



# Intego VirusBarrier Server 3 User Manual

Welcome to the User Manual for Intego VirusBarrier Server 3. Use the Table of Contents below to go to the different sections of the manual. You can come back to this main Table of Contents at any time by clicking the *Go to Main Table of Contents* link at the top of each page.

## Table of Contents

- [1. Welcome to VirusBarrier Server 3](#)
- [2. Using Intego VirusBarrier Server 3](#)
- [3. Protecting Your Server from Viruses and Malware](#)
- [4. Protecting Your Server from Network Attacks](#)
- [5. Using VirusBarrier Server 3 Logs and Monitoring Tools](#)
- [6. VirusBarrier Server 3 Preferences and Configurations](#)
- [7. Creating Custom Firewall Rules](#)



## Welcome to Intego VirusBarrier Server 3

- [Controlling Malware on a Mac OS X Server](#)
- [VirusBarrier Server 3 Features](#)
- [Installing VirusBarrier Server 3](#)
- [Running VirusBarrier Server 3 in Evaluation Mode](#)
- [Connecting VirusBarrier Server 3 to Remote Servers](#)
- [Updating VirusBarrier Server 3 Virus Definitions](#)
- [About Your Copy of VirusBarrier Server 3](#)

[Go to Main Table of Contents](#)

### Controlling Malware on a Mac OS X Server

System administrators are well aware of the threat of viruses and malware on a server. While malware on a client computer can damage files on that computer, and eventually propagate throughout a network via files that are emailed or sent over a network, a virus on a server could damage all the computers on the network. Viruses on a file server that don't affect the server itself, if it is running a different operating system from client computers, can still propagate as users copy files to their computers. Beyond viruses, many types of malware, such as worms and Trojan horses, can infect servers, potentially granting remote access to malicious users.

Mac OS X servers are used in a variety of environments, from Mac-only networks to networks containing a mixture of Macs, Windows PCs and computers running Unix or Linux systems. Protecting a Mac OS X server against viruses requires that not only Mac viruses be detected, but also Windows viruses, Word and Excel macro viruses, and Unix and Linux viruses.

VirusBarrier Server 3 provides this protection, ensuring that infected files that get onto your server don't go any further. VirusBarrier Server 3 also provides network protection, with a powerful two-way firewall, and contains features that block network attacks.

VirusBarrier Server 3 automatically scans every file that is copied to a Mac OS X Server computer where it is installed, as well as any files that are launched on the server. If it finds viruses, the infected files are quarantined, and administrators can determine which actions to take. VirusBarrier Server 3 can also be set to run scheduled scans of

both local and network volumes.

VirusBarrier Server 3 also offers full protection for all e-mail that is sent or received via Mac OS X Server's built-in e-mail server. It automatically scans all e-mail messages that pass through the server, checking e-mails for infected attachments. If it finds malware, the e-mails carrying them are quarantined, and notifications can be sent to administrators informing them of this activity.

VirusBarrier Server 3's Antivandal offers a number of powerful tools to prevent network attacks, such as ping floods, intrusion attempts, port scans and more. Administrators can use the program's Blocked Address and Trusted Addresses lists to blacklist and whitelist specific IP addresses or ranges.

VirusBarrier Server 3 includes a copy of Intego VirusBarrier X6, which, installed on your server, allows you to set some additional options and gives you access to certain functions on the server.

### **Controlling Malware on a Mac OS X Server**

VirusBarrier Server 3 works in several ways. While it watches over your server at all times, protecting you from viruses and malware, you can use the included VirusBarrier X6 client program to manually scan any disk or network volume at any time. You can also set up scheduled scans of both local and network volumes, and have scans run automatically when certain events occur, such as following updates to virus definitions.

### **Automatic Repairs, Quarantine or Deletion of Infected Files**

You can choose how VirusBarrier Server 3 acts when malware is found: It can repair infected files automatically, quarantine them until an administrator can check them, or delete infected e-mail messages.

### **Scan Logs**

VirusBarrier Server 3 provides complete logs of all activity, including the names and locations of malware and suspicious files it finds. It can send e-mail notifications to the recipient of your choice, alerting you to the presence of infected files as soon as it detects them.

### **Firewall Features**

With VirusBarrier Server 3's powerful two-way firewall, you can use basic settings or set up complex rules, which allow you to filter network traffic granularly. Full logs show incoming and outgoing traffic, and the program's Antivandal feature steps in automatically when certain types of attacks are detected.

### **NetUpdate**

VirusBarrier Server 3 works with Intego's NetUpdate, which manages program updates and new threat filters automatically. You can set the update frequency in NetUpdate itself, so the program checks for updates daily, weekly or monthly. For more details, see the [Intego Getting Started Manual](#).

## **VirusBarrier Server 3 Features**

VirusBarrier Server 3 offers:

### **General Features:**

- A GUI administration console
- Detailed logs of all infected files sent automatically to administrators
- Full logs allow users to audit all network activity
- Stores logs in the Apple system log facility
- Automatic updates of program and threat filters via Intego NetUpdate

## Malware Protection:

- Detects and eliminates all known Mac viruses and malware
- Scans files for Windows and Unix viruses
- Protects against Trojan horses
- Protects against adware, hacker tools, dialers, keyloggers and more
- Repairs infected files
- A full quarantine zone to isolate infected files
- Scans all files written to or opened on the server
- Scheduled scans of local and network volumes
- Automatic scans after virus definitions are updated or when volumes are mounted
- Command-line control for remote scans
- Trusted Files zone to disable Real-Time scanning on selected files or folders
- Scans of all e-mail sent and received via the Mac OS X Server e-mail server
- Notifications of infected e-mails sent automatically to administrators
- Scans compressed files and archives
- Archive scanning can be activated by archive type
- Scanning for Windows viruses can be deactivated
- Suspicious file analysis by the Intego Virus Monitoring Center
- Turbo Mode technology for faster scans

## Network protection:

- Controls incoming and outgoing TCP/IP traffic and data
- Protects against all kinds of intrusions
- Protects against network attacks
- Protects against ping floods, port scans, and more
- Simple and advanced firewall modes
- Offers customizable firewall rules
- Logs display real-time network activity with domain name resolution
- Blocked Addresses and Trusted Addresses lists store friendly and malicious IP addresses
- Offers a choice of defense policies, with advanced options for intrusion protection
- Individualized security policies for network attack prevention

# Installing VirusBarrier Server 3

VirusBarrier Server 3 requires Mac OS X 10.5 or later, or Mac OS X Server 10.5 or later, running on an Xserve or any other Mac configured as a server. E-mail scanning is only available on Mac OS X Server's built-in e-mail server.

VirusBarrier Server 3 comes as a set of .pkg files which you can install on remote servers using Apple Remote Desktop or command-line tools. Before installing, you must accept the terms and conditions presented in the "License" file.

Your CD has three folders:

- **VirusBarrier Server Admin.** This is the program you will use on a remote computer, or on your server, to administer VirusBarrier Server 3 on the server. To install VirusBarrier Server Admin, open the VirusBarrier Server Admin folder then double-click the VirusBarrier Server Admin.mpkg file and follow the instructions. You will have to restart your computer after this installation.
- **Packages & Utilities.** This folder contains remote installation packages that must be installed on your server.

They include:

- RMCCClient.pkg
- CommonServices.pkg
- Netupdate.pkg
- VirusBarrier Server 3.pkg

You must install the "CommonServices.pkg" package to use any Intego software.

You can install these files directly on the server, if you can access it in this manner, by simply double-clicking the installer files and following the instructions; the standard Apple Installer application carries out the installation.

The folder also contains a Read Me file for further instructions.

- **Manuals.** This folder contains links to on-line user manuals.

### To install VirusBarrier Server 3 using Apple Remote Desktop 2.x or 3.x:

1. Open Apple Remote Desktop.
2. Select all the target servers.
3. Choose **Manage > Install Packages...**
4. Select the Intego packages you want to install.
5. Click Install.

### To install VirusBarrier Server 3 using command-line tools:

1. Copy the packages to the remote server using ftp, afp or scp.
2. Use the installer command line tool to install each package:  
`sudo /usr/sbin/installer -pkg "/path/to/package.pkg" -target /`
3. Restart the server.

To **uninstall VirusBarrier Server 3**, use the uninstallation shell scripts included in the Remote Installation Packages & Utilities folder of the VirusBarrier Server 3 CD. They are:

- `uninstall_all.command`, which uninstalls all components of VirusBarrier Server 3.
- `uninstall_VirusBarrier.command`, which uninstalls only the VirusBarrier X6 client program.
- `uninstall_VirusBarrier_Server.command`, which uninstalls only the VirusBarrier Server Admin program.

You can run these scripts by double-clicking them on the server from which you want to uninstall the software, or by running them from Terminal.

## Running VirusBarrier Server 3 in Evaluation Mode

VirusBarrier Server 3 offers an evaluation mode, to allow you to discover how the program works before purchasing it. When VirusBarrier Server 3 runs in evaluation mode, it functions for 30 days, during which it will not repair any files.

## Connecting VirusBarrier Server Admin to Remote Servers

For VirusBarrier Server Admin to be able to connect to remote servers, it must be able to accept connections through ports 8500 and 8502 TCP. If servers use a firewall, including that which is part of VirusBarrier Server 3, this port must be open for VirusBarrier Server Admin to be able to access the servers.

## Updating VirusBarrier Server 3 Threat Filters

VirusBarrier Server 3 uses Intego NetUpdate, which is installed with the program, to provide updates to the program's threat filters, as well as to the program itself. For information on using NetUpdate, see the [Intego Getting Started Manual](#).

## About Your Copy of VirusBarrier Server Admin



To get information about your copy of VirusBarrier Server 3, choose **VirusBarrier Server Admin > About VirusBarrier Server Admin**. It gives information about VirusBarrier Server, such as the version number, your support number (a number you will need for technical support), and a clickable link to send e-mail to Intego's support department.

## Technical support

Technical support is available for registered purchasers of Intego products with valid subscriptions from the [Intego Support page](#).

[Using VirusBarrier Server 3 »](#)



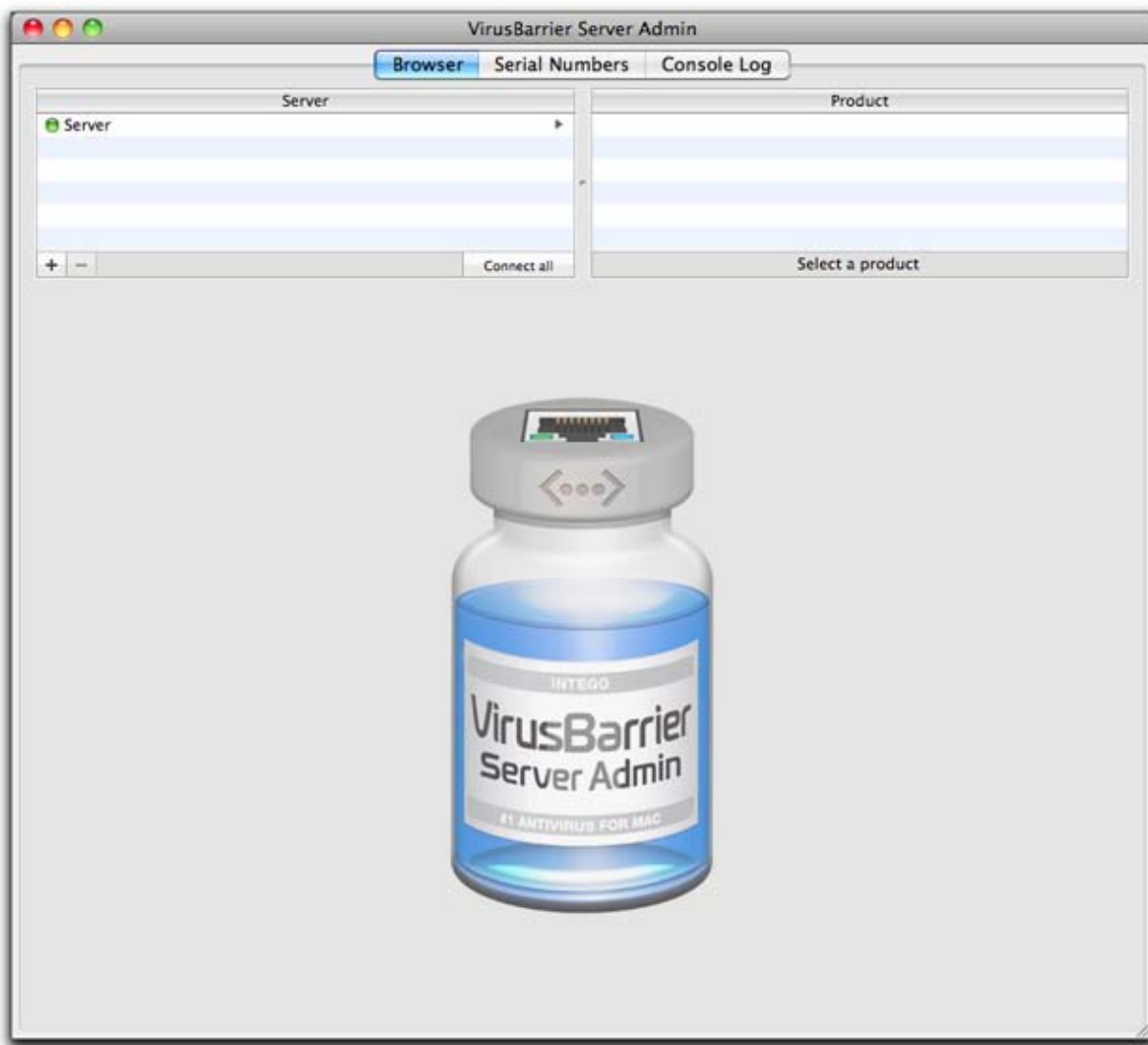
## Using Intego VirusBarrier Server 3

- [Launching VirusBarrier Server Admin](#)
- [Using the Browser](#)
- [Adding Servers to the Browser](#)
- [Managing Products via the Browser](#)
- [VirusBarrier Server 3 Protection Settings](#)
- [Using the Console Log](#)
- [Using the VirusBarrier X6 Application on your Server](#)
- [Using VirusBarrier Server 3 from the Command Line](#)
- [Using VirusBarrier Server 3 and AppleScript](#)

[Go to Main Table of Contents](#)

### Launching VirusBarrier Server Admin

After you've installed VirusBarrier Server 3 on the server you wish to manage, and installed VirusBarrier Server Admin on your administrator's computer, open VirusBarrier Server Admin, located in /Applications/Server. The program displays the Browser tab.



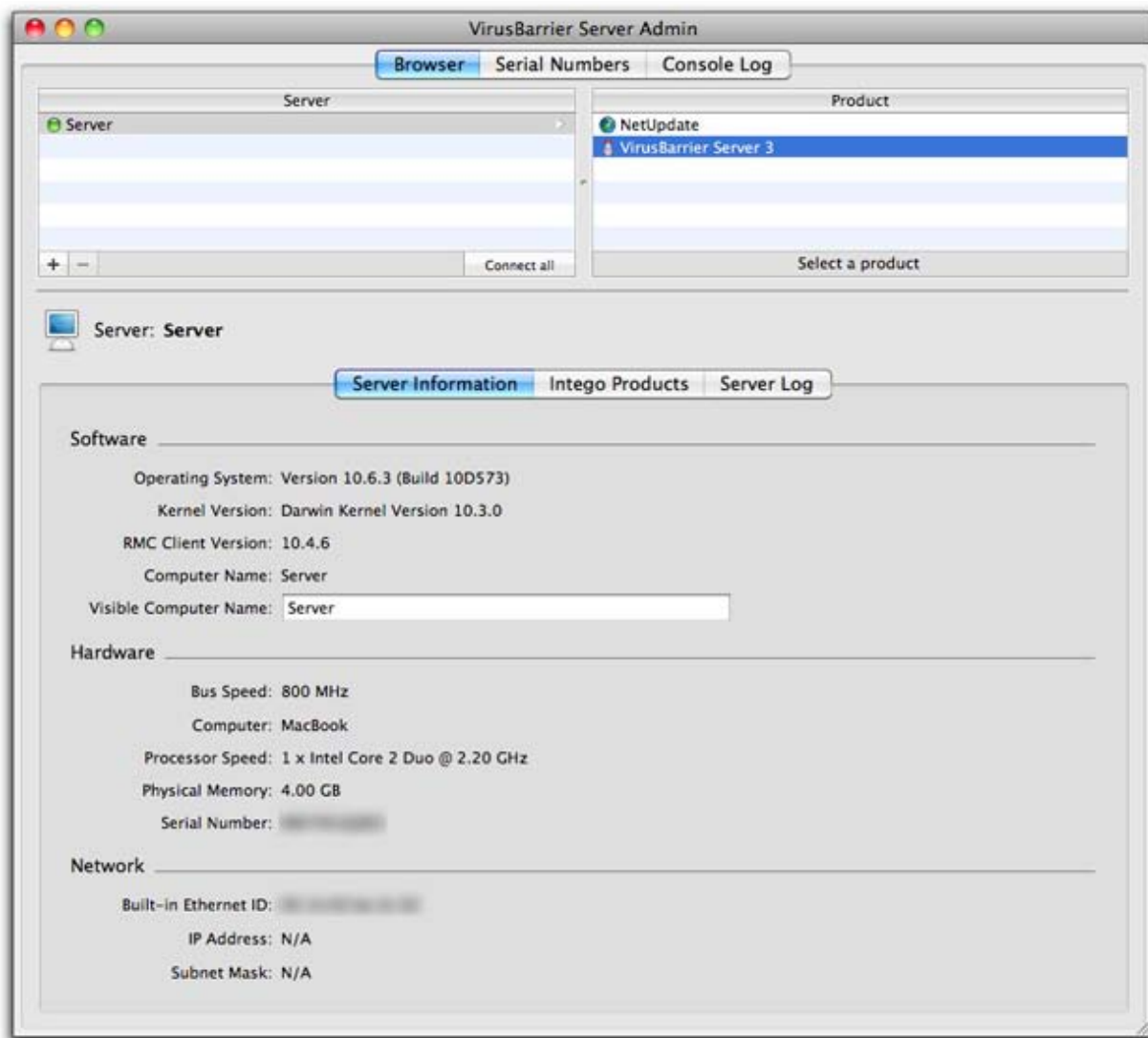
VirusBarrier Server Admin contains three tabs, each of which provides access to information or management functions:

- **Browser:** lets you browse servers and select the VirusBarrier Server 3 programs installed. From this tab you can make changes to settings, view logs and quarantine information, monitor and manage updates via Intego NetUpdate, and control all the malware and network protection features of VirusBarrier Server 3.
- **Serial Numbers:** lets you view the serial numbers used for VirusBarrier Server 3 on the servers you manage.
- **Console Log:** provides a log of all actions made from the VirusBarrier Server Admin application.

## Using the Browser

The VirusBarrier Server Admin browser gives you an overview of servers and Intego products that you can manage. You can view information for specific servers, you can check which Intego products are installed and verify their serial numbers, and you can check logs to see what actions have been applied to specific servers.





When the **Browser** tab is active, VirusBarrier Server Admin displays the Server list, which shows a list of servers that you can manage. If you click on a server in the Server list, VirusBarrier Server Admin displays detailed information about that computer in the **Server Information** tab.

VirusBarrier Server Admin displays the following information about servers:

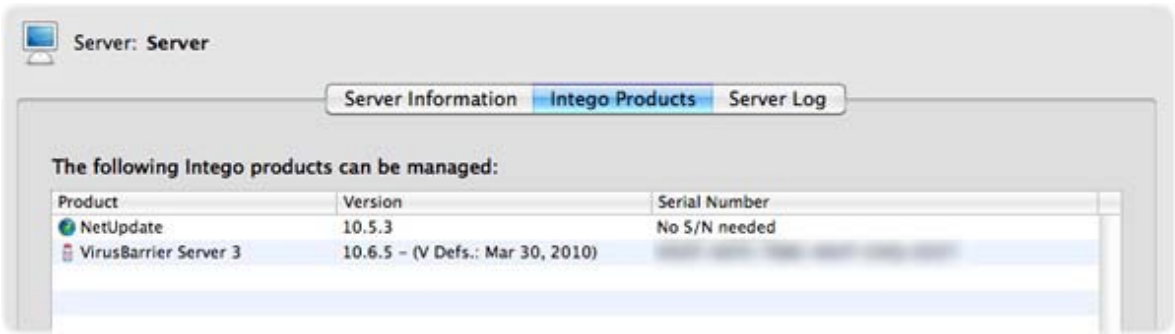
- **Software:** this section displays the operating system version and build, the kernel version, the RMC Client version (an RMC Client component must be installed on the server with VirusBarrier Server 3 to ensure remote management), the computer name (as set on the server), and the visible computer name. You can change this visible computer name by replacing the text in this field.
- **Hardware:** this section shows the type of computer, the processor and bus speed, the amount of RAM installed, and the computer's serial number.
- **Network:** this displays the server's Ethernet (or MAC) address, IP address, and subnet mask.

A colored icon appears before the names of the computers in the server list. Three colored icons may appear in this column:

- **Green:** VirusBarrier Server Admin is connected to the server.
- **Red:** VirusBarrier Server Admin is not connected to the server; the server is not available on the local network.
- **Orange:** VirusBarrier Server Admin is not connected to the server; the connection has failed.

If any servers do not respond you can attempt to reconnect to them by clicking the **Connect All** button.

