Trend Micro®
GateLock™

TREND MICRO

Getting Started Guide

Table of Contents

Chapter A: Appendix A

Document Part No.
Release Date: month-year

This manual, *Trend Micro GateLock Getting Started Guide*, is intended to introduce the main features of the software and install it into your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and online Solution Bank at Trend Micro's Web site.

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend documents, please contact us at **docs@trendmicro.com**. Your feedback is always welcome. Please evaluate this documentation on the following site: http://www.antivirus.com/download/documentation/rating.asp?prod=[ ]&ver=[ ] &doc=[ ] .

Chapter 1

Introducing GateLock

Chapter Overview

This chapter:

- Introduces the main features and advantages of using GateLock
- Lists and illustrates the items included in the standard GateLock package
- Explains the usage of GateLock's indicator lights and ports

What is GateLock?

Trend Micro GateLock is an all-in-one, plug-and-play Internet appliance designed for home and small office/home office (SOHO) networks that use a broadband connection. GateLock protects you from hackers with its powerful firewall features and scans your incoming and outgoing mail using Trend Micro's market-tested antivirus technology.

Your GateLock also serves as a router for your small office/home office network that allows multiple computers to share a single broadband connection to simultaneously access the Internet.

Security

GateLock protects your PC and home network from hackers by blocking unauthorized external connections and cloaking your IP address, making your computer and home network "invisible" to other people on the Internet. With its powerful firewall features, it monitors network traffic and detects and blocks intrusion attempts. GateLock keeps records of detected hacker attempts and can also be configured to send you email notifications about these attempts.

Aside from anti-hacker features, GateLock is also packed with Trend Micro's powerful antivirus technology. It can scan your incoming POP3 and outgoing SMTP mail messages, and even your Web-based email attachments, for viruses. To ensure that your antivirus protection is always up-to-date, you can set up GateLock to automatically download updates for its antivirus components from Trend Micro's update server. GateLock automatically records details of up to 30 most recently detected viruses and antivirus component updates.

Sharing Capability

Your new GateLock also functions as a router that makes it very easy for you to set up your home network. It allows up to 32 users in your home network to simultaneously access the Internet using a single broadband connection. No driver or software is needed to share your broadband connection as long as the TCP/IP protocol is installed.

GateLock can also function as a DHCP server that automatically assigns IP addresses to your devices so that you do not have to choose and manually set up IP addresses.

Ease of Use

GateLock is a plug-n-play device that requires minimal setup. With your preferred Web browser (Microsoft Internet Explorer or Netscape Navigator, 4.0 or above), you can configure GateLock in a matter of minutes.

To make it even easier, a *Quick Setup* wizard is included to lead you through the initial configuration steps. Advanced users who need to perform extra tasks like mapping IP addresses or port numbers for their servers and customizing firewall rules, Gatelock's intuitive configuration console enables quick configuration. Even if

you have no knowledge of networking, you can take advantage of the convenience, protection, and speed afforded by GateLock within minutes.

Summary of Trend Micro GateLock Features

- Antivirus protection with no installation required. Scans POP3 and SMTP mail message and Webmail attachments
- Automatic and manual updates of antivirus components, keeping you constantly protected against virus attacks through the Internet.
- Robust anti-hacker protection and customizable intrusion detection and network traffic control rules
- Email notification for detected hacker attempts and available GateLock software updates
- Internet access sharing
- Multiple PCs (up to 32 computers) can access the Internet through a single xDSL or cable modem line (Network Address Translation) with only one purchased IP address, by connecting GateLock to a hub. Works with any Ethernet connection
- Can act as a DHCP server on the LAN to dynamically assign IP addresses to GateLock. This makes setting up your home network much easier
- If your ISP dynamically assigns IP addresses to you, GateLock can still act as a DHCP client on the WAN to automatically receive each IP address assigned by your ISP
- Hides the IP addresses of your PCs from potential intruders, making it harder for hackers to attack your PC.

Contents of Package

Illustrated below are the items included in your GateLock package.

FIGURE 1-1. *Contents of the GateLock Package*

- The GateLock main unit
- Power cord (connects GateLock to your power source)
- CAT5 UTP Ethernet cable (connects from local GateLock port to Ethernet port on PC, or Uplink port on hub/switch)
- This *GateLock Getting Started Guide*

Layout of GateLock's Back Panel

Figure 1-2 shows the back panel of your GateLock unit. This is where you connect the power adapter and the network cable from you PC or hub and to your xDSL or cable modem. The PC/HUB dipswitch and the Reset button can also be found here.

FIGURE 1-2. *Back Panel of your GateLock unit*

From left to right, the five items on the back panel are:

- **PC-Hub** Switch
- **PC/Hub** Port
- **Internet** Port
- **Reset** Button
- **PWR** (Power Input)

The usage of each of these five items is explained below.

PC-Hub Switch

The **PC-Hub** switch is a dipswitch which toggles between “PC mode” and “Hub mode.” If you will be using GateLock with one PC, move the switch to the right, the **PC** side. If you will be using Gatelock with a hub which is connected to multiple PCs, move the switch to the left, the **HUB** side.

PC/Hub Port

Provided in your GateLock package is a CAT5 UTP Ethernet straight-through cable. Connect one end of this cable to GateLock’s **PC/Hub** port, and connect the other end to the Ethernet port on the PC or Hub.

Internet Port

This is where you will connect your cable or xDSL modem. Connect one end of the UTP Ethernet cross-over cable (provided by your ISP) to GateLock’s **Internet Link** port, and the other end to your cable or xDSL modem.

Reset Button

When you press **Reset**, GateLock’s configuration values will be reset to the default values. To prevent accidental activation, the **Reset** button is slightly recessed within the rear GateLock panel. To reach the **Reset** button, simply insert the tip of a pen or similar object into the opening and push in lightly.

Note: To see all of GateLock’s default settings, as well as the procedure to alter the values to your own specifications, please refer to Chapter 2.

Power Input

The power input port is identified as **PWR** on the back of the GateLock router. This is where you will connect the AC power cord which is included in the GateLock package. (Output: 5 volt direct current, 3 amperes.)

Indicator Lights on Front Panel

Shown below is the front panel of the GateLock box. This is where the various indicator lights are located. All indicator lights display in red when illuminated.

FIGURE 1-3. *Front Panel of your GateLock unit*

The eight lights on the front panel are:

- **Power**
- **Antivirus**
- **Anti-Hacker**
- **Internet**
- **PC/Hub**

The usage of each of these eight lights is explained below.

Power

When GateLock is connected to a power source, the **Power** light will be illuminated. The **Power** light will be off when electricity is not reaching the unit.

Note: To connect Gatelock to a power source, plug the power adapter (furnished in your GateLock package) into the **PWR** port on GateLock's back panel.

Antivirus

If GateLock's Antivirus feature is enabled, the **Antivirus** light will be illuminated. By default, the Antivirus function is enabled and is set to a value of *Delete*. That is, GateLock will scan your incoming email for viruses, and if a virus is found, it will delete the file containing the virus. See Chapter 2 to learn how to change this setting.

Anti-Hacker

If GateLock's Anti-Hacker feature is enabled, the **Anti-Hacker** light will be illuminated. By default, the Anti-Hacker function is enabled and will block unsolicited inbound traffic according to GateLock's internal pre-defined rules. See Chapter 2 to learn how to change this setting.

Note: To see all of GateLock's default settings, as well as the procedure to alter the values to your own specifications, please refer to Chapter 2.

Internet

If the **Internet** light is blinking or flickering, this indicates that there is currently some traffic on the Internet line. When there is no traffic, the light will be off.

PC/HUB

The **PC/HUB** light will blink every few seconds when there is any traffic being sent from a PC to GateLock on the PC/HUB line.

You are now ready for Chapter 2 which explains how to set up your GateLock.

Chapter 2

Installing GateLock

This chapter explains how to set up and connect your GateLock to your PC or hub.

