User Guide for Zone Labs IMsecure Pro

version 1.0

ZONE LABS

Smarter Security™

Zone Labs Inc.
475 Brannan, Suite 300
San Francisco, CA 94107

ZLD 1-0223-0100-2003-08-12

Contents

Tables

Figures

Preface

About this guide

This guide is intended for users of IMsecure and IMsecure Pro. With the exception of encryption, all security component features described in this guide are available only in IMsecure Pro. With IMsecure, you can encrypt the traffic of one instant messaging account. Throughout this guide, these products are collectively referred to as Zone Labs IMsecure Pro.

All screenshots used in this guide depict the user interface elements as displayed in IMsecure Pro.

Conventions

This guide uses the following formatting and graphics conventions.

Convention	Description
Bold, sans-serif font	Used for emphasis within tables, notes, tips, and cautions.
Bold, serif font	Used for user interface elements such as panels, tabs, fields, buttons, and menu options.
Italic, sans-serif	Used for glossary terms, file names, and paths.
|	Used to separate panel and tab selections in procedures. Example: Select **Overview|Status**, then click **Add**.
💡	Tip icon. Suggests alternative methods for accomplishing tasks or procedures.
☑	Note icon. Emphasizes related, reinforcing, or important information.
⚠	Caution icon. Indicates actions or processes that can potentially damage data or programs.

Formatting conventions

Zone Labs IMsecure Pro User Community

Connect with other users of Zone Labs IMsecure Pro. Ask questions, get answers, and see how fellow users get the most out of their IMsecure instant messaging protection. Free to all Zone Labs IMsecure Pro users!

Visit: http://www.zonelabs.com/community

IMsecure third-party software terms and conditions

THIRD PARTY SOFTWARE: OpenSSL

OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THIRD PARTY SOFTWARE: Bzip2

This program, “bzip2” and associated library “libbzip2”, are copyright (C) 1996-2002 Julian R Seward. All rights reserved.

THIRD PARTY SOFTWARE: Regexp

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

Chapter 1

Installation and setup

This chapter describes the Zone Labs IMsecure Pro system requirements, installation, set up, and uninstallation processes.

Topics:

System requirements and supported software

This section lists the hardware and software needed to run Zone Labs IMsecure Pro.

Operating systems

The computer on which you want to install Zone Labs IMsecure Pro must have one of the following operating systems:

- Windows XP, Home or Professional Edition
- Windows 2000 Professional
- Windows 98 SE
- Windows ME

Additional requirements

For additional requirements specific to your operating system, refer to the sections below:

Windows XP Home or Professional Edition

- Intel Pentium 300MHz or higher processor
- 128MB of RAM
- 10MB of available hard-disk space

Windows 2000 Professional

- Intel Pentium 233MHz or higher processor
- 64MB of RAM
- 10MB of available hard-disk space

Windows 98 SE or Windows ME

- Intel Pentium 233MHz or higher processor
- 32MB of RAM (48MB recommended)
- 10MB of available hard-disk space

Supported instant messaging programs

Zone Labs IMsecure Pro supports programs that access instant messaging services using one or more of the following protocols:

- AOL Instant Messenger (as supported in AIM 4.3 or later)
- Yahoo! Messenger (as supported in Yahoo! Instant Messenger 5.0 or later)
- MSN Messenger (as supported in MSN Messenger 4.0 or later)

Installing Zone Labs IMsecure Pro

Before you begin the installation process, you must insert the Zone Labs IMsecure Pro CD into your CD-ROM drive. If you downloaded the software from the Zone Labs web site, browse to the location on your computer where you saved the installation file.

To install Zone Labs IMsecure Pro:

1. Double-click the installation file.
   The setup program starts.
2. Either specify a location for the program, or click **Next** to continue.
   The default location is *C:\Program Files\IMsecure*.
3. Type your name, company (optional), and e-mail address, then click **Next**.
4. Read and accept the license agreement, then click **Install**.
5. Click **Finish** to close the installation program.

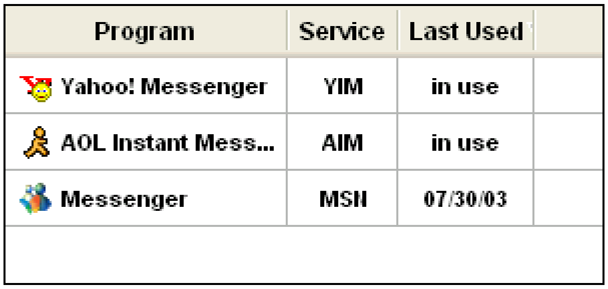
Getting started with Zone Labs IMsecure Pro

To launch Zone Labs IMsecure Pro after installation, double-click on the desktop icon, or select **Zone Labs|IMsecure** from the Windows Start menu. Once launched, Zone Labs IMsecure Pro runs in the background.

Close any open instant messaging programs before launching Zone Labs IMsecure Pro. After launching Zone Labs IMsecure Pro, start up each instant messaging program that you want to protect.

To open the main application window, double-click the Zone Labs IMsecure Pro icon in the system tray.

When you launch the instant messaging programs after launching Zone Labs IMsecure Pro, each program is listed in the Overview panel, along with the date the program was last used.



Program	Service	Last Used
Yahoo! Messenger	YIM	in use
AOL Instant Mess...	AIM	in use
Messenger	MSN	07/30/03

Figure 1-1: Verifying status of instant messaging programs

To close Zone Labs IMsecure Pro, right-click the system tray icon and choose **Shutdown IMsecure Pro**.

Uninstalling Zone Labs IMsecure Pro

If you want to uninstall Zone Labs IMsecure Pro, run the uninstall program included with your installation rather than using the Windows Add/Remove Programs utility. This ensures that all traces of Zone Labs IMsecure Pro are removed from your computer.

To uninstall Zone Labs IMsecure Pro:

1. Select **Start|Programs**.
2. Select **Zone Labs|IMsecure|Uninstall**.

   The Uninstallation program starts.

You must be logged in as a user with administrator privileges in order to uninstall Zone Labs IMsecure Pro.

Chapter 2

Zone Labs IMsecure Pro basics

This chapter offers you a tour of the Zone Labs IMsecure Pro Control Center and helps you perform the basic operations necessary to set up the program.

Topics:

About Zone Labs IMsecure Pro

Zone Labs IMsecure Pro is the first comprehensive instant messaging (IM) security solution for MSN Messenger, Yahoo! Messenger, and AOL Instant Messenger as well as third-party clients such as Trillian. IMsecure Pro keeps IM conversations private and protects PCs from IM spammers, identity thieves, hackers and predators who exploit vulnerable IM connections.