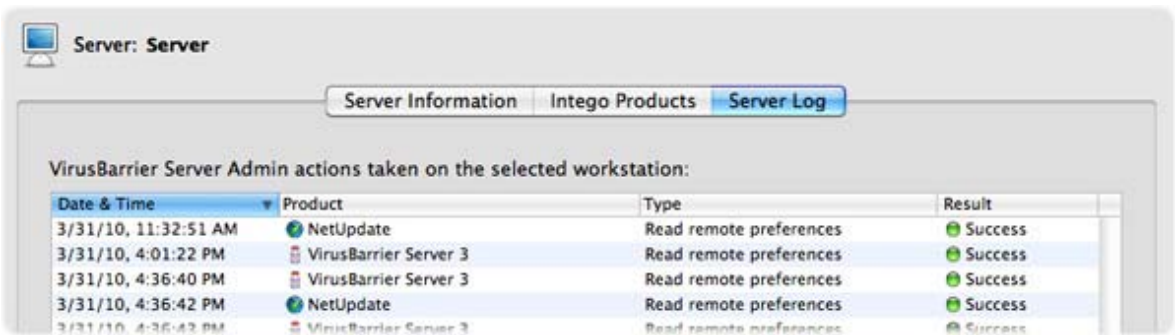
The **Intego Products** tab, which displays when the Browser tab is active and a server is selected, shows a list of all Intego products available on the selected server, their version numbers and their serial numbers.



The **Version** column shows both the version of the Intego product and the date of the last update to VirusBarrier Server 3's virus definitions.

The **Serial Number** column shows you if any serial numbers are not recognized (which also includes serial numbers you have not yet added to VirusBarrier Server Admin for specific products), or if a serial number is not needed, as is the case for Intego NetUpdate. If a product displays **Running in demo mode** in the **Serial Number** column then you haven't yet entered its serial number and it is still within the 30-day evaluation period.

The **Server Log** tab shows which actions have been performed on the selected server. This log displays the **Date & Time**, the Intego program that has been acted on (**Product**), the **Type** of action, and the **Result** of the action, whether it was successful or not.



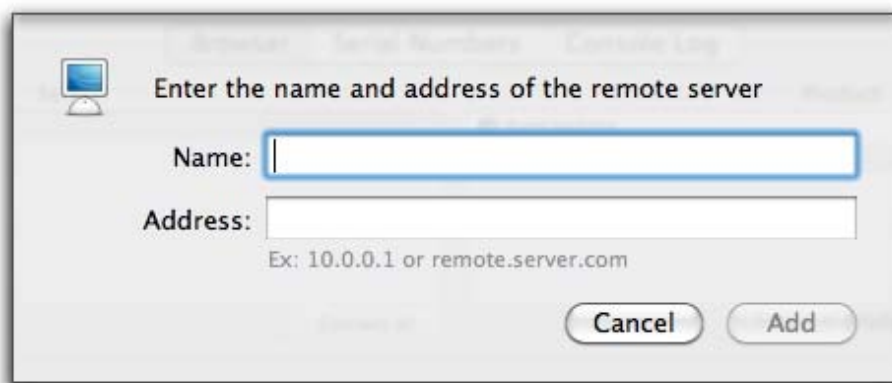
Two icons display in the right-hand column of the **Server Log** list: a green icon indicates that the action was successful, and a red icon that the action failed. Actions such as reading or writing preferences may fail if there is a connection failure with the remote computer while the action is carried out. If an action fails, the **Result** column shows an error message explaining why.

## Adding Servers to the Browser

VirusBarrier Server Admin uses Bonjour to automatically detect all Mac OS X computers on a local network where the RMC client is installed. All servers accessible locally therefore display automatically in the Browser.

The best way to manage Macs outside your local network with VirusBarrier Server Admin is to create a VPN tunnel between the administration computer and remote servers. If you do this, remote computers will display in the **Server** list via Bonjour.

You can also add Macs to the Server list manually. To do this, click the plus (+) button below the Server list. A dialog displays asking you to enter a server name and address.



You can enter any name you wish for the server; this is the visible computer name that will display in the **Server Information** tab of the browser.

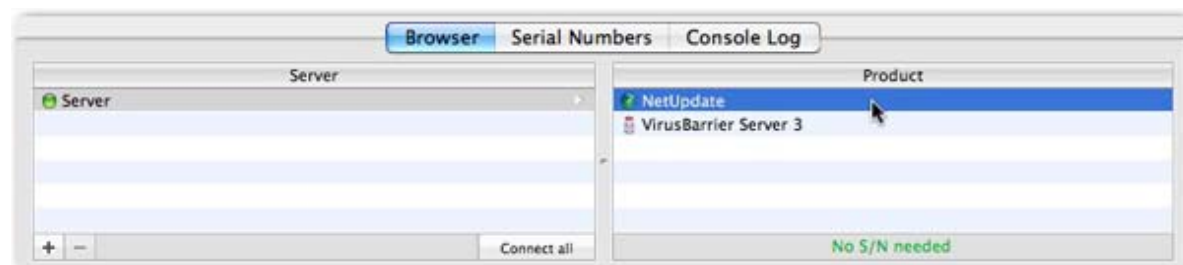
Enter an IP address for the remote computer. You must have direct access to a remote server to add it in this manner; if the server is behind a router, you must set up port mapping so ports 8500 and 8502 TCP are mapped to the remote server.

Once VirusBarrier Server Admin has detected a server, or once you have added one to the browser, it remains in the list even if it is not available when you launch VirusBarrier Server Admin at a later time. You can remove a server, if you wish, by clicking its name to select it, then clicking the minus (–) button below the Server list.

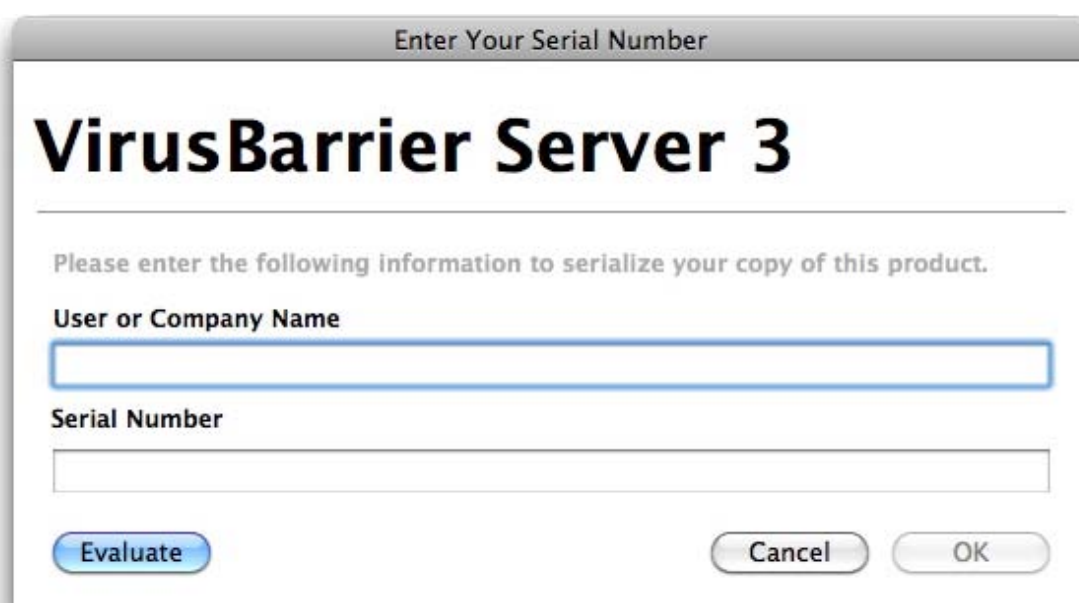
## Managing Products via the Browser

When you click one of the computers in the Server list, a list of available Intego products displays in the **Product** column. You can select one of these products to get information about the product and access its settings.

Below the Browser's **Product** column you can see if a program does not need a serial number (this is the case for NetUpdate), if it is running in demo mode, or if it has been serialized.



The first time you click on a product that requires a serial number in the Browser, VirusBarrier Server Admin will ask you to enter a serial number for the product. The following dialog displays:



Enter your name or company and your serial number, then click OK. If you want to run the program in demo mode, click **Evaluate**.

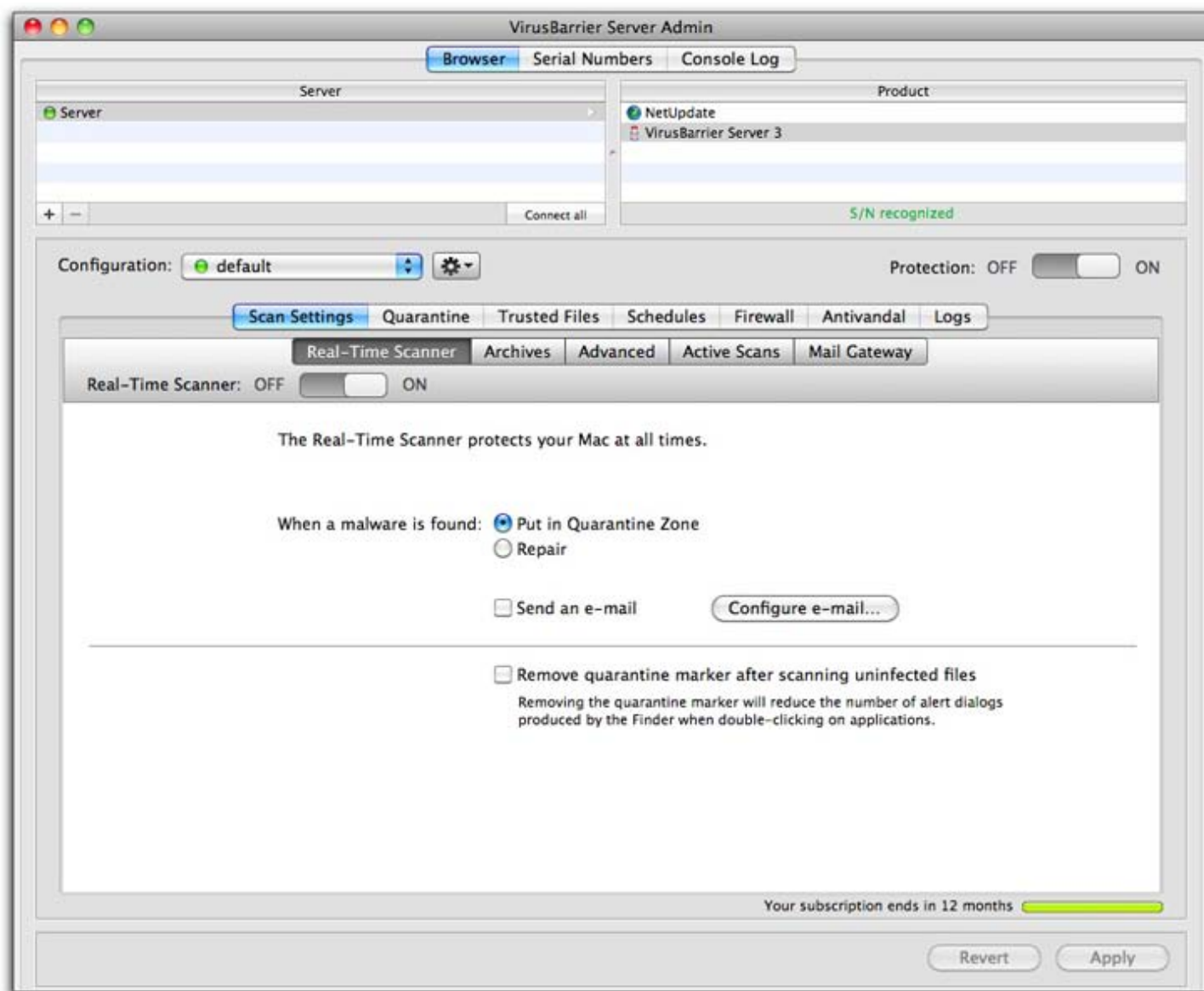
You can also add serial numbers by clicking the **Serial Numbers** tab at the top of the VirusBarrier Server Admin window and clicking the + icon at the bottom of the window; the procedure is the same.

Once you've entered the appropriate serial numbers for the Intego products you are managing, you can make changes to any of these programs from the Browser. To do this, select a server, then a product. This presents an interface that allows you to apply settings and carry out certain actions.

To learn how to keep your Intego programs up to date via the Browser, see the [NetUpdate Scheduling Preferences](#) section of Chapter 6.

## VirusBarrier Server 3 Protection Settings

Selecting VirusBarrier Server 3 from the Product column shows you the following:



These screens, which are very similar to those in VirusBarrier X6, give you access to the many ways that VirusBarrier Server 3 can protect computers on your network. Details on changing these settings are found in the remaining sections of this manual.

## Turning Protection Off

If you ever want to turn off both malware and network protection on a copy of VirusBarrier Server 3, you can do so by dragging the slider from ON to OFF when a server and a copy of VirusBarrier Server 3 are selected as shown above.

## Using the Console Log

The **Console Log** tab shows you a list of all actions you have carried out with VirusBarrier Server Admin on all servers. Like the **Server Log** tab in the Browser, this log shows which actions have been performed on the selected server. This log displays the **Result**, the **Type** of action, the **Date & Time**, and the **Product**, or Intego program that has been acted on. It also shows which server these actions were performed on.

Browser   Serial Numbers   Console Log				
Date & Time	Server	Product	Type	Result
4/1/10, 10:20:20 AM	Server	VirusBarrier Server 3	Read remote preferences	Success
4/1/10, 10:17:36 AM	Server	VirusBarrier Server 3	Read remote preferences	Success
4/1/10, 10:15:10 AM	Server	NetUpdate	Read remote preferences	Success
3/31/10, 7:53:25 PM	Server	VirusBarrier Server 3	Read remote preferences	Success
3/31/10, 7:53:14 PM	Server	VirusBarrier Server 3	Read remote preferences	Success
3/31/10, 7:53:11 PM	Server	NetUpdate	Read remote preferences	Success
3/31/10, 7:53:05 PM	Server	VirusBarrier Server 3	Read remote preferences	Success
3/31/10, 7:52:38 PM	Server	VirusBarrier Server 3	Read remote preferences	Success
3/31/10, 7:49:54 PM	Server	VirusBarrier Server 3	Read remote preferences	Success
3/31/10, 7:38:54 PM	Server	NetUpdate	Read remote preferences	Success
3/31/10, 4:46:51 PM	Server	VirusBarrier Server 3	Read remote preferences	Success
3/31/10, 4:40:30 PM	Server	VirusBarrier Server 3	Read remote preferences	Success
3/31/10, 4:36:43 PM	Server	VirusBarrier Server 3	Read remote preferences	Success
3/31/10, 4:36:42 PM	Server	NetUpdate	Read remote preferences	Success

Two icons display in the right-hand column of the console log: a green icon indicates that the action was successful, and a red icon that the action failed. Actions such as reading or writing preferences may fail if there is a connection failure with the remote computer when the action is carried out. If an action fails, the **Result** column shows an error message explaining why the action was not successful.

You can also narrow down the display in the console log using the search field at the bottom of the window. You can enter a string containing part of a name of a server, a product, a date, type of action or a result. As you type, the log displays only those log entries that contain your search string.

## Using the VirusBarrier X6 Application on your Server

A copy of VirusBarrier X6 is provided with VirusBarrier Server 3. VirusBarrier X6 is not a substitute for VirusBarrier Sever 3; rather, it extends the functions of the server program.





For more on using VirusBarrier X6, see the VirusBarrier X6 manual, available from the **Help** menu of VirusBarrier X6.

## Using VirusBarrier Server 3 from the Command Line

VirusBarrier Server 3 also give you the option of scanning files and volumes from the command line. The following describes the use of this command.

```
/Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers
[-rtcCaz] <pathname_to_scan> [<current_directory_pathname>]
```

The following options are available:

```
-a:   Scans all files, including those symlinked to other volumes
      (or other mount points in /Volumes).
-c:   Counts files before scanning.
-C:   Counts files, but does not scan.
-Q:   Performs a quick scan.
-r:   Repairs infected files.
-t:   Uses Turbo Mode; scans only those files that have not been modified
      since the previous scan.
-T:   Scans all but trusted files.
-z:   Scans compressed archives (including those in e-mail attachments).
```

<pathname\_to\_scan>: This is required; it can be a relative or absolute path.

[<current\_directory\_pathname>]: This is optional; it is the current working directory if a relative path is used as the first argument.

Example:

```
/Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers
-tacz /
```

This scans all volumes for which the user has read permission, scanning archives and counting the number of files to scan before beginning. If you run the command preceded by `sudo`, and authenticate, you can scan all files.

You can also define aliases to simplify the use of this command.

```
For bash:
alias vbscan=/Library/Intego/virusbarrier.bundle/Contents/MacOS/
virusbarriers

For tcsh:
alias vbscan /Library/Intego/virusbarrier.bundle/Contents/MacOS/
virusbarriers

This allows you to run the same command as follows:
vbscan -tacz /

To change network protection settings, use the following option, along with the
operations, objects and data listed below (all commands with firewall options
require sudo):

-W: Execute firewall operations
```

operation	object	data
import export	settings	file_path
revert	settings	
add remove	blocked_address trusted_address	ip_address
print	blocked_address trusted_address	
get	protection	
enable/disable	protection	
enable/disable	trojans	
activate	configuration	configuration_name
print	configuration	

```
For example, to enable firewall protection, run the following command with sudo:
/Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers -W enable protection
```

## Using VirusBarrier Server 3 and AppleScript

VirusBarrier Server 3 offers the ability to run scans using AppleScript. For more information on the program's AppleScript syntax, open the VirusBarrier X6 dictionary on the remote server from Script Editor. VirusBarrier X6 is installed in the /Applications folder of the server.





## Protecting Your Server from Viruses and Malware

- [Real-Time Scanning](#)
- [Running Scheduled Scans](#)
- [Scan Settings](#)
- [Quarantine Zone](#)
- [Trusted Files](#)
- [The VirusBarrier Server 3 Contextual Menu](#)

[Go to Main Table of Contents](#)

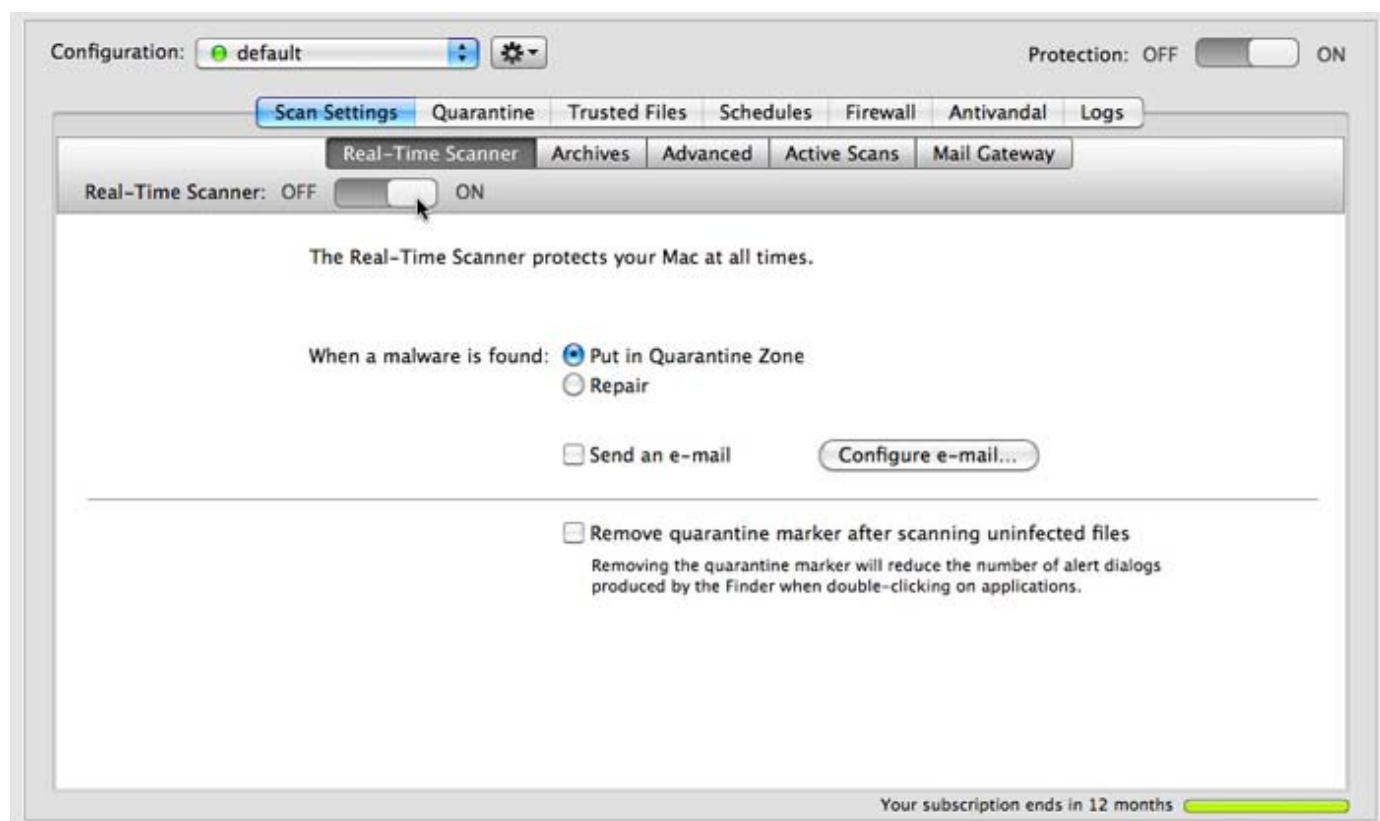
VirusBarrier Server 3's anti-malware protection works in several ways. Its Real-Time Scanner constantly watches over your server, protecting it and the files it contains from viruses and malware. The Real-Time scanner ensures that your server is protected at all times by scanning every file that is created, copied, modified or saved. It does not, however, scan other files. This is why we suggest you run a full scan of all your files when you install VirusBarrier Server 3 and after each update to the program's virus definitions.

