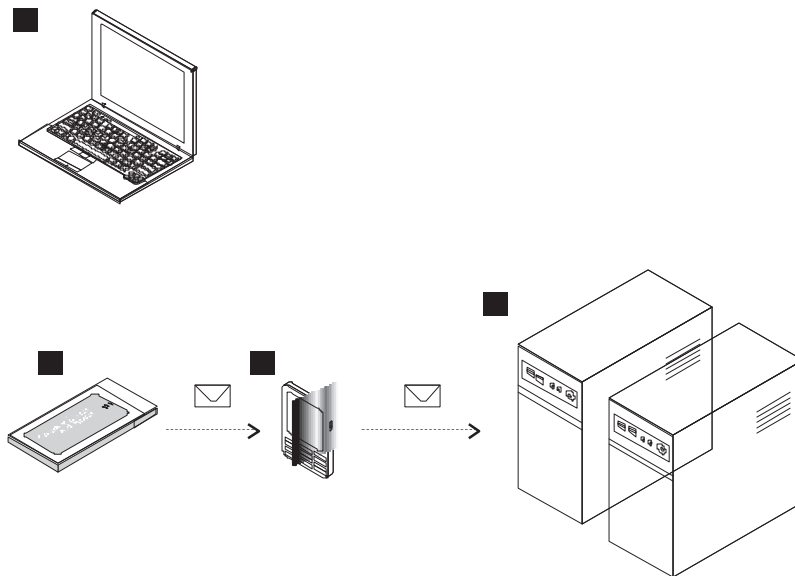
When new e-mails arrive, they are transferred from the mail server to the BlackBerry smartphone. The card receives the e-mails from the BlackBerry smartphone.

Note: When the ThinkPad computer resumes to the working state, the e-mails are replicated from the card to Outlook.
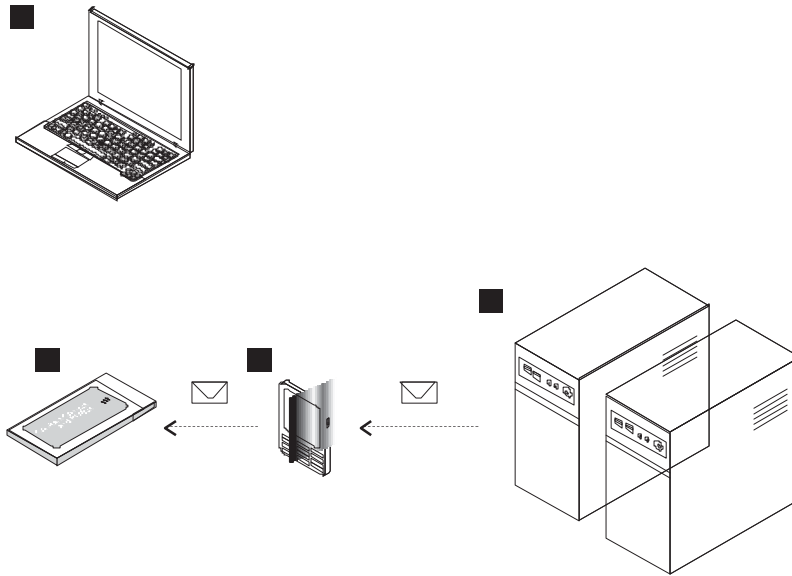
Hardware and software requirements

To use ConstantConnect and the card, your computer must meet the following hardware and software requirements:

v A ThinkPad computer that has been customized to support the ConstantConnect program

The following ThinkPad computer models have been customized to support ConstantConnect and the card:

– T400s

v Microsoft Windows®XP Professional with Service Pack 2 (SP2) or later, or Microsoft Windows Vista® (32-bit) with Service Pack 1 (SP1) or later

v Microsoft Office Outlook 2003 or 2007

v A 34-mm (1.34 inches) ExpressCard slot that can remain powered when your notebook computer is suspended, hibernated, or powered off

v Basic Input/Output System (BIOS) and Embedded Controller (EC) programs that support the ConstantConnect application

v Broadcom Bluetooth module with ThinkPad Bluetooth Enhanced Data Rate software 5.5.0.3000 or later for Windows XP, and

6.2.0.2600 or later for Windows Vista

v BlackBerry®Desktop Manager 4.6 or later

v ThinkPad Power Management Driver 1.53 or later

Note: If you are using the BlackBerry®Storm™   Series, for example, BlackBerry®Storm™ 9530 smartphone, you must download the latest BlackBerry®USB and Modem Driver from the following Web site: http://na.blackberry.com/eng/support/downloads/#tab_tab_desktop

Supported mail servers and BlackBerry smartphone models

Currently, ConstantConnect supports the following mail servers:

v Microsoft Exchange Server 2007

v Microsoft Exchange Server 2003

v POP3/SMTP (Post Office Protocol version 3 / Simple Mail Transfer Protocol) mail servers

ConstantConnect supports the following models of BlackBerry smartphones:

Model	Carrier(s)	Data Mode
8100	AT&T, T-Mobile	GPRS/EDGE
8110	AT&T	GPRS/EDGE
8120	AT&T, T-Mobile	GPRS/EDGE
8130	Verizon Wireless, Sprint	1xEVDO
8300	AT&T	GPRS/EDGE
8310	AT&T	GPRS/EDGE
8320	T-Mobile	GPRS/EDGE
8330	Verizon Wireless, Sprint	1xEVDO
8800	AT&T, T-Mobile	GPRS/EDGE
8820	AT&T, T-Mobile	GPRS/EDGE
8830	Verizon Wireless, Sprint	GPRS/EDGE, 1xEVDO
9000	AT&T	GPRS/EDGE
9530	Verizon Wireless	GPRS/EDGE, 1xEVDO

ConstantProtect – security features

ConstantProtect also protects your notebook computer from malicious intrusion, including viruses, Trojans, spyware, worms, and other Internet attacks, by preventing them from reaching your computer. It enables you to connect your computer to the Internet anywhere and enjoy an extremely high level of protection - the same corporate level, hardware-based security solutions used by highly guarded security organizations.

ConstantProtect combines enterprise-class software with proprietary patent pending developments to provide a comprehensive security solution for known and unknown threats. These solutions include:

v Adaptive security policy

v Multi-layer security agent

v Layer-8 security engine

v URL categorization and filtering

v Anti-spam

v Anti-phishing

v Anti-spyware

v Anti-virus

v Transparent e-mail proxies (POP3/SMTP)

v Transparent Web proxies (HTTP/FTP)

v Intrusion detection/prevention

v VPN client

v Stateful inspection firewall

Before the operating system on your notebook computer accepts any data for processing, a low-level driver redirects the data to the ConstantProtect unit where a full security check is performed. Security breach attempts are identified and thwarted, and only safe, secure data is passed back to notebook computer.

ConstantProtect includes a web-based management console that provides status information, security logs, and reports. It can be used to configure device settings, network settings and security policy.

ConstantProtect offers the following features:

v A standard card in an extremely small size

v Hardware-based security appliance with hardened Linux OS

v Physical separation between the notebook computer and the outside world

v Plug and forget transparent

v Automatic updates

v All-in-one corporate grade security software

v Proprietary security software

v Real-time monitoring and comprehensive reports

v Remote management

Chapter 2. Installing and uninstalling ConstantConnect and Protect

This chapter describes the installation and uninstall scenarios of ConstantConnect and Protect. Before you install the ConstantConnect and Protect program, refer to "Hardware and software requirements" on page 5 to review the prerequisites.

Installing the card

When inserting the card into the ExpressCard slot on your computer, be sure to hold the card correctly with the Lenovo logo and three arrows facing up as shown:
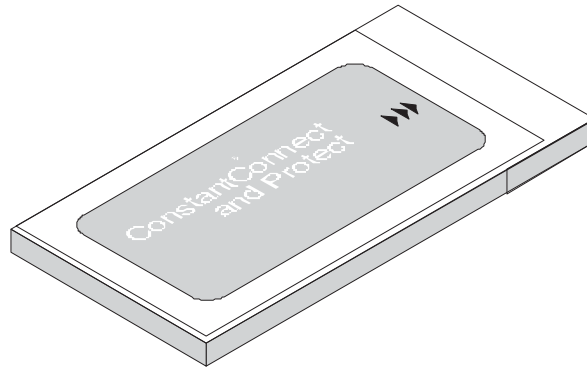
The ExpressCard slot might be different in various computer models. To locate the ExpressCard slot on your computer, find the slot marked with either of the following two icons:

Installing ConstantConnect and Protect

To install ConstantConnect and Protect on your ThinkPad computer, do the following:

1. Pair your BlackBerry smartphone with your notebook computer. For information on how to complete the pairing procedure, refer to "Pairing the BlackBerry smartphone with the notebook computer" on page 13.
2. Connect your BlackBerry smartphone to your notebook computer using the USB cable that came with your BlackBerry smartphone. For more information, refer to "Turning off Mass Storage Mode" on page 13.
3. Insert the card into the ExpressCard slot on your notebook computer.
4. Insert the *Lenovo ConstantConnect and Protect CD* into your CD/DVD drive. The InstallShield Wizard automatically starts. Otherwise, run the launch.exe file to start the InstallShield Wizard. The Welcome window opens.
5. Click **Next**. The License Agreement window opens.
6. Select **I accept the terms in the license agreement**, and click **Next**. The Choose Features Setup will Install window opens.
7. If you wish to enable ConstantProtect, select **ConstantProtect** and click **Next**.
8. Click **Install**. During the installation procedure, the card must remain inserted.
9. When ConstantConnect has been successfully installed on your notebook computer, the InstallShield Wizard Completed window displays, recommending you to configure the settings immediately, so

that your BlackBerry smartphone can synchronize with the card. Select **I want to configure my synchronization settings now (Recommended)**, and click **Finish**.

10. A message displays, asking if you would like to restart your notebook computer. Click **Yes**. When the notebook computer finishes restarting, the Configuration Wizard begins to run. For more information, refer to Chapter 4, "Configuration scenarios," on page 13.

11. If you have selected to enable ConstantProtect, click the **ConstantProtect** icon in the Windows system tray to access the ConstantProtect Management Console for further configuration. For more information, refer to Chapter 6, "Configuring ConstantProtect security," on page 23.

Note: After the InstallShield Wizard has copied files to your hard disk drive, do not delete or modify any files in the C:\Program Files\Lenovo\ConstantConnect directory or its subdirectories.

Uninstalling ConstantConnect and Protect

When you do not need to use ConstantConnect and Protect, it is strongly recommended that you uninstall the program before unpairing your BlackBerry smartphone. When the program is uninstalled, the drivers on the card will also be removed.

To uninstall ConstantConnect and Protect, do the following:

1. Depending on your **Start** menu mode, click **Start → Control Panel** or **Start → Settings → Control Panel**. The Control Panel window opens.

2. Depending on your Control Panel mode, click or double-click **Add or Remove Programs**. The Add or Remove Programs window opens.

3. Click **ConstantConnect and Protect**.

4. Click **Remove** or **Uninstall**.

5. A message displays, asking if you want to remove ConstantConnect and Protect from your computer. Click **Yes**.

6. Another message displays, indicating ConstantConnect and Protect is attempting to uninstall the software on your BlackBerry smartphone. You are prompted to confirm the uninstall. Click **Yes**.

7. If you have set a security password on your BlackBerry smartphone, you will be prompted to type the security password. Click **Submit**.

8. At the end of the uninstall procedure, a message displays, indicating you must restart your computer, so that the configuration settings made to ConstantConnect and Protect can take effect. Click **Yes**.

Chapter 3. Working with Windows Firewall and AT&T VPN Client

This chapter describes how to work with Windows Firewall and AT&T VPN Client after you install ConstantConnect.

Working with Windows Firewall

A firewall application keeps a list of approved applications, and the firewall will accept an incoming network connection for these applications. By adding ConstantConnect to the list, the computer can accept the network connection from the Lenovo ConstantConnect Service. Refer to the documentation of the specific firewall application for instructions about adding applications to the approved application list.

To configure Windows Firewall and allow ConstantConnect access, do the following:

1. Depending on your **Start** menu mode, click **Start → Control Panel** or **Start → Settings → Control Panel**. The Control Panel window opens.
2. Depending on your Control Panel mode, double-click **Windows Firewall** or click **Network and Internet Connections → Windows Firewall**. The Windows Firewall window opens.
3. On the **General** tab, click **On (recommended)**.
4. Deselect **Don't allow exceptions**.
5. On the **Exceptions** tab, select **Configure Utility**.