This release of IMsecure Pro includes the following features:

- **Inbound threat protection** - Guards your PC by filtering invalid messages, buffer overflow, dangerous scripts, and executable URLs.
- **ID Lock** - Defends against unauthorized sending of your sensitive information (e.g., credit card number) from your PC.
- **Spam Blocker**- Blocks messages sent by people not on your contact lists.
- **Message Encryption** - Protects your IM traffic from being intercepted and read by others.
- **Feature Control** - Determines which IM features are allowed on your PC.
- **IM Blocking** - Controls which IM services can be accessed using your PC.
- **Event Logging** - Keeps you informed about IM security events on your PC.

⚠ The protection features described above apply only to one-on-one conversations. Zone Labs IMsecure Pro does not protect conversations with more than one participant (for example, chat room conversations).

Tour of the Zone Labs IMsecure Pro Control Center

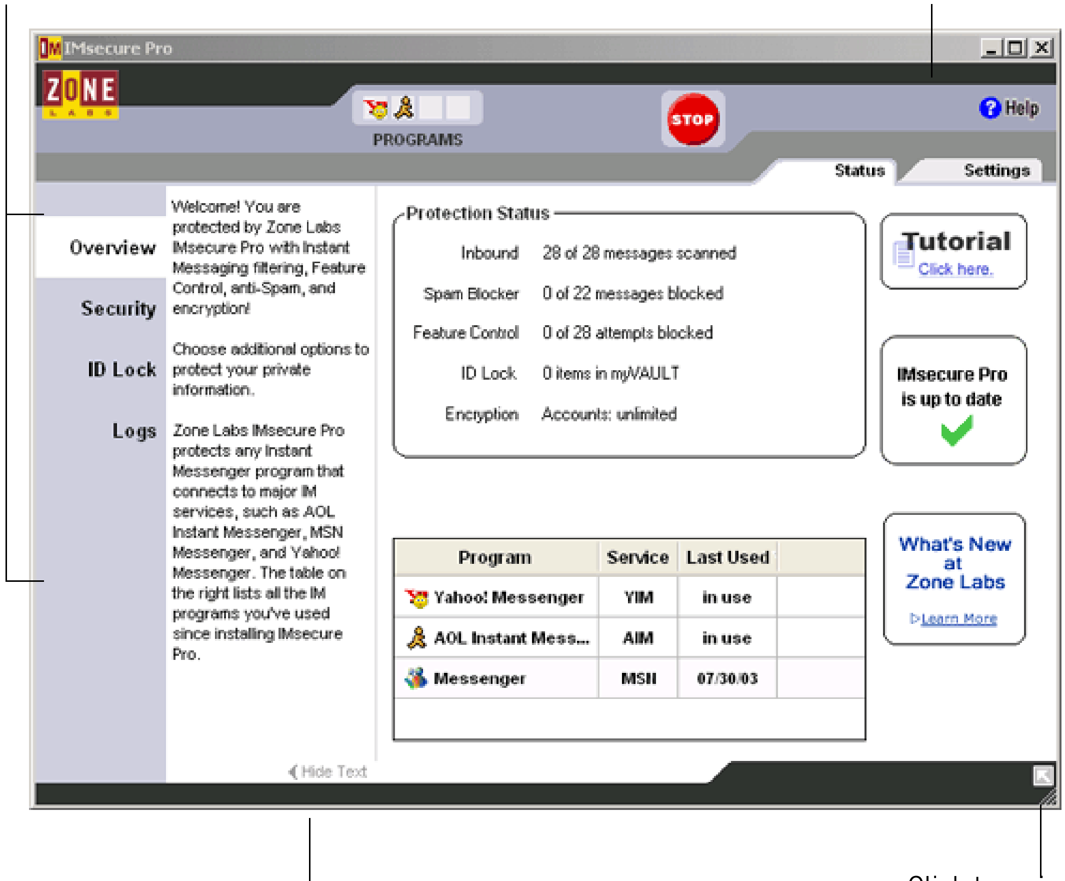
The Zone Labs IMsecure Pro Control Center provides one-stop access to the security features that keep your computer safe. The Zone Labs IMsecure Pro major features are presented in a menu on the left side of the Control Center. When Zone Labs IMsecure Pro is installed and running the icon IM appears in the Windows system tray.

Getting around the Control Center

To move from one feature to another, first click the desired feature in the menu at the left, then click the tab you want to view.

Menu bar

Dashboard



Welcome! You are protected by Zone Labs IMsecure Pro with Instant Messaging filtering, Feature Control, anti-Spam, and encryption!

Choose additional options to protect your private information.

Zone Labs IMsecure Pro protects any Instant Messenger program that connects to major IM services, such as AOL Instant Messenger, MSN Messenger, and Yahoo! Messenger. The table on the right lists all the IM programs you've used since installing IMsecure Pro.

Inbound	28 of 28 messages scanned
Spam Blocker	0 of 22 messages blocked
Feature Control	0 of 28 attempts blocked
ID Lock	0 items in myVAULT
Encryption	Accounts: unlimited

IMsecure Pro is up to date ✓

Program	Service	Last Used
Yahoo! Messenger	YIM	in use
AOL Instant Mess...	AIM	in use
Messenger	MSN	07/30/03

Click to show or hide help text

Click to resize

Figure 2-1: Zone Labs IMsecure Pro Control Center

Menu bar

The menu bar located on the left provides access to available panels. All features within a panel are arranged into tabs.

Show / Hide text

The **Show/Hide text** button is located at the bottom of the application. The help text provides a brief description of the tab and its features. Click the **Show/Hide text** button to show or hide the help text for the selected tab.

Using the dashboard

The dashboard provides constant access to the basic security indicators and functions. To display only the dashboard, click the resize button on the Control Center.

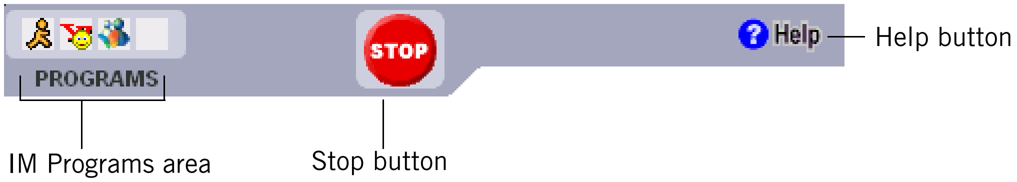


Figure 2-2: Zone Labs IMsecure Pro dashboard.

Programs area

The Programs area shows icons of instant messaging programs that are currently open and that have accessed the Internet during your current session. To see information about these applications, move your mouse pointer over its icon.

When a program is sending or receiving data, its icon will blink.

Stop button

The **Stop** button immediately blocks all instant messaging traffic. Click **Stop** only if you suspect you are being attacked, or when you want to leave your computer unattended and disable messaging functionality temporarily. To re-open access, click the **Stop** button again.

> Clicking the Stop button automatically logs you out of all instant messaging sessions.