### Real-Time Scanning

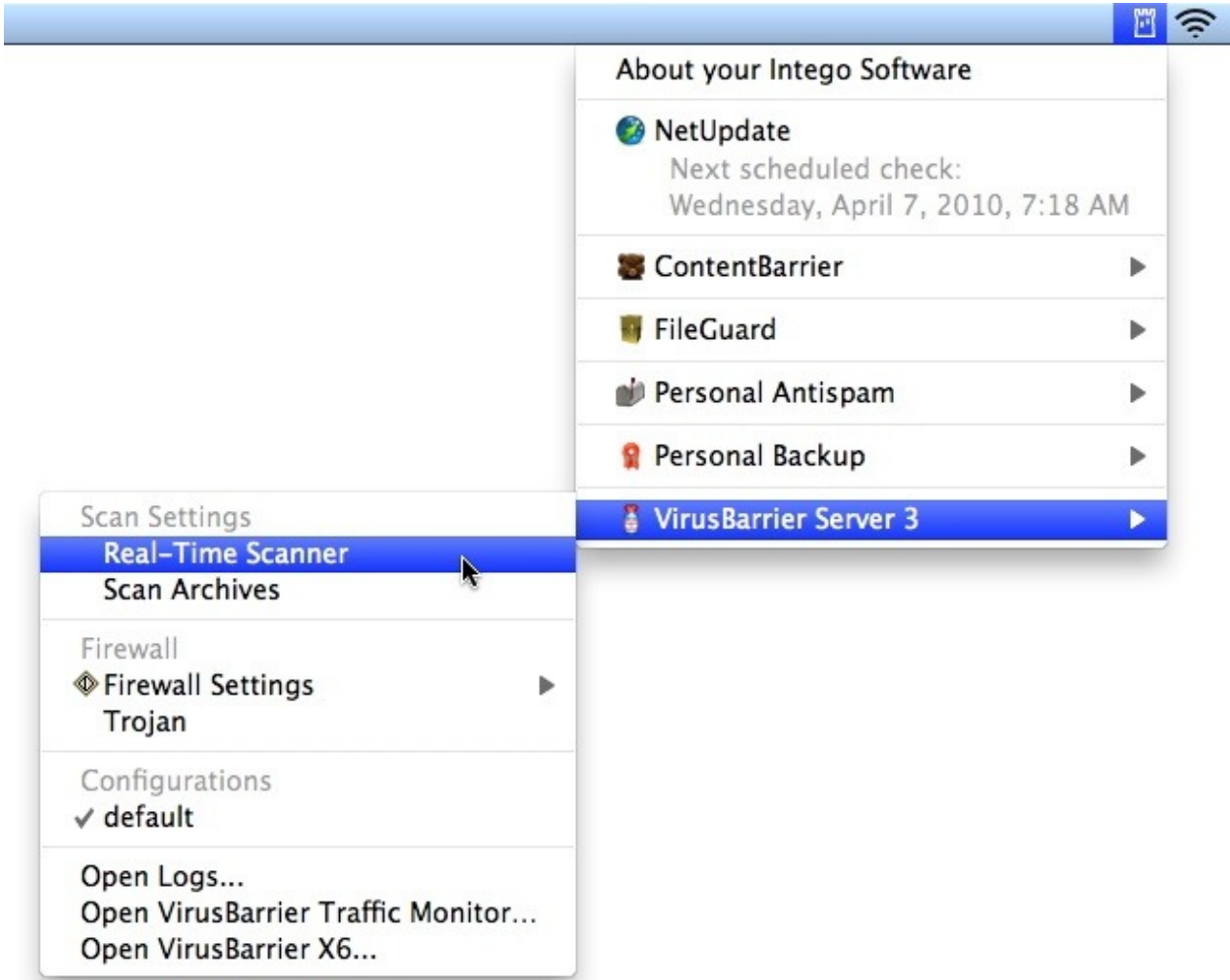
VirusBarrier Server 3's Real-Time Scanner scans your server whenever its contents change. Scans occur instantly, so you never have to worry about being protected.

To turn on the Real-Time Scanner, either:

- Click the **Scan Settings** tab in the Browser window, then click the **Real-Time Scanner** tab. In the resulting pane, move the **Real-Time Scanner** switch from Off to On.

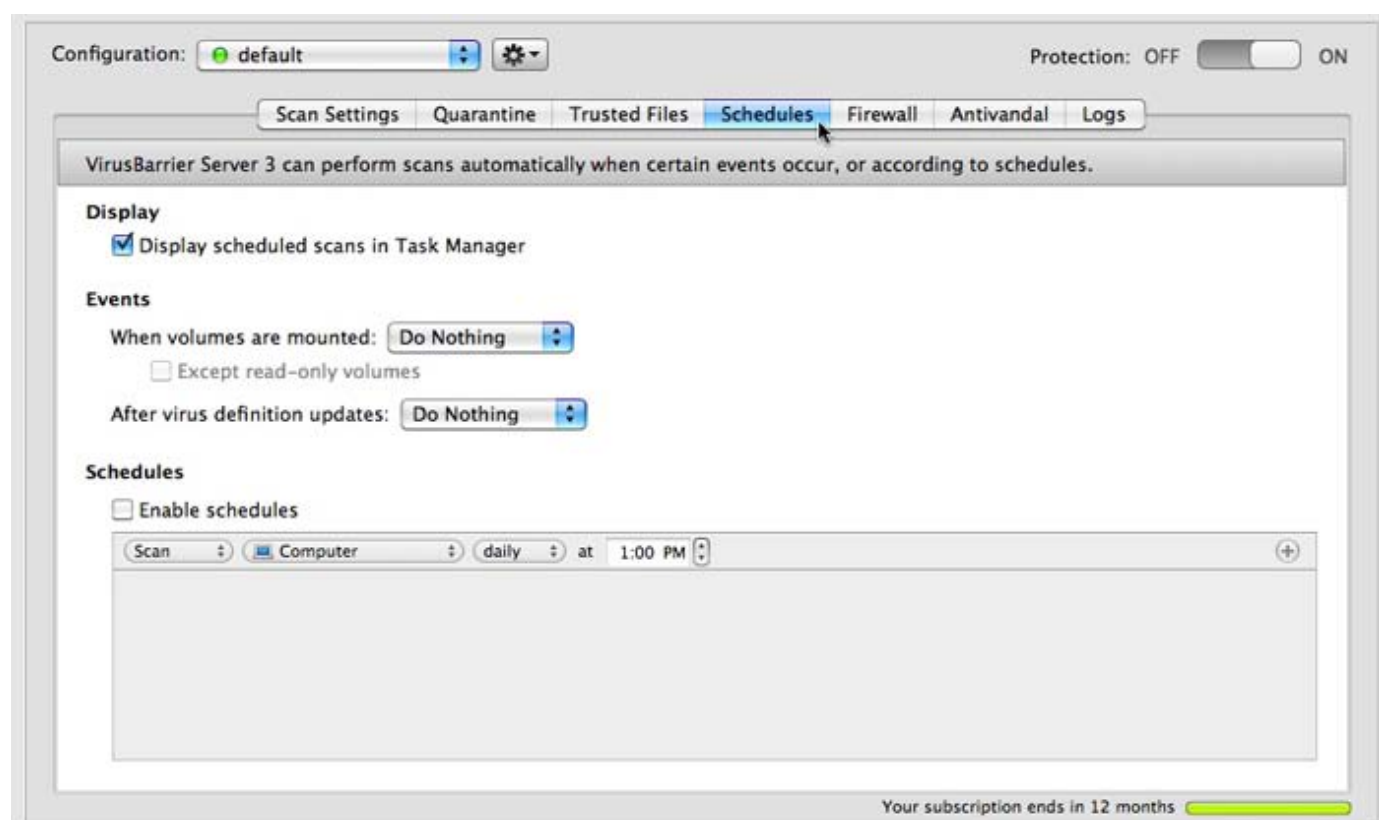


- If you are on the server, you can choose the Intego menu in the menubar, then choose **VirusBarrier Server 3 > Real-Time Scanner**.



## Running Scheduled Scans

VirusBarrier Server 3 can also be set to run automatically at pre-arranged times. To do so, click the **Schedules** tab while in the Browser window. The Schedules pane appears. There are three sections: **Display**, **Events** and **Schedules**.



- The **Display** section has only one checkbox: **Display scheduled scans in Task Manager**. When checked, you'll see a small window appear whenever your server executes scheduled scans; when unchecked, such scans will occur without notification (unless a virus is found).
- The **Events** section lets you direct VirusBarrier Server 3 to automatically run a scan, do repairs, or do nothing when certain events occur.

The first event, **When volumes are mounted**:, is triggered whenever you mount a new storage device, whether local (such as a hard drive) or remote (such as a network drive). If the **Except read-only volumes** checkbox is checked, VirusBarrier Server 3 will perform the action only on those volumes where it could change the drive being scanned (for example, to repair an infected file on a disk).

The second event, **After virus definition updates**:, lets you tell VirusBarrier Server 3 what to do after the program downloads and installs new virus definitions and threat filters. These are updated regularly, and especially when new malware is discovered to offer protection against that threat. Therefore, you should perform a new scan at those times to check for the new malware, either manually or (by checking this checkbox) automatically.

- The **Schedule** section lets you determine when VirusBarrier Server 3 will run automated scans.

Below these settings is a scheduling selector, where you can say which folder should be examined, and when.

- The first popup menu lets you choose whether you'd like to **Scan**, **Quick Scan**, or **Repair** the selected files at the scheduled time. If you choose **Quick Scan**, you cannot choose specific folders to scan; the second menu will disappear. (Quick scans scan only those locations where malware is commonly installed. The files and folders scanned may change as new malware appears, and the locations scanned may be different with newer versions of VirusBarrier X6's virus definitions.)
- The second popup menu lists the areas you are most likely to want to scan. The default choice, **Computer**, directs VirusBarrier Server 3 to scan all folders for all users on your server.
- The third popup menu lets you choose whether you want to perform the operation **daily**, **weekly**, or

**monthly**. If you select **daily**, you'll be able to choose the time you prefer; select **weekly**, you'll also choose your preferred day; select **monthly**, you'll choose which day of the month.

You can create multi-part schedules, for example to scan your Users folder every night, and your entire server once a week. To do so, click the + button to the right of the schedule item: another schedule item will appear beneath it. Make changes in that schedule item as you like. You can add as many schedule items as you like this way; to remove one of them, click the – button next to it.

## Schedules

☒ Enable schedules

Scan	Documents	daily	at	9:00 PM	–	+
Scan	/	weekly	on	Saturday	at	1:00 AM

The order of schedule items is not important; if you've scheduled two scans to run at the same time, they will occur simultaneously.

To turn off all pending schedules, uncheck the **Enable schedules** button.

## Scan Settings

VirusBarrier Server 3 gives you a number of options to tell the program how it should scan your server, what types of files it should scan, and what types of malware it should look for. To access these settings, click the **Scan Settings** tab. On that pane, the **Real-Time Scanner** tab is selected.

Configuration: default Protection: OFF ON

Scan Settings | Quarantine | Trusted Files | Schedules | Firewall | Antivandal | Logs

Real-Time Scanner | Archives | Advanced | Active Scans | Mail Gateway

Real-Time Scanner: OFF ON

The Real-Time Scanner protects your Mac at all times.

When a malware is found: ☒ Put in Quarantine Zone ☐ Repair

☐ Send an e-mail [Configure e-mail...](#)

☐ Remove quarantine marker after scanning uninfected files  
Removing the quarantine marker will reduce the number of alert dialogs produced by the Finder when double-clicking on applications.

Your subscription ends in 12 months

The Scan Settings pane contains five tabs:

- **Real-Time Scanner**, which controls how VirusBarrier Server 3 runs scans in the background;
- **Archives**, which tells VirusBarrier Server 3 whether to scan archives and what types of archives to scan;
- **Advanced**, which provides additional scan settings;
- **Active Scans**, which gives information on scans currently being performed;
- **Mail Gateway**, which gives further information on e-mail protection that VirusBarrier Server 3 is providing.

## Real-Time Scanner Settings

In normal operation, you will not need to disable the Real-Time Scanner; this is only useful for troubleshooting when you have a problem, or to speed up the transfer of files that you know to be safe. You can disable the Real-Time Scanner either by moving the switch to **OFF**, or from the Intego menu by selecting **VirusBarrier Server 3 > Real-Time Scanner**.

**When malware is found.** Your options are:

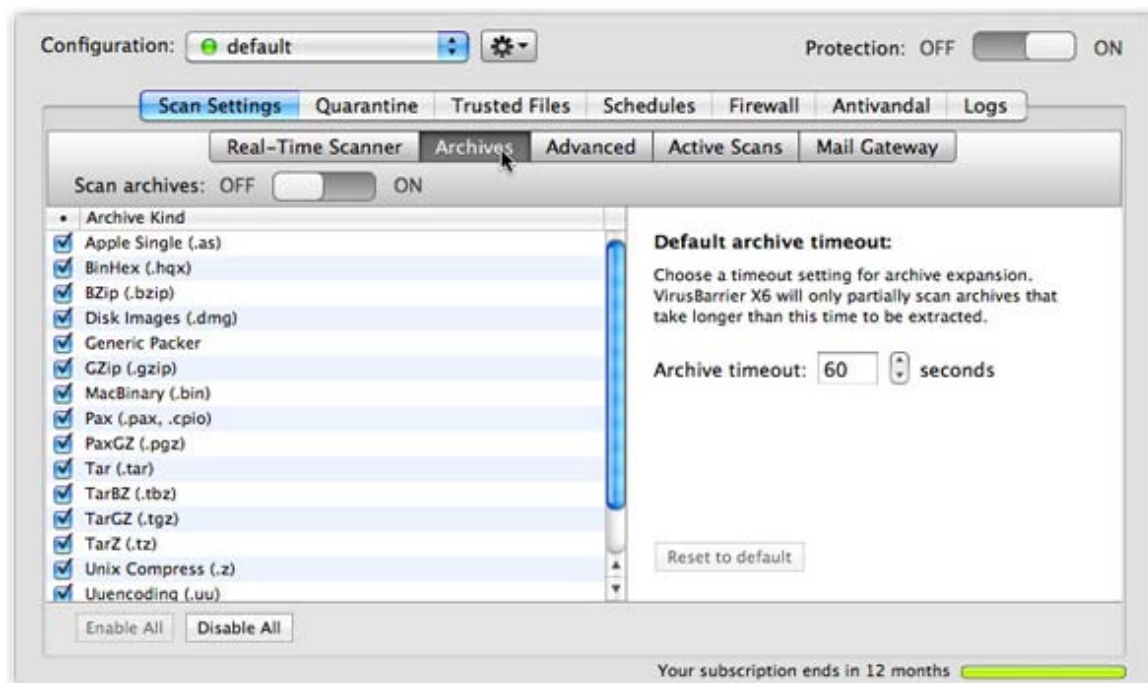
- **Put in Quarantine Zone:** this ensures that the file cannot be opened or read. See the Quarantine Zone section below for more about using the Quarantine Zone.
- **Repair:** this tells VirusBarrier Server 3 to attempt to remove the malware. If, for any reason, the file cannot be repaired, it will be placed in the Quarantine Zone.

In addition, you can choose to have VirusBarrier Server 3 send you an e-mail whenever it discovers a virus. To set this up, check the **Send an e-mail** checkbox, then click the **Configure e-mail...** button next to it. Enter the necessary information for your e-mail account in **Mail Settings** dialog that displays.

The last section of the Real-Time Scanner settings tab, **Remove quarantine marker after scanning uninfected files**, tells VirusBarrier Server 3 to remove the Mac OS X dialog warning that asks you whether you're sure you want to open downloaded files.

## Archive Settings

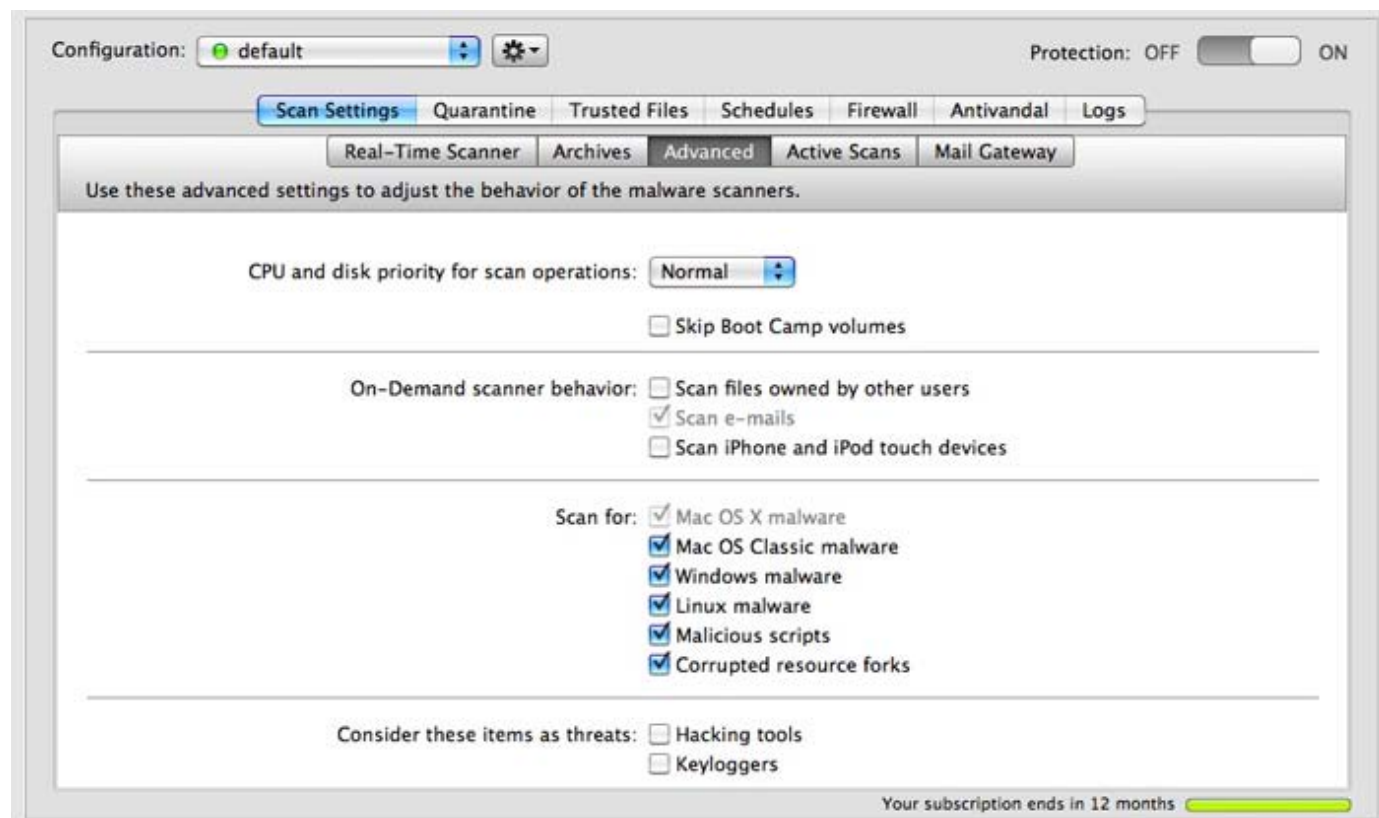
VirusBarrier Server 3 can look inside several popular types of archives, scanning not only the archive file itself, but also the files that it contains. To see these settings, click the **Archives** tab.



By default, VirusBarrier Server 3 will scan all archive types that it understands; however, you could choose to scan only certain archive types by unchecking different types of archives in the Archive Kind list.

The **Default archive timeout** setting lets you tell VirusBarrier Server 3 to stop scanning archives that take more than a certain amount of time to uncompress and scan. By default, this is set to 60 seconds. However, any files that have been uncompressed before the end of this timeout will be scanned.

## Advanced Scan Settings



This tab lets you be more specific about how VirusBarrier Server 3 examines your server for malware. The options are:

- **CPU and disk priority for scan operations.** You can choose **Low**, **Normal** or **High** from a popup menu. This setting tells VirusBarrier Server 3 to adjust its scanning so other applications don't get slowed down. This setting affects both the processor (CPU) for the scan and the reading of your hard disk(s). Note that this also applies to scans set to run automatically when you mount external disks or after you update VirusBarrier Server 3's filters. So if you want those scans to complete more quickly, you should choose **Normal** or **High**; if you don't care how long they take, or want your server to have more priority, choose **Low**.

The **Skip Boot Camp volumes** setting tells VirusBarrier Server to not scan Boot Camp volumes during scans.

Three options affect On-Demand scanner behavior:

- **Scan files owned by other users** allows VirusBarrier Server 3 to scan files owned by all users. If you select this option, and you're not already logged in as the server's administrator, you'll immediately be required to enter an administrator password; if you don't have that password, the checkbox will revert to its unchecked state. If you don't check this option and VirusBarrier Server 3 finds an infected file owned by a different user or by the system, VirusBarrier Server 3's alert and Quarantine Zone window will display a crossed-out pencil icon, signifying that you will need to enter an administrator's user name and password to perform any action on the file.
- **Scan e-mails.** VirusBarrier Server 3 scans incoming and outgoing e-mails, both for their content and any



attachments they contain, during manual scans. You can't turn off this function; the check box serves as a reminder that VirusBarrier Server 3 will examine e-mail messages.