Working with AT&T VPN Client

If you need to use AT&T VPN Client on your notebook computer, install the program before installing ConstantConnect.

After the installation, be sure to remove the network filter by doing the following:

1. Depending on your **Start** menu mode, click **Start → Control Panel** or **Start → Settings → Control Panel**. The Control Panel window opens.
2. Depending on your Control Panel mode, double-click **Network Connections** or click **Network and Internet Connections → Network Connections**.
3. Right-click the connection for **Lenovo ConstantConnect**.
4. Click **Properties** in the pop-up window. The Local Area Connection Properties window opens.
5. On the **General** tab, make sure you deselect the following items:
   v **AGN Filter Interface**
   v **AT&T Wi-Fi Support Driver**
6. Click **OK**.

Chapter 4. Configuration scenarios

This chapter presents information on how to configure your BlackBerry smartphone, BlackBerry Enterprise Server, Outlook, and ConstantConnect before you use the solution to send and receive e-mails.

Configuring your BlackBerry smartphone

To successfully run ConstantConnect, you need to configure your BlackBerry smartphone before, within, and after the ConstantConnect configuration procedure.

Pairing the BlackBerry smartphone with the notebook computer

Before configuring ConstantConnect, you must pair the BlackBerry(R) smartphone with the notebook computer. You should enable Bluetooth on your BlackBerry smartphone by clicking **Options** → **Bluetooth** → **Enable Bluetooth**. Then you can use the ThinkPad Bluetooth Enhanced Data Rate Software to pair the devices. For more information about this software, refer to the *Bluetooth Support File* on the Lenovo Support Web site at:
http://www.lenovo.com/think/support

For more information, refer to the documentation that came with your BlackBerry smartphone.

Note: Immediately after the pairing procedure, a message might display on your BlackBerry smartphone, saying **"Pairing complete. Connect to** *[remote Bluetooth device name]***?"** The *[remote Bluetooth device name]* might be the machine name. Be sure to click **No** to avoid Bluetooth signal interference.

Configuring your notebook computer as a trusted device on your BlackBerry smartphone

Immediately after pairing your BlackBerry smartphone with your notebook computer, be sure to manually configure your notebook computer as a trusted device:

1. Click **Options** → **Bluetooth**, and then select the machine name that you have paired with your BlackBerry smartphone.
2. Click the **Device Properties** menu. Set the **Trusted** field to **Yes**.
3. Click the trackwheel. Click **Save**.
4. If a message appears asking whether you will accept the connection request from the notebook computer, click **Yes**.

Turning off Mass Storage Mode

When you are connecting your BlackBerry smartphone to the notebook computer, you need to turn off the Mass Storage Mode. Your BlackBerry smartphone displays a message, saying **"Do you want to turn on Mass Storage Mode? You might not be able to access some media files in this mode."** Be sure to select **No**. Otherwise, the SD Card in your BlackBerry smartphone will be fully controlled by the notebook computer and recognized as a USB memory key.

Allowing ConstantConnect access

When ConstantConnect has been successfully installed on your BlackBerry smartphone, it needs to automatically restart. The following messages might appear:

1. **"Would you like to grant ConstantConnect Trusted Application status?"**
   Click **Yes**.
2. **"The application ConstantConnect is attempting to access phone information. Would you like to allow access?"**

Select **Do not ask again**, and click **Yes**.

3. **"The application ConstantConnect has requested an ssl (tls or other encryption methods) connection to** *[outgoing mail server]***."**

   Select **Do not ask for ssl (tls or other encryption methods) to** *[outgoing mail server]*, and click **Allow**.

4. **"The application ConstantConnect has requested a file connection to ///SDCard/."**

   Select **Do not ask again for file connections to ///SDCard/**, and click **Yes**.

Attention: The messages above might be accidentally ignored, and clicking the wrong answers might cause unexpected consequences to ConstantConnect. Therefore, make sure you click **Yes** or **Allow** when responding to these messages. If you accidentally click **No** for the second and fourth messages, the windows for granting the authorization requirement will not pop up again. To grant the authorization requirement, refer to "Allowing connections and interactions."

Allowing connections and interactions

After you run the Configuration Wizard on your ThinkPad computer, be sure to complete the following two procedures on your BlackBerry smartphone:

Procedure One

1. Click **Options → Advanced options → Applications**.
2. Click the **Modules** menu. Click **Common**.
3. Click the **Edit Permissions** menu. Set the **Connections** and **Interactions** fields to **Allow**.
4. Click the trackwheel. Click **Save**.

Procedure Two

1. Click **Options → Advanced options → Applications**.
2. Click the **Modules** menu. Click **ConstantConnect**.
3. Click the **Edit Permissions** menu. Set the **Connections** and **Interactions** fields to **Allow**.
4. Click the trackwheel. Click **Save**.

Configuring BlackBerry Enterprise Server

If your BlackBerry smartphone can send and receive corporate e-mail messages, it is using the BlackBerry®Enterprise Server and Microsoft Exchange Server to transfer data. You need to configure the BlackBerry Enterprise Server properties by doing the following:

Procedure One

1. Open the BlackBerry®Manager on the computer with the BlackBerry Enterprise Server installed.
2. Select **Explorer View**.
3. Expand the **BlackBerry Domain** category.
4. Expand the **Servers** category.
5. Click *[machine name]_***MDS-CS_1**.
6. Click **Edit Properties** on the right pane. The BlackBerry MDS Connection Service window opens.
7. Select **Properties → General → Flow Control**. Set the **Maximum KB/Connection** value to **1024**.
8. Select **Properties → HTTP → Authentication**. Set the **Support HTTP Authentication** value to **True**.
9. Select **Properties → HTTP → Connection Timeouts**. Set the **HTTP Device Connection Timeout** value to **300000**.
10. Click **OK** to save the settings.

Procedure Two

1. Open the BlackBerry Manager on the computer with the BlackBerry Enterprise Server installed.
2. Select **Explorer View**.
3. Click **BlackBerry Domain**.
4. Click **Edit Properties** on the right pane. The Global Properties window opens.
5. Select **Properties → Media Content Management**.
6. Double-click **Media Content Types**.
7. Click **New...**.
8. Set the **Media Content Type** value to **text/xml**.
9. Set the **Maximum KB/Connection** value to **5120**.
10. Set the **Disallow content** value to **False**.
11. Click **OK** to save the settings.

Configuring Microsoft Office Outlook

ConstantConnect requires the .NET Programmatically Support feature installed in Outlook. To verify whether the .NET Programmatically Support feature is installed or to install this feature, do the following:

1. Depending on your **Start** menu mode, click **Start → Control Panel** or **Start → Settings → Control Panel**. The Control Panel window opens.
2. Depending on your Control Panel mode, click or double-click **Add or Remove Programs**. The Add or Remove Programs window opens.
3. Click the **Microsoft Office Outlook** or **Microsoft Office Suite** entry appropriate to your installed version.
4. Click **Change → Add or Remove Features → Continue**.
5. Expand the **Microsoft Office Outlook** category to see whether the .NET Programmatically Support feature is installed. If it is not installed, click **Run from My Computer**.
6. Follow the instructions on the screen to complete the installation procedure.

Before running the Configuration Wizard, you must set at least one same mail account both in Outlook and on the BlackBerry smartphone. If the listed mail account looks different from your expectations, do the following to configure the settings in your Outlook:

1. In the Selecting mail accounts to synchronize window of the Configuration Wizard, click **Configure Outlook mail...**. The Mail window opens.
2. Click **Add...**. Select **Prompt for a profile to be used** or **Always use this profile** as needed. Click **OK**. The New Profile window opens.
3. Type a profile name to create the new profile. Click **OK**. The Add New E-mail Account window opens.
4. Set up your mail account by typing your name, mail address, and password. Click **Next**.
5. Choose your mail service by clicking **Internet E-mail** or **Microsoft Exchange**. Click **Next**.
6. Type the name of your mail server, and the name of your mail box set up by your administrator. For more information, contact your system administrator. Click **Next**.
7. Click **Finish**. Open your Outlook to synchronize data and reflect the most recent change.

Configuring ConstantConnect

When your notebook computer is not connected to the network, or if it is suspended, hibernated, or powered off, the ConstantConnect program can synchronize your BlackBerry smartphone to your e-mails. Before enabling the synchronization, you need to configure the ConstantConnect program. The Configuration Wizard starts the first time you use the ConstantConnect program, or when you have finished the installation and selected to synchronize settings immediately.

Getting started

The first time you use the Configuration Wizard, the Getting started window opens. Be sure to do the following required steps:

1. Connect your BlackBerry smartphone to your notebook computer using the USB cable that came with your BlackBerry smartphone. For more information, refer to "Turning off Mass Storage Mode" on page 13.

   Notes:

   a. Make sure your BlackBerry smartphone has been paired with your notebook computer. If not, you can click **Help me do this** to start the pairing process immediately. For information on how to complete the pairing procedure, refer to "Pairing the BlackBerry smartphone with the notebook computer" on page 13.

   b. If you have previously configured your BlackBerry smartphone with another notebook computer, be sure to unpair your BlackBerry smartphone before pairing and configuring it with a new notebook computer.

   c. Make sure only the BlackBerry smartphone you are configuring with ConstantConnect is attached.

   d. The Configuration Wizard can detect the BlackBerry smartphone(s) that have been previously paired. If the detected BlackBerry smartphone(s) include the one that is currently attached to your notebook computer, confirm it by selecting this BlackBerry smartphone. Otherwise, you need to click **Help me do this** to pair the correct BlackBerry smartphone.

2. Insert the card into the ExpressCard slot on your notebook computer.

3. Make sure you have an Internet connection. When you have completed these steps, click **Next**. The Installing ConstantConnect to Devices window displays. Be sure not to disconnect your BlackBerry smartphone from your notebook computer, or power off either of them. During the installation progress, you need to respond to certain prompts on your BlackBerry smartphone.

Notes:

1. In the installation procedure, if the BlackBerry smartphone has not been paired, or the Bluetooth communication test fails, an error message will appear indicating that you need to pair your BlackBerry smartphone again.

2. If you have set a password on your BlackBerry smartphone, you will need to type the password in the Failed to install on BlackBerry window, so that the installation procedure continues.

Attention: If the password you typed is incorrect, be sure not to exceed the maximum number of attempts. Otherwise, your BlackBerry smartphone might lose all personal data and revert to the factory configuration. Refer to the documentation that came with your BlackBerry smartphone for more information.

After installing ConstantConnect to the BlackBerry smartphone, you need to grant ConstantConnect as a trusted application, allow ConstantConnect to access phone information, and allow file connection to the SD Card. For more information, refer to "Allowing ConstantConnect access" on page 13.

If Bluetooth is disabled on your BlackBerry smartphone, your BlackBerry smartphone might display a message, saying **"ConstantConnect requires the Bluetooth to be enabled. Would you like to enable it?"** After you click **Yes**, your BlackBerry smartphone might not be able to automatically turn on Bluetooth. In

this case, be sure to manually configure Bluetooth on your BlackBerry smartphone. For detailed information, refer to "Pairing the BlackBerry smartphone with the notebook computer" on page 13.

When your BlackBerry smartphone has finished restarting, click **Next** to continue.

Selecting mail accounts to synchronize

In the Selecting mail accounts to synchronize window, the ConstantConnect program displays and synchronizes the mail account(s) that you have configured both in Outlook and on the BlackBerry smartphone. If the listed mail account(s) look different from your expectations, click the **Configure Outlook mail...** button to manage your Outlook mail account(s). You also need to check your mail settings on your BlackBerry smartphone to make sure the account(s) are configured on both devices. For more information, refer to "Configuring Microsoft Office Outlook" on page 15. Then click **Refresh** to reflect the most recent changes in the **Accounts to synchronize on** *[device name]* list.

Note: Make sure your notebook computer is connected with your mail server through the Internet.

After you have selected the mail account(s) you want to synchronize, the Mail authentication window requires you to type the username and password for the mail account(s). To remove a mail account from the ConstantConnect program, click **Remove account**, and then click **Yes**.

When you have finished typing the authentication information, click **Test accounts**. If the testing procedure fails, an error message will appear indicating that authentication failed for the mail account(s) that you specified.

After the first time you run the Configuration Wizard, if the authentication for the mail account(s) has been recently updated, the ConstantConnect account authentication window opens. Type the new password, and click **Test accounts**. You can also choose to remove this account, or close this window without updating the authentication information.

Click **Next**. The Congratulations window opens.