Help button

To immediately get help for the current panel, click the **Help** button in the right-hand corner of the panel. The Zone Labs IMsecure Pro online Help system will display the information on the current tab.

Setting preferences

Use the **Settings** tab to set or change your Zone Labs IMsecure Pro password, log in or log out, manage updates, set the general options for the display of the Control Center.

Setting your password

By setting a password, you prevent anyone but you from shutting down or uninstalling Zone Labs IMsecure Pro, or changing your security settings. Setting a password will not prevent other people from accessing instant messaging programs from your computer unless you also have blocked access to all instant messaging programs.

If your version of Zone Labs IMsecure Pro was installed by an administrator with an installation password, the administrator can access all functions.

When you set a password for the first time, be sure to log out before leaving your computer. Otherwise, others can still change your settings.

To set or change a Zone Labs IMsecure Pro password:

1. Select **Overview|Settings**.
2. Click **Set Password**.
3. Type and verify your password in the fields provided, then click **OK**.

Valid passwords are between 6 and 31 characters long. Valid characters include A-Z, a-z, 0-9, and characters !,@,#,$,%,^,&,*.

Once you have set a password, you must log in before you can change the settings.

Setting update options

When you purchase Zone Labs IMsecure Pro, you receive either one or two years of free updates, depending on your subscription period. You can check for updates manually or set Zone Labs IMsecure Pro to do it automatically.

To configure the updates checking settings:

1. Select **Overview|Settings**.
2. In the **Check for Updates** area, choose an update option.

Automatically	Zone Labs IMsecure Pro automatically notifies you when an update is available.
Manually	You monitor the Status tab for updates.

Setting general preferences

By default, Zone Labs IMsecure Pro starts automatically when you turn on your computer. Use the settings in the **General** area if you need to change this option, to decide when the Control Center will be displayed, to protect the Zone Labs IMsecure Pro software, and to customize its appearance.

To set the general display preferences:

1. Select **Overview|Settings**.

2. In the **General** area, specify your preferences.

Load Zone Labs IMsecure Pro on startup	Zone Labs IMsecure Pro will start automatically when you turn on your computer.
Remember the last tabs visited in the panels	Zone Labs IMsecure Pro will open to the tab that was open the last time you closed the Control Center.
Notify my contacts that I am protected by IMsecure	When you initiate a conversation with a contact after installing Zone Labs IMsecure Pro, your contact will receive notification that you are protected. **Note:**This notification occurs only during the first session after installation. Your contacts will not be notified during subsequent sessions.
Notify me of the encryption status of each IM session	Zone Labs IMsecure Pro marks beginning of each IM session with the specified label.
Mark each INCOMING encrypted message with	Attaches the specified label to Zone Labs IMsecure Pro to **encrypted** incoming messages. The default label is “encrypted.”
Mark each INCOMING unencrypted message with	Attaches the specified label Zone Labs IMsecure Pro to **unencrypted** incoming messages. The default label is “unencrypted.”
Notify me when harmful content is filtered	Zone Labs IMsecure Pro will display a message in your IM window when potentially harmful content is filtered from an IM conversation.

When the options “Mark each...message with” are selected, Zone Labs IMsecure Pro will mark only the incoming messages with the specified label, as there is no mechanism for marking outgoing messages. If you tend to have more than one instant messaging window open at a time, set these options so that you can be sure which conversations are secure.

Licensing, registration, and support

In order to receive support and updates from Zone Labs, you must have a valid license.

If you have been using a trial or beta license key and you have purchased a full license, or if your trial or beta version is about to expire, you can purchase a full license from Zone Labs.

To change your license key:

1. Select **Overview|Settings**.
2. In the **Licensing Information** area, click **Change Lic**.
   The **License Information** dialog will appear.
3. In the space provided, either type or paste your license key.
4. Click **Apply**, then click **OK**.

Registering Zone Labs IMsecure Pro

Register Zone Labs IMsecure Pro to receive security news from Zone Labs.

To register Zone Labs IMsecure Pro:

1. Select **Overview|Settings**.
2. In the Registration area, click **Change Reg**.
   The Registration Information dialog appears.
3. Type your name, organization, and e-mail address in the fields provided.
4. To get the product news, and to be notified of the updates, select the **Inform me of important updates and news** check box.
5. Click **OK**.

To change your registration information:

☞ Select **Overview|Settings**, then click **Change Reg**.

Accessing technical support

If you are eligible for technical support, you can access support resources such as FAQs and known issues directly from Zone Labs IMsecure Pro.

To access support resources:

1. Select **Overview|Settings**.
2. In the **Support and Update Information** area, click **Click here**.
3. The Zone Labs Support Center Web site will appear.
4. Click **Support & Services**, then select the product for which you need support.

Status information

The protection area of the Status tab tells you which instant messaging services are installed, which protection components are enabled, and provides a summary of security activity. From the Status tab you can:

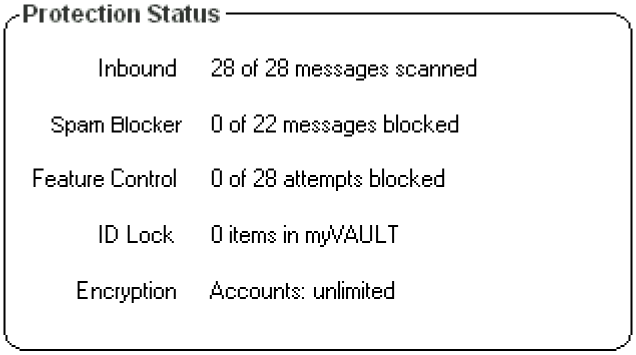
- See at a glance if your computer is secure
- See a summary of Zone Labs IMsecure Pro's activity
- See if your version of Zone Labs IMsecure Pro is up to date
- Access the product tutorial

To learn more about Zone Labs IMsecure Pro, click the **Learn more** link.

Protection Status

The Protection Status area provides a summary of activity for installed security components. In addition, the Status page provides a list of installed instant messaging programs, along with the last date of use.

If you are using Zone Labs IMsecure Pro, you already have access to each of the security components listed below. If you are using IMsecure, you can click on any of the components listed below to go to the purchase area of the Zone Labs IMsecure Pro Web site where you can buy a license for Zone Labs IMsecure Pro.


Protection Status

Inbound	28 of 28 messages scanned
Spam Blocker	0 of 22 messages blocked
Feature Control	0 of 28 attempts blocked
ID Lock	0 items in myVAULT
Encryption	Accounts: unlimited

Figure 2-3: Protection Status area

The following security components are currently available:

Features	Description
Inbound protection	Blocks the incoming links to executable files and validating messages thus guarding your computer from Trojan horses and hacker attacks.
Spam Blocker	Blocks messages sent by people who are not in your contact list.
Feature Control	Helps parents protect their children from getting unwanted media content through instant messaging services.
ID Lock	Prevents unauthorized sending of your private information (for example, a credit card number) from your computer.
Encryption	Encrypts all incoming and outgoing correspondence in supported Instant Messengers. Other users should have Zone Labs IMsecure Pro installed and support the same IM software in order to use encryption.