- **Scan iPhone, iPod touch and iPad** tells VirusBarrier Server 3 to show any iPhone, iPod touch or iPad that is connected to your server. To scan these devices, you must use the VirusBarrier X6 client program that is installed with the server software.

The **Scan for** section lets you choose to have VirusBarrier Server 3 scan certain types of files or applications:

- **Mac OS X malware:** this is dimmed, because it is always active. VirusBarrier Server 3 always scans for Mac OS X malware. This includes all types of malware that affects Mac OS X, such as Word and Excel macro viruses; the other categories are types of malware that cannot harm Mac OS X.
- **Mac OS Classic malware:** malware that only affects Classic Mac OS. If you or your users still use any Mac OS Classic applications you can check this; if not, leave it unchecked.
- **Windows malware:** checking this tells VirusBarrier Server 3 to look for viruses that affect Windows. Although these files can't damage your server, they could infect Windows computers on your network, and they could affect you if you use Windows on your Apple computer through a program such as Apple Boot Camp, VMware Fusion or Parallels Desktop. (VirusBarrier Server 3 does not, however, scan Windows virtual disks.)
- **Linux malware:** if this is checked, VirusBarrier Server 3 will scan for malware that affects the Linux operating system.
- **Malicious scripts:** checking this tells VirusBarrier Server 3 to scan for malicious scripts such as PHP, shell scripts, JavaScripts, Perl, etc.
- **Corrupted resource forks:** while this type of corrupted file is not necessarily malware, corrupted resource forks – parts of certain files – can cause Macs to crash in certain cases. Checking this can protect your Mac from crashes caused by this type of corrupted file.

A final section lets you tell VirusBarrier Server 3 to look for two other types of malware:

- **Hacker tools** are malicious programs that may not directly harm your Mac, but that may be used by hackers to attack other computers. It is especially useful to check this option if your server is publicly accessible.
- **Keyloggers** are programs that record all your keystrokes. While some such programs may be malicious, others may be installed intentionally to monitor computer users. If this is checked, users being monitored may be alerted to the existence of such software on their Mac.

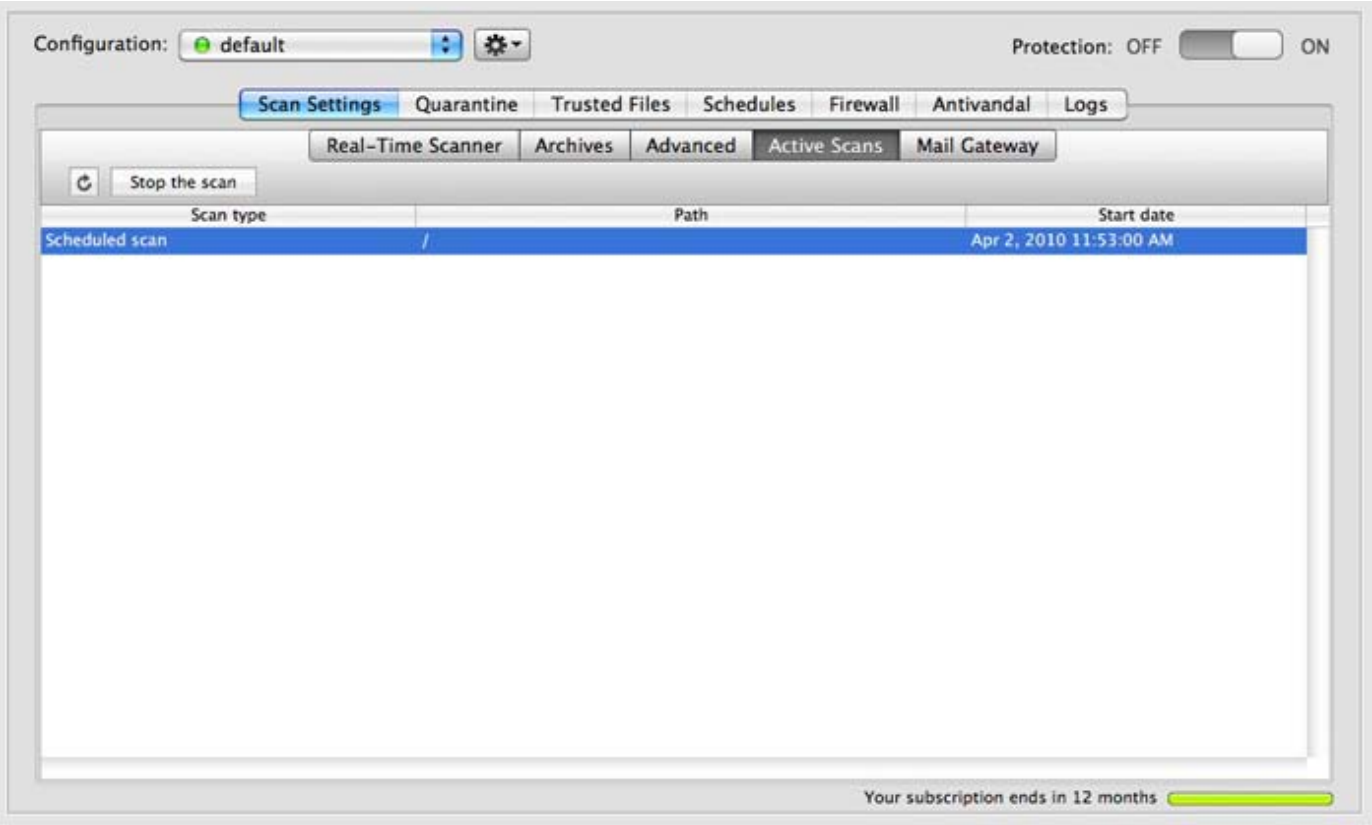
## Active Scan Settings

This tab will show any currently active scans, such as those [set in a schedule](#), launched following an event such as a mounted volume or a virus definition update (see above), manual scans run locally using VirusBarrier X6, or command line scans run locally or remotely.

If you don't see a scan that's running, click the  button to refresh the screen.

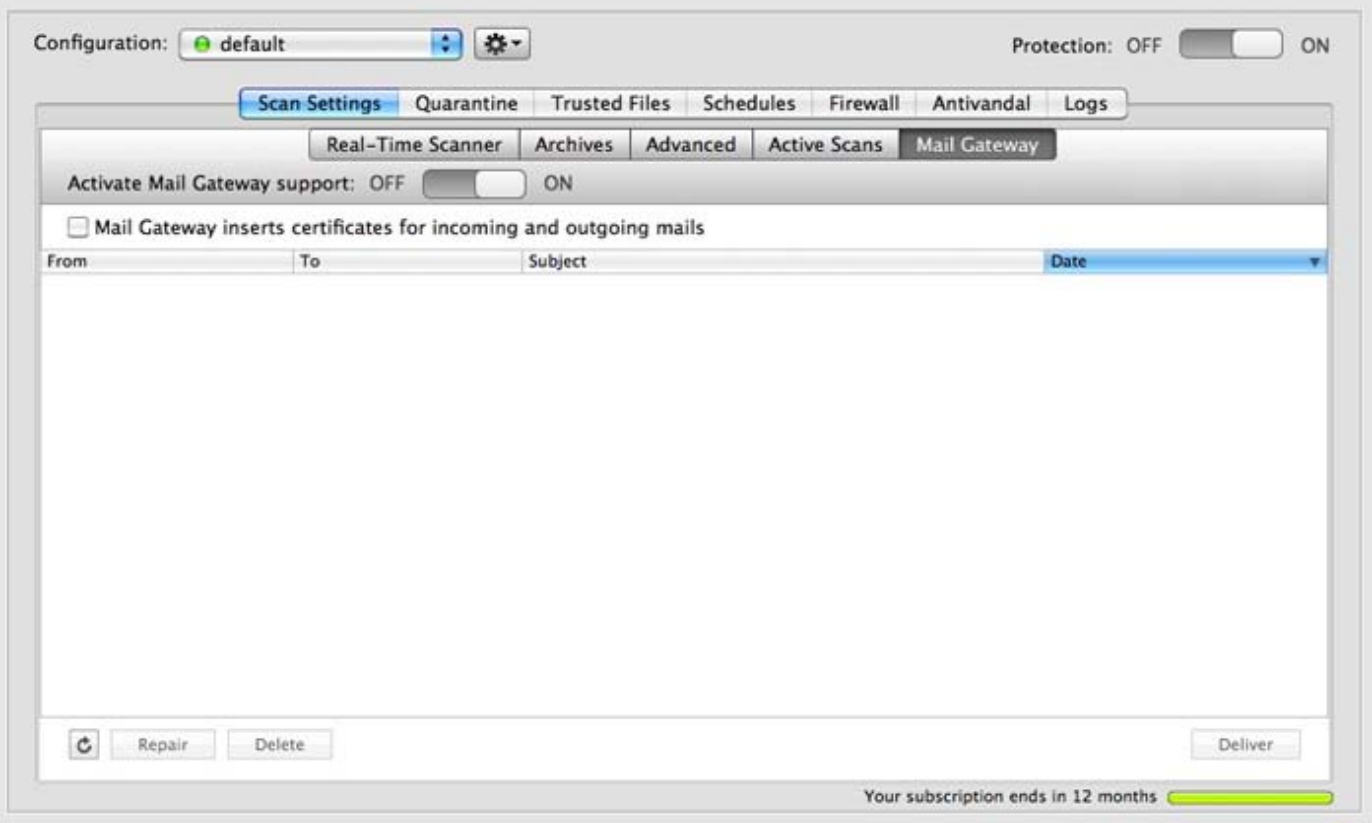
If you wish to stop any scan that is running, select it then click Stop the Scan. This cannot be done for manual scans.





Mail Gateway

The Mail Gateway tab allows you to control settings for virus scans of e-mail messages and attachments. To activate the Mail Gateway, move the **Activate Mail Gateway support** switch to **ON**. In addition to turning on mail protection, this deactivates the built-in antivirus solution.

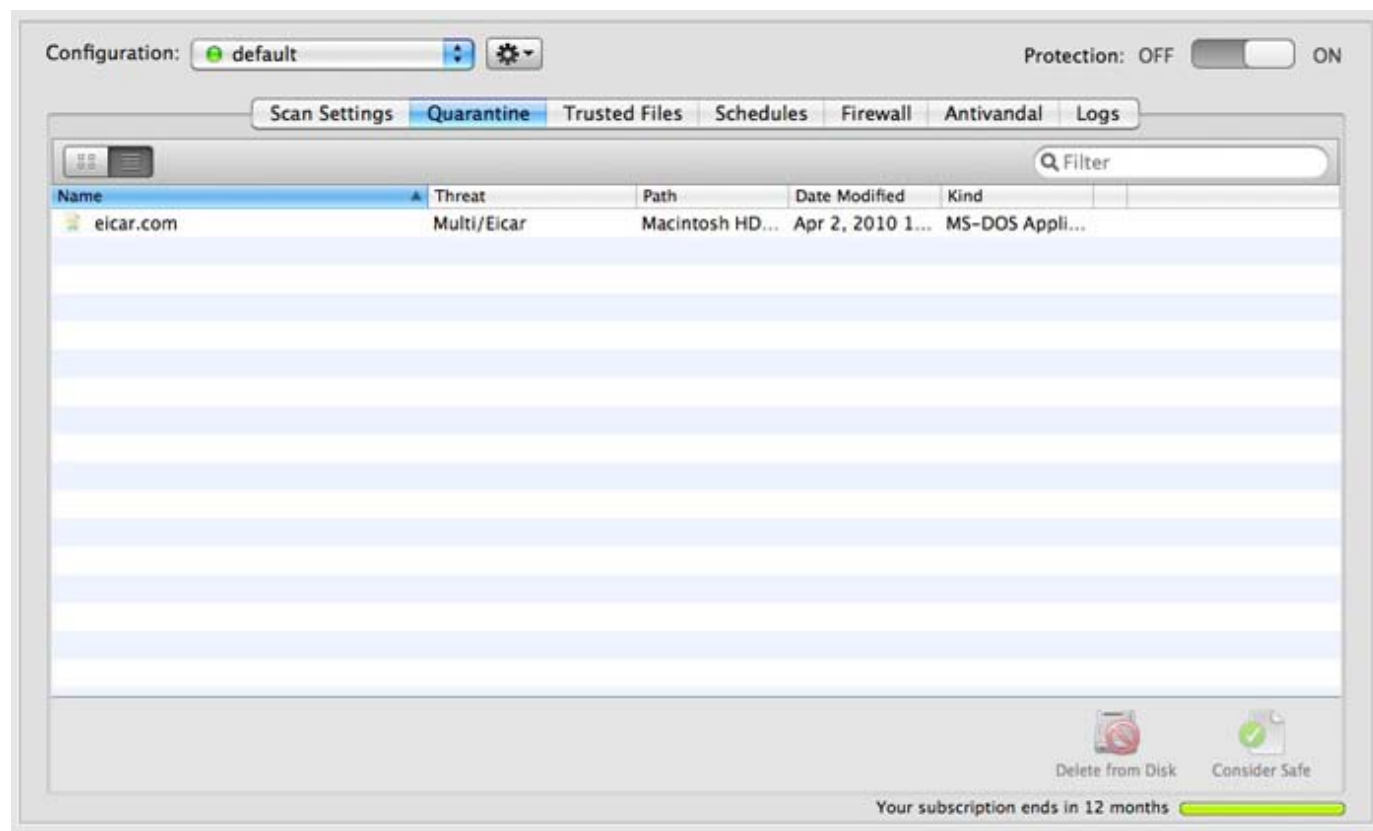


The **Mail Gateway inserts certificates for incoming and outgoing mails** control adds an X-SCANNED header to all messages that says they were scanned "by Intego VirusBarrier Server 3 Scanner at \$mydomain". If VirusBarrier Server 3 finds an infected attachment and removes it, the e-mail message containing that attachment will display the text, "Attachment removed by Intego VirusBarrier Server 3 [name of attachment]".

## Quarantine Zone

If you don't want to repair files automatically, you can have VirusBarrier Server 3 put them in its Quarantine Zone. When files are quarantined, they can't be opened or read, ensuring that they cannot infect your server. This is useful for administrators who want to check files before running VirusBarrier Server 3's repair functions.

As mentioned in the section about [Scan Settings](#), you can tell VirusBarrier Server 3 to place malware in the Quarantine Zone when found. You can then check these files and decide what to do.



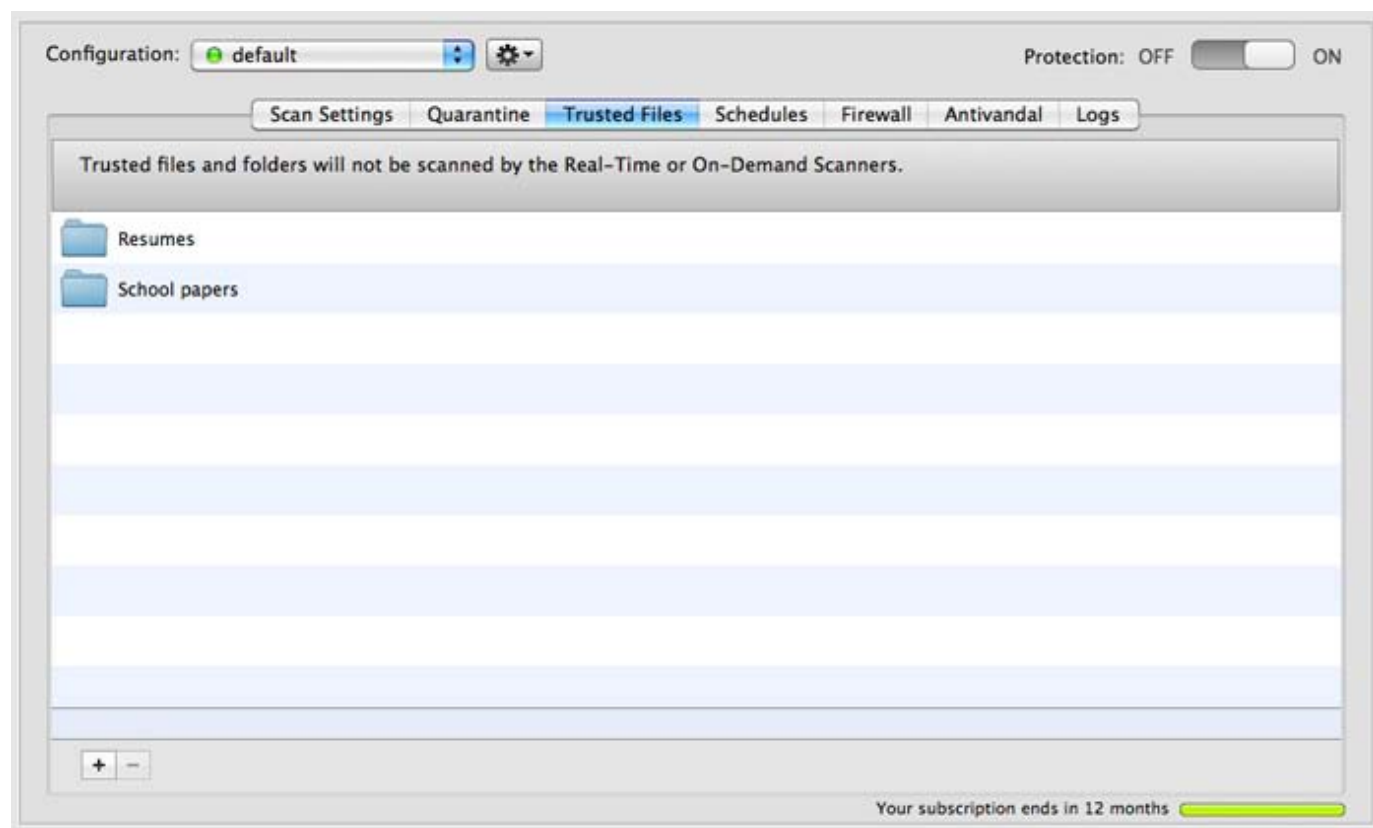
To act on any of the files, select one of them and then click the appropriate button at the bottom right of the window to:

- **Delete from Disk**, which removes the file from your server.
- **Consider Safe** which tells VirusBarrier Server 3 that you think this file is not infected, and adds the file to VirusBarrier Server 3's [Trusted Files](#) list. This may occur for false positives. However, be *very careful* when you click this button: only do so if you are sure the file is safe. If not, it may infect your entire server.

If you display the Quarantine Zone in list mode, a **Threat** column will tell you which types of malware your files are infected by.

## Trusted Files

VirusBarrier Server 3 offers the option to add files, folders or volumes to a list of **Trusted Files**. VirusBarrier Server 3 will assume that these files are all safe and will not scan them. You should only use this for files that have already been scanned by VirusBarrier Server 3.



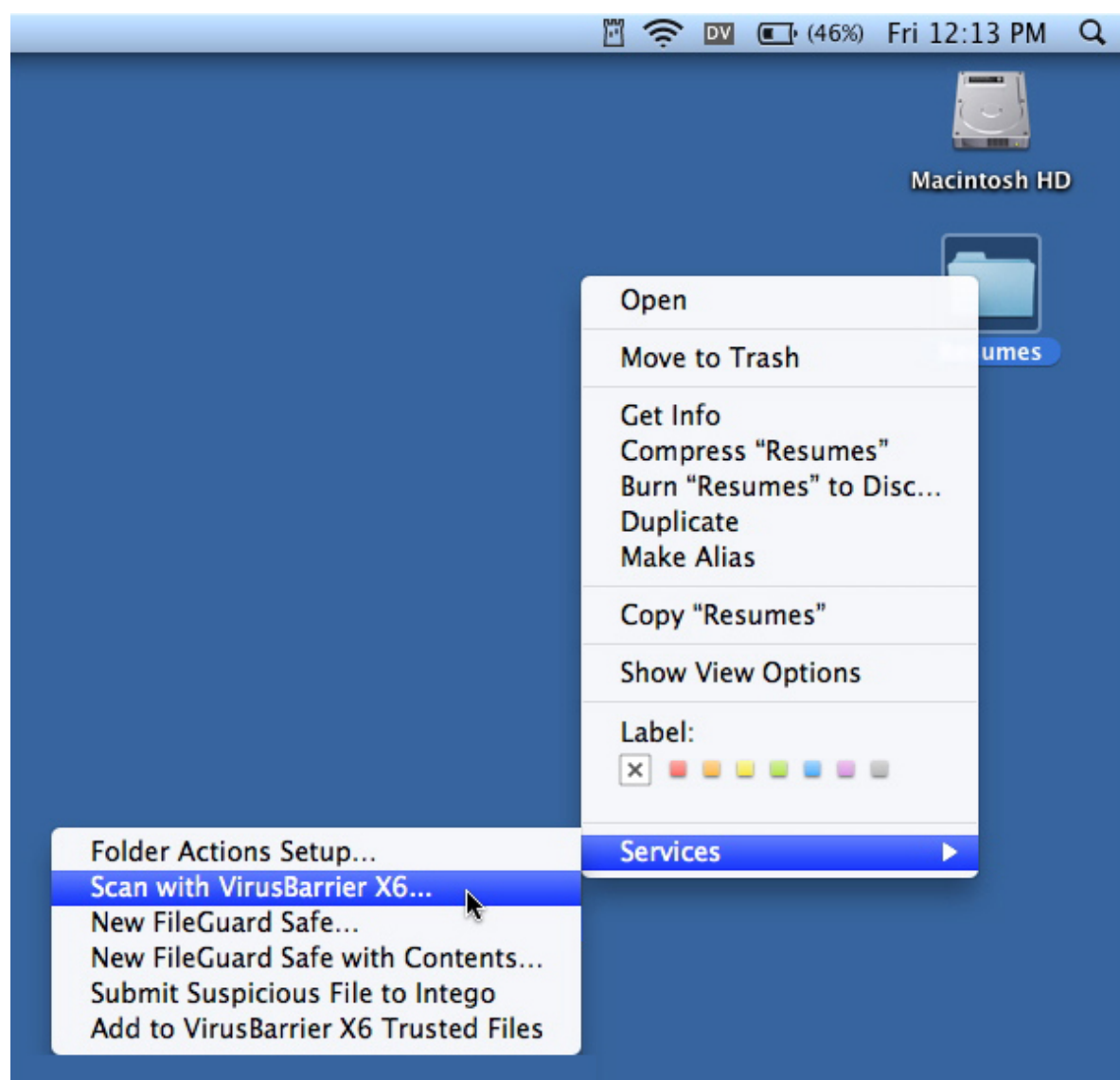
To add files to the Trusted Files list, click the small + button at the bottom-left corner of the screen, enter credentials to access the computer in question, navigate to the item you'd like to add, then click the **Choose** button.