Confirming and finishing the configuration

The Congratulations window displays the BlackBerry smartphone model that you have configured, the mail account(s) to be synchronized, and the frequency that your card will look for new e-mails. These settings can be modified in the ConstantConnect program.

For detailed information on the LED indicators and the **Synch Now** button, refer to the *ConstantConnect Help*. To view the *ConstantConnect Help*, do the following:
1. Depending on your **Start** menu mode, click **Start → Programs → Lenovo → ConstantConnect**, or click **Start → All Programs → Lenovo → ConstantConnect**. The ConstantConnect Configuration window opens.
2. Click **Help**. The *ConstantConnect Help* opens.

Click **Finish** to complete the configuration procedure.

After running the Configuration Wizard, you also need to manually configure two permission settings on your BlackBerry smartphone, so that it can connect and interact with ConstantConnect. For more information, refer to "Allowing connections and interactions" on page 14.

Upgrading the modules

After installing a newer version of the ConstantConnect program, you need to upgrade the ConstantConnect modules on your BlackBerry smartphone. To upgrade the ConstantConnect modules, do the following when the Starting to upgrade modules window displays:

1. Connect your BlackBerry smartphone to your computer with the USB cable that came with your BlackBerry smartphone.

   Note: If your BlackBerry smartphone is disconnected from your computer, be sure to reconnect it.

2. Make sure your BlackBerry smartphone has been previously configured on your computer.

   Note: If the BlackBerry smartphone you are connecting is not the same one you configured before, be sure to connect the correct BlackBerry smartphone.

3. If you have completed the steps above, a message appears indicating the ConstantConnect modules have been successfully upgraded on the BlackBerry smartphone. Click **Finish**.

4. Re-configure the ConstantConnect program.

Chapter 5. Sending and receiving e-mails

This chapter presents information on how ConstantConnect sends and receives e-mails in different conditions. The following involves ConstantConnect, the mail client (Outlook), the ThinkPad computer, the card, the BlackBerry smartphone, and the mail server.

Sending e-mails

This section describes how ConstantConnect sends e-mails in different conditions.

Condition A

> If Outlook is online, after you draft a new e-mail and click **Send**, Outlook stores the e-mail in the Outbox folder. ConstantConnect replicates the e-mail to the card. Outlook connects to the mail server, transfers the e-mail, and stores the e-mail in the Sent folder. ConstantConnect deletes the e-mail from the card.

Condition B

> If Outlook is offline and the BlackBerry smartphone is in proximity, Outlook stores the new e-mail in the Outbox folder. Then ConstantConnect replicates the e-mail to the card and places the e-mail in a queue to send later. The Activity LED blinks until all data has been transferred to the card. Then the card transfers data to the BlackBerry smartphone through Bluetooth communication. The BlackBerry smartphone sends the e-mail to the mail server. If ConstantConnect detects the e-mail has not been sent by Outlook, the e-mail will be stored in the Outlook Sent folder.

Condition C

> If Outlook is offline and the BlackBerry smartphone is not in proximity, Outlook stores the new e-mail in the Outbox folder. Then ConstantConnect replicates the e-mail to the card and places the e-mail in a queue to send later. The Activity LED blinks until all data has been transferred to the card.
>
> When the ThinkPad computer becomes suspended, hibernated, or powered off, any e-mail not completely sent to the card stays in the Outbox folder, and cannot be sent by the card.
>
> When the ThinkPad computer resumes to the working state, ConstantConnect determines whether the e-mail was sent by the card. If it was sent, ConstantConnect moves the e-mail to the Sent folder. If not, the e-mail remains in the Outbox folder.

Condition D

> If Outlook is online but unable to send the e-mail to the mail server, ConstantConnect detects the e-mail was not successfully sent, and sends it following **Condition B** and **Condition C**.

Condition E

> If Outlook is offline, the BlackBerry smartphone is in proximity, and the ThinkPad computer is working, follow **Condition B**.

Condition F

> If Outlook is closed with one or more e-mails in the Outbox folder, and the ThinkPad computer is working, ConstantConnect will send the e-mail(s). For more information, refer to **Condition B** to **Condition E**.

Condition G

> If Outlook is offline and Bluetooth communication is disabled, refer to **Condition C**.

Condition H

> In any conditions, if the e-mail is not completely sent, it remains in the Outbox folder, as well as in the queues on the card and the BlackBerry smartphone.

Condition I

If the card and the BlackBerry smartphone does not have sufficient memory to store data, the e-mail remains in the Outbox folder without being sent by ConstantConnect. You will receive an error message.

Condition J

If the new e-mail exceeds the e-mail size limit that you previously configured, you will receive an error message.

Condition K

If you delete an e-mail from the Outbox folder, see the following:

v If ConstantConnect has placed the e-mail in the queue, it will be deleted.

v If the BlackBerry smartphone has sent the e-mail or is sending it, the e-mail will be considered sent.

Condition L

If you create and send a new e-mail directly using the BlackBerry smartphone, ConstantConnect will play no role.

Condition M

If ConstantConnect cannot deliver the e-mail, ConstantConnect will scan the contents of the local data stores, and automatically delete any e-mail that has been held in a data store for more than approximately 30 days.

Receiving e-mails

This section describes how ConstantConnect receives e-mails in different conditions.

Condition A

If Outlook is online, the mail server receives the new e-mail. Outlook establishes communication with the mail server, receives the e-mail from the server, and stores it in the Inbox folder. ConstantConnect searches all e-mail folders for a match. If there is a match, ConstantConnect removes the copy previously received from the card, and replaces it with the new copy from the mail server.

Condition B

If Outlook is offline, the BlackBerry smartphone is in proximity, and the ThinkPad computer is working, the copy received by the card and the BlackBerry smartphone will be deleted after Outlook receives the e-mail. If the BlackBerry smartphone is not in proximity, the copy on the card will be deleted, and the copy on the BlackBerry smartphone will be deleted the next time the BlackBerry smartphone becomes in proximity.

The BlackBerry smartphone receives the new e-mail from the mail server. The BlackBerry smartphone refers to the ConstantConnect configuration settings to determine whether it should download the complete e-mail and attachment from the mail server. The BlackBerry smartphone downloads prioritized e-mails before others and stores the data.

ConstantConnect communicates with the BlackBerry smartphone and determines the new e-mail is available. ConstantConnect stores the new e-mail on the card and turns on the Inbox LED. The e-mail on the BlackBerry smartphone is deleted.

ConstantConnect deletes the e-mail on the card, stores the e-mail in the Inbox folder if it has not been received by Outlook, and turns off the Inbox LED on the card.

Condition C

If the ThinkPad computer is suspended, hibernated, or powered off, and the BlackBerry smartphone is in proximity, the BlackBerry smartphone receives the new e-mail from the mail server. The BlackBerry smartphone refers to the ConstantConnect configuration settings to determine whether it should download the complete e-mail and attachment from the mail server. The BlackBerry smartphone downloads prioritized e-mails before others and stores the data.

ConstantConnect communicates with the BlackBerry smartphone and determines the new e-mail is available. ConstantConnect stores the new e-mail on the card and turns on the Inbox LED. The e-mail on the BlackBerry smartphone is deleted.

When the ThinkPad computer resumes to the working state, ConstantConnect deletes the e-mail on the card, stores the e-mail in the Inbox folder if it has not been received by Outlook, and turns off the Inbox LED on the card.

Condition D

If the new e-mail exceeds the e-mail size limit that you have configured, the BlackBerry smartphone can receive only part of the e-mail and display a message indicating it is not the complete e-mail.

Condition E

If you have configured more than one profile in Outlook, ConstantConnect examines the recipient address and compares it to the mail account(s) configured in the current profile. If the recipient address is associated with an mail account in the current profile, ConstantConnect stores the e-mail in an appropriate folder and handles the e-mail in a way similar to one of the other conditions.

If the recipient address is not associated with the current profile, Outlook places the e-mail in its local data store.

When you log in to Outlook using another profile, ConstantConnect checks for a mail account again in the new profile. If the mail account is found, ConstantConnect handles the e-mail in a way similar to one of the other conditions.

Condition F

If ConstantConnect receives an e-mail for a profile, but you never log in to this profile, ConstantConnect places the e-mail in its local data store for no more than approximately 30 days, and then automatically deletes it.

Chapter 6. Configuring ConstantProtect security

The ConstantProtect Management Console (Management Console) provides access to the ConstantProtect management features through your Web browser. You can monitor security activity, view and print security reports and logs, view and configure security, system and user settings, view and print non-security event system logs, and more. The Management Console can be accessed in the following ways:

v ConstantProtect icon: if the ConstantProtect driver/software is installed, access the Management Console from this icon.

v Web browser: if for some reason the ConstantProtect icon is not available, you can manually access the Management Console through a standard Web browser.

Accessing the Management Console from the ConstantProtect icon

The ConstantProtect Management Console can be accessed from the ConstantProtect icon:

1. In the Windows notification area, right-click the ConstantProtect icon.
2. Select Open Management Console from the pop-up menu. The Login dialog box opens.

   Note: You can also double-click the ConstantProtect icon to open the Management Console.
3. Enter the following information:
   v Username - admin
   v Password - enter your ConstantProtect password (the default password is yoggie)
4. Click **OK**. The Management Console opens.

Manually accessing the Management Console

For some reason, if the ConstantProtect icon is not available, you can manually access the Management Console through a standard Web browser. The Management Console can be manually accessed by entering the ConstantProtect Management Console URL into the address field of your Web. To manually access the Management Console, do the following:

1. Open a Web browser and enter the following ConstantProtect Management Console URL into the address field of the browser:
   https://yoggie.yoggie.com:8443
   The Login dialog box opens.
2. Enter the following information:
   v Username: admin
   v Password: enter your ConstantProtect password (the default password is yoggie)
3. Click **OK**. The Management Console opens.

Changing the Interface language

You can change the language of the user interface (labels and dialogs) in your ConstantProtect Management Console at any time by doing the following:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.
2. Click the **System** tab. The ConstantProtect Details page appears in the Display pane.
3. Click **Language**. The Language Settings page appears.
4. Select the language you want to use from the list.

5. Click **Apply**. The selected interface language will be used, and the main ContantProtect Details page appears.

Changing your password

You can change your ConstantProtect Management Console password at any time by doing the following:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.
2. Click the **System** tab. The ConstantProtect Details page appears in the Display pane.
3. Click **Change Password**. The Password Settings page appears.
4. Enter the following information:
   v Current password: enter your current password
   v New password: enter the new password
   v Confirm password: enter the new password again
5. Click **Apply**.

Changing the privacy settings

ConstantProtect collects only security-related information in order to improve the quality of the products and service. It is highly recommended that you use the default privacy settings. Lenovo will never share any private information with a third-party or make any other use of this information.

Change the settings by doing the following:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.
2. Click the **System** tab. The ConstantProtect Details page appears in the Display pane.
3. Click **Privacy**. The Privacy Settings page appears.
4. Choose if you want to register your name and e-mail with Lenovo.
5. Select your privacy setting from the drop-down list box. You may choose one of the following options:
   v Share security logs with Lenovo: share all the security events collected by the ConstantProtect logs with Lenovo
   v Hide specific spam and URL information: do not share security events that contain the source and destination of spam e-mails or destination URL. Share all other security events collected by the ConstantProtect logs with Lenovo
   v Do not share any security events: do not share any security events collected by the ConstantProtect logs with Lenovo
6. Click **Apply**. The ConstantProtect Details page appears.

Setting the time zone

The current date and time are displayed in the main Settings page of the Management Console. To change the time, set a new time zone, so that the time and date are instantly updated and displayed. Set the time zone by doing the following:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.
2. Click the **System** tab. The Lenovo Details page appears in the Display pane.
3. Under **Time Zone**, click **Modify**. The Time Zone Settings page appears.
4. Select your location from the **Time Zone** drop-down list box.

5. Click **Apply**. The selected time zone is displayed, and the current date and time are updated. The Lenovo Details page appears.

Monitoring security activity

The Management Console provides several options for monitoring security activity. You can view the following:

v Current security status

v Security activity charts (including 3-D charts)

v Security and system logs

You can also view and print security activity reports.

Viewing security status

The Status page of the Management Console enables you to view your current risk level (a rating based on current activity) and security events. The Status page contains a risk level gauge, as well as event counters that indicate the number of security breach attempts thwarted by your ConstantProtect during the last 15 minutes, when ConstantProtect was connected and working.

Note: The Status page does not show the ConstantProtect security level, but the intensity of security breach attempts. ConstantProtect protects your notebook computer at all risk levels.