Table 2-3: Available security components displayed in the Protection Status area

Chapter 3

Using Zone Labs IMsecure Pro

Zone Labs IMsecure Pro is your front line of defense against instant messaging threats. Zone Labs IMsecure Pro's default security levels give you immediate protection against hackers, spam, and provides controls that prevent inappropriate Web content from being sent to your instant messaging client. ID Lock protects you from identity thieves by keeping your personal data secure.

Topics:

Setting security options

IMsecure Pro protects you by applying restrictions to instant messaging software, filtering spam, and encrypting Instant Message traffic. In addition, the ID Lock prevents your personal data from leaving your computer without your authorization. You can specify your desired level of protection by using pre-defined options, or by manually customizing individual security settings.

Setting protection level

The key to getting the right level of protection for your needs is to set the appropriate protection level.

The default Medium protection level balances security with convenience by allowing instant messaging functions, while ensuring that your instant messaging communications are secure.

The High security setting prevents your instant messaging programs from sending media files of all types, filters spam messages, and enables encryption of instant messaging traffic.

The Off setting disables instant messaging protection. Disabling protection leaves your computer vulnerable to hacker attacks. Your instant messaging conversations could be intercepted and read by others.

To set the global protection level:

1. Select **Security|Status**.
2. In the **Protection Level** area, click the slider and drag it to the desired setting.

High	The High security setting prevents your instant messaging programs from sending media files of all types, filters spam messages, executable URLs, and encrypts instant messaging traffic.
Medium	This is the default setting. The Medium security setting encrypts instant messaging traffic and filters executable URLs.
Off	All security settings are disabled.

Customizing protection settings

By setting the Protection Level to High, Med, or Off, you specify globally whether instant messaging programs can send files, JavaScript, and links to your instant messaging client. In some cases, you may want to specify settings for an individual service that are different than these global settings allow. For example, if you wanted to allow your contacts on a particular instant messaging service to send and receive video, but keep security High for all other instant messaging services, you could set the permission for that service to Allow.

To customize protection settings:

1. Select **Security|Settings**.
2. Locate the service you want to modify, then right-click in the column for the content you want to customize.

Access	Controls whether instant messaging communication is allowed or blocked. If set to Block, instant messaging traffic is stopped.
Spam Blocker	Specifies whether to block or allow messages sent by people who are not in your contact list.
Feature Control	Specifies whether transmission of Audio, Video, or Files is allowed or blocked.
Inbound	Specifies whether formatting tags, such as JavaScript or executable links, can be contained in inbound communication.
Encrypt	Specifies whether instant messaging traffic should be encrypted.

> To return to the default Medium protection level, select **Security|Status**, then click **Reset to Defaults**.

Access

The Access control lets you allow or block traffic for a particular instant messaging service.

To block or allow IM traffic for a particular service:

1. Select **Security|Settings**.
2. In the **Access** column, click beside the instant messaging for which you want to block or allow traffic.
3. Select **Allow** or **Block**.

Blocking Spam

Zone Labs IMsecure Pro provides a Spam Blocker control that filters out unsolicited communications from senders who are not on your contact list. By default, Spam Blocker is enabled only when the Protection Level is set to High, however you can customize your settings to enable Spam Blocker for a particular service regardless of the protection level.

With Spam Blocker enabled, any communication that is sent by someone who is not in your contact list is filtered out.

> You will not see visual confirmation that Zone Labs IMsecure Pro blocked an incoming message, however, you can refer to the log to determine the sender's identity. If you wish to receive future messages from the sender, be sure to add the sender's ID to your contact list. Blocked messages appear in the Log Viewer with "A message from someone not on your contact list was blocked" in the Type column.

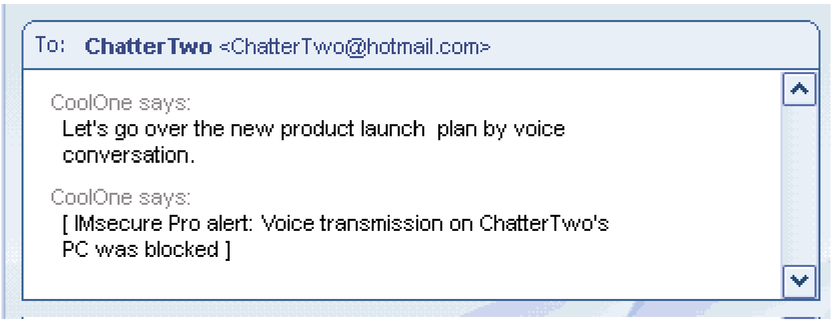
To enable or disable Spam Blocker for a particular service:

1. Select **Security|Settings**.
2. Locate the instant messaging service you want to customize, then click in the **Spam Blocker** column.
3. Choose **On** or **Off**.

Feature Control

Feature Control settings allow you to restrict the types of media that you receive during an instant messaging session. Because inappropriate content can be sent in many forms, Zone Labs IMsecure Pro allows parents to protect their children by blocking audio, video, and other types of files.

Figure 3-1 depicts a conversation in which a voice conversation was blocked. This particular example illustrates what the sender—in this case, **CoolOne—**-sees in his instant messaging window when he attempts to initiate a voice conversation with his contact **ChatterTwo**, who has set the Feature Control Audio option to **Block**.

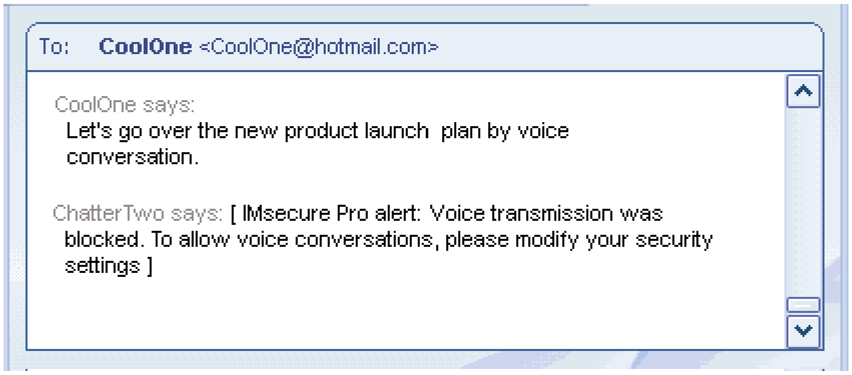

To: **ChatterTwo** <ChatterTwo@hotmail.com>

CoolOne says:
Let's go over the new product launch plan by voice conversation.