Adding a folder or volume tells VirusBarrier Server 3 to trust *all* files contained in the selected item, including in any subfolders it contains now, or may contain in the future.

To remove an item from the Trusted Zone, click it to select it, then click the – button.

## The VirusBarrier Server 3 Contextual Menu

You have access to a number of VirusBarrier Server 3's protections directly from the Finder using a Contextual Menu, via the VirusBarrier X6 program that's installed along with VirusBarrier Server 3. Control-click or right-click on any item – a file, folder or volume – and a contextual menu will open. In Mac OS X 10.6 ("Snow Leopard") these menu items are grouped at the bottom of the contextual menu; however, if you have enough such items, you'll find a Services menu item, and VirusBarrier Server 3's menu items will be in the Services sub-menu. In Mac OS X 10.5 ("Leopard"), the VirusBarrier Server 3 menu appears under a "More" menu.



The contextual menu lets you do the following:

- Scan the selected item (and repair it if your settings allow).
- Send a copy of the item to Intego by selecting Submit Suspicious File to Intego. This is especially useful if you have files that you suspect are infected with new or unrecognized viruses. If you choose this option, Intego's virus experts can examine the file and produce the virus definitions you and other users will need to protect their systems, if necessary.
- Add the item to the Trusted Files list.

[« Using Intego VirusBarrier Server 3](#)

[Protecting Your Server from Network Attacks »](#)



## Protecting Your Server from Network Attacks

- [Firewall Protection](#)
- [Trojan Horse Protection](#)
- [Antivandal Protection](#)
- [Blocked Addresses and Trusted Addresses](#)

[Go to Main Table of Contents](#)

In addition to its powerful anti-malware features, VirusBarrier Server 3 protects your server from network attacks with tools that fall into two groups:

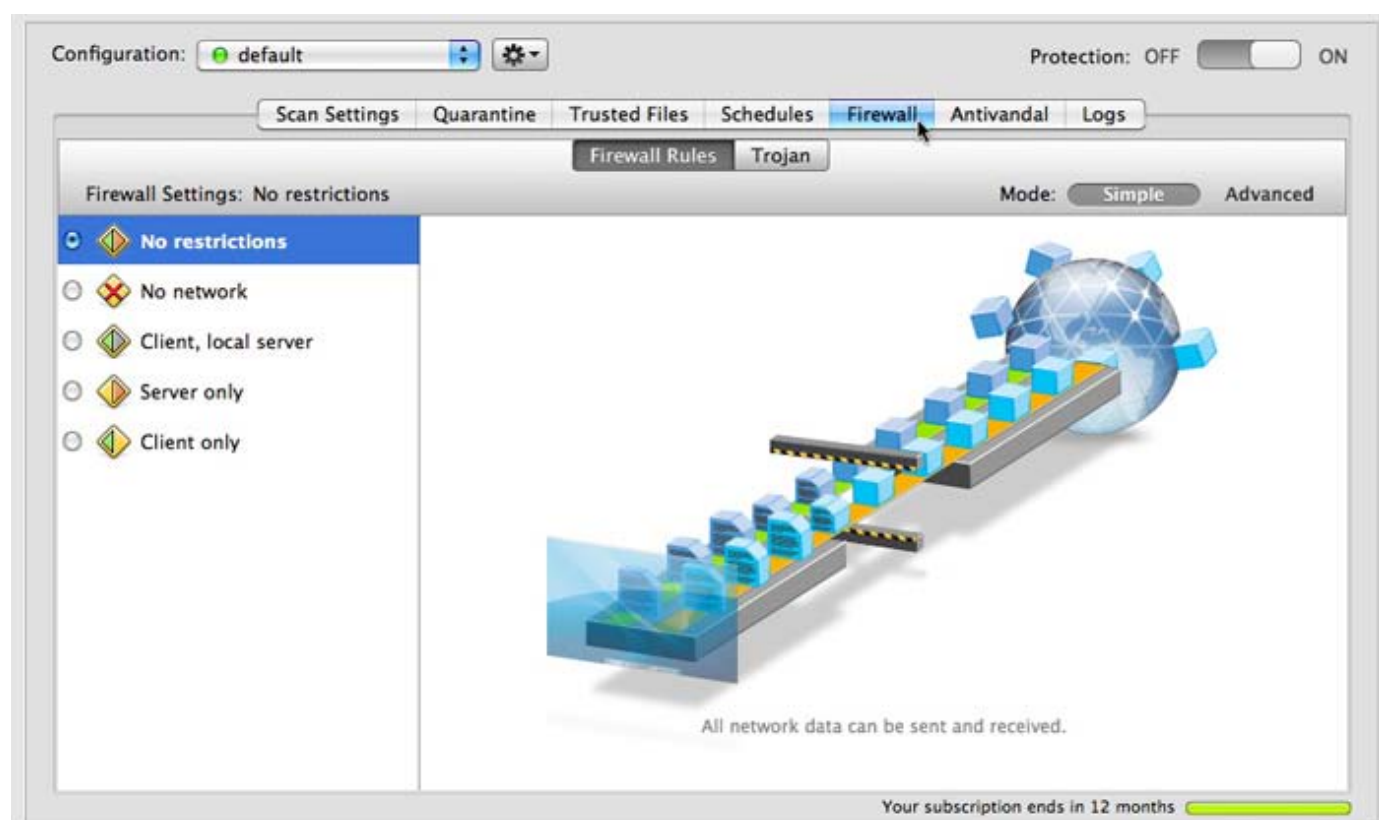
- **Firewall** tools, which define the network communications that your server will allow;
- **Antivandal** tools, which spot and block different types of network attacks.

These tools protect you against virtually every kind of attack possible, including Trojan horses, ping attacks, and port scans.

### Firewall Protection

VirusBarrier Server 3 includes a two-way firewall that filters all data packets entering or leaving your server through the Internet or a local TCP/IP network. It also protects you from Trojan horses by blocking the ports they use.

To view or change Firewall settings, click the **Firewall** tab.



When you click the **Firewall** button, VirusBarrier Server 3 presents its Simple mode for controlling Firewall settings. There are five preset firewall settings that cover all the situations that you will encounter in normal use, each accompanied by an animation that graphically shows the effect of applying the setting. The screen closest to you represents your server; the globe represents the Internet; the screen halfway between the two represents the limit of your local network. Here the default setting, **No restrictions**, shows how your computer can send and receive information without blockage in either direction.

The five firewall settings are:

- **No restrictions:** VirusBarrier Server 3's firewall allows all incoming and outgoing network data to be sent and received.
- **No network:** VirusBarrier Server 3's firewall prevents all data from entering or leaving your server to or from the Internet or a local TCP/IP network.
- **Client, local server:** VirusBarrier Server 3's firewall allows your server to function as a client and local network server. Your server can access the Internet as a client computer (but not as a server), and as both a client and server on a local network.
- **Server only:** VirusBarrier Server 3's firewall allows your server to function only as a server: all client functions, including your ability to surf the Internet from this computer, are blocked.
- **Client only:** VirusBarrier Server 3's firewall allows your server to function only as a client on a local network or the Internet. The server and file-sharing functions of your server are blocked.

These five settings are sufficient for most uses, but if you want more granular control over the firewall you need to switch to VirusBarrier Server 3's Advanced mode.

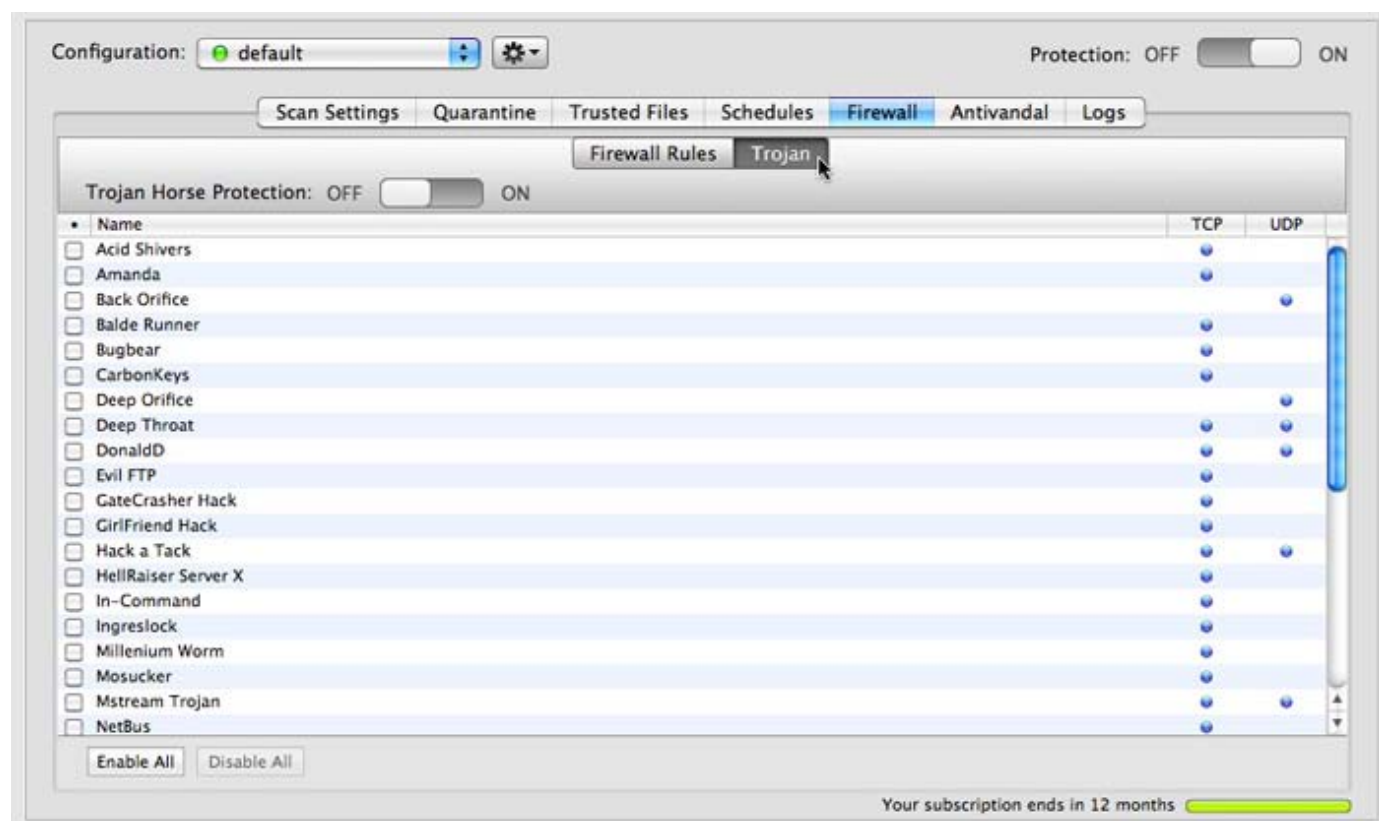
## Advanced Mode

VirusBarrier Server 3 also offers an advanced firewall mode you can use to create your own rules to choose exactly which types of traffic you want to allow or block to and from your server. For more on using Advanced Mode, see [Creating Custom Firewall Rules](#).

# Trojan Horse Protection

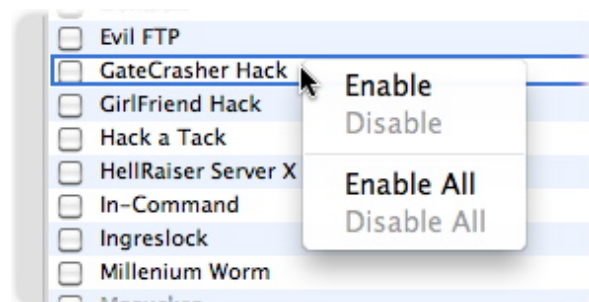
VirusBarrier Server 3 knows how to spot the actions of the most common Trojan horses and stop them in their tracks. Some such programs send information about users' browsing habits to a central server; other Trojan horses open "back doors" in your computer that allow hackers to take control of it or steal files. In addition, VirusBarrier Server 3 recognizes the actions of Windows Trojan horses, so if you are running Windows in virtualization – with a program such as VMware Fusion or Parallels Desktop – and sharing your server's Internet connection in NAT mode, you'll be protected.

To see VirusBarrier Server 3's Trojan Horse controls, click the **Trojan** tab at the top of the **Firewall** screen.



To turn on Trojan horse protection, set the **Trojan Horse Protection** slider to **ON**, then click the checkboxes of individual Trojans to select them. The **Enable All** and **Disable All** buttons at the bottom are handy shortcuts that select or deselect all checkboxes at once.

You can also enable Trojan blocking for an individual Trojan horse, or for all Trojan horses, by right-clicking on the name of a Trojan, and choosing the appropriate command from the contextual menu that displays.





# Antivandal Protection

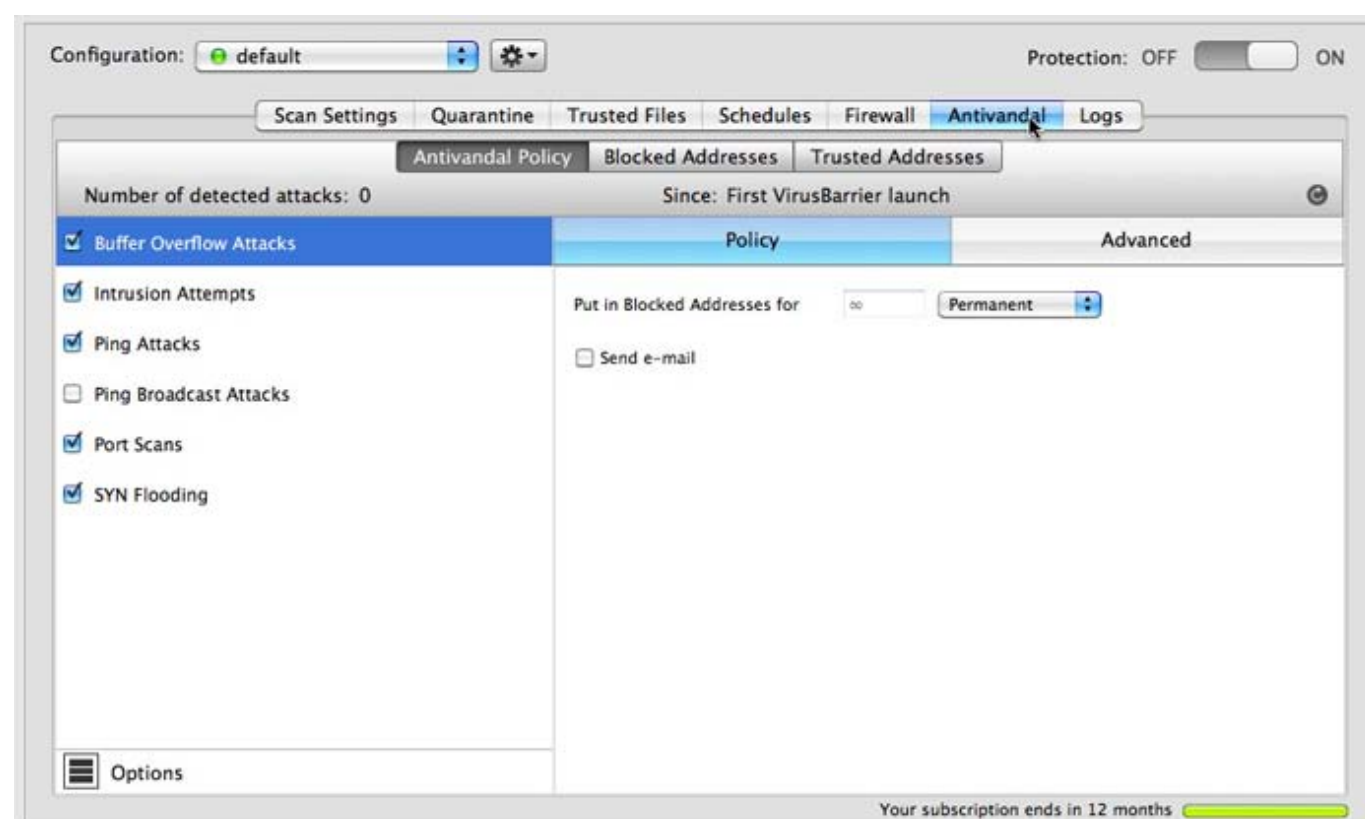
VirusBarrier Server 3's Antivandal watches over data entering your server and filters it, looking for signs of intrusion. This filtering is transparent: the only time you'll see signs of it working is if it detects suspicious data, in which case an alert displays. Otherwise, Antivandal silently monitors your server's network activity at all times.

To go to the Antivandal screen, click the **Antivandal** tab.

The **Antivandal Policy** tab controls how data entering your computer is filtered. The **Blocked Addresses** and **Trusted Addresses** tabs store specific hosts, or IP addresses, that you deem suspicious or trustworthy.

## Antivandal Policy

The Antivandal Policy panel provides tools to prevent six types of intrusions.



- **Buffer Overflow Attacks:** Attacks that may occur when certain software has flaws in the way it handles memory, allowing malicious users to get into your server.
- **Intrusion Attempts:** Attempts to access your server through a preset number of incorrect password requests within a given period of time. Different settings are available for AppleShare IP (ASIP), FTP, HTTP, IMAP, POP and SMTP.
- **Ping Attacks:** Your server receives a number or frequency of ping requests so great that responding would cause a strain on your server.
- **Ping Broadcast Attacks:** Ping requests to broadcast addresses, where a single ping is multiplied throughout your local network.
- **Port Scans:** Attempts by remote computers to search your server's ports for vulnerabilities. You may want to leave this unchecked if your computer is functioning as a server.
- **SYN Flooding:** Multiple TCP requests sent by an attacker who then doesn't complete the final stage of the exchange, causing the target computer to consume resources.



Clicking the checkbox next to each of these enables or disables protection for that intrusion type. By default, clicking on the name of any intrusion type shows the notification and action policies for all intrusion types in the mini-pane to the right. You can implement separate policies for each intrusion type by changing a setting in the Antivandal options: See the section "Unifying Policy Options" below for details.