Requirements

- You must have a broadband connection installed in your home. The broadband connection may be via an xDSL (ADSL, SDSL, IDSL, or VDSL) modem or cable modem.
- If you are using GateLock to connect multiple PCs to the Internet, you will need a hub. The hub is not included in the GateLock package. You can purchase it at most computer stores. Please refer to the Appendix of this Getting Started Guide and to the user manual furnished with your hub for information about how to connect your PCs to a hub.

FIGURE 2-1. *Broadband Connection of One Computer to the ISP Without GateLock*

Step 1 of 2: Connect the Cables

If you are connecting a single PC to the Internet:

FIGURE 2-2. *Connecting One PC to the Internet with GateLock*

1. Plug one end of your network cable to your PC's LAN/Ethernet card port and plug the other end into the **PC/HUB** port on GateLock's rear panel.
2. Take the red network cable that comes with your GateLock package:
   a. Plug one end of the red network cable into the **Internet** port on GateLock's rear panel.
   b. Plug the other end of the red network cable into your xDSL or cable modem's network port.
   c. Move the **PC/HUB** dipswitch on GateLock's rear panel to the **PC** side.
3. Connect the power adapter that comes with your GateLock to the **PWR** port on the rear panel and plug the other end into a power socket.

If you are connecting multiple PCs to the Internet:

FIGURE 2-3. *Connecting Multiple PCs to the Internet with GateLock*

1. For each PC, plug one end of the network cable into your PC's LAN/Ethernet port and plug the other end into one of the ports of your hub.
2. Take the red network cable that comes with your GateLock package:

   a. Plug one end of the red cable into the **PC/HUB** port on the rear panel of GateLock.

   b. Connect the hub to your GateLock:

   - If your hub has a network port labeled "Uplink," plug the other end of the red network cable into the "Uplink" port of the hub. Move the **PC/HUB** dipswitch on GateLock's rear panel to the **PC** side.
   - If your HUB does *not* have a network port labeled "Uplink," plug the other end of the red network cable into any port of the HUB. Move the **PC/HUB** dipswitch on GateLock's rear panel to the **HUB** side.
3. Plug one end of another network cable into the **Internet** port on GateLock's rear panel and plug the other end into your xDSL or cable modem's network port.
4. Connect the power adapter that comes with your GateLock to the **PWR** port on the rear panel and plug the other end into a power socket.

Step 2 of 2: Make Sure Your PC Can Talk to GateLock

For each PC that is directly connected to GateLock, or indirectly connected to GateLock through a hub:

1. Restart your PC.
2. Open your Web browser (Netscape Navigator version 4.0 or above, or Microsoft Internet Explorer 4.0 or above) on your PC, and go to **http://192.168.1.254**. If you can see the welcome screen of GateLock's configuration console, your PC can successfully recognize GateLock. Skip the succeeding steps and go directly to *Configuring GateLock* starting on page 2-1.
3. If you cannot see the welcome screen of GateLock's configuration console:

   - Verify that your PC is obtaining its IP address automatically via DHCP. Detailed instructions for this procedure can be found in the section of the Appendix entitled *Setting the Properties for TCP/IP* on page A-5. If you changed your PC's TCP/IP settings, please repeat Steps 1 and 2.
   - If, after you have changed your PC's TCP/IP settings, you still cannot see the welcome screen of GateLock's configuration console, check if your Web browser's proxy settings are correct. Detailed instructions for this procedure

can be found in the section of the Appendix entitled *Setting the Proxy Servers in Your Browser* on page A-1.

- Toggle the **PC/HUB** dipswitch on GateLock's rear panel and repeat Steps 1 and 2.
- For further assistance, contact your GateLock dealer.

If you see the welcome screen of the configuration console, you are now ready for Chapter 3 which explains how to configure your GateLock's various functions.

Chapter 3

Configuring GateLock

This chapter discusses the pre-configuration tasks you should perform and explains how to access the setup screens to configure GateLock. It also tells you how to upgrade GateLock and submit a question to Trend Micro's technical support.

GateLock is remarkably easy to set up with its intuitive Web browser-based configuration console. To facilitate configuration, GateLock's configuration console includes a *Quick Setup* wizard that makes changes after asking questions about your environment. For those who have to perform advanced setup tasks or who want to change GateLock's settings, hyperlinks on the sidebar have been provided for easy access and seamless configuration.

Configuration Console Layout

The browser-based configuration console has been designed for quick and easy access to GateLock's various functions and features. It has two parts:

- The sidebar (left-hand navigation frame) contains links that open the main functional areas.
- The main frame of the configuration console displays the screens that you use to configure your GateLock settings, including antivirus, anti-hacker and firewall settings.

Opening the Configuration Console

After connecting GateLock to your PC or hub, the next step is to customize GateLock's settings. Do the following:

1. Open your Web browser. In the *Address* field, enter the following IP address:

   `http://192.168.1.254`

2. Press the <*Enter*> key. Your Web browser will display the first setup screen, as shown in Figure 3-1.

FIGURE 3-1. *GateLock's Welcome Screen*

3. GateLock ships with a blank password, by default. Simply click Enter to open the configuration console. The *Quick Setup* screen loads.
4. Note there are 8 main hyperlinks on the sidebar as shown in Figure 3-2. Clicking these hyperlinks will open GateLock's main configuration screens. What these 8 main screens are and how use them to configure GateLock's settings are discussed in the order of their appearance in the list.

FIGURE 3-2. *The Sidebar*

Quick Setup

The *Quick Setup* screen opens when you click the Enter button on GateLock's welcome screen. *Quick Setup* allows you to easily set up GateLock by providing you with step-by-step onscreen instructions.

Specify how GateLock will obtain its IP address

Click one of the three option buttons on this screen (*Metered xDSL*, *Static IP Address*, or *Dynamic IP Address*). A brief description follows each option to help you determine which button to select. By default, *Metered xDSL* is selected as shown in Figure 3-3.

FIGURE 3-3. *"Specify how GateLock will obtain its IP address" screen*

Metered xDSL

If you are an xDSL/broadband user *and* your Internet Service Provider uses PPPoE (Point-to-Point Protocol over Ethernet), click the *Metered xDSL* button. Remember to remove any existing PPPoE applications you have on your computer. Click Start at the bottom of the screen to advance to the next screen.

FIGURE 3-4. *"Metered xDSL" screen*

1. On the next screen (see Figure 3-4.), type *Your email address* and the *Password* you use to log on to your ISP.
2. Click *Connect automatically when disconnected* if you want GateLock to keep you always connected to your ISP.

   Click *Do not connect automatically* if you want to manually connect to your ISP whenever you are disconnected. This option is selected by default.
3. Click *Disconnect if idle for X minutes* if you want GateLock to automatically disconnect your Internet connection when it detects no Internet activity for the specified length of time. Using the drop-down menu, you can change the default length of time to any of these: 5 minutes, 10 minutes, 30 minutes or 1 hour.

   Click *Disable maximum idle time* if you do not want GateLock to automatically disconnect your Internet connection.

Click Next when you finish typing your information and selecting from the options. The information screen appears, displaying the settings you have just specified, as shown in Figure 3-5. These settings were already saved when you clicked Next in the previous screen; it simply shows you what has been saved.

When *Metered xDSL* is selected, the *Internet* light on GateLock's front panel will be illuminated after it has successfully connected to your ISP, indicating that you can connect to the Internet.

FIGURE 3-5. *Metered xDSL information screen*

Note: Select *Metered xDSL* if your ISP has given you a user name and a password. You must use GateLock's setup screens to specify this information so that it can be recognized by GateLock.

WARNING! *When using GateLock with Metered xDSL, always remember to disconnect your Internet connection using On-Demand Connection on GateLock's configuration console. You will stay connected to the Internet even if you turn off your PC as long as GateLock is on. You will only be automatically disconnected when the maximum idle time you have specified is reached.*

Static IP Address

If you select the Static IP address option:

1. Type the required information in the blank fields on the screen that appears after you click Start. See Figure 3-6.
   - *IP address*: Type the IP address given to you by your ISP.
   - *Subnet mask*: Type the Subnet Mask address given to you by your ISP.