CoolOne says:
[IMsecure Pro alert: Voice transmission on ChatterTwo's PC was blocked]

Figure 3-1: Sending a voice transmission that is blocked

Figure 3-2 shows the same conversation from the point-of-view of the recipient—in this case **ChatterTwo**, who has blocked an incoming Audio transmission sent by his contact **CoolOne**.


To: **CoolOne** <CoolOne@hotmail.com>

CoolOne says:
Let's go over the new product launch plan by voice conversation.

ChatterTwo says: [IMsecure Pro alert: Voice transmission was blocked. To allow voice conversations, please modify your security settings]

Figure 3-2: Blocking an incoming voice transmission

To customize Feature Control settings:

1. Select **Security | Settings**.
2. Locate the instant messaging service you want to customize, then click in the **Feature Controls** column.
3. Click in the **Audio**, **Video**, or **Files**, then choose **Allow** or **Block**.

Inbound protection

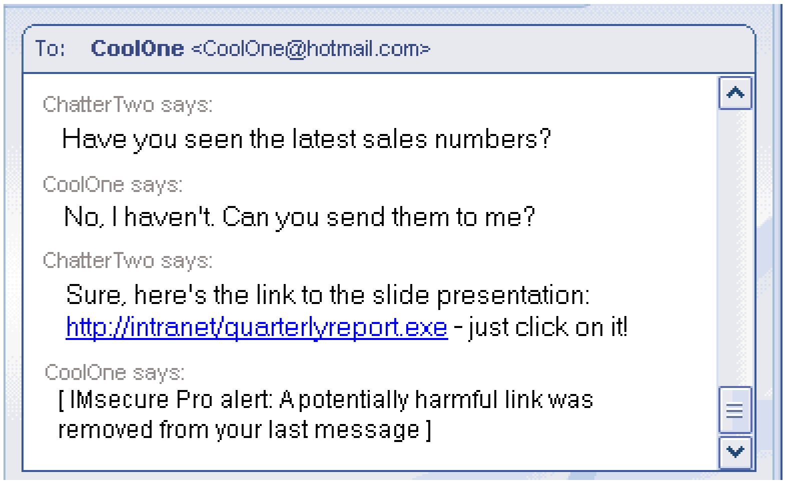
Inbound protection settings let you specify which instant messaging services are allowed to transmit active links and formatting tags, such as JavaScript, in incoming messages. Active links and formatting tags can contain viruses that can attack your computer when you click on a link in a message.

The Inbound “Tags” setting removes extra formatting that could contain scripts and other potentially harmful code.

> Be aware that the Tags setting also removes innocuous visual formatting, such as bold, underline, italic, etc.

The “Active” setting blocks links that, if clicked, could execute code or download dangerous files onto your computer.

Figure 3-3 depicts an IM conversation in which the sender, **ChatterTwo**, attempts to send an executable link to his contact **CoolOne**, who has set the Inbound Active control to **Block**.



To: **CoolOne** <CoolOne@hotmail.com>

ChatterTwo says:
Have you seen the latest sales numbers?

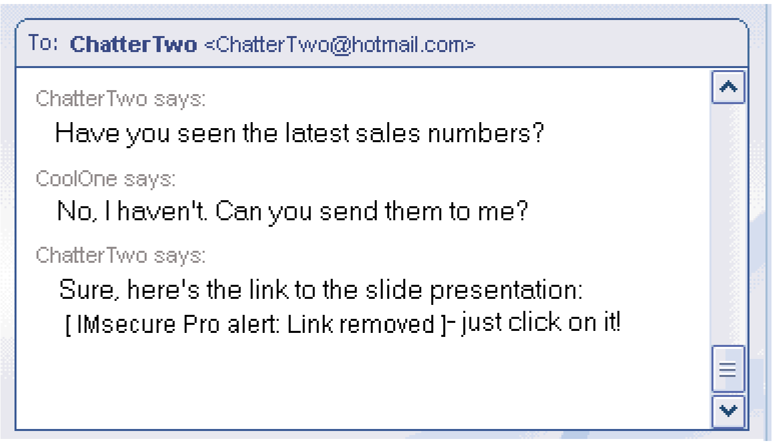
CoolOne says:
No, I haven't. Can you send them to me?

ChatterTwo says:
Sure, here's the link to the slide presentation:
http://intranet/quarterlyreport.exe - just click on it!

CoolOne says:
[IMsecure Pro alert: A potentially harmful link was removed from your last message]

Figure 3-3: Sending an executable URL to a contact

Figure 3-4 below, shows the same conversation from the point-of-view of the recipient, CoolOne. Notice how the link **http://intranet/quarterlyreport.exe** was removed before being transmitted to the recipient’s computer.



To: **ChatterTwo** <ChatterTwo@hotmail.com>

ChatterTwo says:
Have you seen the latest sales numbers?

CoolOne says:
No, I haven't. Can you send them to me?

ChatterTwo says:
Sure, here's the link to the slide presentation:
[IMsecure Pro alert: Link removed]- just click on it!

Figure 3-4: Potentially harmful link removed

To customize inbound protection settings:

1. Select **Security**|**Settings**.
2. Locate the instant messaging service you want to customize, then click in the **Inbound** column.

3. Click below **Tags** or **Active**, then choose **Allow** or **Block**.

Encrypting instant messaging traffic

Zone Labs IMsecure Pro relies on the *OpenSSL* library for cryptographic services. The text of each message in a secure session is encrypted with the *DES* 56-bit cipher.

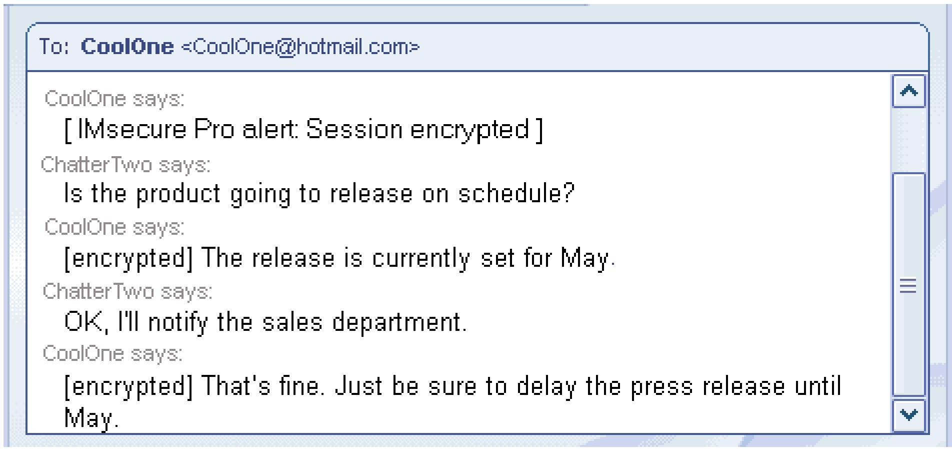
IMsecure Pro automatically and transparently creates a *self-signed certificate* for each of the user's IM accounts upon the first login. At the beginning of the first IM conversation between two Zone Labs IMsecure Pro users after installing Zone Labs IMsecure Pro, the certificates are transparently exchanged between the users and stored on their computers. The public key from one of the certificates is used to encrypt the session key to be used for the duration of the session. To encrypt conversations with your contacts, they must have Zone Labs IMsecure Pro installed and have an account on the same supported IM service.