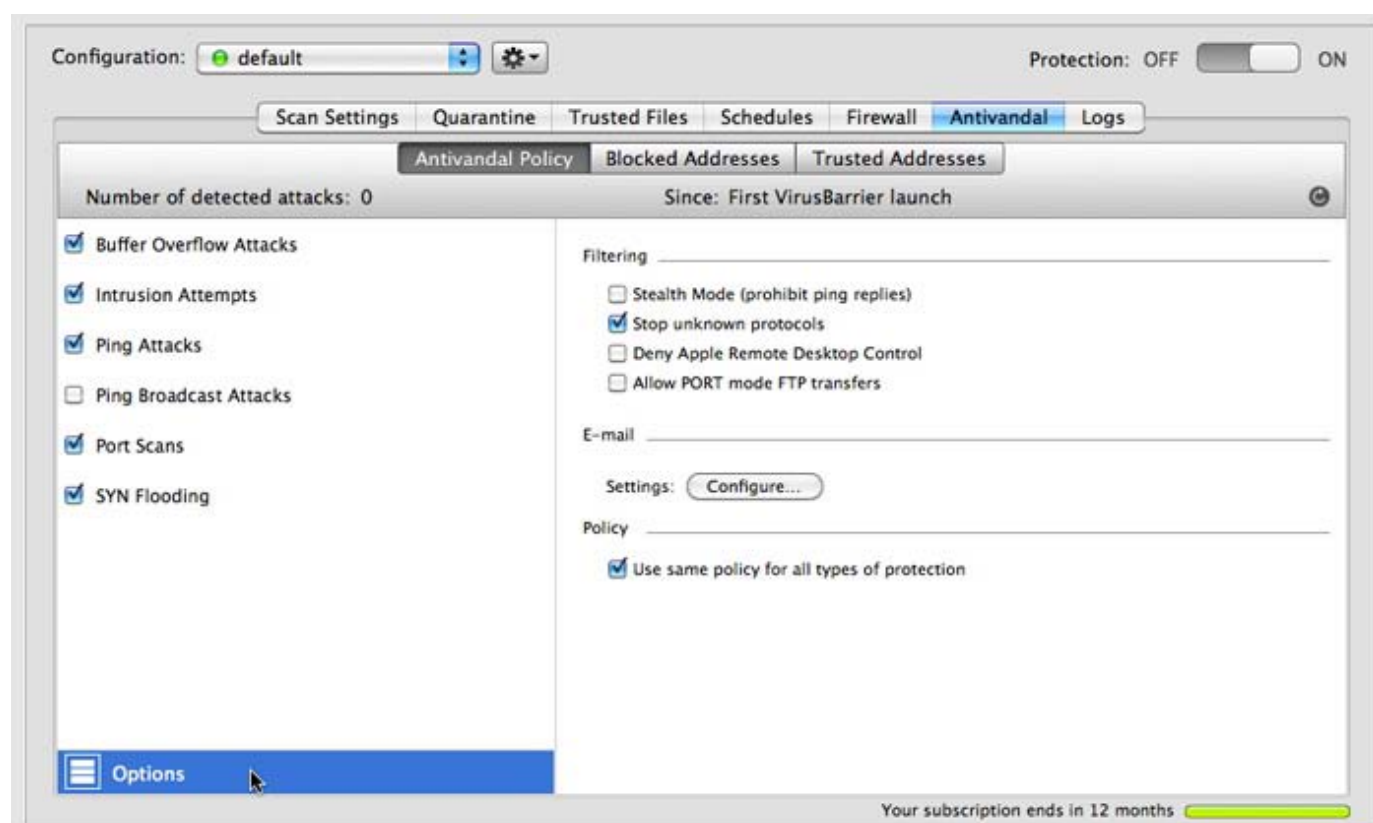
The two settings allow you to determine how long an address should be considered blocked, and whether you should be informed of the action via e-mail. If you've requested e-mail notification, you must configure your e-mail settings to receive any alert notifications by e-mail. In the **Policy** section, you do that by clicking **Options**, then clicking the **Configure...** button. Enter the necessary information for your e-mail account in **Mail Settings** dialog that displays. (Before it sends an e-mail message, VirusBarrier Server 3 waits for 30 seconds to see whether there are other intrusion attempts and bundles them all together into one message, rather than sending separate e-mail messages for each one.)

While an intrusion type is selected, clicking the **Advanced** tab in the right-side pane brings up additional options that are specific to that intrusion type. These are:

- **Buffer Overflow Attacks:** No advanced settings.
- **Intrusion Attempts:** You can separately set the number of incorrect password attempts permitted for AppleShare IP (ASIP), FTP, HTTP, IMAP, POP and SMTP.
- **Ping Attacks:** Ping flood sensitivity, measured in milliseconds (ms) permitted between ping attempts. If your computer is on a network, it is normal that your network administrator ping your computer from time to time. But if your computer is isolated, pings are rarer. One exception is if you have a DSL or cable connection; your ISP might ping your computer to check if it is on line.
- **Ping Broadcast Attacks:** No advanced settings.
- **Port Scans:** A slider lets you adjust the sensitivity from low to high in increments according to an internal calculation.
- **SYN Flooding:** Sensitivity, measured in number of attempted connections allowed per second.

## Options

Click the **Options** button in the bottom-left corner of the **Antivandal Policy** screen to adjust additional filtering settings. The options appear in the pane to the right.



- **Stealth mode (prohibit ping replies):** If this is checked, your computer will be invisible to other computers on the Internet or on a local network. You will not, however, be anonymous – any requests you send to other hosts will include your computer's IP address.
- **Stop unknown protocols:** If this is checked, VirusBarrier Server 3 automatically blocks any unknown protocols.
- **Deny Apple Remote Desktop Control:** If this is checked, VirusBarrier Server 3 blocks all access to your server by Apple Remote Desktop software.
- **Allow PORT mode FTP transfers:** If this is checked, you will be able to make FTP transfers when functioning in Client Only firewall mode.

The second part of this screen allows you to be notified by e-mail when an attack is detected; see the previous section for more information.

## Unifying Policy Options

Each type of intrusion has settings that determine what actions are taken when that type of intrusion is detected.

The **Use same policy for all types of protection** checkbox unifies all notifications and actions. With this box unchecked, you could, for example, choose to receive an e-mail when a buffer overflow attack is detected, but not when an intrusion attempt occurs. Checking the box tells VirusBarrier Server 3 that you want to get the same sort of response no matter what type of intrusion occurs.

When you activate this option, you'll see a dialog box that asks which settings should become the model that other intrusion types will follow.

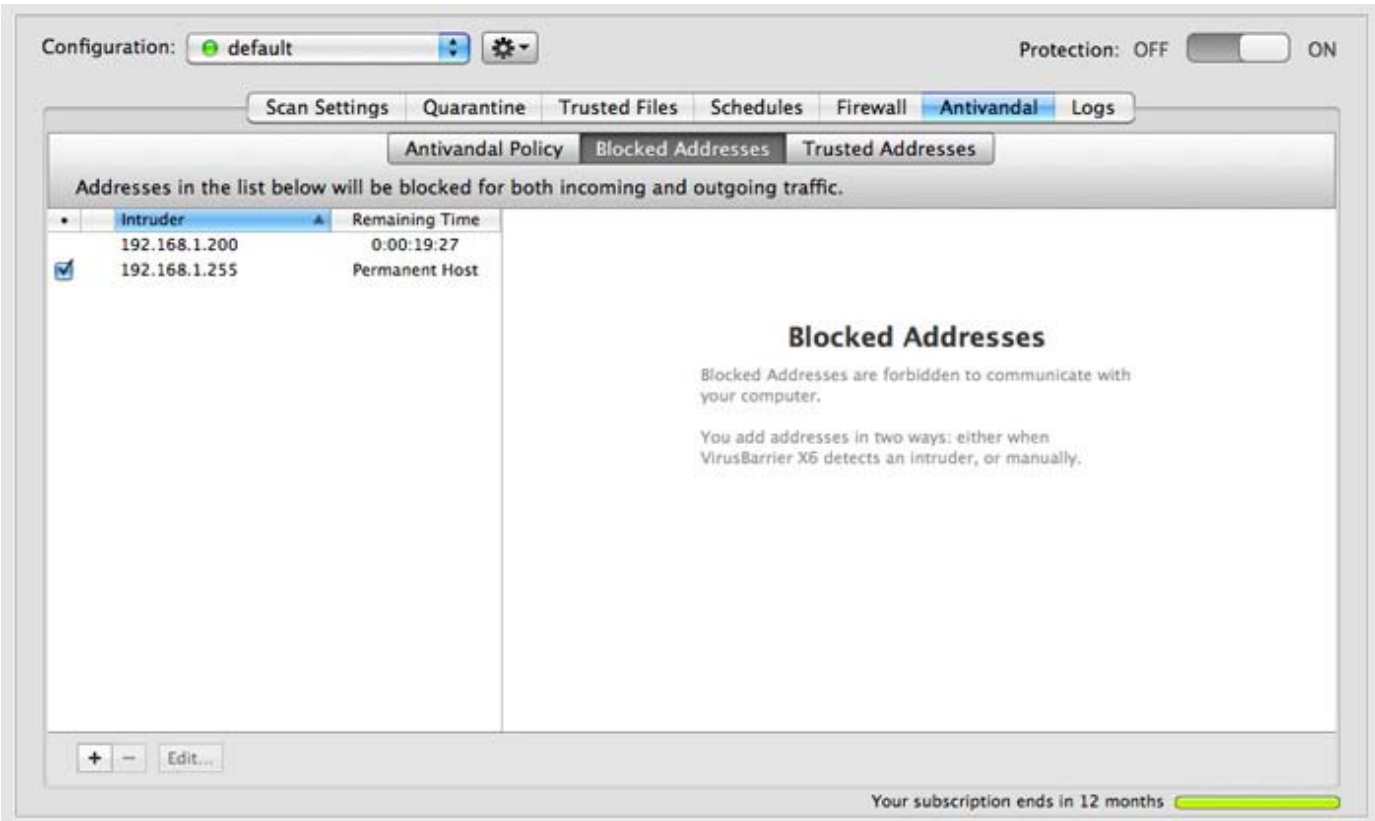


## Blocked Addresses and Trusted Addresses

The Blocked Addresses list ensures that once an attempted attack or intrusion has been foiled, communication between the attacking machine and your server won't occur for a period of time that you define.

The Trusted Addresses list is the opposite of the Blocked Addresses list: it lists "friendly" computers that *are* allowed to connect to your server. While the Blocked Addresses list protects you from foes, the Trusted Addresses list opens the door to your friends. VirusBarrier Server 3's Antivandal tool will not block access to computers listed in the Trusted Addresses list, nor will it set off alerts for any actions they carry out. However, computers in the Trusted Addresses list will still be affected by all active Firewall rules.

The interface for the Trusted Addresses window is essentially the same as for the Blocked Addresses window, so we'll examine them both at the same time, pointing out differences as necessary. Here's the Blocked Addresses window.

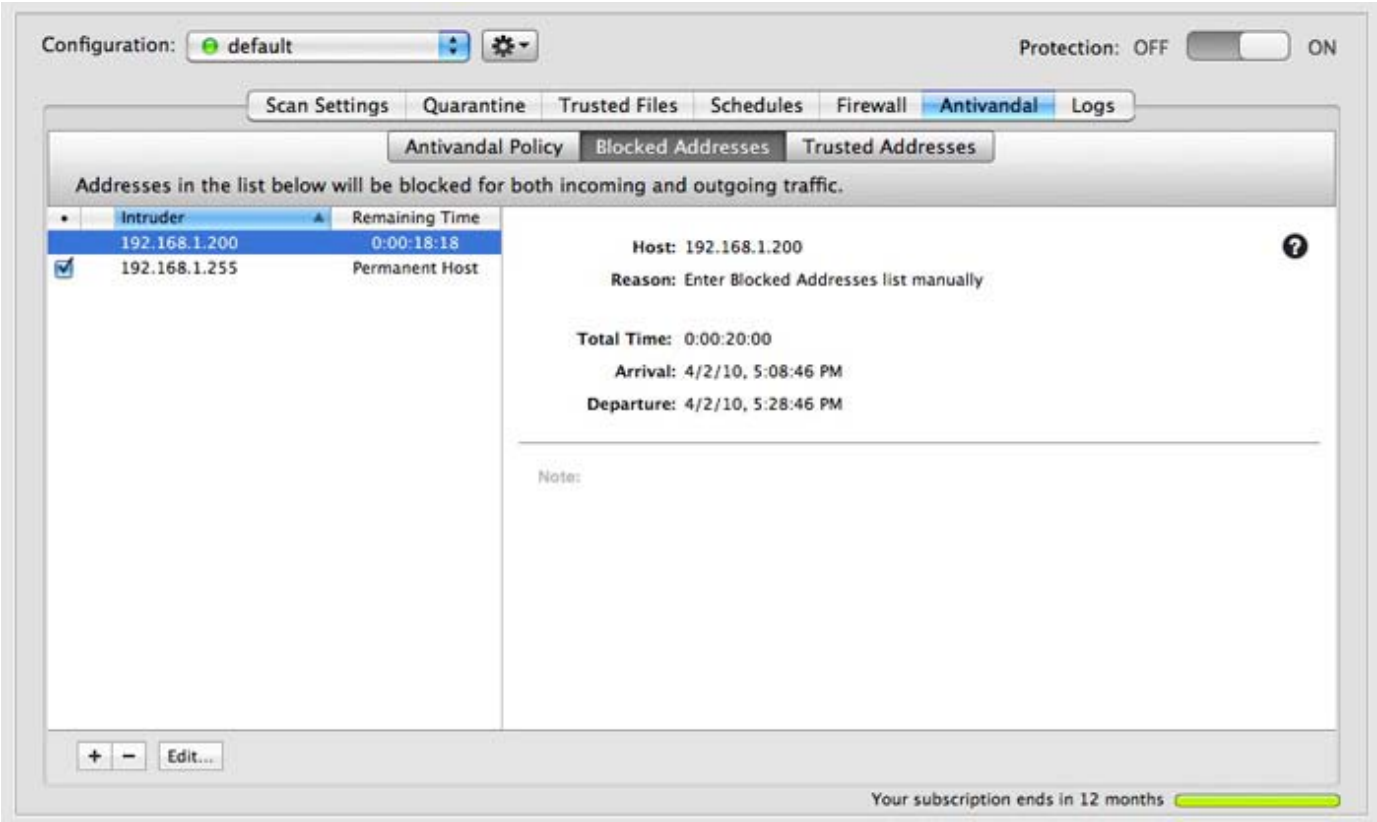


The panel on the left displays information about the various IP addresses that are currently in the Blocked Addresses list or Trusted Addresses list, if any.

- **Checkbox:** You can temporarily disable a Blocked/Trusted Address by unchecking this box, which is checked by default when you add a host to either list. When disabled, clicking it enables the item again. (This checkbox only appears if the IP address is set to be blocked permanently.)
- **Intruder/Host:** The second column shows the intruding IP address (in the Blocked Addresses list) or friendly IP address (in the Trusted Addresses list).
- **Remaining Time:** If you've set this IP address to be blocked or allowed for a specific period of time, this column shows how much time is remaining, updated every second. Otherwise, this column says **Permanent Host** to indicate that the IP address will be there until you remove it manually.

Blocked/Trusted Address Information

Clicking an item in the Blocked/Trusted Address lists shows some additional information on the right side of the panel. Double-clicking the item opens a new window with the same information.



- **Host:** The host's IP address. If you opened a new window by double-clicking the item, you can manually change the IP address listed. By clicking the DNS lookup button (the ?), you can toggle from the numerical IP address to the actual domain name of the offender, if there is one. You can display this address in large type by moving your cursor over the word **Host**, clicking, and selecting **Large Type** from the contextual menu that appears.
- **Reason:** Why the IP address was added to the Blocked Addresses list. This text doesn't appear in the Trusted Addresses list, as all items there are added manually.
- **Total Time:** The amount of time the host is to remain in the Blocked/Trusted Address list. Clicking the words **Total Time** changes the display to show **Remaining Time**; clicking again shows **Elapsed Time**, indicating how long the offender has been in the Blocked Addresses list. Clicking **Elapsed Time** will display the **Total Time** once again.
- **Arrival:** When the address was added to the Blocked/Trusted Addresses list.

**Departure:** If you specified an amount of time for an IP address to remain in the Blocked/Trusted Addresses list, the time it will be released is given here.

- **Note:** Any comments you have entered for this IP address. VirusBarrier Server 3 will also automatically add comments to this field when it puts an item in the Blocked Addresses list.

## A Note About DNS Lookups

In various places throughout VirusBarrier Server 3's interface you'll see a question mark in a dark circle. Clicking it toggles nearby information from a numerical IP address to its associated domain name and back again.



Be aware that IP addresses do not always have a one-to-one relationship to domain names. For example, a large domain might have `www.example.com` hosted on one IP address, `forums.example.com` hosted on another, and `blog.example.com` hosted on another.

Meanwhile, small domains often share one IP address with others, all hosted as "virtual domains" on a single computer. In such cases a domain lookup gives an IP address that actually leads to the larger, unexpected machine name, for example `apache2-vat.market.example.com`.

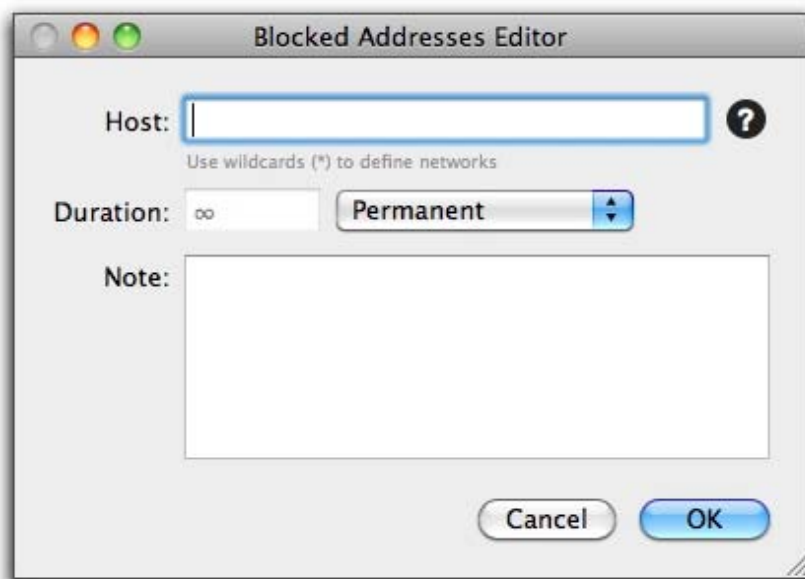
As a result, entering an IP address could block (or allow) traffic from unintended domains, while entering a domain might not block (or allow) all desired traffic. This is the nature of the Internet domain structure, and isn't an error of VirusBarrier Server 3. If you have problems with unexpectedly blocked or permitted traffic, try using a domain name instead of an IP address, or vice-versa.

## Adding Addresses

There are two ways to manually add addresses to the Blocked Addresses list or Trusted Addresses list. (VirusBarrier Server 3 can also add addresses automatically to the Blocked Addresses list in response to attacks, as defined by Antivandal policy.)

The first way to add an address to the Blocked Addresses list or Trusted Addresses list is by selecting an IP address in the Log window and choosing **Add to Blocked Addresses** or **Add to Trusted Addresses** from the contextual menu. For more on this, see [Using VirusBarrier Server 3 Monitoring Tools](#).

You can also manually add addresses to the Blocked/Trusted Addresses list by clicking the + button at the bottom of the list. A window appears.



Enter an IP address in the **Host** field, and select the time this address is to remain in the Blocked Addresses list or Trusted Addresses list by entering a number in the **Duration** field. Then, select a time unit from the popup menu. If you do not know the numerical IP address of the host you wish to add, enter its name and click the **?** button. VirusBarrier Server 3 queries your DNS server and enters the correct number in the field. You can also add comments, such as the reason for adding the address, in the **Note** field. If you decide you do not wish to add this address to the Blocked Addresses list or Trusted Addresses list, click **Cancel**.

## Using Wildcards

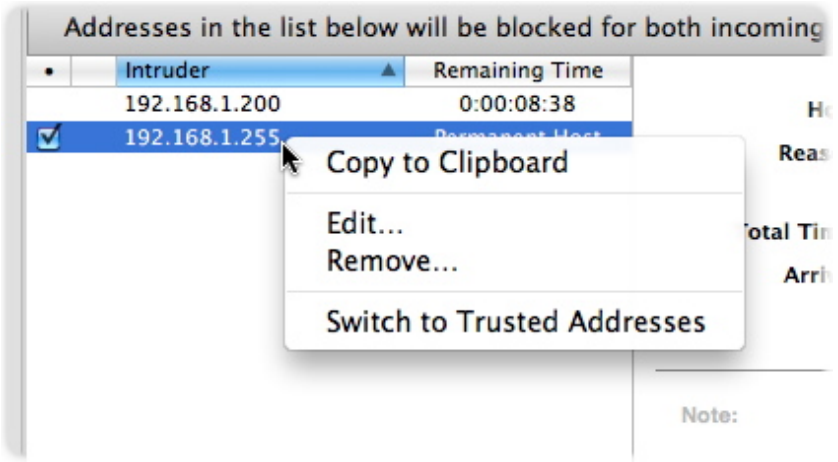
You can use wildcards to indicate ranges of IP addresses in the Blocked Addresses list or Trusted Addresses list. To do so, enter the first part of the IP address you wish to block, followed by asterisks. For example, 192.168.1.\* will block all IP addresses from 192.168.1.0 to 192.168.1.255 inclusive; 192.168.\*.\* will block IP addresses from 192.168.[0–255].[0–255]; and so on.



## Removing and Moving Addresses

To remove an address from the Blocked Addresses or Trusted Addresses list, click the address you want to remove, then click the – button.

Another way to remove an address is by right-clicking it then selecting **Remove...** from the resulting contextual menu. From this contextual menu, you can also move an address from the Blocked Addresses list to the Trusted Addresses list, or vice-versa.



Editing an Address

There are three ways to edit an address in the Blocked Addresses or Trusted Addresses list:

- Click the address you would like to edit, then click the **Edit...** button at the bottom left side of the pane,
- Double-click the address, or
- Right-click the address, then select **Edit...** from the contextual menu.

The Blocked/Trusted Addresses Editor window appears. You can change the address, add or change comments, or change the amount of time you want the item to remain on the Blocked/Trusted Addresses list.



## Using Intego VirusBarrier Server 3 Logs and Monitoring Tools

- [The Malware Log](#)
- [The Network Log](#)
- [VirusBarrier Traffic Monitor](#)

[Go to Main Table of Contents](#)

VirusBarrier Server 3 contains logs and monitoring tools to help you see which actions the program has carried out on malware, to record network activity and intrusion attempts, and to give you an overview of your server's activity in real time.

The Logs window displays two buttons at the top-left: Malware and Network. View either of these two logs by clicking the appropriate button.