- *Gateway*: Type the IP address of the gateway device that allows contact between GateLock and your ISP.
- *Primary DNS*: Your ISP will give you at least one DNS (Domain Name System) address. You must type one here.
- *Secondary DNS*: It is common to have multiple DNS IP settings. If you have another DNS address, you may type it here. This field is optional.

Note: Even if you selected Static IP Address, you should still select *Obtain an IP address automatically* in your PC's TCP/IP Properties. GateLock will automatically assign each of your PC an IP address between 192.168.1.100 and 192.168.1.131. For detailed instructions on how to set the TCP/IP Properties, see *Setting the Properties for TCP/IP* starting on Page A-5.

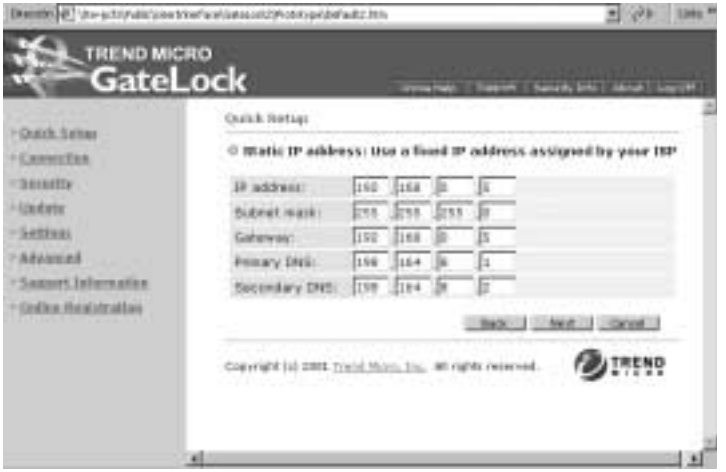

FIGURE 3-6. *Static IP Address screen*

2. Click Next when done typing the required information. The information screen appears, displaying the information you have just specified, as shown in Figure 3-7. These settings were already saved when you clicked Next in the previous screen; it simply shows you what has been saved.

FIGURE 3-7. *Static IP address information screen*

When this button is active, the *Internet* light on GateLock's front panel should always be illuminated, indicating that you can connect to the Internet.

Note: Select *Static IP Address* if your ISP has given you a specific IP address. Your ISP should have also provided information on how to set up your subnet mask, gateway, primary DNS, and secondary DNS. You must use GateLock's setup screens to specify this information so that it can be recognized by GateLock.

Tip:

Dynamic IP Address

Selecting *Dynamic IP address* means DHCP (Dynamic Host Configuration Protocol) will be used to automatically assign an IP address to GateLock. You do not have to manually assign a permanent IP address to your GateLock device. Simply click the Start button at the bottom of the screen to advance.

The information screen shown in Figure 3-8. appears, indicating that you have chosen to use *Dynamic IP Address* for GateLock to connect to the Internet.

FIGURE 3-8. *Dynamic IP Address*

Note: Select *Dynamic IP Address* if your ISP assigns you an IP address automatically using DHCP. If this is the case, you do not have to do anything. The *Internet* light on GateLock's front will be illuminated, and you should now be able to connect to the Internet. You can confirm this by successfully connecting to *http://www.antivirus.com* with your Web browser.

Antivirus Options

One of GateLock's powerful features is antivirus protection. It scans incoming and outgoing POP3 and SMTP email messages and Web-based email attachments for viruses.

After configuring how GateLock will connect to the Internet, click Next to advance to *Antivirus Options* screen, shown in Figure 3-9.

FIGURE 3-9. *Antivirus Protection screen*

GateLock's antivirus feature is enabled by default. If you wish to disable antivirus protection, deselect the *Enable virus scanning of incoming and outgoing mail* checkbox. However, we highly recommend that you keep GateLock's antivirus feature enabled to protect your computer environment against viruses.

If you keep antivirus protection on, you must specify the action that GateLock will take when it detects a virus in your email messages.

1. Specify the action that you want GateLock to take if it finds a virus in your email message.
   - Click *Clean* if you want GateLock to try to remove the virus from the infected file. This is selected by default. You must also select an alternative action from the drop-down menu in case GateLock is unable to clean the file.
     i. Select *Delete* if you want GateLock to delete the entire file containing the uncleanable virus.
     ii. Select *Pass* if you want GateLock to do nothing to the infected or malicious file.

WARNING! *Passing an uncleaned virus to your computer puts your system at risk and is not recommended.*

- Click *Delete* if you want to remove the infected or malicious file from your computer. Some malicious files, for example those infected by Trojans or worms, cannot be cleaned and must therefore be deleted.
- Click *Pass* if you want GateLock to record the details of the infected or malicious file in the antivirus log but do nothing to it.

2. Click Next to save your antivirus protection settings. The information screen shown in Figure 3-10. appears, displaying the settings you have just saved.

FIGURE 3-10. *Antivirus Protection information screen*

3. Click Next to advance to the Anti-Hacker Protection screen.

Anti-Hacker Protection

Another very important security feature of GateLock is anti-hacker protection. It can protect your computer from hacker attacks with its built-in firewall and intrusion detection features.

To protect your computer from unwanted intrusion, GateLock uses “port blocking.” Think of a port as being similar to a door into your computer. Each service on the

Internet has a port associated with it, which hypothetically leaves a lot of “doors” open. GateLock guards these "open doors" against hackers.

GateLock offers 3 anti-hacker security levels to choose from.

1. Select your preferred security level:
   - Click *High* if you want GateLock to block hacker attacks and record intrusion attempts to the anti-hacker logs.
   - Click *Medium* if you only want GateLock to block hacker attacks.
   - Click *Low* if you want to use minimum firewall features.
2. Click Next. The anti-hacker information screen loads, as shown in Figure 3-11.

FIGURE 3-11. *Anti-Hacker Protection information screen*

3. Click Next to advance to the next configuration screen

Email Notification Options

You can configure GateLock to send you email notifications about detected hacker intrusion attempts and available GateLock software updates.

Although this section is optional, we strongly recommend that you provide your email address to stay informed about hacker attacks on your computer or network and new versions of the GateLock software to which you may upgrade.

FIGURE 3-12. *Email Notification Options configuration screen*

To receive email notifications:

1. Type the name of your ISP's SMTP server in the ISP's SMTP server field. This information should be included in the account information sheet that you received from your service provider. It can either be a SMTP name (SMTP.yourisp.com) or an IP address (254.254.1.1). If you are not sure about this information, please contact your Internet Service Provider.
2. Type your email address(es) in the field provided. This is where GateLock will send the email notifications. If you are typing more than one email address, separate each entry with a semicolon (e.g., mail1@isp.com**;** mail2@isp.com)
3. Confirm your email addresses by retyping the email address(es) you have entered in the previous field. You can simply select the email address(es) you have typed, copy and paste into the second email address field.
4. Click the *Hacker Intrusion* check box if you want to receive notifications about detected hacker attempts on your computer or network. Click the sample email hyperlink to view an example of the email message that you will receive from GateLock.

5. Click the *Available Software Updates* check box if you want to receive information about new software versions of GateLock. Click the sample email hyperlink to view an example of the email message that you will receive from GateLock.
6. Click Next when finished. The email notification information screen loads, as shown in Figure 3-13., displaying the information you have just provided. This information has already been saved.

FIGURE 3-13. *Email Notification information screen*

7. Click Next to open the next configuration screen.

Online Registration

Your GateLock comes with one-year free software upgrades and maintenance service. However, you must register your GateLock online before you can receive these benefits.

Use the *Register Your GateLock* configuration screen to register online. Your product information, which include your GateLock version and serial number, is displayed on the upper part of the configuration screen.