Encrypted and unencrypted conversations

When you initiate a conversation with another IMsecure Pro user, and you both have encryption enabled for the IM service you're connected to, the word **encryption** appears in brackets after your contact's instant messaging ID. If you initiate a conversation with a contact who is not using IMsecure Pro but does not have encryption enabled, you will see the word **unencrypted** after the contact's instant messaging ID.

The words "encrypted" and "unencrypted" that appear in your instant messaging window are the default settings. You can customize the label applied to encrypted and unencrypted sessions by customizing your preference settings. See "Setting general preferences," on page 12.

Figure 3-5 below shows an example of an encrypted conversation. **ChatterTwo**, who is the sender of this message, sees the label [encrypted] at the beginning of each message received from his contact, **CoolOne**.

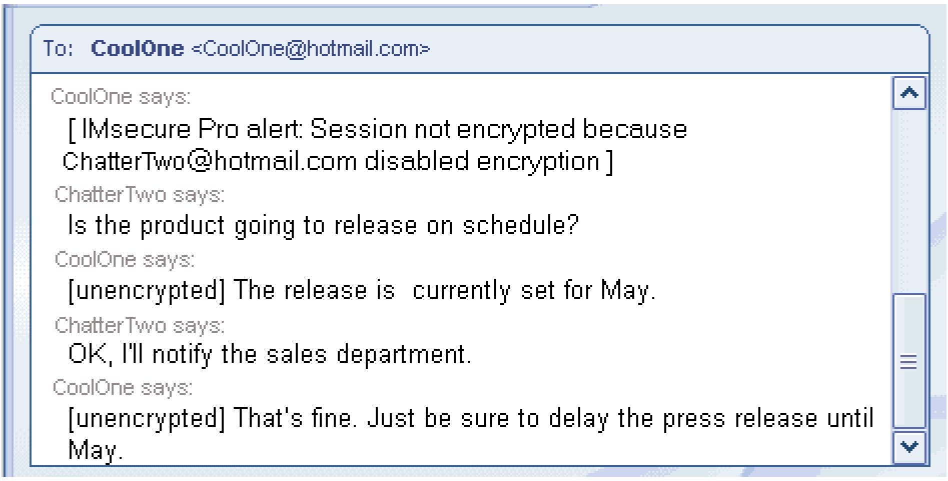


To: **CoolOne** <CoolOne@hotmail.com>

CoolOne says:
[IMsecure Pro alert: Session encrypted]
ChatterTwo says:
Is the product going to release on schedule?
CoolOne says:
[encrypted] The release is currently set for May.
ChatterTwo says:
OK, I'll notify the sales department.
CoolOne says:
[encrypted] That's fine. Just be sure to delay the press release until May.

Figure 3-5: Example of an encrypted conversation

Here is the same conversation shown above, but in unencrypted mode this time.



To: **CoolOne** <CoolOne@hotmail.com>

CoolOne says:
[IMsecure Pro alert: Session not encrypted because ChatterTwo@hotmail.com disabled encryption]
ChatterTwo says:
Is the product going to release on schedule?
CoolOne says:
[unencrypted] The release is currently set for May.
ChatterTwo says:
OK, I'll notify the sales department.
CoolOne says:
[unencrypted] That's fine. Just be sure to delay the press release until May.

Figure 3-6: Example of an Unencrypted conversation

To enable or disable encryption for a particular IM service:

1. Select **Security|Settings**.
2. In the Encrypt column, click beside the service whose traffic you want to encrypt.
3. Select **Allow** or **Block**.

Understanding the ID Lock

Because of the convenience provided by the Internet, many transactions that once were conducted in person or by telephone—such as paying bills, applying for a loan, or booking a flight—are now conducted online, providing a welcome convenience for many, and an unwelcome risk for some. Unfortunately, the rise of e-commerce also has resulted in a rise in the incidents of identity theft.

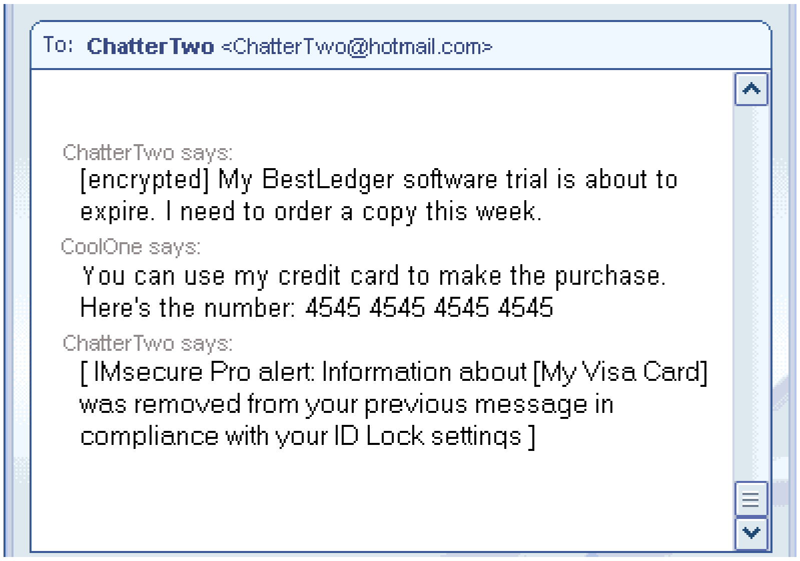
Every time you or someone else using your PC enters personal information—such as a credit card number, your address, or social security number—into an instant messaging window, it is possible that your information could fall into the wrong hands. The ID Lock feature provides a secure area, called myVAULT, where you can store personal information that you want to protect. The contents of myVAULT are blocked from being transmitted, whether by you, someone else using your PC, or by a Trojan horse attempting to use an open instant messaging channel to transmit your personal information.

Enabling and disabling ID Lock

By enabling the ID Lock, you ensure that the data entered in myVAULT will be protected from hacker attacks and identity theft during your instant messaging sessions.

Figure 3-7 illustrates an instant messaging conversation in which **CoolOne** transmits information that is stored in myVAULT. The description of the item stored in myVAULT (in this example, My Visa Card) appears in brackets.

Although CoolOne can see the credit card number he has entered, Zone Labs IMsecure Pro removes the information before it sends the message to his contact **ChatterTwo**.