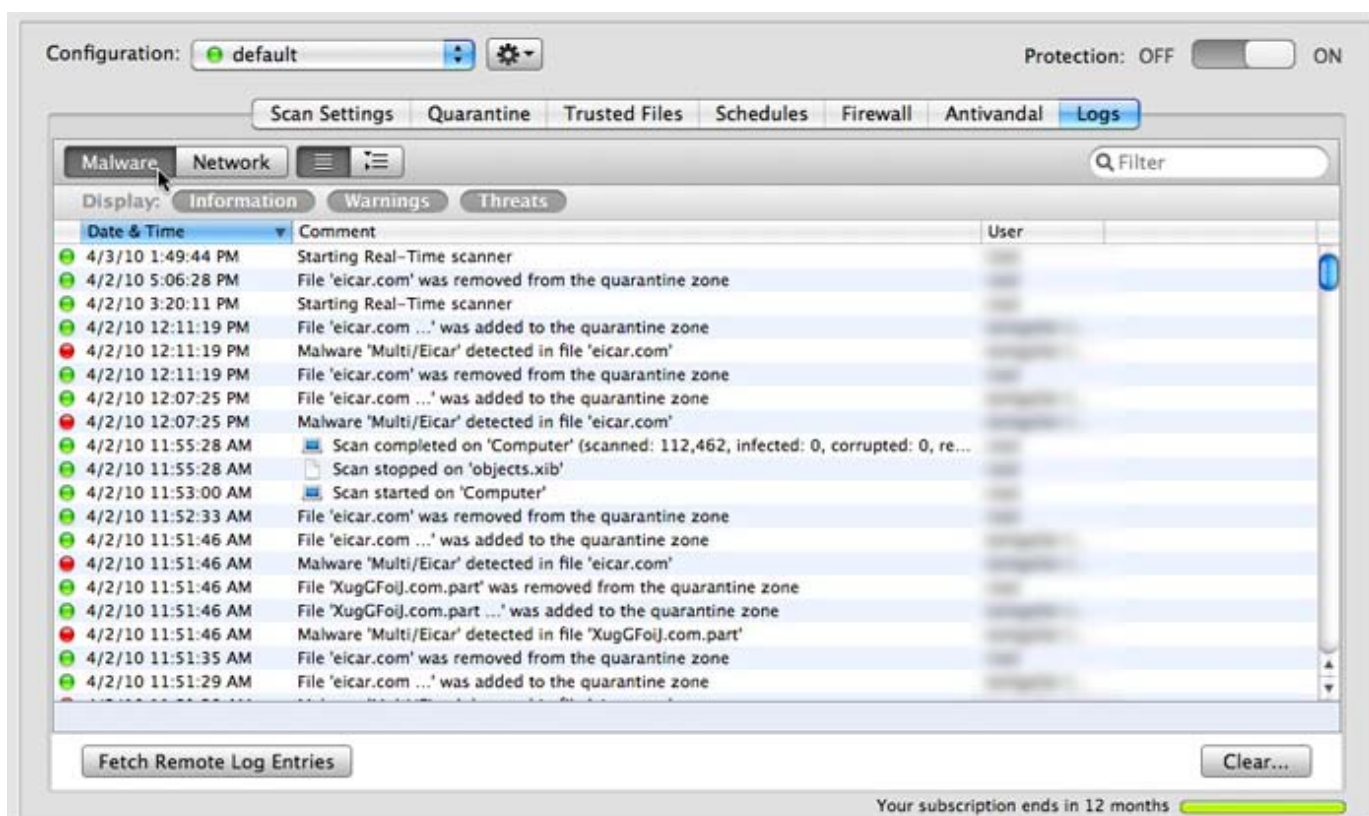


### The Malware Log

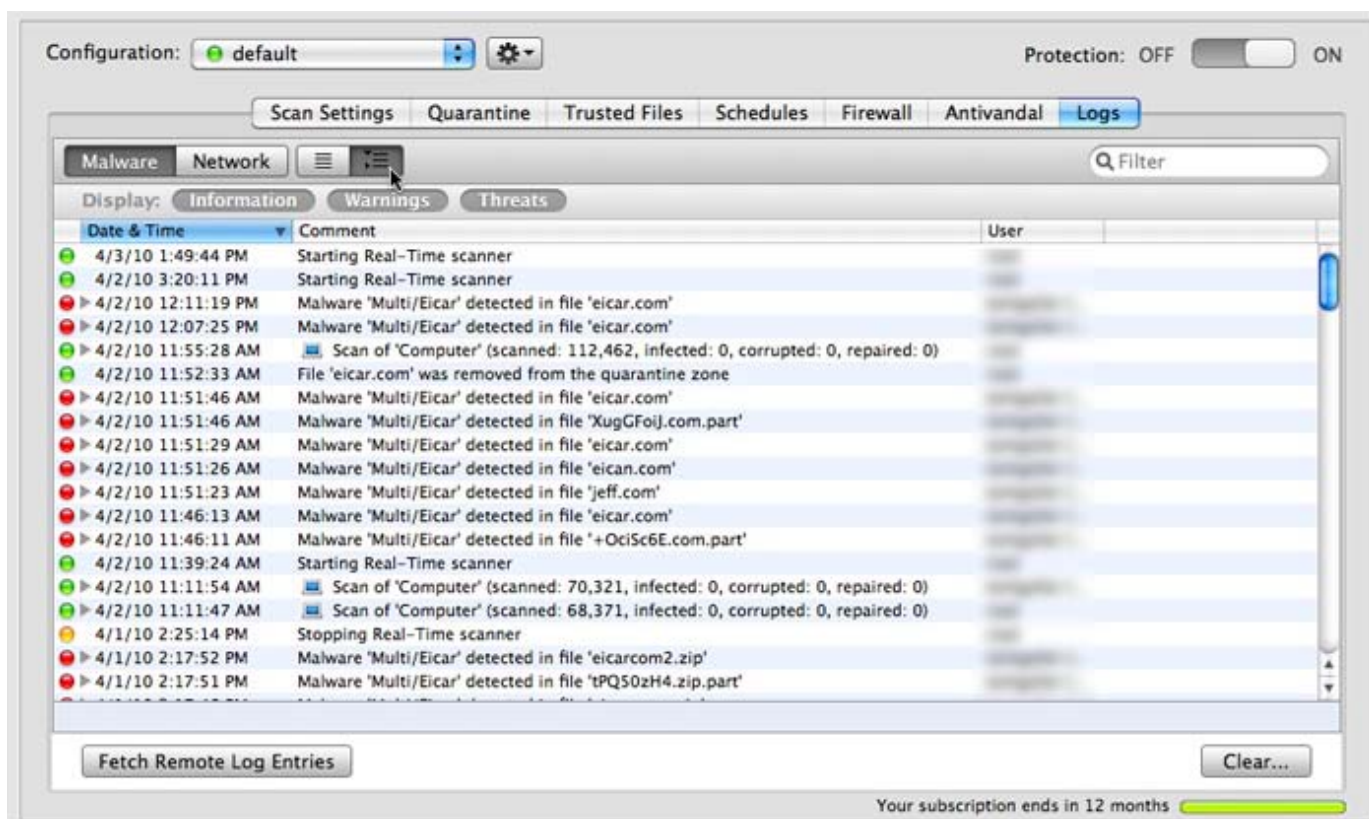
The malware log shows a record of malware activity that VirusBarrier Server 3 has observed, including all manual and scheduled scans and the results of these scans. As with the network log, you can filter it to highlight issues of interest.

To access the malware log, click the **Malware** button.

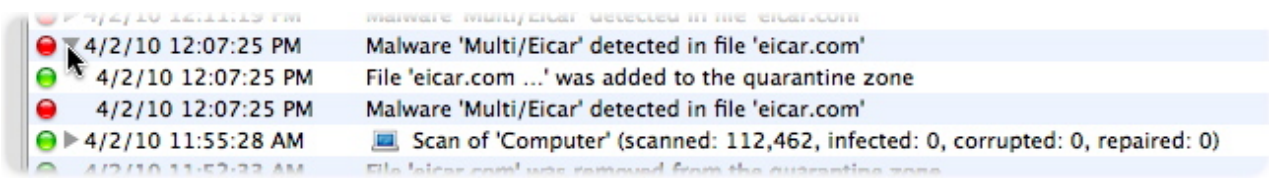




There are two ways you can display log information. In the example above, log entries are shown in linear order, each one taking up one line. You can click the second button at the top-left of the window and display log entries in hierarchical order, where disclosure triangles group related entries.



Clicking a disclosure triangle reveals related entries.

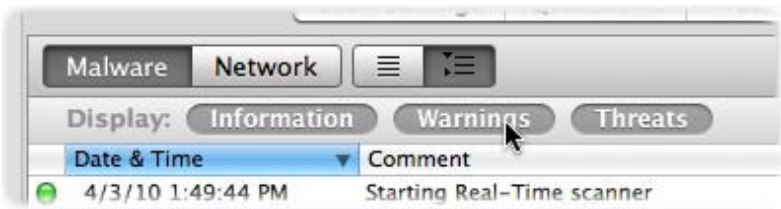


The Log shows every time that:

- You start a scan
- You cancel a scan in mid-process
- You start or stop the real-time scanner
- VirusBarrier Server 3 finishes a scan, with its results
- VirusBarrier Server 3 discovers a virus
- VirusBarrier Server 3 discovers a corrupted file
- VirusBarrier Server 3 repairs an infected file
- Files are added to or removed from the Quarantine Zone
- Files are added to or removed from the Trusted Files list
- Virus definitions are updated

The colored dots in the leftmost column show you what types of entries are displayed in the log. Green dots indicate *information*, such as starting the real-time scanner or updating virus definitions. Orange dots are for *warnings*, such as stopping the real-time scanner. Red dots indicate *threats*, such as when infected or corrupted files are found. The files, folders or volumes selected for each scan are named, as are all problems found.

You can choose to only display certain types of information by clicking one of the three log type buttons to hide or display their entries.



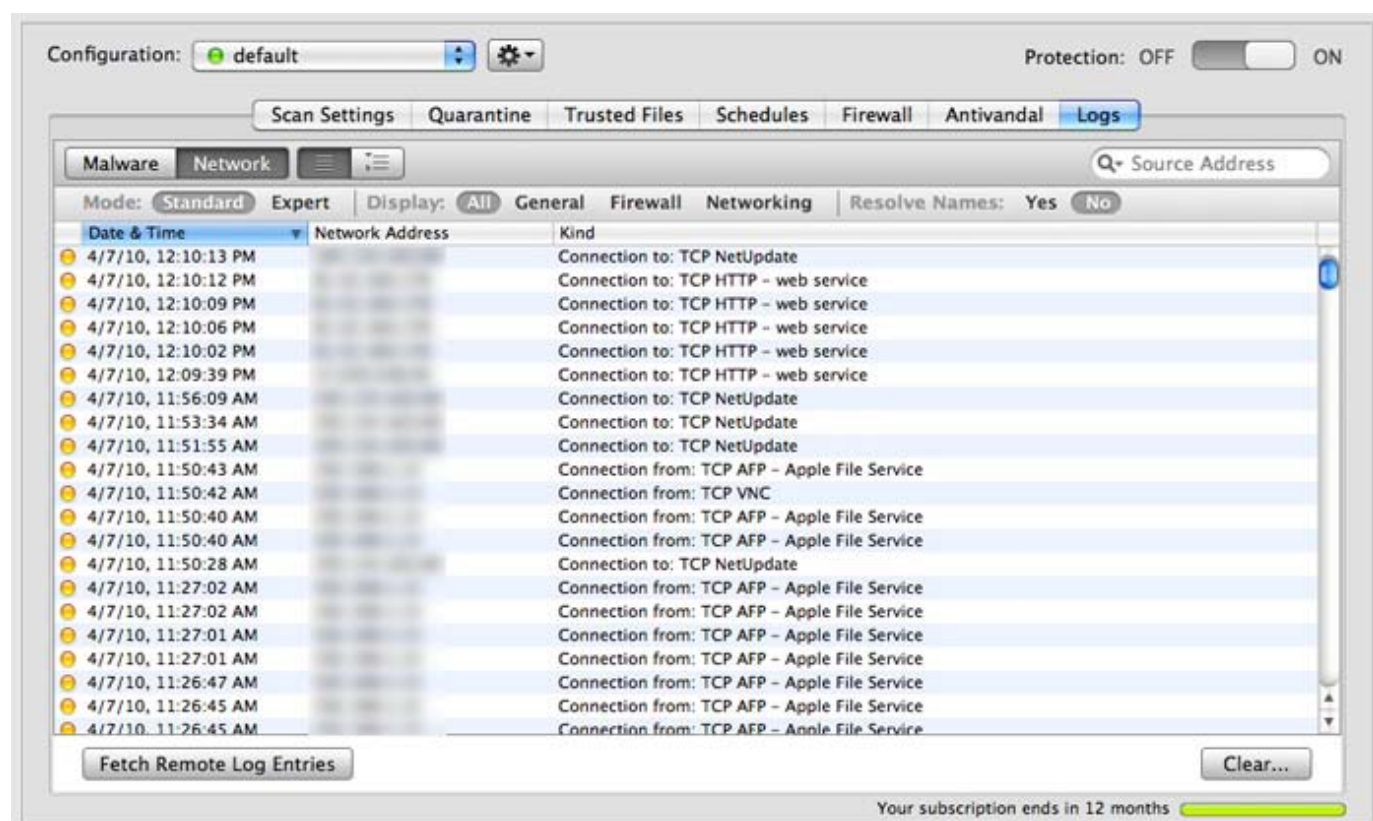
You can filter search results by entering text in the search field in the window's toolbar. As you type text, the results will narrow down, showing only those log entries that contain the text you have typed.



## The Network Log

The network log shows a record of all network activity that VirusBarrier Server 3 has observed, as well as all intrusion attempts that VirusBarrier Server 3 has blocked. You can apply filters to it on several criteria to highlight issues of interest.

Click the **Network** button to display the network log window, then click **Fetch Remote Log Entries** to tell VirusBarrier Server Admin to retrieve log entries for the currently selected server.



The top of the log window contains three groups of options that affect how the log appears.

- The **Mode** group toggles between the default Standard view and an extended Expert view;
- The **Display** group shows subsets of log activity to help you see potential issues more clearly;
- The **Resolve Names** group lets you choose whether to view raw IP addresses or domain names using DNS lookup.

We'll examine each of these sets of options separately.

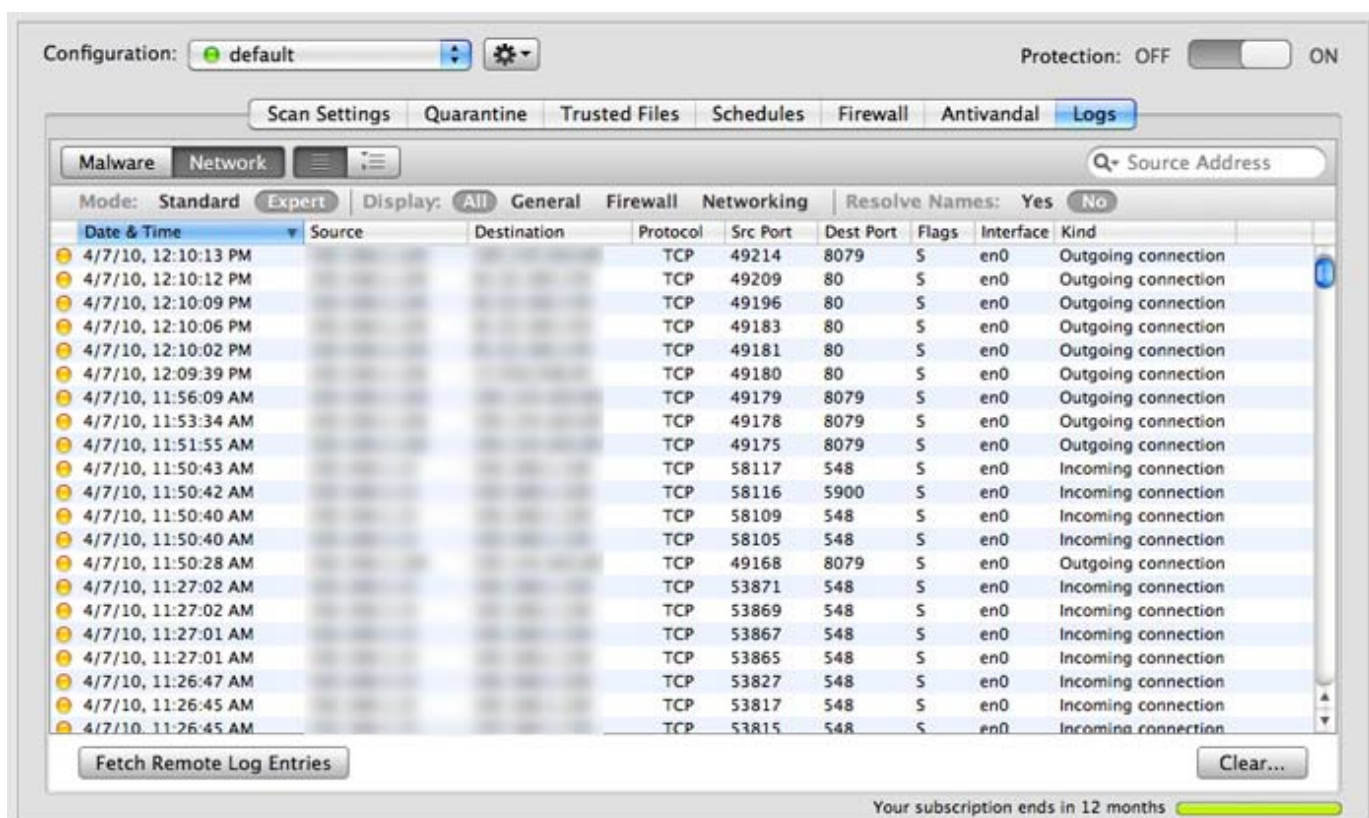
## Network Log Modes

**Standard** mode (shown above) is the default for the Log screen. This displays only four pieces of information for each Log entry:

- **Type of activity**, indicated by dot color:
  - Green: Informational entry.
  - Yellow: Notable event, such as an outgoing connection, incorrect login, blocked outgoing data, etc.
  - Red: Network attack, blocking of address in the Blocked Addresses list, Anti-Spyware blocking, etc.
- **Date & Time** of activity, according to your server's clock setting.
- **Network Address**, given by default as an IP address. If you've checked **Resolve Names** (see below), you'll see the domain names for those addresses that VirusBarrier Server 3 was able to resolve.
- **Kind**, a short description of the activity.

**Expert** mode gives an extended view, showing the following additional fields where applicable.





- **Source**, which is the originating IP address (or domain) of the incident. For most activities, the source will be your server's IP address, although for attacks or other incoming connections it will be that of the remote computer. If you have checked Resolve Names, you will see the domain names for those addresses that VirusBarrier Server 3 was able to resolve.
- **Destination**, given by default as an IP address.
- **Protocol**, which describes how the connection was attempted, i.e. TCP, UDP, ICMP or IGMP.
- **Source Port**, the port from which data was sent.
- **Destination Port**, the intended port for the data.
- **Flags**, or TCP flags, A (acknowledge), S (synchronize), F (end of data), or R (reset).
- **Interface**, the network interface used to send the data, such as Ethernet or AirPort, given by BSD Name.
- **Kind**, a short description of the activity.

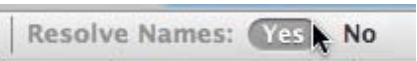
## Displaying Subsets of the Network Log

The **Display** section categorizes activities in three groups: General, Firewall and Networking. You can choose to see activities relating to all the groups at once, or only activities relating to a specific one. Click one of the buttons to change the log view.

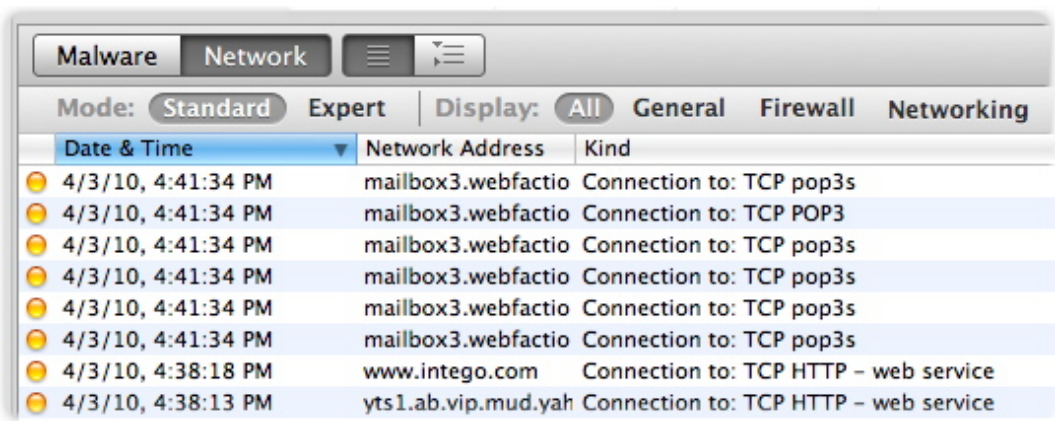


- **All**: All activity that VirusBarrier Server 3 tracks. This is the default setting.
- **General**: Activity related to the operation of VirusBarrier Server 3 itself, such as instances when you launched and quit the program, entered items into the Blocked Addresses or Trusted Addresses list, and so forth.
- **Firewall**: Incidents when network activity triggered a firewall rule, if logging was turned on for that rule. Records of any Trojan horse attacks also appear in the Log, if you've turned on Trojan protection.
- **Networking**: All connections to networks or the Internet, and when IP addresses in the Blocked Addresses list attempt to connect to your computer.

## Resolving Domain Names in the Network Log



The **Resolve Names** section of VirusBarrier Server 3 helps you track down intruders by resolving the domain names of your connections. When Resolve Names is checked in the Log panel, VirusBarrier Server 3 will attempt to find the names for each of the Internet addresses shown in the log. If VirusBarrier Server 3 can find this information, it then displays it in name form rather than as numbers.