To view security status, click **Status** in the Navigation pane of the Management Console. The Status page appears in the Display pane with the following gauges for monitoring security activity:

v Risk level: displays your current security risk level, based on the ConstantProtect analysis of all firewall, IDS/IPS, and malware security events

v Firewall events: displays the number of attempted firewall attacks that took place over the last 15 minutes

v IDS/IPS event: displays the number of attempted security breaches detected and defeated by the Intrusion Detection System/Intrusion Protection System (IDS/IPS) over the last 15 minutes

v Malware events: displays the number of virus, spyware, active content, and other similar execution attempts that took place over the last 15 minutes

Note: The digital gauges (event counters) under each event gauge display the total of each type of security breach attempt. The number displayed is the number of attempts since the last reset.

Viewing and printing reports

ConstantProtect provides reports about types of security events in the form of graphic charts. These charts reflect information gathered during the last 24 hours of operation. You can click a chart to view it as a 3-D graph, and then click and drag it to change its orientation. You can also navigate through the charts, view them in 2-D, replay animations, and print them.

To view reports, do the following:

1. Click **Reports** in the Navigation pane of the Management Console. The main chart page of the **Charts** tab appears in the Display pane and displays the following charts:

   v Total: displays the total number of security breach events

   v Firewall: displays the total attempted firewall attacks

   v IDS/IPS: displays the total number of attempted security breaches detected and defeated by the IDS/IPS

   v E-Mail: displays total phishing, spam, and other e-mail threats

   v Malware: displays the total virus, spyware, active content, and other similar execution attempts

v Spam: displays the e-mail spam distribution score (the number of e-mail messages that are likely to be spam)

Note: All charts display information gathered during the last 24 hours of operation.

2. In the **Charts** tab, click a chart to display it in 3-D.
3. In the 3-D display, click:
   v Replay: reruns an animation
   v 2-D: displays the chart in 2-D
   v Print: prints the 3-D chart
   v Prev: displays the previous chart in 3-D
   v Next: displays the next chart in 3-D
   v Charts: returns to the main chart page

Viewing the security log

The ConstantProtect Security Log displays security event information. You can view the initial log and details for each event.

To view the security log, do the following:

1. Click **Reports** in the Navigation pane of the Management Console. The main chart page of the **Charts** tab appears in the Display pane.
2. Click the **Security Log** tab. The security log is displayed
3. To display the details of an event, click it. A small window pops up displaying the details.

   Note: To close the window, click the **X** button in the upper right corner.
4. To navigate to subsequent/previous Security Log pages as required, click the right/left arrow buttons.
5. To export the Security Log, click the **Export** link. A file save dialog appears. Navigate to the location where the compressed security log file will be saved on your computer, and click **Save**. The log file is saved to your computer.

Viewing the system log

The system log displays all important, non-security system events.

To view the system log, do the following:

1. Click **Reports** in the Navigation pane of the Management Console. The main chart page of the **Charts** tab appears in the Display pane.
2. Click the **System Log** tab. The system log is displayed.
3. Click the right/left arrow buttons to navigate to subsequent/previous System Log pages, as required.

Viewing the VPN log

The VPN log displays VPN-related events.

To view the VPN log, do the following:

1. Click **Reports** in the Navigation pane of the Management Console. The main chart page of the **Charts** tab appears in the Display pane.
2. Click the **VPN Log** tab. The VPN log is displayed.
3. Click the right/left arrow buttons to navigate to subsequent/previous VPN Log pages, as required.

Configuring security

Configuring ConstantProtect security policy is simple and intuitive. There are three levels of security:

v High policy: the most secure policy. This policy provides the highest security, but may reduce functionality.

v Med policy: the recommended policy. This policy provides the recommended level of security, while maintaining functionality.

v Low policy: least secure policy. This policy provides minimal security, while providing maximum functionality.

To set the security policy, do the following:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.
2. Click the desired security level on the **Security Level** bar. The **Apply** and **Cancel** buttons appear.
3. Click **Apply**. The security policy is set.

Configuring ConstantProtect network settings

Your current network settings are displayed under the **Network** tab in the **Settings** menu. If you normally connect to the Internet through a proxy server, this server must be defined in the Management Console.

Configuring ConstantProtect network settings

You can change your internal network settings as needed by doing the following:

1. Click **Settings** in the Navigation pane of the Management Console. The main Settings page appears.
2. Click the **Network** tab. The Internal Network Settings page appears in the display area.
3. Click **Modify**. The **IP Address** and **Subnet Mask** fields appear.
4. In the **IP Address** field, type the new device IP address.
5. In the **Subnet Mask** field, type the new device subnet mask.
6. Click **Apply**.

Configuring proxy settings

If you connect to the Internet using a proxy server, you must configure basic settings by doing the following:

1. Click **Settings** in the Navigation pane of the Management Console. The main Settings page appears.
2. Click the **Network** tab. The Network Settings page appears in the display area.
3. Click **Advanced**. The Proxy Settings page appears.
4. Select the **Manual** proxy configuration.
5. In the **HTTP Proxy** field, enter the web address of the proxy server.
6. In the **Port** field, enter the port number on which the proxy server is providing service.
7. Configure additional settings if needed. See "Configuring additional settings."
8. Click **Apply**. The proxy settings are configured.

Configuring additional settings

ConstantProtect includes two additional settings for optimizing performance:

v MTU: If you use a PPPOE dialer to establish an Internet connection, or if you have trouble sending or receiving e-mails, browsing the internet, or receiving updates to ConstantProtect, you might need to adjust the MTU (Maximum Transmission Unit) setting. This is because the Windows MTU setting might be configured to less than the standard MTU, which is 1500. ConstantProtect must be configured to the same MTU as Windows.

v Web Filtering RPC Mode: Some firewalls restrict access to UDP port 9020, which is used by ConstantProtect Web Filtering engine. To overcome this problem, ConstantProtect can allow the Web

Filtering engine to operate on the well-known HTTP port 443, which is always open on the Firewall. This mode of operation is called Remote Procedure Call (RPC) mode.

Note: This feature might slow browsing a little bit, therefore you should only enable it if necessary.

To configure MTU and RPC settings, do the following:

1. Click **Settings** in the Navigation pane of the Management Console. The main Settings page appears.
2. The main Settings page appears. The Network Settings page appears in the display area.
3. Click **Advanced**. The Additional Settings page appears.
4. To change the MTU, select the **Custom MTU** check box and enter the new MTU (default is 1500 bytes).

   Note: Start at 1400 MTU, and then try lower numbers if necessary.
5. To enable RPC mode, select the **Web Filtering RPC mode** check box.
6. Click **Apply**. The settings are saved, and the main Network Settings page appears.

Configuring VPN settings

ConstantProtect includes a generic VPN client that enables you to safely connect to various Remote IPSec VPN Servers. You can enable or disable the VPN client at any time.

Enabling or disabling a VPN connection

To enable or disable a VPN connection, do the following:

1. Click **Settings** in the Navigation pane of the Management Console. The main Settings page appears.
2. Click the **VPN** tab.
3. Do one of the following:
   - v To disable the VPN connection, select **VPN Connection Disabled**.
   - v To enable the VPN connection, click **VPN Connection Enabled**. A confirmation message is displayed.
4. Click **OK**. The VPN Status, displayed below the two options, changes.

Configuring VPN client settings

ConstantProtect supports a number of VPN clients. Each client and the procedure to use is as follows:

- v CheckPoint: Configuring a CheckPoint VPN Connection
- v Cisco: Configuring a Cisco VPN Connection
- v Fortinet: Configuring a Generic VPN Connection
- v Generic: Configuring a Generic VPN Connection
- v IPCop: Configuring a Generic VPN Connection
- v Jupiter: Configuring a Generic VPN Connection
- v NetASQ: Configuring a Generic VPN Connection
- v Zywall P1: Configuring a Generic VPN Connection

Configuring a generic VPN connection

The following procedure is used to configure a Fortinet, IPCop, NetASQ, Jupiter, Zywall P1, or generic VPN connection.

1. Click **Settings** in the Navigation pane of the Management Console. The main Settings page appears.
2. On the **VPN** tab, click **View Settings**. The VPN Settings screen appears.
3. In the **VPN Type** drop-down list box, select one of the following VPN types: **NetASQ**, **Juniper**, **Zywall P1**, **IPCop**, or **Generic**.
4. In the **Connection Type** field, select one of the following connection types: **IPSec Tunnel** or **IPSec Transport**.

5. In the **VPN Gateway Address** field, type the **IP Address** of the remote VPN server.

6. In the **Remote Network Address** field, type the remote network address.

7. In the **Remote Network Mask** field, type the remote network subnet mask.

8. In the **Local ID** field, type the local ID as configured on the remote VPN server.

9. In the **Remote ID** field, type the remote ID as configured on the remote VPN server.

10. If required by the remote VPN server, enable **PFS (Perfect Forward Secrecy)** by selecting the **PFS** check box.

11. If required by the remote VPN server, enable **Aggressive Mode** by selecting the **Aggressive Mode** check box.

12. Under **Authentication Method**, do one of the following:

    v If the authentication method between the client and the server uses a Preshared key, select **Preshared Key** and type the key.

    v If the authentication method between the client and the server uses a certificate, select **Certificate** and click **Browse** to select and upload the certificate file.

13. The default VPN settings use the DES algorithm for encryption and SHA1 message digest for authentication. However, you can set the encryption and authentication methods manually. To do this, select the **Use Manual Settings** check box, and then click **Encryption Method** and **Authentication Method** from the drop-down list boxes.

14. Click **Apply**.

Configuring a CheckPoint VPN connection

To configure a CheckPoint VPN connection, do the following:

1. Click **Settings** in the Navigation pane of the Management Console. The main Settings page appears.

2. On the **VPN** tab, click **View Settings**. The VPN Settings screen appears.

3. In the **VPN Type** drop-down list box, select **CheckPoint**.

4. In the **Remote Network Address** field, type the remote network address.

5. In the **VPN Gateway Address** field, type the IP address of the remote VPN server.

6. In the **Remote Network Mask** field, type the remote network subnet mask.

7. In the **User Name** and **User Password** fields, type your VPN user name and password.

8. In the **Certificate** field, click the **Browse** button to select and upload the certificate file.

9. Click **Apply**.

Configuring a Cisco VPN connection

To configure a Cisco VPN connection, do the following:

1. Click **Settings** in the Navigation pane of the Management Console. The main Settings page appears.

2. On the **VPN** tab click View Settings. The VPN Settings screen appears.

3. In the **VPN Type** drop-down list box, select **Cisco**.

4. In the **Gateway** field, type the IP address of the remote VPN server.

5. In the **Group Name** field, type the name of the IPSec group to which you belong. This entry is case-sensitive.

6. In the **Group Password** field, type the password for your IPSec group. This entry is case-sensitive.

7. In the **User Name** and **User Password** fields, type your VPN user name and password.

8. Select the **NAT-T** box. This option enables the VPN client and the VPN device to automatically detect when to use IPSec over UDP to work properly in Port Address Translation (PAT) environments.

9. Click **Apply**.

Spam e-mail protection settings

Spam is unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or news groups.

Phishing is an Internet scam designed to trick recipients into revealing credit card numbers, passwords, Social Security numbers, and other personal information to individuals who intend to use them for fraudulent purposes.

ConstantProtect provides protection against Spam and Phishing by integrating the powerful MailShell engine. Every e-mail, incoming or outgoing, is scanned by the ConstantProtect to identify and neutralize any security threats in the same manner as all network data is scanned. This includes viruses, spyware, and active content. These e-mails are tagged by Lenovo, and one of the following is inserted into the subject line:

v [Spam]

v [Probably Spam]

v [Phishing]

If needed, you can supplement the tagging of the MailShell engine with your own Custom E-mail rules. For further information, see "Creating custom e-mail rules."

ConstantProtect also generates two spam header files, which can be found in the message source and include the following information:

v SpamLevel: indicates Spam, Probably Spam, Phishing, or empty if not spam

v SpamScore: the exact spam score, from 0 to 100. 100 is definitely spam, and 0 is definitely not spam

Using these header files, you can create rules in your e-mail program to handle these tagged e-mails. For example, you could create rules to automatically delete all e-mails tagged by ConstantProtect as "Spam", or move all messages tagged as "Probably Spam" to a special folder. See the documentation that came with your e-mail program for further information.

Configuring spam protection settings

To configure the spam protection settings, do the following:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.
2. Click the **Email** tab. The Email Settings screen appears.
3. If you want ConstantProtect to tag subject lines of suspicious spam e-mails, select the **Tag Subject lines of suspicious spam** checkbox.
4. Click **Apply**.