To: **ChatterTwo** <ChatterTwo@hotmail.com>

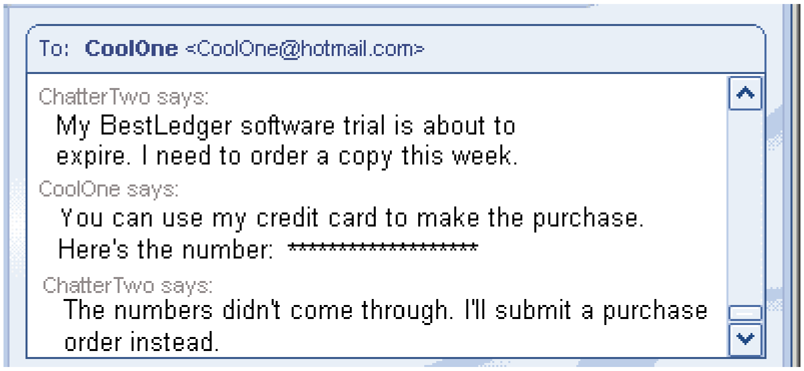
ChatterTwo says:
[encrypted] My BestLedger software trial is about to expire. I need to order a copy this week.

CoolOne says:
You can use my credit card to make the purchase. Here's the number: 4545 4545 4545 4545

ChatterTwo says:
[IMsecure Pro alert: Information about [My Visa Card] was removed from your previous message in compliance with your ID Lock settings]

Figure 3-7: Transmission of myVAULT contents

Figure 3-8 shows how the transmitted information is displayed to the recipient. Notice how the protected information is replaced with asterisks so that it is unreadable.



To: **CoolOne** <CoolOne@hotmail.com>

ChatterTwo says:
My BestLedger software trial is about to expire. I need to order a copy this week.

CoolOne says:
You can use my credit card to make the purchase. Here's the number: *******************

ChatterTwo says:
The numbers didn't come through. I'll submit a purchase order instead.

Figure 3-8: Receipt of myVAULT contents

To enable or disable ID Lock:

1. Select **ID Lock|Main**.

2. In the ID Lock area, specify **On** or **Off**. .

On	Blocks transmission of identity information.
Off	Allows sending identity information.

Monitoring ID Lock status

Zone Labs IMsecure Pro's Status area keeps track of the number of items stored in myVAULT, and displays the number of times your information was protected.

Using myVAULT

The myVAULT feature provides a secure area for entering your critical personal data—data that could be used by hackers and identity thieves. When it detects an attempt to send data stored in myVAULT to another PC, Zone Labs IMsecure Pro determines whether the information should be blocked or allowed.

While you can store any type of information in myVAULT, it is a good idea only to store information that you wish to keep secure, such as credit card numbers and identification numbers. If you were to store your state (for example, California) in myVAULT separately from the rest of your address, any time you typed "California" during an instant messaging session Zone Labs IMsecure Pro would block transmission of the data.

If you're unsure of the type of information that should be entered into myVAULT, refer to the pre-defined categories for guidance. You can access the list of categories by Selecting **ID Lock|myVAULT**, then clicking **Add**

To add information to myVAULT:

1. Select **ID Lock|myVAULT**.

2. Click **Add**.

The **Add information to myVAULT** dialog box will appear.

3. Enter information as follows:

Description	Data description.
Category	Choose one of the following predefined categories: • Access PIN • Address • American Express card • Bank account • Credit card • Driver's license • E-mail address • International Tax ID • Mother's maiden name • Name • Passport number • Password • Phone • Social security number • Other
Information to protect	Data to be protected. Data format is defined and validated by the selected category.

Asterisks will appear in place of the data you entered and an encrypted form of your data will be stored in myVAULT. Zone Labs IMsecure Pro will compare the encrypted data with your outgoing messages.

Data encryption is enabled by default. If you do not want to encrypt your data, clear the "Use one-way encryption..." check box. Because of the sensitive nature of the data, PIN numbers, passwords, the last four digits of your social security number, and the last four digits of your credit card numbers will always be displayed as asterisks, whether or not you choose to encrypt them.

4. Click **OK** to save your the changes.

To view myVAULT contents:

1. Select **ID Lock|myVAULT**.

2. Click an entry to view personal information details.

To edit or remove myVAULT contents:

1. Select **ID Lock|myVAULT**.

2. Select the entry you want to edit or remove, then click **Edit** or **Remove**.

Logging security events

Zone Labs IMsecure Pro's logging feature keeps you aware of what's happening on your computer and enables you to go back at any time to investigate past events.

Enabling and disabling event logging

Use the **Event Logging** area to enable or disable event logging.

To enable or disable event logging:

1. Select **Alerts and Logs|Settings**.

2. In the **Event Logging** area, specify the desired setting.

On	Creates a log entry for all events.
Off	No events are logged.

Viewing log entries

If **Event Logging** option is turned on, each event is added in the event log. You can sort the list by any field by clicking the column header. The arrow next to the header indicates the sort order. Click the same header again to reverse the sort order.

To view events in the Log Viewer:

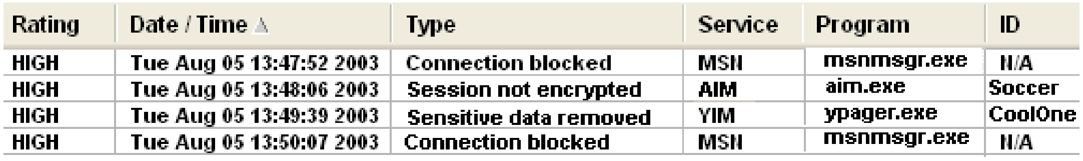
1. Select **Alerts and Logs|Log Viewer**.

2. Select the number of alerts to display in the alerts list (from 1 to 999).

3. Click a log entry to view the entry details.

Log Viewer fields

The **Log Viewer** shows security events that have been recorded in the Zone Labs IMsecure Pro event log. Figure 3-9 shows an excerpt from the event log as displayed in the Log Viewer.



Rating	Date / Time	Type	Service	Program	ID
HIGH	Tue Aug 05 13:47:52 2003	Connection blocked	MSN	msnmsgr.exe	N/A
HIGH	Tue Aug 05 13:48:06 2003	Session not encrypted	AIM	aim.exe	Soccer
HIGH	Tue Aug 05 13:49:39 2003	Sensitive data removed	YIM	ypager.exe	CoolOne
HIGH	Tue Aug 05 13:50:07 2003	Connection blocked	MSN	msnmsgr.exe	N/A

Figure 3-9: Log Viewer details

Table below provides an explanation of each of these log viewer fields.