FIGURE 3-14. *GateLock Online Registration form*

To register your GateLock:

1. Type your *First name*, *Last name*, *Email address*, and *Telephone number* in the fields provided and select your *Country* from the drop-down menu. This is required information. We recommend that you also complete the other optional fields.
2. Click Finish to submit your registration form online.

FIGURE 3-15. *Registration Successful screen*

3. The screen shown in Figure 3-15. will appear if your registration successfully completed. After a few seconds, a second screen (shown in Figure 3-16.) will load, informing you that you have completed Quick Setup.

FIGURE 3-16. *Quick Setup completed screen*

Connection

Clicking the *Connection* hyperlink on the sidebar display two menu items: *Connection Settings* and *On-Demand Connection*.

Connection Settings

Connection Settings allows you to change your *Quick Setup* configuration about how GateLock obtains its IP address.

For example, assume that you were using a dynamic IP address to connect to the Internet but later decided to change your ISP. Your new ISP has assigned you a static IP address. You must modify your GateLock's connection settings to be able to connect to the Internet.

FIGURE 3-17. *Connection Settings screen*

To modify your connection settings:

1. Click *Connection* > *Connection Settings* on the sidebar.
2. Specify how GateLock will obtain its IP address from the 3 options.
   - Click *Dynamic IP address* if your ISP automatically assigns you an IP address.
   - Click *Static IP address* if your ISP has assigned you a fixed IP address and type the required information in the blank fields provided. See *Static IP Address* on page 6 for details.
   - Click Metered xDSL if you use PPPoE to connect your ISP. Type *Your email address* and the *Password* you use to connect to the Internet. Indicate if you want GateLock to automatically connect to your ISP if disconnected and if you want it to automatically disconnect your Internet connection when there is no activity for a specified length of time. See *Metered xDSL* on page 4.
3. Click Apply.

On-Demand Connection

On-demand connection is only for GateLock users with metered xDSL. This allows the user to check the Internet connection and to manually connect or disconnect from the Internet.

To verify if you are connected to the Internet, click *Connection* > *On-Demand Connection* from the sidebar. The *On-Demand Connection* page loads, displaying your connection status and your connection settings.

- If you are disconnected from the Internet and want to connect, click Connect Now at the bottom of the page.
- If you are connected from the Internet and want to disconnect, click Disconnect at the bottom of the page.

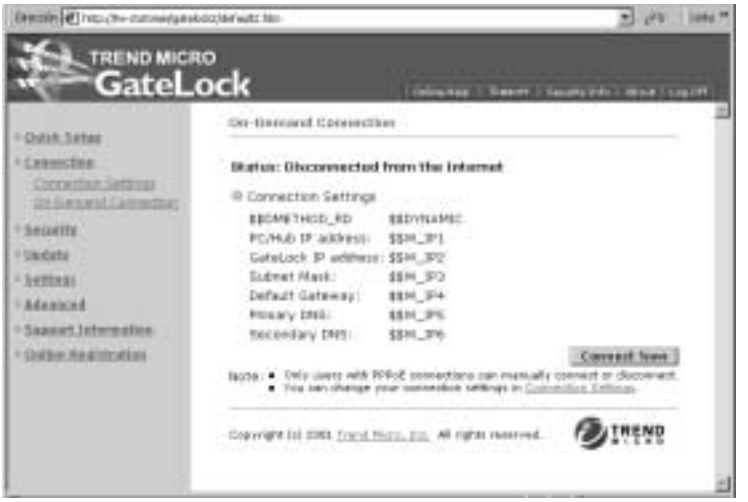

FIGURE 3-18. *The On-Demand Connection screen displaying your connection settings and the Connect Now button*

Security

Clicking the *Security* hyperlink on the sidebar exposes four menu items: *Antivirus Options, Antivirus Logs, Anti-Hacker Options, and Anti-Hacker Logs.*

Antivirus Options

Antivirus Options allows you to change your antivirus protection settings. You can disable GateLock's antivirus protection or change the action GateLock will take when a virus is detected in your incoming and outgoing email messages. However, we recommend that you keep the antivirus protection enabled to secure your computer and network environment.

See *Antivirus Options* on page 9 for detailed information on how to configure your GateLock's antivirus settings.

Antivirus Logs

GateLock keeps a record of the viruses that have been detected in your incoming and outgoing email messages. It can record up to 30 of the most recent virus-detection incidents.

To view the antivirus logs, click *Security > Antivirus Logs.*

The next screen displays recently detected viruses, including the date and time of detection, the result of the action you have configured, the sender and the other recipient(s), and the name of the file that contained the virus.

FIGURE 3-19. *Sample of an Antivirus Log*

Anti-Hacker Options

Anti-Hacker Options allows you to change your anti-hacker protection settings. You can select from GateLock's 3 anti-hacker security levels: High, Medium, or Low.

See *Anti-Hacker Protection* on page 11 for detailed information on how to configure your anti-hacker settings.

Anti-Hacker Logs

GateLock also records detected hacker intrusion attempts on your computer or network. It can keep up 30 of the most recent hacker attack records.

To view your anti-hacker logs, click *Security > Anti-Hacker Logs*.

The log loads, displaying the most recent hacker intrusion attempts that were detected by your GateLock. The record includes the date and time of the hacker attack, the method used by the hacker, the IP address of the computer used by the hacker and the number of attempts made.

FIGURE 3-20. *Sample of an Anti-Hacker Log*

Update

Clicking the *Update* hyperlink on the sidebar loads 2 more hyperlinks: *Product Update and Update History.*

Product Update

To maintain up-to-date antivirus and anti-hacker protection, you should regularly update your GateLock software components. These components include the GateLock software, virus pattern file, scan engine and firewall rule.You must be connected to the Internet for GateLock to check for updates.

To check for available updates, click *Update* > *Product Update*. GateLock will automatically connect to Trend Micro's Internet update site and look for new GateLock components.

If updates are available, a pop-up dialog box will appear as the *Product Update* screen opens with the message "New components are available for download." Click Update Now to immediately download the updates.

If there is no update available, the pop-up dialog box will show the message, "No available updates."

FIGURE 3-21. *The Product Update screen*

If you want GateLock to automatically check for and download available updates whenever you are connected to the Internet, click the *Enable automatic update* check box.

The screen also tells you if you have configured your GateLock to receive email notifications whenever there are available updates.

Update History

You can track how many times you have updated your GateLock components by accessing its *Update History* screen.

To view your GateLock's update history, click *Update* > *Update History* from the sidebar. The *Update History* loads, displaying *X* of your most recent update dates, including the versions of your GateLock software, scan engine, virus pattern and firewall rule.

FIGURE 3-22. *Update History screen*

Settings

Clicking the *Settings* hyperlink on the sidebar loads 3 more hyperlinks: *Email Notification, Password Protection and Time Zone*.

Email Notification

Email Notification allows you to change your settings for receiving email messages about detected hacker attacks or available software updates.

To open the email notification screen, click *Settings* > *Email Notification* on the sidebar. The same window you used to configure your email notification settings in *Quick Setup* loads.

You may change your ISP's SMTP server or add, delete or modify your email address(es). You may also disable email notification for *Hacker Intrusion* or *Available Software Updates* to stop receiving email messages about detected hacker attacks on your computer or network and information about new GateLock

components. However, we strongly recommend that you keep the email notifications enabled to stay informed about hacker attacks and available updates.

See *Email Notification Options* on page 12 for detailed configuration instructions.

Password Protection

To control access to the GateLock configuration console, you can enable password-protection. This will ensure that only you can change GateLock's settings thus allowing you to continually secure your computing or network environment.

To enable the GateLock console's password-protection:

1. Click *Settings* > *Password Protection* on the sidebar.
2. Select the *Password-protect GateLock's configuration console* check box.
3. Type your *Current password*. If this is your first time to password-protect the configuration console, leave the *Current password* field blank.
4. Type your *New password*. Your password must have between 6 to 10 alphanumeric characters and must not include a space.
5. Confirm your new password by retyping it in the *Re-enter new password* field.
6. Click *Apply* when finished.