Creating custom e-mail rules

You can configure your own spam e-mail definitions by creating custom e-mail rules.

1. Click the + **(plus)** button. The **Custom Email Rules** dialog box appears.
2. In the **Rule Name** field, enter a descriptive name for the rule.
3. In the **If the following condition is met** section, define the condition under which action will be taken.
4. In the **Perform the following action** section, select the action to perform if the condition is met:

   v Allow: does nothing to the e-mail (generally used to create exceptions to other rules)

   v Tag with: tags the message with the text you enter in the text box
5. Click **OK**. The rule is added to the rule list.
6. Click **Apply**. The rule is saved.

Note: Defining a rule adds it to the rule list, but it is saved only when you click **Apply**. Therefore, if you attempt to move to another screen in the ConstantProtect Management Console before clicking **Apply**, you will receive a warning that you must first save your work.

Changing the order in which e-mail rules are applied

If you create multiple e-mail rules, you can determine the order in which the rules are applied. The rule at the top of the list is applied first.

To change the order of custom e-mail rules, select a rule and click the up arrow button to move the rule up in the list or the down arrow button to move the rule down in the list.

Modifying, activating/deactivating, and deleting e-mail rules

You can modify existing rules and delete them when they are no longer needed. You can also temporarily deactivate a rule. To modify a custom e-mail rule, do the following:

1. Double-click the rule you want to modify. The Custom E-mail Rules dialog box appears.
2. Edit the relevant fields. (See "Creating custom e-mail rules" on page 30).
3. Click **OK**.
4. Click **Apply**. The selected rule is modified.

Note: Edits to a rule are saved only when you click **Apply**. Therefore, if you attempt to move to another screen in the ConstantProtect Management Console before clicking **Apply**, you will receive a warning that you must first save your work.

To activate or deactivate a custom e-mail rule, select or clear the check box in the **Active** column of the rule you want to activate or deactivate.

To delete a custom e-mail rule, do the following:

1. Select the rule you want to delete.
2. Click the **- (minus)** button. The rule is deleted from the rule list.
3. Click **Apply**. The deletion is saved.

Note: Deleting a rule removes it from the rule list, but the deletion is saved only when you click **Apply**. Therefore, if you attempt to move to another screen in the ConstantProtect Management Console before clicking **Apply**, you will receive a warning that you must first save your work.

Advanced Security Settings

ConstantProtect includes a number of advanced security settings that give you maximum protection and flexibility:

v Web filtering/parental content control: ConstantProtect can block unwanted Web content. This advanced configuration option enables you to specify the unwanted content categories to be blocked.

v Firewall: ConstantProtect can block unwanted outbound traffic using lists of port numbers, or a whitelist or blacklist.

v Size policy: ConstantProtect can scan files up to 10 MB. You can specify that ConstantProtect block files larger than 10 MB or scan to the size limit.

v Protocols: ConstantProtect uses application layer scanners (Anti-virus, anti-spyware, anti-spam, anti-phishing, Web filtering, and more) on different incoming communication protocols. This advanced configuration option enables you to enable or disable application-level scanning of certain protocols.

v IDS/IPS: ConstantProtect features IDS/IPS protection. This advanced configuration option enables you to specify the security policies for each activity.

Web filtering / parental content control

ConstantProtect can block unwanted Web content. You can determine which types of content should be blocked by selecting from an extensive list of categories. You can also create your own categories by creating custom Web rules. Once created, these rules can be modified, disabled temporarily, and deleted when no longer relevant.

To configure Web filtering categories, do the following:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.
2. Click **Advanced**.
3. Click **Web Filtering**. The Web Filtering screen appears.
4. Select the **Web Filtering enabled** check box to enable Web filtering.
5. Select the check box of the categories you want to filter.
6. To select all categories, click **Block All**. To clear all categories, click **Allow All**.
7. Click **Apply**.

Configuring firewall settings

ConstantProtect can block unwanted inbound and outbound traffic using the following methods:

Direction	Method	Description
Outbound	Blacklist	List of ports over which traffic is blocked.
Outbound	Whitelist	List of ports over which traffic is allowed (for example, all outbound traffic is blocked except the ports on this list).
Inbound and outbound	Rules	Individual ports or port ranges that you either allow or block.

The default predefined security policy specifies that:

v All inbound connections are blocked

v All outbound connections are allowed, with the exception of the predefined blacklist

To modify the policy, you can:

v For both inbound and outbound traffic, add manual policy rules.

v For outbound traffic, modify the Blacklist, or specify the Whitelist (list of acceptable ports) to be used.

The following precedence convention is applied:

1. When there are two or more rules, a rule positioned higher in the list takes precedence over lower ones
2. Rules override (for example, take precedence over) the Blacklist/Whitelist specifications, both predefined and customized. If both the Whitelist and the Blacklist are enabled, the Whitelist overrides any specifications in the Blacklist.

To enable/disable Blacklist/Whitelist-based blocking:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.
2. Click **Advanced**.
3. Click **Firewall**.
4. Do either of the following:

v Clear the **Blacklist** checkbox to disable outbound port blocking (for example, to allow *all* traffic except as specified in the **Rules** in the bottom portion of the screen)

v Select the **Whitelist** check box to block outbound traffic based on the Whitelist (for example, to allow traffic *only* on ports checked in the Whitelist, except as specified in the **Rules** in the bottom portion of the screen)

Note: The Whitelist overrides the Blacklist, thus when the Whitelist is checked, it does not matter whether the Blacklist is checked.

5. To modify the Blacklist or Whitelist, see the procedures below.

6. Click **Apply**. The security policy is set.

   Note: The Blacklist settings will be ignored if a Whitelist is used.

To modify the Blacklist:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.

2. Click **Advanced**.

3. Click **Firewall**. The firewall screen appears.

4. Click the Blacklist link. The Blacklist screen opens.

5. Check all ports to be blocked and clear all ports to be allowed.

6. Click **Apply**. The security policy is set.

Note: Blacklist settings are ignored if a Whitelist is used (See the procedure above to enable/disable Blacklist-based blocking).

To modify the Whitelist:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.

2. Click **Advanced**.

3. Click **Firewall**. The firewall screen appears.

4. Click the Whitelist link. The Whitelist screen opens.

5. Check all ports to be allowed and clear all ports to be blocked.

6. Click **Apply**. The security policy is set (See the procedure above to enable/disable Whitelist-based blocking).

To create and sequence firewall rules:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.

2. Click **Advanced**.

3. Click **Firewall**. The firewall screen appears.

4. Click the + **(plus)** button. The Add firewall rule dialog appears.

5. Specify the following Rule components:

   v Direction: Inbound or outbound traffic

   v Remote IP address: For Inbound traffic, select **Any** or select the option below **Any** and type the IP address of the source. For Outbound traffic, specify **Any** or select the option below **Any** and type the IP address of the destination

   v Port range: Type the range of port numbers (The minimum is 1 and the maximum is 65535). For a single port, use the same port number in both (do not leave one of the two fields blank)

   v Type: Select **UDP**, **TCP**, or Both

   v Action: Select **Allow** or **Block**

    v Comment: Type any free text needed for your personal use. This text appears in a column in the summary table in the **Security** tab. Number of characters permitted is 10.

6. Click **OK**. The rule is added to the list.

7. Repeat the above steps for all rules you want to define. For example, you can create several blocking rules, and then add one at the end that blocks all other traffic.

8. To re-sequence the list of rules:

    v Select a rule and click the up arrow button to move the rule up in the list, or click the down arrow button to move the rule down in the list (Remember that rules higher in the list take precedence over lower ones).

    v Repeat for any other rules to be repositioned.

9. Click **Apply** to save and apply the changes.

To delete a firewall rule:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.

2. Click **Advanced**.

3. Click **Firewall**. The firewall screen appears.

4. Select the rule you want to delete.

5. Click the **- (minus)** button. The rule is deleted from the rule list.

6. Click **Apply**. The deletion is saved.

Note: Deleting a rule removes it from the rule list, but the deletion is saved only when you click **Apply**. Therefore, if you attempt to move to another screen in the ConstantProtect Management Console before clicking **Apply**, you will receive a warning that you must first save your work.

Size policy

ConstantProtect can scan files up to 10 MB. You can specify that ConstantProtect blocks files larger than 10 MB or scans to the size limit.

To configure the size policy:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.

2. Click **Advanced**.

3. Click **Size Policy**. The Size Policy screen appears. If you want ConstantProtect to block all files larger than 10 MB downloaded from the Web (HTTP), select the check box (Not selecting this option means these files will go through but will be scanned for up to 10 MB of their size).

4. Click **Apply**. ConstantProtect blocks or allows large files from the Web according to the specified settings.

Configuring protocol scanning

ConstantProtect uses application layer scanners and engines (Anti-virus, anti-spyware, anti-spam, anti-phishing, Web filtering and more) on different incoming communication protocols. The **Component configuration** option lets you enable or disable application-level scanning of certain protocols and activate or deactivate application-level engines.

To configure protocol scanning:

1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.

2. Click **Advanced**.

3. Click **Components**.

4. Select the check boxes of the protocols you want ConstantProtect to scan.

5. Select the check box of the Security Engine you want ConstantProtect to use:
   - v Select **Mailshell** if you want to activate spam e-mail checks
   - v Select **L-8 Security Agent** if you wish to activate Layer-8 protection
6. Click **Apply**. ConstantProtect scans the protocols according to the specified settings.

Configuring IDS/IPS

ConstantProtect features IDS/IPS protection. In this advanced configuration option you can specify the security policies for each activity.

To configure IDS/IPS protection:
1. Click **Settings** in the Navigation pane of the Management Console. The **Security** tab appears in the Display pane.
2. Click **Advanced**.
3. Click **IDS/IPS**. The IDS/IPS Policy screen appears.
4. Select the **IDS/IPS Enabled** check box.
5. For each activity/threat, select one of the following settings from the drop-down list box:
   - v Allow: ConstantProtect allows this activity and does not log it
   - v Log: ConstantProtect allows this activity and logs it
   - v Block: ConstantProtect blocks the activity and logs it
6. Click **Apply**.

Appendix A. Troubleshooting

The following information provides some troubleshooting hints and tips to assist you if you experience any problems with ConstantConnect.

Problem: The device driver and software installation procedure does not successfully complete. The **Next** button becomes gray and does not respond when clicked. The InstallShield Wizard displays a notification.

Solution: This problem indicates that the device driver and software installation procedure did not successfully complete. To solve the problem, follow the notification in the InstallShield Wizard.

The following are some possible reasons that might stop the device driver and software installation procedure from successfully completing:

v The card is not installed in the computer.
v The BlackBerry smartphone is not attached to the USB connector of the computer.
v The BIOS and Embedded Controller programs do not support the ConstantConnect program. Go to the Lenovo Support Web site (http://www.lenovo.com/support) to upgrade the BIOS and Embedded Controller programs of your computer.
v The ThinkPad Bluetooth Enhanced Data Rate software driver version is earlier than version 5.5. Update it to version 5.5 or later.

Problem: You might fail to receive e-mails using the BlackBerry Enterprise Server.

Solution: Contact your IT administrator to make sure the anti-virus software on the server is not blocking Internet e-mails.

Problem: When you are configuring ConstantConnect outside the Intranet, you might fail to authenticate your Exchange Server mail account(s).

Solution: Use Virtual Private Network (VPN) to gain access to the Exchange Server and authenticate your mail account(s).

Problem: If your IT administrator has configured Exchange Server 2003 using different ports, which means the HTTP Service Port is not 80 (TCP) or the SSL port is not 443 (TCP), ConstantConnect might encounter problems when transferring e-mails.

Solution: You need to add a registry entry to notify ConstantConnect of the different ports:
[HKEY_LOCAL_MACHINE\SOFTWARE\Lenovo\ConstantConnect\ServerPorts*Server_Name*] REG_DWORD "HTTPPort" = *HTTP_Port*

Notes:

1. *Server_Name* refers to your mail server name. For example, if your mail account is myname@mycompany.com, Server_Name = mycompany.com.
2. *HTTP_Port* refers to your HTTP port configured by the IT administrator.

Problem: After you configure ConstantConnect, some e-mails that are blank, sent, or received might be placed in the Draft folder of Outlook.

Solution: The e-mails work as temporary e-mails in the ConstantConnect system. When ConstantConnect has used the temporary e-mails, ConstantConnect may not delete them automatically. You can manually delete the e-mails.

Problem: If you have unpaired the BlackBerry smartphone, a message might continuously ask you to type the link key for the card.