Field	Explanation
Rating	Event rating based on the **Protection Level** of the security option.
Date/Time	Date and time the event occurred
Type	Brief description of the event. Depending upon the security settings that were violated (for example, Spam Blocker, ID Lock, etc.), this field may contain any of the following descriptions: • Connection blocked • A message from someone not on your contact list was blocked • Media transmissions • Potentially harmful content removed • A link to active content removed • Encrypted session established • Session not encrypted • Sensitive data removed
Service	The service on which the event occurred.
Program	The instant messaging program (displayed as the application file) that was connected when the event occurred.
ID	The user ID of the instant messaging contact that triggered the event.

Log Viewer field explanations

Troubleshooting

If you experience problems while using Zone Labs IMsecure Pro, consult the following section for guidance and troubleshooting tips.

Connecting to the Internet fails after installation

If you are unable to connect to the Internet after installing Zone Labs IMsecure Pro, the first troubleshooting step is to determine whether Zone Labs IMsecure Pro is the cause. If you are unable to follow the steps below, for example, if you cannot clear the Load Zone Labs IMsecure Pro at startup box, uninstall Zone Labs IMsecure Pro, then reboot your system.

To determine if Zone Labs IMsecure Pro is the cause of connection problems:

1. Select **Overview|Settings**.
2. In the General area, clear the check box **Load Zone Labs IMsecure Pro at startup**.
3. Restart your computer, then try to connect to the Internet.

If you can connect	Your Zone Labs IMsecure Pro settings may be the cause of your connection problems. Make sure that your browser has access permission.
If you cannot connect	Your Zone Labs IMsecure Pro settings are not the cause of your connection problems.

If you are using Windows 98, 2000, ME, or XP, reboot your system into Safe Mode (with no networking if you have that option). If you are unsure how to reboot your system in Safe Mode, consult your Windows documentation.

If you still cannot access the Internet after uninstalling Zone Labs IMsecure Pro, run the file *zlimclnup.exe* located in the system directory, and reboot again.

Instant messaging programs do not appear in Overview panel

If you currently have an instant messaging program running but it does not appear in the table on the Overview panel, exit and then restart the program.

This can occur if your instant messaging programs and Zone Labs IMsecure Pro are set to launch on startup. To prevent this from recurring, modify the settings for your instant messaging programs to allow a manual launch.

Alert reference

This section provides an explanation of the types of alert messages that may appear during an instant messaging session that is protected by Zone Labs IMsecure Pro.

The table below lists the alert messages that can appear when using Zone Labs IMsecure Pro. Consult the table for an explanation of why these alerts appear and to determine whether any action is required on your part. All alert messages appear in brackets [ ] in your instant messaging window.

Alert text	Explanation
Session not encrypted due to ID/name mismatch in a certificate	This alert appears when the digital certificate used by IMsecure to encrypt your conversation with a contact does not match the contact's instant messaging ID.
Voice transmission was blocked. To allow voice conversations, please modify your security settings	This alert appears when you have blocked audio transmission and you attempt to initiate a voice conversation with a contact.
A file transfer was blocked. To allow file transfers, please modify your security settings	This alert appears when you have blocked file transfers and you attempt to send a file to a contact
Video transmission as blocked. To allow video transmissions, please modify your security settings	This alert appears when you have blocked video transmission and you attempt to send a video file to a contact
Potentially harmful formatting or scripting was removed from the message	This alert appears when a contact sends you a message that contains potentially harmful formatting or scripting.
Message discarded due to potentially harmful content	This alert appears when the message being received is malformed, which is often a sign of an attempted buffer overflow attack.
Encryption is disabled. To enable encryption, please modify your security settings	This alert appears when you have disabled encryption and are having an instant messaging conversation with a contact who is protected by Zone Labs IMsecure Pro with encryption enabled.
Encrypted session negotiation failed	This alert appears when Zone Labs IMsecure Pro is unable to encrypt an instant messaging session. This may occasionally occur in busy network traffic conditions. IMsecure Pro will make repeated attempts to re-establish the secure session. Often, restarting the instant messaging program resolves the issue.
Session not encrypted because [contact's IM ID] disabled encryption	This alert appears when you have encryption enabled, but your contact has disabled encryption.
Session not encrypted because [contact's IM ID] is not protected by IMsecure	This alert appears in your instant messaging window when you are having a conversation with a contact who is not using Zone Labs IMsecure Pro.

Alert messages displayed when using Zone Labs IMsecure Pro

Alert text	Explanation
Information about [description] was removed from your previous message in compliance with your ID Lock settings	This alert appears when you attempt to transmit information that is stored in myVAULT. The description of the item as it appears in myVAULT is displayed between brackets.
Link removed	This alert appears in the message recipients's window in place of a removed link.
Session encrypted	This alert appears at the beginning of an encrypted instant messaging conversation.
Potentially harmful content was removed from this message	This alert is appended to the filtered message.
Your message was blocked because you are not on [contact's IM ID]'s contact list	This alert appears when you attempt to send a message to someone who has Spam Blocker enabled, but who does not have you on his or her contact list.
A file transfer on [contact's IM ID]'s PC was blocked	This alert appears when you attempt to send a file to a contact, but the contact has blocked file transfers in Zone Labs IMsecure Pro.
Video transmission on [contact's IM ID]'s PC was blocked	This alert appears when a you attempt to transmit video to a contact, but the contact has blocked video transmission.
Potentially harmful formatting or scripting was removed from your last message	This alert appears when your contact set the Inbound protection option for Tags to Block, and you attempt to send a message to a contact that includes formatting or scripting.
A potentially harmful link was removed from your last message	This alert appears when your contact set the Inbound protection option for Active to Block, and you attempt to send a message to a contact that includes an executable link.

Alert messages displayed when using Zone Labs IMsecure Pro

Glossary

DES

Short for Data Encryption Standard, a popular symmetric-key encryption method using a 56-bit key.

Encryption

The process of transmitting scrambled data so that only authorized recipients can unscramble it. For instance, encryption is used to scramble credit card information when purchases are made over the Internet.

hash

A hash is a number generated by a formula from a string of text in such a way that it is unlikely that some other text would produce the same value. Hashes are used to ensure that transmitted messages have not been tampered with.

Instant Messenger (IM)

A chat program that allows two or more people to communicate over the Internet via real-time keyed-in messages.

myVAULT

A secure area where you can store private information, such as credit cards and passwords to be blocked from leaving your computer through an open IMchannel.

OpenSSL

OpenSSL is an open source security protocol is based on the SSLlibrary developed by Eric A. Young and Tim J. Hudson.

self-signed certificate

A public-key certificate for which the public key bound by the certificate and the private key used to sign the certificate are components of the same key pair, which belongs to the signer.

SHA1

An algorithm used for creating a hash of data.

Spam

An inappropriate attempt to use a mailing list or USENET or other networked communications facility as if it were are broadcast medium by sending unsolicited messages to a large number of people.

Index