FIGURE 3-23. *The Password Protection screen*

Time Zone

For accurately recording of the date and time on GateLock's various logs, you need to specify your correct time zone.

To specify your time zone:

1. Click *Settings* > *Time Zone.*
2. Select your time zone from the drop-down menu.
3. Click **Apply**.

FIGURE 3-24. *The Time Zone screen*

Advanced

Clicking the *Advanced* hyperlink on the sidebar loads 2 hyperlinks that allow you configure GateLock's advanced options: *IP Port Forwarding* and *Network Traffic Control.*

IP Port Forwarding

If you are connecting GateLock to your home network and you have servers (e.g., Web, FTP, email) that you want to publish outside your network, you need to configure GateLock for this purpose. This configuration task is called IP port forwarding.

IP port forwarding allows you to redirect service requests from outside sources to your internal servers. With GateLock, you have total control over incoming network traffic: you can allow, reject, or ignore connection requests to your servers.

To configure IP port forwarding for GateLock:

1. Select *Advanced* > *IP Port Forwarding* from the sidebar. The *IP Port Forwarding* screen loads, as shown in Figure 3-25.
2. By default, no connection request from external sources will be allowed to pass through GateLock, thus your servers cannot be accessed from outside your network. Click Add Service.

FIGURE 3-25. *Use the IP Port Forwarding screen to control access to your servers*

Adding a service

The *Add Service* screen, shown in Figure 3-26, is where you assign a port for an Internet service that you want to publish.

1. Choose the type of service that you want to add, either *Commonly-used service* or *User-specified service*. *Commonly-used service* includes a drop-down list of popular Internet services, such HTTP, FTP, Telnet, Netmeeting, and the port numbers that are normally assigned to them.

FIGURE 3-26. *Add IP Port Forwarding Service*

- If you select *Commonly-used service*:
  - **a.** Choose the service that you want add from the drop-down list.
  - **b.** Assign an IP address to the server that will host the Internet service you are adding by completing the blank field for *Service IP address*. GateLock will direct connection requests for this Internet service to this IP address.
  - **c.** If there are specific Web addresses or IP addresses that you do not want to access the service you are publishing, add these sources in the *Deny Service*

List. You can choose to *Reject* or *Drop* the connection request from these sources.

- To reject a request from a specific source, type the Web address or IP address in the blank field under *Reject Connection* and click the ">>" button. When this address attempts to connect to your server, it will be informed that it is not authorized to connect.
- To ignore a request from a specific source, type the Web address or IP address in the blank field under *Drop Connection* and click the ">>" button to add to the list. This address will not be able to conect to your server and will not receive any information.
- To remove a Web address or IP address from the *Deny Service List*, highlight the address and click the "<<" button.

- If you select *User-specified service*:

  a. Assign any port number between 1 to 65535 that is currently not in use in the *Port* field.

  b. Type a description for this service (optional), e.g., File Transfer (FTP), to help you easily identify it.

  c. Assign an IP address to the server that will host the Internet service you are adding by completing the blank field for *Service IP address*. GateLock will direct connection requests for this Internet service to this IP address.

  d. If there are specific Web addresses or IP addresses that you do not want to access the service you are publishing, add these sources in the *Deny Service List*. You can choose to *Reject* or *Drop* the connection request from these sources.

  - To reject a request from a specific source, type the Web address or IP address in the blank field under *Reject Connection* and click the ">>" button. When this address attempts to connect to your server, it will be informed that it is not authorized to connect.
  - To ignore a request from a specific source, type the Web address or IP address in the blank field under *Drop Connection* and click the ">>" button to add to the list. This address will not be able to conect to your server and will not receive any information.
  - To remove a Web address or IP address from the *Deny Service List*, highlight the address and click the "<<" button.

2. Click Apply when finished. The IP Port Forwarding screen opens, displaying details of the service you have added. See Figure 3-27.

FIGURE 3-27. *What the IP Port Forwarding screen looks like after Internet services have been added*

Deleting an existing service

To delete an existing service:

1. Click the corresponding icon for the service. A confirmation dialog box appears.
2. Click OK.

Editing an existing service

To edit an existing service:

1. Click the corresponding icon. The *Edit Service* screen loads.
2. Modify the settings by changing the port number or the description for the service. You may also add or delete Web or IP addresses to the *Deny Service List*.
3. Click Save when finished.

Network Traffic Control

In addition to giving you total control over incoming traffic, GateLock likewise allows you to control your network's outgoing traffic by customizing outgoing traffic rules. For example, you can prevent the computer used by your children on your home network from accessing adult Web sites. To do this, you must configure GateLock to drop or reject connection requests from your network to specific Web sites or Internet destinations.

By default, all outgoing traffic is allowed to pass through GateLock.

Adding an outgoing traffic rule

To customize GateLock's outgoing traffic rules:

1. Select *Advanced* > *Network Traffic Control* on the sidebar. The screen, as shown in Figure 3-28, loads.

FIGURE 3-28. *The Network Traffic Control screen*

2. Click Add Outgoing Rule to add an outgoing rule. The screen shown in Figure 3-29 loads.
3. Create a outgoing traffic rule.

- In *Priority Level*, specify the level of importance for the rule you are creating. There are four priority levels, with 1 having the highest priority. Specifying Priority 1 for your rule will ensure that this will be followed first before the other rules, including the default rule.
- In *Source*, specify to which IP address or addresses the rule will be applied. Since GateLock assigns an IP address to every PC on your network beginning with *192.168.1.x*, you only need to type the last digit or set of digits of the IP address. If you want to apply the rule to all PCs on your network, type the wildcard character which is the asterisk (*) symbol.
- In *Protocol*, specify the type of protocol to which the rule will be applied. This gives you more flexibility in implementing the rule. For example, you apply the rule to all PCs on your network, thus *192.168.1.**, but you only want to specifically apply this to PCs that use the Hypertext Transfer Tranfer Protocol (HTTP) which is used to connect to the Internet. You must thus select HTTP from the drop-down list to apply the rule to ALL computers on your network that use HTTP.
- In *Destination address*, type the Web address or IP address.
- In *Destination port*, type the destination port number for which the rule will be applied. Typing the wildcard character in this field will apply the rule to all ports of the destination address.
- In *Action*, click the action that you want GateLock to take when connection requests for the specified destination address are made by the specified sources.

  i. Choose *Allow* to allow the connection to be made.

  ii. Choose *Ignore* to block the outgoing request without notifying the user.

  iii. Choose *Reject* to block the outgoing request and inform the user that he/she is not authorized to connect to the destination.

4. Click Save when finished. The IP Port Forwarding page loads, displaying the rules you have created, as shown in Figure 3-29.
5. To add another rule, click Customize rules again.

Deleting an outgoing traffic rule

To delete an existing outgoing rule:

1. Click the corresponding  icon. A confirmation dialog box appears.
2. Click OK.

Editing an outgoing traffic rule

To edit an existing outgoing rule,

1. Click the corresponding icon. The *Modify Outgoing Traffic Rule* screen loads.
2. Edit the rule by changing the *Priority Level* or *Protocol* for the rule. You can also change the entries in *Source* and *Destination ports* or the specified *Action*.
3. Click Save when finished.

FIGURE 3-29. *The Add Outgoing Traffic page with sample data*

Support Information

If you have any questions concerning GateLock that are not answered by this GateLock Getting Started Guide, you can submit them to Trend Micro via email. In the *Support Information* screen, click the Gatelock@trend.com.tw link. This will open an email window similar to the one shown in Figure 3-31.

FIGURE 3-30. *Support Information screen*

FIGURE 3-31. *Send your questions to Trend Micro using this email format.*

In this email window, type your question, comment, and/or a description of the problem you are experiencing. Then click the Send button.

The Button Bar

Near the top of the GateLock setup screen is a button bar, illustrated in Figure 3-32., which contains 5 buttons. This section briefly explains the usage of these buttons.

FIGURE 3-32. *The Button Bar*

Online Help

When you click the Online Help button, a new Web browser window opens. It contains a link that allows you to access HTML-based help files about all of GateLock's main functions.