Solution: If you have unpaired the BlackBerry smartphone and the ThinkPad computer by using the BlackBerry smartphone, the BlackBerry smartphone cannot inform ConstantConnect whether you unpair the device or Bluetooth communication breaks. If ConstantConnect does not receive the message that you need to unpair them, the ThinkPad computer or the card will continuously try to connect to the BlackBerry smartphone. To avoid this problem, you should unpair the BlackBerry smartphone and the ThinkPad computer by using the ThinkPad computer. To solve this problem, use the Configuration Wizard to delete or replace the BlackBerry smartphone.

Problem: When you configure ConstantConnect after connecting the BlackBerry smartphone to the ThinkPad computer using the USB cable that came with your BlackBerry smartphone, information for more than one BlackBerry smartphone displays in the Configuration Wizard.

Solution: If you have paired other BlackBerry smartphones with the ThinkPad computer, information for more than one BlackBerry smartphone exists in the ThinkPad computer. If you select the currently connected BlackBerry smartphone to continue the configure scenarios, ConstantConnect will work normally. Otherwise, the configuration will fail in the last step. To solve the problem, switch the BlackBerry smartphone in the Configuration Wizard until you find the currently connected BlackBerry smartphone.

Problem: After you configure ConstantConnect, the Deleted Items folder has many redundant e-mails.

Solution: ConstantConnect transfers the e-mails received offline to the Outlook mail client, and displays them in the Inbox folder of Outlook. When you log in to Outlook, it replicates the e-mails from the mail server, and ConstantConnect will delete the redundant e-mails. Part of the deleted e-mails still exist in the Deleted Items folder. Outlook will delete them automatically in a certain period of time. You can also manually delete them.

Problem: The LED indicator on the card does not turn on.

Solution: Take the card out of the ThinkPad computer, and then insert the card to the ThinkPad computer after at least 15 seconds.

Problem: After you disable ConstantConnect on the BlackBerry smartphone, the Bluetooth indicator on the BlackBerry smartphone flickers at intervals.

Solution: The BlackBerry smartphone might not inform ConstantConnect if you disable ConstantConnect or if Bluetooth communication breaks. If ConstantConnect does not receive the message that you disable ConstantConnect, the ThinkPad computer or the card will continuously try to connect to the BlackBerry smartphone. The BlackBerry smartphone will ignore the connection request.

Problem: After you install ConstantConnect on your ThinkPad computer, the BlackBerry Desktop Manger link is in the **Start** menu. If you run the BlackBerry Desktop Manger by clicking the link, a message might display indicating that this application fails to start because the product.dll file is not found.

Solution: Because ConstantConnect does not install the whole software package of BlackBerry Desktop Manager, you need to reinstall it. Go to the BlackBerry®Web site to download it, or find it on the CD or DVD that came with your BlackBerry smartphone.

Problem: The Configuration Wizard prompts you to select a mail account for ConstantConnect during configuration, but no mail account is available.

Solution: Try the following procedure to fix the problem:

1. Make sure that there are common mail account(s) between Outlook and the BlackBerry smartphone.

2. Make sure that the USB connection between the ThinkPad computer and the BlackBerry smartphone works well.
3. Close the ConstantConnect Configuration Wizard, and then run the Outlook mail client. Send a test mail to any other mail account from the ConstantConnect mail account, and make sure it is successfully sent. Close the Outlook mail client and restart the Configuration Wizard.

Problem: The connection between the ThinkPad computer and the BlackBerry smartphone fails. It might be caused by one of the following reasons:

1. Bluetooth on the BlackBerry smartphone is not enabled.
2. Bluetooth on the ThinkPad computer is not enabled.
3. The BlackBerry smartphone that you connect to the ThinkPad computer is not the same one that you select from the device list.
4. No mail account has been configured on the BlackBerry smartphone.
5. When the BlackBerry smartphone attempts to connect to the ThinkPad computer through Bluetooth communication, the messages on the BlackBerry smartphone receive no response.
6. Bluetooth Headsets might interfere with the connection between the BlackBerry smartphone and the ThinkPad computer.
7. The BlackBerry smartphone that you select from the device list is connected to another ThinkPad computer through Bluetooth communication.
8. The ThinkPad computer has been running for a long period of time.

Solution: The following methods can fix the problem. Try the method that corresponds to your problem to solve it:

1. Enable Bluetooth on the BlackBerry smartphone.
2. Enable Bluetooth on the ThinkPad computer.
3. Replace the BlackBerry smartphone, or select the correct BlackBerry smartphone.
4. Configure a mail account on the BlackBerry smartphone.
5. Respond to the messages on the BlackBerry smartphone. For detailed information, refer to "Configuring your BlackBerry smartphone" on page 13.
6. Pause the Bluetooth Headsets and continue to use them later.
7. Connect the BlackBerry smartphone to the correct ThinkPad computer.
8. Restart the ThinkPad computer. Alternatively, you can disable ConstantConnect, and then enable it.

Problem: When the Installing ConstantConnect to Devices window displays in the Configuration Wizard, a warning message might display indicating that a problem is encountered when ConstantConnect is setting the IP address for the card. After you reinsert the card, the problem might remain.

Solution: Do the following to enable the connection for the card.

1. Depending on your **Start** menu mode, click **Start → Control Panel** or **Start → Settings → Control Panel**. The Control Panel window opens.
2. Depending on your Control Panel mode, double-click **Network Connections** or click **Network and Internet Connections → Network Connections**.
3. Right-click the connection for **Lenovo ConstantConnect**.
4. Click **Properties** in the pop-up window.
5. Click **Configure...**.
6. In the **Device usage** drop-down list box, select **Use this device (enable)**.

Problem: If the model number of your BlackBerry smartphone is 8330 or 8830, the network type is CDMA, and the BlackBerry®Device Software version is 4.5, the **"Bad Socket ID"** or **"Connection closed"** message might display when you are sending an e-mail with an attachment larger than approximately 10 KB.

Solution: You need to check the BlackBerry smartphone model number and the BlackBerry Device Software version by clicking **Options → About**. Check the network type by referring to the top right corner on the BlackBerry smartphone desktop.

For most carriers other than Verizon, you can download a different version (4.2 recommended) of the BlackBerry Device Software from the BlackBerry Web site at: http://na.blackberry.com/eng/support/downloads/#tab_tab_desktop

For the Verizon carrier, if the model number of your BlackBerry smartphone is 8830, download the BlackBerry Device Software version 4.2 from the Verizon Web site at: http://vzw.smithmicro.com/blackberry/

For the Verizon carrier, if the model number of your BlackBerry smartphone is 8330, only the BlackBerry Device Software version 4.5 is available to download. Therefore, you need to contact Verizon for support.

After you downgrade the BlackBerry Device Software, the applications specifically designed for version 4.5 might not be supported.

Problem: Multiple mail accounts might conflict when different users with administrator privileges are using ConstantConnect on the same notebook computer.

Solution: Configure only one mail account in ConstantConnect on the computer shared among multiple users with administrator privileges.

Problem: If you start the Configuration Wizard, and then log in from a limited user account in Microsoft Windows XP, you will not be able to continue using the Configuration Wizard.

Solution: Log in to a user account with administrator privileges before configuring ConstantConnect.

Problem: If Outlook is offline, you might fail to send or reply mails to the short name of a recipient mail address.

Solution: Add the short name into the Outlook mail address book and specify the full mail address.

Problem: If you install AT&T VPN Client to your notebook computer after installing ConstantConnect, a blue screen might appear when you are using ConstantConnect.

Solution: To avoid the blue screen, remove the network filter by referring to "Working with AT&T VPN Client" on page 11.

Problem: After pairing your BlackBerry smartphone with your notebook computer, you might receive a connection request that prompts multiple times on your BlackBerry smartphone.

Solution: By default, the Bluetooth connection is set to **Prompt** on your BlackBerry smartphone, which means the connection request will pop up. You need to manually set the value to **Yes**, which means the Bluetooth connection is allowed, and the connection request will not pop up. For detailed information, refer to "Configuring your notebook computer as a trusted device on your BlackBerry smartphone" on page 13.

Problem: When you are sending or receiving e-mails using ConstantConnect, you might receive a message, saying **"Failed to connect to mail server"** or **"Tunnel failed."**

Solution: Contact your carrier supplier to configure your BlackBerry smartphone with the correct APN settings.

Limitation: After you successfully send an e-mail when the notebook computer is working, the e-mail is stored in the Sent Items folder of Outlook. An error message might display, saying **"The message has not been sent."** The **Send** button might also appear in the Sent Items folder.

Limitation: When you are using a Bluetooth Headset, the Bluetooth connection might become unstable when you are configuring ConstantConnect. If this occurs, make sure you do not block the configuration procedure of ConstantConnect.

Limitation: When the network connection of your BlackBerry smartphone is weak, the ConstantConnect program will have difficulties in sending e-mails with an attachment larger than approximately 600 KB to your recipients.

Limitation: After you change the settings on the **Mail size limit** tab or the **Mail prioritization** tab, the new settings take effect for only the new e-mails. These settings do not apply to the e-mails that ConstantConnect previously sent or received.

Appendix B. Service and Support

The following information describes the technical support that is available for your product, during the warranty period or throughout the life of your product. Refer to the Lenovo Limited Warranty for a full explanation of Lenovo warranty terms.

Registering your option

Register to receive product service and support updates, as well as free and discounted computer accessories and content. Go to:
http://www.lenovo.com/register

Online technical support

Online technical support is available during the lifetime of a product at:
http://www.lenovo.com/support

Product replacement assistance or exchange of defective components also is available during the warranty period. In addition, if your option is installed in a Lenovo computer, you might be entitled to service at your location. A Lenovo technical support representative can help you determine the best alternative.

Telephone technical support

Installation and configuration support through the Customer Support Center will be available until 90 days after the option has been withdrawn from marketing. After that time, the support is cancelled, or made available for a fee, at Lenovo's discretion. Additional support is also available for a nominal fee.

Before contacting a Lenovo technical support representative, please have the following information available: option name and number, proof of purchase, computer manufacturer, model, serial number and manual, the exact wording of any error message, description of the problem, and the hardware and software configuration information for your system.

Your technical support representative might want to walk you through the problem while you are at your computer during the call.

Telephone numbers are subject to change without notice. The most up-to-date telephone list for Lenovo Support is always available at:
http://www.lenovo.com/support/phone

Country or Region	Language	Telephone Number
Africa	--	Africa +44 (0)1475-555-055 South Africa +27-11-3028888 and 0800110756 Central Africa Contact the nearest Business Partner
Argentina	Spanish	0800-666-0011
Australia	English	131-426
Austria	German	0043 0810 100654 (Warranty service and support)

Country or Region	Language	Telephone Number
Belgium	Dutch	02-225-3611 (Warranty service and support)
	French	02-225-3611 (Warranty service and support)
Bolivia	Spanish	0800-10-0189
Brazil	Brazilian Portuguese	Calls made from within the Sao Paulo region (11) 3889-8986 Calls made from outside the Sao Paulo region 0800-701-4815
Brunei	English, Bahasa Melayu	801-1041
Canada	English, French	1-800-565-3344
Caribbean (Bermuda, Jamaica, Tortola)	English	1-877-426-7378
Chile	Spanish	800-361-213 or 188-800-442-488 Toll free
China	Mandarin	ThinkPad®battery recall 8008103315 (Toll free) 86-10-58859595
		Technical Support Line 800-990-8888 86-10-58851110
China (Hong Kong S.A.R.)	Cantonese, English, Mandarin	ThinkPad battery recall 2516-3900 (Hong Kong)
		ThinkPad (Technical enquiry hotline): 2516-3939 (Hong Kong)
		ThinkPad Service Center: 2825-6580 (Hong Kong)
		ThinkCentre®Commercial PC: 8205-0333 (Hong Kong)
		Multimedia Home PC: 800-938-228 (Hong Kong)
China (Macau S.A.R.)	Cantonese, English, Mandarin	ThinkPad battery recall 0800-839 (Macau)
		ThinkPad (Technical enquiry hotline): 0800-839 (Macau)
		ThinkPad Service Center: 2871-5399 (Macau)
		ThinkCentre Commercial PC: 795-9892 (Macau)
		Multimedia Home PC: 0800-336 (Macau)
Colombia	Spanish	1-800-912-3021
Costa Rica	Spanish	0-800-011-1029
Croatia	--	0800-0426
Cyprus	--	+357-22-841100
Czech Republic	--	+420-2-7213-1316