Support

When you click the Support button, a new Web browser window will open, displaying Trend Micro's "Technical Support" home page.

Security Info

When you click the Security Info button, a new Web browser window will open displaying Trend Micro's "Virus Information Center" home page at http://www.antivirus.com/vinfo/. This site is a very comprehensive reference offering an abundance of useful information concerning known viruses as well as alerts concerning the newest threats. Several free services are also available.

About

When you click the About button, the *About* screen displays, as shown below. It displays copyright information and the version number of GateLock, as well as links to Trend Micro's WWW home page.

FIGURE 3-33. *The About screen*

Log Off

Clicking the Log Off button opens the Welcome screen of GateLock's configuration console. We recommend that you password-protect and log off the console every time you finish configuring GateLock's settings to control access.

Chapter 4

Troubleshooting and Technical Support

This chapter:

- Provides troubleshooting tips for common problems
- Tells you how to run a self-test on GateLock
- Presents various on-line resources provided by Trend Micro, where you can register your product, test it and find additional information
- Tells you how you can contact Trend Micro if you need to speak with a support engineer

Troubleshooting

This section lists possible solutions to problems that might arise while installing, configuring, or using GateLock.

Ethernet Cables

GateLock's ports are wired similar to a network adapter's port. First, check if all connected devices are powered on. Then verify if the cables are properly connected as described in Chapter 2.

Connection Timed Out

If you get a “Proxy Reports: Connection Timed Out” error message when you type an IP Address or a URL, check if your GateLock is:

1. Powered on
2. Connected to your PC or hub
3. Properly configured

If it is, check your Internet connection (cable and modem). GateLock is compatible with any cable or xDSL modem that supports Ethernet.

Using PING

“PING” (Packet Internet Groper) is a program that can be used to check if a computer is active and available. You can specify the destination name of a computer when using PING, or the actual IP address. “Destination name” refers to the text equivalent assigned to the actual numeric IP addresses. For example, “www.antivirus.com” is a destination name and “216.33.22.211” is its equivalent IP address. You can type either of the two in your Web browser’s address bar and your Web browser will take you to the Trend Micro home page.

In addition, sometimes an Internet Service Provider will shorten the server address to a single word to make it easier to remember or type. If your ISP has configured your email and Web server addresses as arbitrary single words, GateLock might have a problem accessing the Internet or sending and receiving mail because it has not been configured to recognize the ISP’s shorter addresses. If you can’t get the actual IP address from your ISP directly via a phone call, you can use PING to determine the actual IP address of your ISP’s servers. You will then be able to use that actual address with GateLock.

You can initiate PING directly at the DOS prompt, or you can initiate it through Windows.

To initiate PING through Windows:

1. Click the Start button, then click the Run... command.
2. Type `ping` followed by the destination name or IP address in the Open field of the Run window. For example, if your ISP has given the name “email” to its mail server, you can type:

```
ping email
```

into the *Run* window, then click OK. The data will be displayed in a DOS window. Write down the IP address given, for future reference.

To initiate PING directly at the DOS prompt:

1. Type the word `command` in the Open field of the Run window.
2. Click OK. A DOS window will open.
3. Type `ping email` at the DOS prompt. The data will appear in the same DOS window. Write down the IP address given, for future reference. Figure 4-1 shows that the IP address for this ISP's mail server is 203.69.216.43.

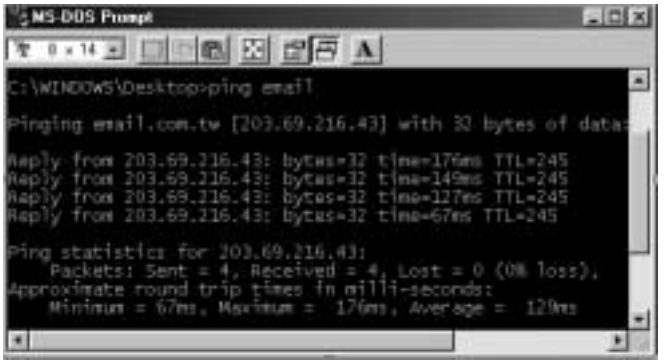

FIGURE 4-1. *Using PING to Determine the IP Address for a Sample Mail Server*

The example tells you the IP address of your ISP's mail server. Now, to determine the Web address of this IP address, precede it with `ping -a` at the DOS prompt. Since the IP address returned in the example above is 203.69.216.43, you would type `ping -a 203.69.216.43` and then press <*Enter*>. The Web address will be returned in the same DOS window (in this case, "sambaserver.") This is shown in the illustration below.

Write the Web address down for your future reference. This is the Web address that is assigned to the IP address you pinged. Normally, it is better to configure GateLock to recognize this Web address, because it is less likely to change than the IP address.

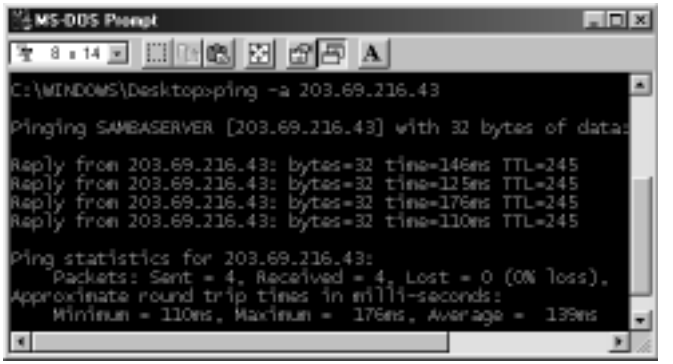

FIGURE 4-2. *Using PING to Determine the Web Address of an IP Address*

In GateLock, replace the “shortened” server address from the ISP with the actual server address you just discovered using PING. After you have done this, GateLock should have no problem accessing the Internet.

If you can successfully PING the IP address of a device’s local port, this indicates that the device and the cable are working properly.

If you cannot successfully PING the IP address of your Internet Service Provider’s gateway or DNS server, check if your cable/xDSL modem is working properly and if GateLock is correctly configured to connect to your ISP.

If you can successfully PING your ISP’s gateway but cannot PING a site on the Internet, the problem is probably located within the ISP.

Performing A Self-Test On GateLock

Your GateLock is equipped with a self-test utility that can help you determine if it has any hardware problems that might prevent you from optimally using it with your PC or network of PCs. Symptoms of hardware problems can include your PC's inability to connect to the Internet, etc.

Before performing a self-test on GateLock, do the following:

- Unplug GateLock from your PC or HUB.
- Take the red cable that came with the GateLock package. Plug one end of the cable into the Internet port on GateLock’s rear panel and the other end into the PC/HUB port.

- Move the PC/HUB dipswitch to the PC side.

To start GateLock' self-test function, do the following:

1. Unplug your GateLock's power cable from the PWR input port.
2. Press the Reset button on GateLock's rear panel and plug in the power cable while keeping the Reset button pressed. To reach the Reset button, insert the tip of a pen or similar object through the small opening and push in lightly. The Reset button must be pressed for at least 5 seconds to trigger GateLock's self-test utility.
3. When GateLock's self-test utility is triggered, the LED indicators for Antivirus, Anti-Hacker, and Internet will blink intermittently for a few seconds and then stop.
4. The Internet LED indicator will stay illuminated for a few seconds, after which it will start blinking. The blinking indicates that GateLock is checking itself for hardware problems. When the blinking stops, it indicates that self-test is complete. The whole self-test process takes only about a minute to complete.
5. If your GateLock does not have any hardware problems, the Antivirus, Anti-Hacker, and Internet LEDs will be illuminated after the self-test.

   If any of these 3 LEDs is not illuminated after the self-test, it indicates that your GateLock has a hardware problem. Call your GateLock vendor or contact Trend Micro's support center.
6. If you want to use GateLock after the self-test is completed, unplug the power cable first and plug it back in. This will ensure that GateLock will function normally after the self-test.