Country or Region	Language	Telephone Number
Denmark	Danish	7010-5150 (Warranty service and support)
Dominican Republic	Spanish	1-866-434-2080
Ecuador	Spanish	1-800-426911
Egypt	--	+202-35362525
El Salvador	Spanish	800-6264
Estonia	--	+372 66 00 800 +372 6776793
Finland	Finnish	+358-800-1-4260 (Warranty service and support)
France	French	Hardware 0810-631-213 (Warranty service and support) Software 0810-631-020 (Warranty service and support)
Germany	German	01805-004618
Greece	--	+30-210-680-1700
Guatemala	Spanish	1800-624-0051
Honduras	Spanish	Tegucigalpa: 232-4222 San Pedro Sula: 552-2234
Hungary	English, Hungarian	+36 1 3825716 +36 1 3825720
India	English	1800-425-2666 +91-80-2535-9182
Indonesia	English, Bahasa Indonesian	021 5238 823 001-803-606-282 (Local number only) +603 8315 6859 (DID)
Ireland	English	01-881-1444 (Warranty service and support)
Israel	Hebrew, English	ThinkPad battery recall 972-3-5313742 (03-5313742)
	Hebrew, English	+972-3-531-3900 - Givat Shmuel Service Center
Italy	Italian	+39-800-820094 (Warranty service and support)
Japan	--	ThinkPad battery recall 0120-277-874
	Japanese, English	PC Products Toll free: 0120-20-5550 For International: +81-46-266-4716 **Note:** The above numbers will be answered with a Japanese language voice prompt. For telephone support in English, please wait for the Japanese voice prompt to end, and an operator will answer. Please ask for ″English support please,″ and your call will be transferred to an English speaking operator.
	Japanese	IntelliStation and xSeries Inside Japan and overseas calls: +81-46-266-1358
	Japanese	PC Software 0120-558-695 (Overseas calls: +81-44-200-8666)

Country or Region	Language	Telephone Number
Korea	Korean	1588-6782
Latvia	--	+371 7070360
Lithuania	--	+370 5 278 66 00
Luxembourg	French	+352-360-385-343
Malaysia	English, Bahasa Melayu	1800-88-1889 (Local number only) +603 8315 6855 (DID)
Malta	--	+35621445566
Mexico	Spanish	001-866-434-2080
Middle East	--	+44 (0)1475-555-055
Netherlands	Dutch	+31-20-514-5770
New Zealand	English	0800-733-222
Nicaragua	Spanish	001-800-220-1830
Norway	Norwegian	8152-1550 (Warranty service and support)
Panama	Spanish	206-6047
		001-866-434-2080 (Lenovo Customer Support Center - Toll free)
Peru	Spanish	0-800-50-866
Philippines	English, Filipino	1800-1601-0033 (Local number only) +603 8315 6858 (DID)
Poland	Polski	General number +48 22 760-73-00
Portugal	Portuguese	+351 21 892 7046
Romania	--	+4-021-224-4015
Russia	Russian	Moscow +7 (495) 258 6300 Toll free 8 800 200 6300
Singapore	English	800 6011 343 (Local number only) +603 8315 6856 (DID)
Slovakia	--	+421-2-4954-5555
Slovenia	Slovenian	+386-1-200-50-60
Spain	Spanish	91-714-7983 0901-100-000
Sri Lanka	English	+9411 2493547 +9411 2493548
Sweden	Swedish	077-117-1040 (Warranty service and support)
Switzerland	German, French, Italian	0800-55-54-54 (Warranty service and support)
Taiwan	Mandarin	886-2-8723-9799 0800-000-700
Thailand	Thai, English	1-800-060-066 (Local number only) 66 2273 4088 +603 8315 6857 (DID)

Country or Region	Language	Telephone Number
Trinidad and Tobago	English	1-800-645-3330
Turkey	Turkish	00800-4463-2041
United Kingdom	English	08705-500-900 (Standard warranty support)
United States	English	1-800-426-7378 For Aptiva 2270 or NetVista 2276 systems: 1-800-584-9182
Uruguay	Spanish	000-411-005-6649
Venezuela	Spanish	0-800-100-2011
Vietnam	Vietnamese, English	For Northern Area and Hanoi City: 844 3 946 2000 or 844 3 942 6457 For Southern Area and Ho Chi Minh City: 848 3 829 5160 or 844 3 942 6457

Generating a support file

You can generate and save a support file that contains all ConstantConnect logs, configuration data, and other relevant information. This file can then be sent to a Lenovo support expert for analysis.

To generate a support file:

1. Click **Support** in the Navigation pane of the Management Console. The main Support page opens.
2. Click the **Support Tools** tab.
3. Click **Support File**. The support file is generated and the **File Download** window opens.
4. Specify the file name and click **Save**. The Save As window opens.
5. Navigate to the directory where you want to save the support file and then click **Save**.

Appendix C. Lenovo Limited Warranty

L505-0010-01 04/2008

This Lenovo Limited Warranty applies only to Lenovo branded hardware products you purchased for your own use and not for resale. This Lenovo Limited Warranty is available in other languages at www.lenovo.com/warranty.

What this Warranty Covers

Lenovo warrants that each hardware product that you purchase is free from defects in materials and workmanship under normal use during the warranty period. The warranty period for the product starts on the original date of purchase specified on your sales receipt or invoice unless Lenovo informs you otherwise in writing. The warranty period and type of warranty service that apply to your product are designated below under the section titled ″**Warranty Information.**″

THIS WARRANTY IS YOUR EXCLUSIVE WARRANTY AND REPLACES ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF EXPRESS OR IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. IN THAT EVENT, SUCH WARRANTIES APPLY ONLY TO THE EXTENT REQUIRED BY LAW AND ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. NO WARRANTIES APPLY AFTER THAT PERIOD. SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATION ON DURATION MAY NOT APPLY TO YOU.

How to Obtain Warranty Service

If the product does not function as warranted during the warranty period, you may obtain warranty service by contacting Lenovo or an approved service provider. Each of them is referred to as a ″Service Provider.″ A list of Service Providers and their telephone numbers is available at www.lenovo.com/support/phone.

Warranty service may not be available in all locations and may differ from location to location. Charges may apply outside a Service Provider's normal service area. Contact a local Service Provider for location-specific information.

What Your Service Provider Will Do to Correct Problems

When you contact a Service Provider, you must follow the problem determination and resolution procedures specified.

Your Service Provider will attempt to diagnose and resolve your problem over the telephone, e-mail, or through remote assistance. Your Service Provider may direct you to download and install designated software updates.

Some problems can be resolved with a replacement part that you can install yourself called a ″Customer Replaceable Unit″ or ″CRU.″ If so, your Service Provider will ship the CRU to you for you to install.

If your problem cannot be resolved over the telephone or remotely, through your application of software updates or the installation of a CRU by you, your Service Provider will arrange for service under the type of warranty service designated for the product under the section titled ″**Warranty Information**.″

If your Service Provider determines that it is unable to repair your product, your Service Provider will replace it with one that is at least functionally equivalent.

If your Service Provider determines that it is unable to either repair or replace your product, your sole remedy is to return the product to your place of purchase or to Lenovo for a refund of your purchase price.

Replacement of a Product or Part

When the warranty service involves the replacement of a product or part, the replaced product or part becomes Lenovo's property and the replacement product or part becomes your property. Only unaltered Lenovo products and parts are eligible for replacement. The replacement product or part provided by Lenovo may not be new, but it will be in good working order and at least functionally equivalent to the original product or part. The replacement product or part shall be warranted for the balance of the period remaining on the original product.

Before your Service Provider replaces a product or part, you agree to:
1. remove all features, parts, options, alterations, and attachments not under warranty service;
2. ensure that the product or part is free of any legal obligations or restrictions that prevent its replacement; and
3. obtain authorization from the owner to have your Service Provider service a product or part if you do not own it.

Your Additional Responsibilities

Where applicable, before service is provided, you agree to:
1. follow the service request procedures that your Service Provider specifies;
2. backup or secure all programs and data contained in the product;
3. provide your Service Provider with all system keys or passwords and sufficient, free, and safe access to your facilities to perform service; and
4. ensure that all information about identified or identifiable individuals (″Personal Data″) is deleted from the product or that, with respect to any Personal Data that you did not delete, you are in compliance with all applicable laws.

Use of Personal Information

If you obtain service under this warranty, Lenovo will store, use, and process information about your warranty service and your contact information, including name, phone numbers, address, and e-mail address. Lenovo will use this information to perform service under this warranty and to improve our business relationship with you. We may contact you to inquire about your satisfaction regarding our warranty service or to notify you about any product recalls or safety issues. In accomplishing these purposes, we may transfer your information to any country where we do business and may provide it to entities acting on our behalf. We may also disclose it where required by law.

What this Warranty Does not Cover

This warranty does not cover the following:
v uninterrupted or error-free operation of a product;
v loss of, or damage to, your data;
v any software programs, whether provided with the product or installed subsequently;
v failure or damage resulting from misuse, accident, modification, unsuitable physical or operating environment, natural disasters, power surges, or improper maintenance by you;
v damage caused by a non-authorized service provider;
v failure of, or damage caused by, any third party products, including those that Lenovo may provide or integrate into the Lenovo product at your request; and

v any technical or other support, such as assistance with ″how-to″ questions and those regarding product set-up and installation.

This warranty is voided by removal or alteration of identification labels on the product or its parts.

Limitation of Liability

Lenovo is responsible for loss or damage to your product only while it is: 1) in your Service Provider's possession; or 2) in transit in those cases where the Service Provider is responsible for the transportation.

Neither Lenovo nor your Service Provider is responsible for any of your data including confidential, proprietary, or personal data contained in a product. You should remove and/or backup all such information from the product prior to its service or return.

Circumstances may arise where, because of a default on Lenovo's part or other liability, you may be entitled to recover damages from Lenovo. In each such instance, regardless of the basis of your claim against Lenovo (including breach, negligence, misrepresentation, or other contract or tort claim), except and to the extent that liability cannot be waived or limited by applicable laws, Lenovo shall not be liable for more than the amount of actual direct damages suffered by you, up to the amount you paid for the product. This limit does not apply to damages for bodily injury (including death) and damage to real property or tangible personal property for which Lenovo is liable under law.

This limit also applies to Lenovo's suppliers, resellers, and your Service Provider. It is the maximum amount for which Lenovo, its suppliers, resellers, and your Service Provider are collectively responsible.

UNDER NO CIRCUMSTANCES SHALL LENOVO, ITS SUPPLIERS, RESELLERS, OR SERVICE PROVIDERS BE LIABLE FOR ANY OF THE FOLLOWING EVEN IF INFORMED OF THEIR POSSIBILITY: 1) THIRD PARTY CLAIMS AGAINST YOU FOR DAMAGES; 2) LOSS OR DAMAGE TO YOUR DATA; OR 3) SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, BUSINESS REVENUE, GOODWILL OR ANTICIPATED SAVINGS. AS SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

Dispute Resolution

If you acquired the product in **Cambodia, Indonesia, Philippines, Vietnam or Sri Lanka**, disputes arising out of or in connection with this warranty shall be finally settled by arbitration held in Singapore and this warranty shall be governed, construed and enforced in accordance with the laws of Singapore, without regard to conflict of laws. If you acquired the product in **India**, disputes arising out of or in connection with this warranty shall be finally settled by arbitration held in Bangalore, India. Arbitration in Singapore shall be held in accordance with the Arbitration Rules of Singapore International Arbitration Center (″SIAC Rules″) then in effect. Arbitration in India shall be held in accordance with the laws of India then in effect. The arbitration award shall be final and binding on the parties without appeal. Any award shall be in writing and set forth the findings of fact and the conclusions of law. All arbitration proceedings, including all documents presented in such proceedings, shall be conducted in the English language, and the English language version of this warranty prevails over any other language version in such proceedings.

Other Rights

THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE OR JURISDICTION TO JURISDICTION. YOU MAY ALSO HAVE OTHER RIGHTS UNDER APPLICABLE LAW OR WRITTEN AGREEMENT WITH LENOVO. NOTHING IN THIS WARRANTY AFFECTS STATUTORY RIGHTS, INCLUDING RIGHTS OF

CONSUMERS UNDER NATIONAL LEGISLATION GOVERNING THE SALE OF CONSUMER GOODS THAT CANNOT BE WAIVED OR LIMITED BY CONTRACT.

European Economic Area (EEA)

Customers in the EEA may contact Lenovo at the following address: EMEA Service Organisation, Lenovo (International) B.V., Floor 2, Einsteinova 21, 851 01, Bratislava, Slovakia. Service under this warranty for Lenovo hardware products purchased in EEA countries may be obtained in any EEA country in which the product has been announced and made available by Lenovo.

Warranty Information

Product Type	Country or Region of Purchase	Warranty Period	Type of Warranty Service
Lenovo ConstantConnect and Protect	United States, Canada, United Kingdom, Italy, France, Germany, and Spain	1 year	1, 4

If required, your Service Provider will provide repair or exchange service depending on the type of warranty service specified for your product and the available service. Scheduling of service will depend upon the time of your call, parts availability, and other factors.

A warranty period of three (3) years on parts and one (1) year on labor means that Lenovo will provide warranty service without charge for:

a. parts and labor during the first year of the warranty period (or a longer period as required by law); and

b. parts only, on an exchange basis, in the second and third years of the warranty period. Your Service Provider will charge you for any labor provided in performance of the repair or replacement in the second and third years of the warranty period.

Types of Warranty Service

1. Customer Replaceable Unit (″CRU″) Service

Under CRU Service, your Service Provider will ship CRUs to you for installation by you. CRU information and replacement instructions are shipped with your product and are available from Lenovo at any time upon request. CRUs that are easily installed by you are called Self-service CRUs, while Optional-service CRUs may require some technical skill and tools. Installation of Self-service CRUs is your responsibility. You may request that a Service Provider install Optional-service CRUs under one of the other types of warranty service designated for your product. An optional service offering may be available for purchase from Lenovo to have Lenovo install Self-service CRUs for you. You may find a list of CRUs and their designation in the publication that ships with your product or at www.lenovocom/ CRUs. The requirement to return a defective CRU, if any, will be specified in the materials shipped with a replacement CRU. When return is required: 1) return instructions, a prepaid return shipping label, and a container will be included with the replacement CRU; and 2) you may be charged for the replacement CRU if your Service Provider does not receive the defective CRU within thirty (30) days of your receipt of the replacement.

2. On-site Service

Under On-Site Service, your Service Provider will either repair or exchange the product at your location. You must provide a suitable working area to allow disassembly and reassembly of the Lenovo product. For some products, certain repairs may require your Service Provider to send the product to a designated service center.

3. Courier or Depot Service

Under Courier or Depot Service, your product will be repaired or exchanged at a designated service center, with shipping arranged by your Service Provider. You are responsible for disconnecting the product. A shipping container will be provided to you for you to return your product to a designated service center. A courier will pick up your product and deliver it to the designated service center. Following its repair or exchange, the service center will arrange the return delivery of the product to you.

4. Customer Carry-In or Mail-In Service

Under Customer Carry-In or Mail-In Service, your product will be repaired or exchanged at a designated service center, with delivery or shipping arranged by you. You are responsible to deliver or mail, as your Service Provider specifies, (prepaid by you unless specified otherwise) the product, suitably packaged to a designated location. After the product has been repaired or exchanged, it will be made available for your collection. Failure to collect the product may result in your Service Provider disposing of the product as it sees fit. For Mail-in Service, the product will be returned to you at Lenovo's expense, unless your Service Provider specifies otherwise.

5. Product Exchange Service

Under Product Exchange Service, Lenovo will ship a replacement product to your location. You are responsible for its installation and verification of its operation. The replacement product becomes your property in exchange for the failed product, which becomes the property of Lenovo. You must pack the failed product in the shipping carton used to ship the replacement product and return it to Lenovo. Transportation charges, both ways, are paid by Lenovo. Failure to use the carton in which the replacement product was received may result in your responsibility for damage to the failed product during shipment. You may be charged for the replacement product if Lenovo does not receive the failed product within thirty (30) days of your receipt of the replacement product.

Suplemento de Garantía para México

Este Suplemento se considera parte integrante de la Garantía Limitada de Lenovo y será efectivo única y exclusivamente para los productos distribuidos y comercializados dentro del Territorio de los Estados Unidos Mexicanos. En caso de conflicto, se aplicarán los términos de este Suplemento.

Todos los programas de software precargados en el equipo sólo tendrán una garantía de treinta (30) días por defectos de instalación desde la fecha de compra. Lenovo no es responsable de la información incluida en dichos programas de software y/o cualquier programa de software adicional instalado por Usted o instalado después de la compra del producto.

Los servicios no cubiertos por la garantía se cargarán al usuario final, previa obtención de una autorización.

En el caso de que se precise una reparación cubierta por la garantía, por favor, llame al Centro de soporte al cliente al 001-866-434-2080, donde le dirigirán al Centro de servicio autorizado más cercano. Si no existiese ningún Centro de servicio autorizado en su ciudad, población o en un radio de 70 kilómetros de su ciudad o población, la garantía incluirá cualquier gasto de entrega razonable relacionado con el transporte del producto a su Centro de servicio autorizado más cercano. Por favor, llame al Centro de servicio autorizado más cercano para obtener las aprobaciones necesarias o la información relacionada con el envío del producto y la dirección de envío.

Para obtener una lista de los Centros de servicio autorizados, por favor, visite:

http://www.lenovo.com/mx/es/servicios

Manufactured by:
Lenovo Centro Tecnológico S. de R.L. de C.V.
Apodaca Technology Park
Boulevar Escobedo #316
Apodaca, Nuevo León, México
C.P. 66601

Marketing by:
Lenovo México S. de R.L. de C.V.
Av. Santa Fe 505, Piso 15
Col. Cruz Manca
Cuajimalpa, D.F., México
C.P. 05349
Tel. (55) 5000 8500

Appendix D. Electronic emission notices

The following information refers to ConstantConnect and Protect.

Federal Communications Commission (FCC) Emission Notice

ConstantConnect and Protect - (3321-20U)

FCC ID: XGE210SA1

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
v Reorient or relocate the receiving antenna.
v Increase the separation between the equipment and receiver.
v Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
v Consult an authorized dealer or service representative for help.

Changes or modifications to this equipment not expressly approved by the party responsible for compliance Yoggie Security Systems Ltd. could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

If the FCC ID is not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module.

Responsible party:
    Yoggie Security Systems
    280 Northern Blvd
    Great Neck, NY 11021
    U.S.A.
    Phone number: 1-866-428-0040

FC

SAR Statement

The radiated energy from the ConstantConnect and Protect card radio module conforms to the FCC limit of the SAR (Specific Absorption Rate) requirement set forth in 47 CFR Part 2 section 1093, when installed in the host notebook computer.

55

Interference Statement

An improper installation or unauthorized use may cause harmful interference to radio communications. Also, any tampering with the internal antenna will void the FCC Certification and your warranty. Refer to the Appendix D, "Electronic emission notices," on page 55 for more detail.

Industry Canada Class B emission compliance statement

This Class B digital apparatus complies with Canadian ICES-003.

Canada – Industry Canada (IC)

ConstantConnect and Protect IC ID: 8443A-210SA1

Low Power License-Exempt Radio Communication Devices (RSS-210)

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Exposure of humans to RF fields (RSS-102):

ConstantConnect and Protect employs low gain integral antennas that do not emit RF field in excess of Health Canada limits for the general population; consult Safety Code 6, obtainable from Health Canada's Web site at: http://www.hc-sc.gc.ca/rpb

European Union - Compliance to the Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. Lenovo and Yoggie Security Systems Ltd. cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the installation of option cards from other manufacturers.

This product has been tested and found to comply with the limits for Class B Information Technology Equipment according to European Standard EN 55022. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communication devices.

Europe - EU Declaration of Conformity for ConstantConnect and Protect

Products intended for sale within the European Union are marked with the Conformité Européenne (CE) Marking, which indicates compliance with the applicable Directives and European Norms, and amendments, identified below.

Yoggie Security Systems Ltd. declares that ConstantConnect and Protect is in conformity with the protection requirements of Council RTTE Directive 1999/5/EC of the European Parliament and of the council on radio equipment and telecommunications terminal equipment. Conformity with these Directives has been assessed for this product by demonstrating compliance to the following harmonized standards:
    EN 300328 V1.7.1 :2006
    EN 301489-1 V1.8.1 :2008
    EN 301489-17 V1.3.2 :2008

EN 60950-1: 2006

Responsible party:
   Yoggie Security Systems Ltd.
   Beth Halevy, Israel
   P.O. Box 156

Hereby, Lenovo (Singapore) Pte. Ltd. declares that ConstantConnect and Protect is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Par la présente **Lenovo (Singapore) Pte. Ltd.** dćclare que l'appareil **Lenovo ConstantConnect and Protect** est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Hiermit erklärt **Lenovo (Singapore) Pte. Ltd.,** dass sich das Gerät **Lenovo ConstantConnect and Protect** in Übereinstimmung mit der grundlegender Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.

Por medio de la presente **Lenovo (Singapore) Pte. Ltd.** declara que el **Lenovo ConstantConnect and Protect** cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

YOGGIE

the end of efear

yoggie security systems ltd. Beth Halevy, Israel 42870 P.O. Box 156   972.9.894.4900 · 972.9.894.4800

EC Declaration of Conformity

For Product: Wireless network application card
Model: ConstantConnect and Protect
P/N: 210-SA-0001.

which is equivalent to Lenovo branded product:
Lenovo ConstantConnect and Protect (P/N: 3321-20U)

We, Yoggie Security Systems Ltd., declare under sole responsibility that the above products,
manufactured by:

**Yoggie Security Systems Ltd.
Beth Halevy, Israel
P.O. Box 156**

to which this declaration relates, is in conformity with the requirements of the following EC Directives:

- Council Directive 1999/5/EC of the European Parliament and of the council on radio equipment and telecommunications terminal equipment.

Conformity with these Directives has been assessed for this product by demonstrating compliance to the following harmonized standards:

EN 300328 V1.7.1 :2006
EN 301489-1 V1.8.1 :2008
EN 301489-17 V1.3.2 :2008
EN 50371: 2002
EN 60950-1: 2006

Signed: _____   Date: 13/8/09
    Yoggie Security System Ltd.
    Ami Oz, Director of Hardware Development

Last two digits of the year in which the CE marking was affixed: ___09___

Place of issue: Yoggie Security Systems, Beth Halevy, Israel

Yoggie Security Systems Confidential Information   Page 1 of 1
Jan 2009

Appendix E. Important information for the European Directive 2002/96/EC

EU Only

The Waste Electrical and Electronic Equipment (WEEE) mark applies only to countries within the European Union (EU) and Norway. Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive. Users of electrical and electronic equipment (EEE) with the WEEE marking per Annex IV of the WEEE Directive must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to them for the return, recycle, recovery of WEEE and minimize any potential effects of EEE on the environment and human health due to the presence of hazardous substances. For additional WEEE information go to: http://www.lenovo.com/lenovo/environment.

PDF created with pdfFactory trial version www.pdffactory.com

Appendix F. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Recycling information

Lenovo encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. Lenovo offers a variety of programs and services to assist equipment owners in recycling their IT products. For information on recycling Lenovo products, go to: http://www.lenovo.com/lenovo/environment/recycling

Trademarks

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Lenovo
The Lenovo logo
ThinkCentre
ThinkPad

BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ and related trademarks, names and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world. Used under license from Research In Motion Limited.

Lenovo ConstantConnect and Protect is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited.

Microsoft, Outlook, and Windows are trademarks of the Microsoft group of companies.

Other company, product, or service names may be trademarks or service marks of others.

Appendix G. Hardware specifications

Components	
CPU	Freescale iMX31L
Flash memory	512 MB
RAM	256 MB
Combo radio	AW – GH600
Form factor	34mm (1.34 inches) card compatible with a hidden antenna
Interface	
Power supplying interface	Connect to PCI-Express slot of the notebook computer complying with EN60950-1:06. It is powered by 3.3V dc from the computer through standard PCI interface with available power up to a maximum of 25 W
USB	Compatible with ExpressCard interface specification/USB 2.1 + EDR (supports host and slave modes)
LED Indicators	Two green LEDs
Sync Now button	Tells the card to immediately wake up and check for new e-mail.
Power management	Always on, even when the computer is S3/S4/S5, and the USB connection coming into the selective suspend Power Management: Remote power management using SM BUS
Environmental	
Dimensions	Standard card 34 mm (1.34 inches)
Weight	16 gram
Power consumption	Maximum 2W
Supply voltage	3.3 V +/-10%
Environmental compliance	RoHS
Operating temperature	0 to 65°C (32°F to 149°F)
Storage temperature	-20°C to 80°C (-4°F to 176°F)
Operating humidity	10 to 80% non-condensing
Storage humidity	5 to 90% non-condensing

lenovo

Part Number: 45K1937

Printed in China

(1P) P/N: 45K1937