Trend Micro Contact Info and Online Resources

Technical Support

Trend Micro provides a full year of free technical support for our customers worldwide. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

In the United States, Trend Micro representatives can be reached via phone, fax, or email. Our Web and email addresses follow:

```
http://www.antivirus.com
support@trendmicro.com
```

General US phone and fax numbers follow:

```
Toll free: 800-228-5651 (sales)
Voice: 408-257-1500 (main)
Fax: 408-257-2003
```

Our US headquarters are located in the heart of Silicon Valley:

```
Trend Micro, Inc.
10101 N. De Anza Blvd., 2F
Cupertino, CA 95014
```

Registering GateLock

Registering GateLock with Trend Micro is important because it entitles you to the following benefits:

- One year of free updates to the program files
- One year of free technical support
- Important product information

You can register via the Internet or by mail. To register over the Internet, use the following URL:

```
http://www.antivirus.com/vinfo/
```

To register by regular postal mail, fill out and send the self-addressed, stamped Registration Card included with the product.

Note: You must register via the Internet if you wish to obtain pattern file updates.

Testing Installation

After you have installed and configured GateLock, you can check its antivirus function and see how it handles viruses.

The European Institute of Computer Antivirus Research (EICAR), along with antivirus vendors, has developed a test file that can be used in checking your installation and configuration.

The file, named **eicar.com**, does *not* contain an actual virus. It will cause no harm and will not replicate. Rather, it is a specially created file whose “signature” has been

included in the Trend Micro virus pattern file, and therefore can be detected by the scan engine used by GateLock.

You can download this file from Trend Micro at:

`http://www.antivirus.com/vinfo/testfiles/`

Click **eicar.com** to start downloading the file. If GateLock is properly installed and configured to detect viruses, it should be able to detect the "infected" file.

Trend Micro Security Center

Comprehensive security information is available via the Internet at our free antivirus center:

`http://www.antivirus.com`

Use the **Security Information Center** to find out about:

- Computer virus hoaxes
- A weekly virus alert, listing the viruses that will trigger during the current week
- Information about spam email, and a list of known spammers
- How to determine if a virus detection is a false alarm
- Trend Micro's Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- A basic guide to computer viruses
- Trend Micro's virus reading room, with dozens of articles about the latest issues in computer viruses, including the threat posed by Java applets and ActiveX controls
- Product details and white papers

Sending Your Virus-Infected Files to Trend Micro

You can send your virus-infected files to Trend Micro via email. If you have a file that you think is infected with a virus, but the scan engine does not detect it or cannot clean it, we encourage you to send the suspect file to:

`virus_doctor@trendmicro.com`

Please include a brief description of the symptoms you are experiencing in the message text. Our team of virus engineers will "dissect" the file to identify and characterize any virus it may contain, and return the cleaned file to you – usually within 72 hours.

Appendix A

This appendix:

- Explains how to set up the proxy properties of your Web browser so that you can successfully open GateLock's browser-based configuration console.
- Provides more detailed instructions and illustrations about how to set up the TCP/IP protocol on your computer (Chapter 2 furnished condensed instructions).
- Lists technical and environmental specifications.
- Provides a glossary of terms used in this document.

Setting the Proxy Servers in Your Browser

Since the IP address of GateLock's PC/HUB port (**http://192.168.1.254**) is a private IP address, it is important that you set up your Proxy Server setting correctly. You can either:

- Disable the Proxy Server setting

  — OR —

- Use a Proxy Server, but make 192.168.1.254 an exception

Disabling the Proxy Server using Internet Explorer

1. Select **Internet Options...** from the Tools Menu.
2. In the *Connections* tab, click the **LAN Settings...** button.

3. Make sure the *Use a Proxy Server* checkbox is not selected.
4. Make sure the *Bypass Proxy Server for Local Addresses* checkbox is selected, then click **OK**.

Enabling the Proxy Server with an Exception using Internet Explorer

1. Select Internet Options... from the Tools Menu.
2. In the *Connections* tab, click the **LAN Settings...** button.
3. Make sure the *Use a Proxy Server* checkbox is selected.

Note: If both *Use a Proxy Server* and *Bypass Proxy Server for Local Addresses* are selected, the GateLock IP address (192.168.1.254) will be bypassed because it is on the same LAN as the IP address from the ISP.

---

4. Click the **Advanced...** button. The *Proxy Settings* window will open.
5. In the *Exceptions* field, type **`192.168.1.254`** (this is the IP address of GateLock), then click **OK**.

Disabling the Proxy Server using Netscape

1. Select **Preferences...** from the Edit Menu.
2. In the left frame, click *Advanced*, then click *Proxies* (under *Advanced*).
3. Select *Direct Connection to Internet*, then click **OK**.

Enabling the Proxy Server with an Exception using Netscape

1. Select **Preferences...** from the Edit Menu.
2. In the left frame, click *Advanced*, then click *Proxies* (under *Advanced*).
3. Select **Manual Proxy Configuration**.
4. In the **Exceptions** field, type **`192.168.1.254`** (this is the IP address of GateLock), then click **OK**.

Activating the TCP/IP Protocol

Before you can use a PC for Internet access, you must have TCP/IP software running. This must be done for each computer you wish to use in conjunction with GateLock. (If you have already installed TCP/IP, skip to the next section now to set it up for use with GateLock.)

1. Click the **Start** button. The Start menu will open.
2. Point to **Settings** on the Start menu, then select **Control Panel** from the menu.
3. Double-click on the Network icon in the Control Panel window.

FIGURE A-1. *The Network icon in the Control Panel*

The *Network* window will then appear, as shown below in Figure A-2.

FIGURE A-2. *Making a **TCP/IP** Selection in the Configuration Tab*

4. Display the *Configuration* tab of the Network window, then click on the appropriate selection for the binding of TCP/IP and your Ethernet adapter. (You might have more than one TCP/IP selection available.)
5. Click the **Add...** button. The *Select Network Component Type* window will appear, as shown in Figure A-3.

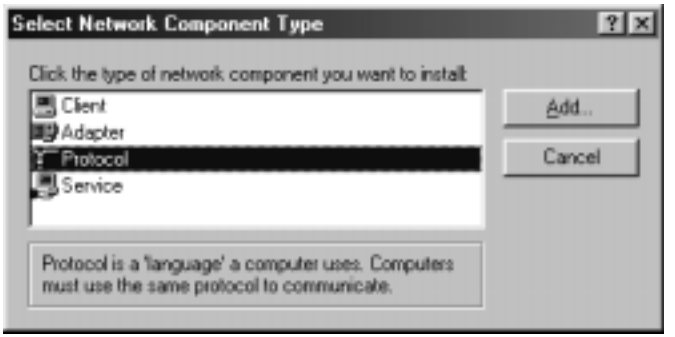

FIGURE A-3. *Specifying **Protocol** for TCP/IP Installation*

6. In the *Select Network Component Type* window, select *Protocol* (as shown above) and then click the **Add...** button. Or, simply double-click on *Protocol*. The *Select Network Protocol* window will open.
7. In the *Select Network Protocol* window, select *Microsoft* in the *Manufacturers* list on the left side of the window. Then select *TCP/IP* from the *Network Protocols* list on the right side of the window. This is illustrated in the Figure A-4 example.

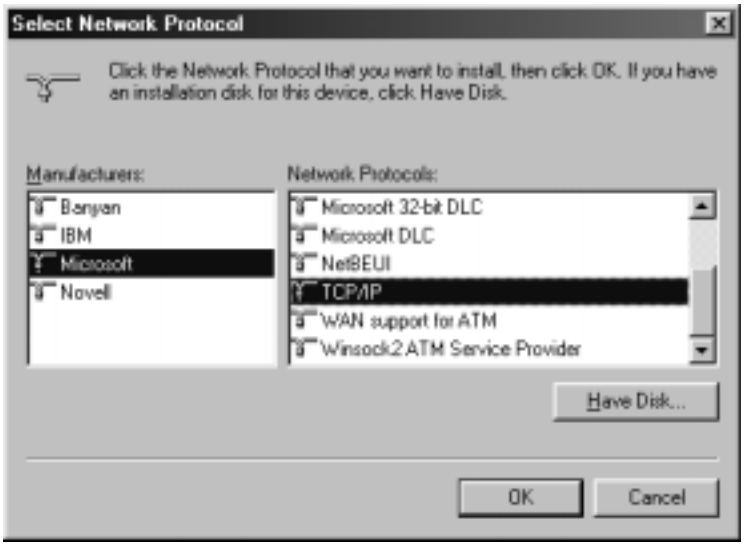

FIGURE A-4. *Selecting **Microsoft** and **TCP/IP** in Select Network Protocol*

8. Click **OK**. You are now ready to set the IP address property for TCP/IP.

Setting the Properties for TCP/IP

After each PC you wish to use in conjunction with GateLock has TCP/IP running as its active network protocol, you need to set the IP Address properties, in addition to checking other settings, as explained below.

1. Click the **Start** button. The Start menu will open.
2. Point to **Settings** on the Start Menu, then select **Control Panel** from the menu.
3. Double-click on the **Network** icon in the *Control Panel* window.

4. In the *Configuration* tab of the *Network* window, select *TCP/IP* from the list, as shown in Figure A-5.

FIGURE A-5. *Selecting **TCP/IP** in the Network Window*

5. Click the **Properties** button. The *TCP/IP Properties* window will appear, as shown in Figure A-6.

FIGURE A-6. *Configuring the IP Address Tab of the TCP/IP Properties Window*

6. Make sure the *Obtain an IP address automatically* button is selected, as shown in the illustration above. This will ensure that your computer gets its IP address from GateLock via DHCP (Dynamic Host Configuration Protocol) after you complete the connection and installation instructions as explained in Chapter 2.

> **Note:** Do not assign a specific IP address or Subnet Mask to your PC in this tab. If you do, you will not be able to access the Internet when using GateLock.

7. Click the *WINS Configuration* tab in the *TCP/IP Properties* window, and select *Disable WINS Resolution*, as shown in Figure A-7.

FIGURE A-7. *Configuring the WINS Configuration Tab*

8. Click the *Gateway* tab in the *TCP/IP Properties* window, and make sure there are no gateways installed. If there are, highlight any installed gateways and click the **Remove** button until there are none listed in the *Gateway* tab, as shown in Figure A-8.

FIGURE A-8. *Configuring the Gateway Tab*

5. Click the *DNS Configuration* tab and make sure the *Disable DNS* button is selected, as shown in the illustration below.

FIGURE A-9. *Configuring the DNS Configuration Tab*

6. Click **OK**, which will close the *TCP/IP Properties* window, and at the same time will save all of the TCP/IP settings you specified. You will be returned to the *Network* window.
7. Click the **OK** button in the *Network* window to close it. You will then be prompted to restart the PC. At this time, power down the computer, and follow the connection and installation instructions as explained in Chapter 2.

Technical Specifications

Protocols	IP, NAT, ARP, CSMA/CD, ICMP, DHCP, TCP/IP
Standards supported	IEEE 802.3 10BaseT, 802.3u 100BaseTX
Local (PC/HUB) Port	10BaseT, RJ-45 Ethernet
Uplink (Internet) Port	10BaseT Broadband
Cable Type	10BaseT — Category 3 or 5 UTP/STP 100BaseTX — Category 5 UTP/STP
Speed	WAN Router — 10M bps (10BaseT Ethernet) LAN Router — 10M bps (10BaseT Fast Ethernet)
LED Indicators	Power, Antivirus, Anti-Hacker, Internet, PC/HUB
Topology	Star

Environmental Data

Physical Dimensions	16.3 x 21.3 x 4.3 centimeters (6.4 x 8.4 x 1.7 inches)
Unit weight	14 ounces
Certifications	FCC Class B, CE Mark Commercial
Operating Temperature	0 to 40 degrees Celsius (32 to 104 degrees F)
Operating Humidity	10% to 80% non-condensing
Storage Temperature	-20 to +70 degrees Celsius (-4 to 158 degrees F)
Storage Humidity	Maximum 85% non-condensing

Glossary

ADSL

Asymmetric Digital Subscriber Line. This is one popular type of broadband line. In this manual, we use the term **xDSL** to denote all varieties of DSL, such as ADSL, IDSL, SDSL, VDSL, G-lite, etc.

DHCP

Dynamic Host Configuration Protocol. DHCP is software that automatically assigns IP addresses to clients who log into a TCP/IP network. (This type of IP address is called a **dynamic IP address**.) This software usually runs on Routers, Servers, and other network devices. By default, your GateLock router is set up to use DHCP so that you do not have to manually assign permanent IP addresses to every device on your network. We recommend that you not change this, so your PC will be recognized as a DHCP server.

Ethernet Card

A plug-in circuit board in a PC that takes parallel data from the computer and converts it into serial data. It then sends the data via 10BASE-T cable on the LAN in packet format. Also referred to as a Network Interface Card (NIC).

Gateway IP

The IP address of the gateway device that allows GateLock and a host to make contact.

Hub

A device that enables two or more computers to use one cable modem/broadband line. You would need to connect GateLock to the Hub, and then you could connect up to 32 computers to the Hub.

IP Address

Each IP (Internet Protocol) address is unique and consists of 32 bits. Every device on a network must have an IP address. An IP address consists of a network address (which is assigned by a government agency), and a host address (which is assigned by a company administator to each host computer). Although text characters are often used to represent an IP address, the actual address consists of digits. For example, the IP address for `http://www.antivirus.com` is **216.33.22.211**.

- **Dynamic** — A **dynamic IP address** is one that is assigned to a device on a TCP/IP network automatically by a DHCP server. The IP address would change every time

the device connects to the network, or when the modem is shut off. Therefore, a dynamic IP address does not necessarily change very often.

- **Static** — A **static IP address** is a permanently assigned address to a device on a TCP/IP network. For example, a printer would typically have a static IP address because it is repeatedly accessed by users. Since the static IP address is a "constant" address, it is more susceptible to attacks from hackers. GateLock helps to hide the IP addresses to make it harder for hackers to access your PCs. To check whether you have static DHCP IP addresses, consult your Internet Service Provider.

NAT

Network Address Translation. GateLock uses NAT and TCP/IP port inspections. NAT "converts" IP addresses on a local area network so that only one address is sent out publicly on the Internet. This means that the actual IP addresses of multiple computers connected to a private local area network is never made public on the Internet. In addition to this protection, NAT provides another benefit to users of GateLock. If you are using a cable/xDSL modem and have only one TCP/IP address provided by an Internet Service Provider, you can have multiple other private addresses behind the one address provided by the ISP.

Subnet Mask

Also known as Network Mask. A subnet is actually a network subdivision. It identifies the specific network and host addresses, by determining which part of an IP (Internet Protocol) address constitutes the network portion, and which part identifies the host portion. GateLock is furnished with a Subnet Mask of 255.255.255.0. The first three numbers, with a value of "255," indicate that the first three numbers are the IP address of a network. The last digit should be between 1 and 254 and identifies a host on that network. So, when subnetting is used, the IP address is divided into a subnet number and a host number. Hosts, as well as gateways, use the Subnet Mask to identify the bits used for the network and subnet number.

Appendix A Government compliance notices

D.1 FCC compliance

This Broadband Sharing Router has been tested and found to comply with the limits for a Class B personal computer and peripherals, 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 unit does cause harmful interference to radio or television reception, which can be determined by turning the unit off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Index

Trend Micro Incorporated
10101 N. De Anza Blvd., 2nd Floor
Cupertino, CA., 95014 USA
www.antivirus.com

For Sales:
Tel: +1-800-228-5651 (US and Canada)
Tel: +1-408-257-1500 (outside US and Canada)
Fax: +1-408-257-2003

Item Code: xxxx-xxxx