VirusBarrier Server 3 is not able to resolve the names of all Internet addresses, since some addresses have no name equivalents.

## Filtering Data in the Network Log Window

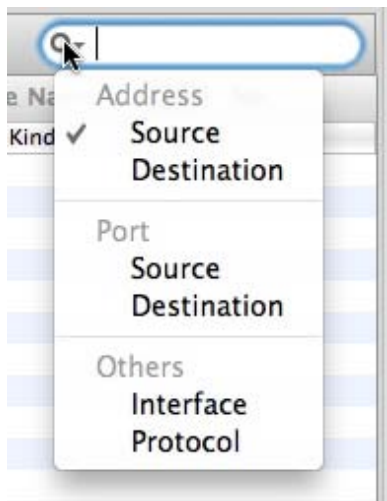
At the top of the log window toolbar is a search field that lets you filter data according to several criteria, displaying only those entries that contain the selected criteria in the following categories:

- Source address
- Destination address
- Source port
- Destination port
- Interface
- Protocol

Source Address is the default criterion, as the search field shows.



To search for log data containing any of these criteria, click the disclosure triangle next to the Search icon.



Select the criterion you want to search for, then enter a string in the search field. You don't need to enter the entire string; the display is dynamic, and automatically narrows down log data as you enter characters in the search field.

## Clearing Logs

To clear either the Malware or Network log, and erase all information it contains, click the **Clear...** button in the lower-right corner. A dialog appears, asking you to confirm your request.

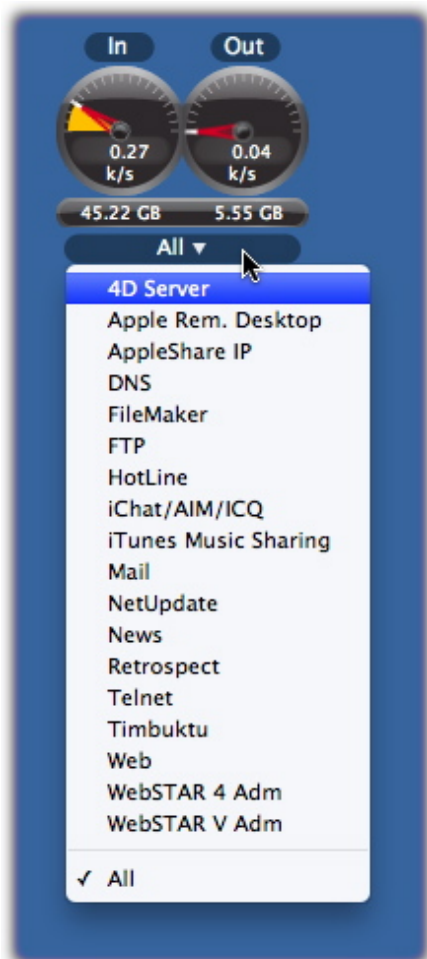
## VirusBarrier Traffic Monitor

The VirusBarrier Server 3 installer also places an application called VirusBarrier Traffic Monitor in your Applications folder. You can launch this program by double-clicking its icon, or from the Intego Menu by choosing **VirusBarrier Server 3 > Open VirusBarrier Traffic Monitor**.

The VirusBarrier Traffic Monitor application provides a small, floating window that lets you keep an eye on network activity at all times. You can move this window location by clicking it and dragging to a new place on your screen.



By default, VirusBarrier Traffic Monitor displays the total network traffic for all services. You can change what kind of traffic is displayed by clicking **All** at the bottom of the VirusBarrier Traffic Monitor window, and selecting a service from the popup menu.



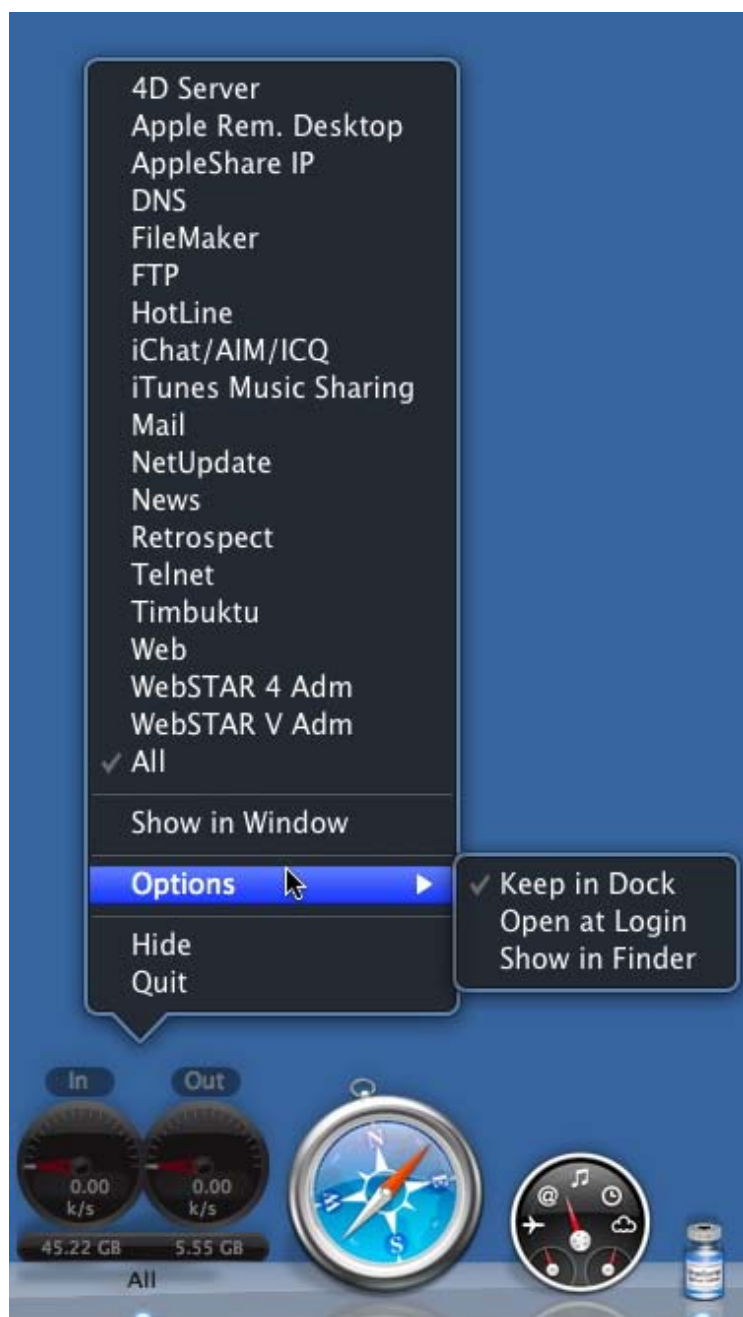
Right-clicking anywhere in the VirusBarrier Traffic Monitor window offers you the option to put the gauge in Mac OS X's Dock. While there, the activity gauges continue to show you network traffic in real time.



Network activity also appears in the VirusBarrier Traffic Monitor icon you see when you switch among applications by pressing Command-Tab.

To return VirusBarrier Traffic Monitor to its window, right-click on the VirusBarrier Traffic Monitor Dock icon, and choose **Show in Window**.

When VirusBarrier Traffic Monitor displays in the Dock, you can change its display by right-clicking on its Dock icon, and selecting a different service from its Dock menu.

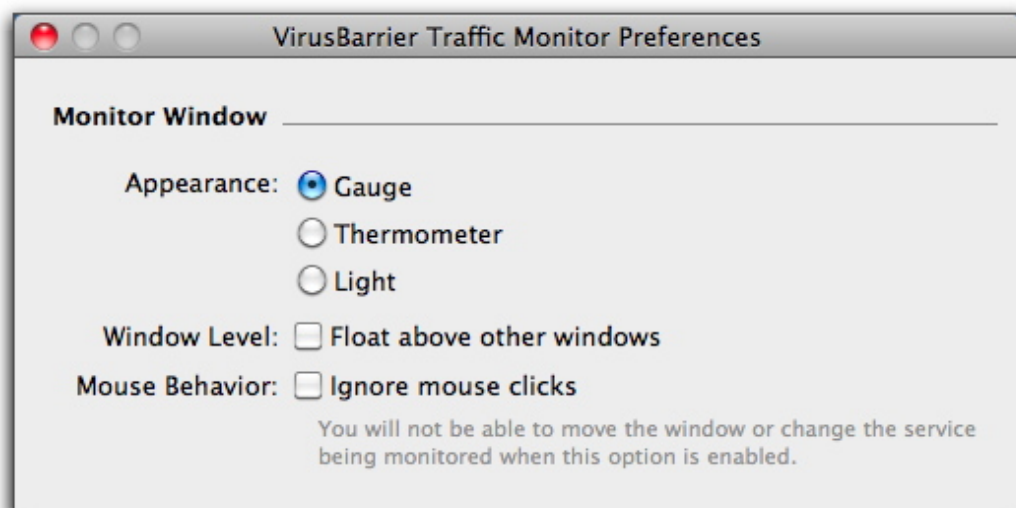


The Keep in Dock selection makes the VirusBarrier Traffic Monitor icon a permanent fixture in the Dock, even when the program is not running, so you can open it just by clicking its Dock icon. The Open at Login selection starts the program each time you start a user's session on your server.

## VirusBarrier Traffic Monitor Preferences

Several preference settings affect the behavior of VirusBarrier Traffic Monitor. To set them, go to **VirusBarrier Traffic Monitor > Preferences** or press Command-comma while VirusBarrier Traffic Monitor is running.





- **Appearance:** Choose from Gauge, Thermometer or Light:



- **Window Level: Float above other windows** makes VirusBarrier Traffic Monitor always appear in the foreground, above all other applications.
- **Mouse Behavior: Ignore mouse clicks** prevents you from moving VirusBarrier Traffic Monitor's window or changing the service it monitors.

## The VirusBarrier Traffic Monitor Widget

VirusBarrier Server 3 installs the VirusBarrier Traffic Monitor widget that loads into Mac OS X's Dashboard to show you network activity when you are in Dashboard.

To display the VirusBarrier Traffic Monitor widget, activate Dashboard. Click the + button to display all the widgets available on your computer. Select VirusBarrier Traffic Monitor from the list. Its icon looks like this:



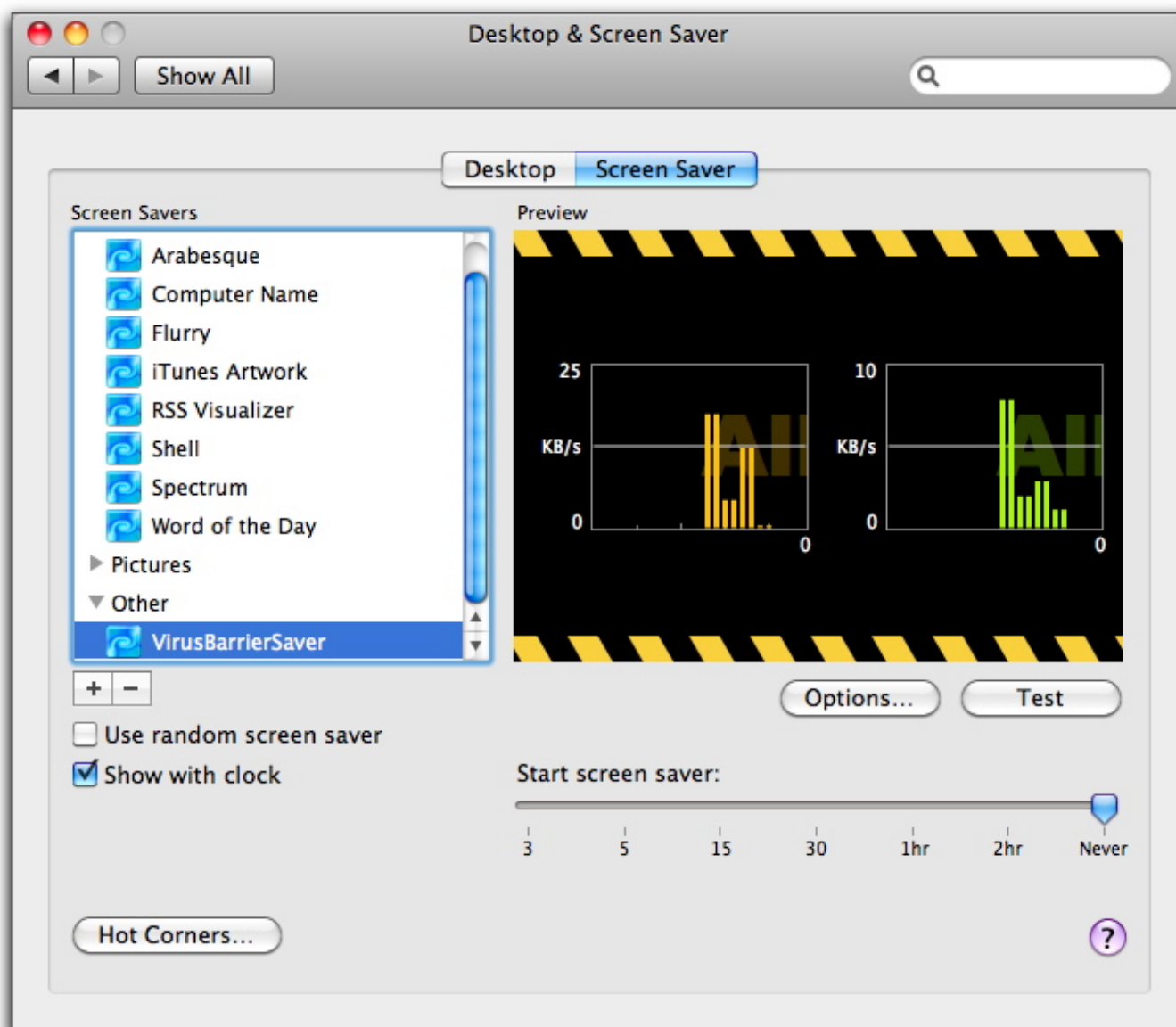
If you add it to your active widgets, you will see VirusBarrier Traffic Monitor whenever you switch to Dashboard. As with the VirusBarrier Traffic Monitor application, you can move the window or change the type of activity displayed.

## The VirusBarrier Server 3 Traffic Monitor Screen Saver

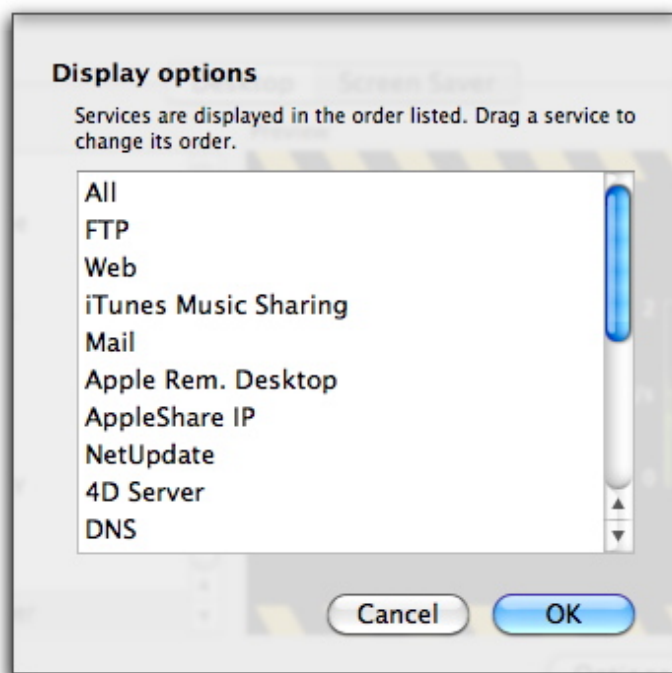
VirusBarrier Server 3 installs a screen saver that gives you an overview of network activity when your computer is

otherwise idle. In addition, if your Macintosh is running as a server, you can use this screen saver to keep an eye on its network activity.

To use the VirusBarrier Server 3 screen saver, open the System Preferences from the Apple menu, click on **Desktop & Screen Saver**, and click the **Screen Saver** tab. Select **VirusBarrierSaver** in the screen saver list.



The preview screen only shows all traffic; however, it will show traffic broken down by service when actually running. Click **Options** to choose the order in which services are displayed.



Drag them into the order you want. The number of services displayed depends on your screen resolution and the number of screens you have: therefore, the ones most important to you should be listed first.

For more on screen saver settings, see the Mac OS X help.

[« Protecting Your Server from Network Attacks](#)

[VirusBarrier Server 3 Preferences and Configurations »](#)



## VirusBarrier Server 3 Preferences and Configurations

- [VirusBarrier Server Admin Preferences](#)
- [NetUpdate Scheduling Preferences](#)
- [Working with Configurations](#)

[Go to Main Table of Contents](#)

### VirusBarrier Server Admin Preferences

VirusBarrier Server Admin preferences only offers one option: the choice of whether the program asks for an administrator password on launch. To access this setting, choose **VirusBarrier Server Admin > Preferences**, and check the option.



These preferences also give you access to NetUpdate, a program that checks if any Intego programs have been updated. This program is installed at the same time as VirusBarrier Server Admin or other Intego programs. It checks for updates for all Intego programs at the same time, and can download and install updates for the programs installed on your computer. To check for updates, click **Check Now**.

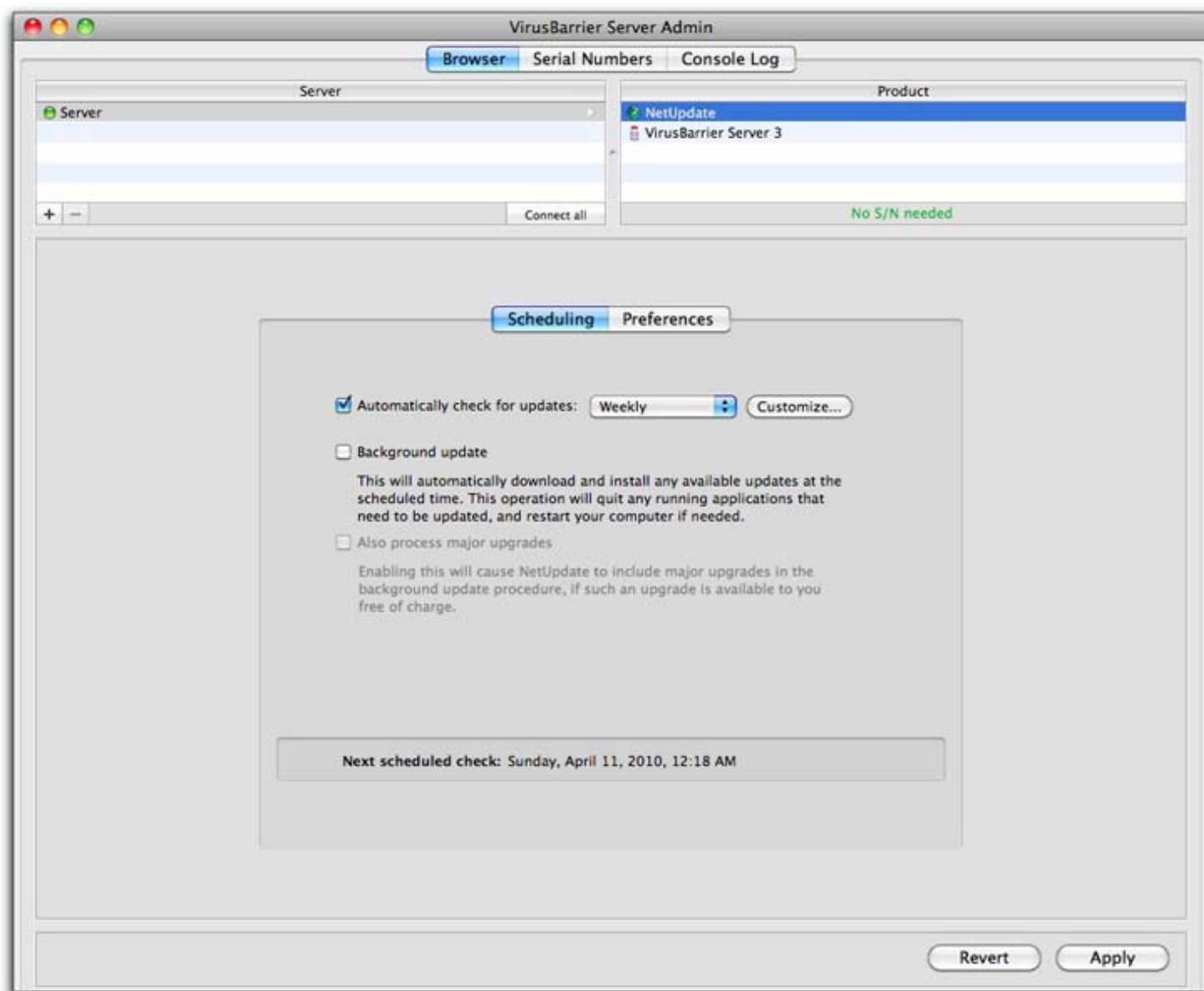
For more on using NetUpdate, see the [Intego Getting Started Manual](#).

## NetUpdate Scheduling Preferences

Through the VirusBarrier Server Admin program, you can set how Intego NetUpdate checks for new versions of your Intego software. To do so:

1. Click the **Browser** tab,
2. Click your server in the upper-left pane,
3. Click **NetUpdate** in the upper-right pane.

The **Scheduling** pane provides access to the following controls:



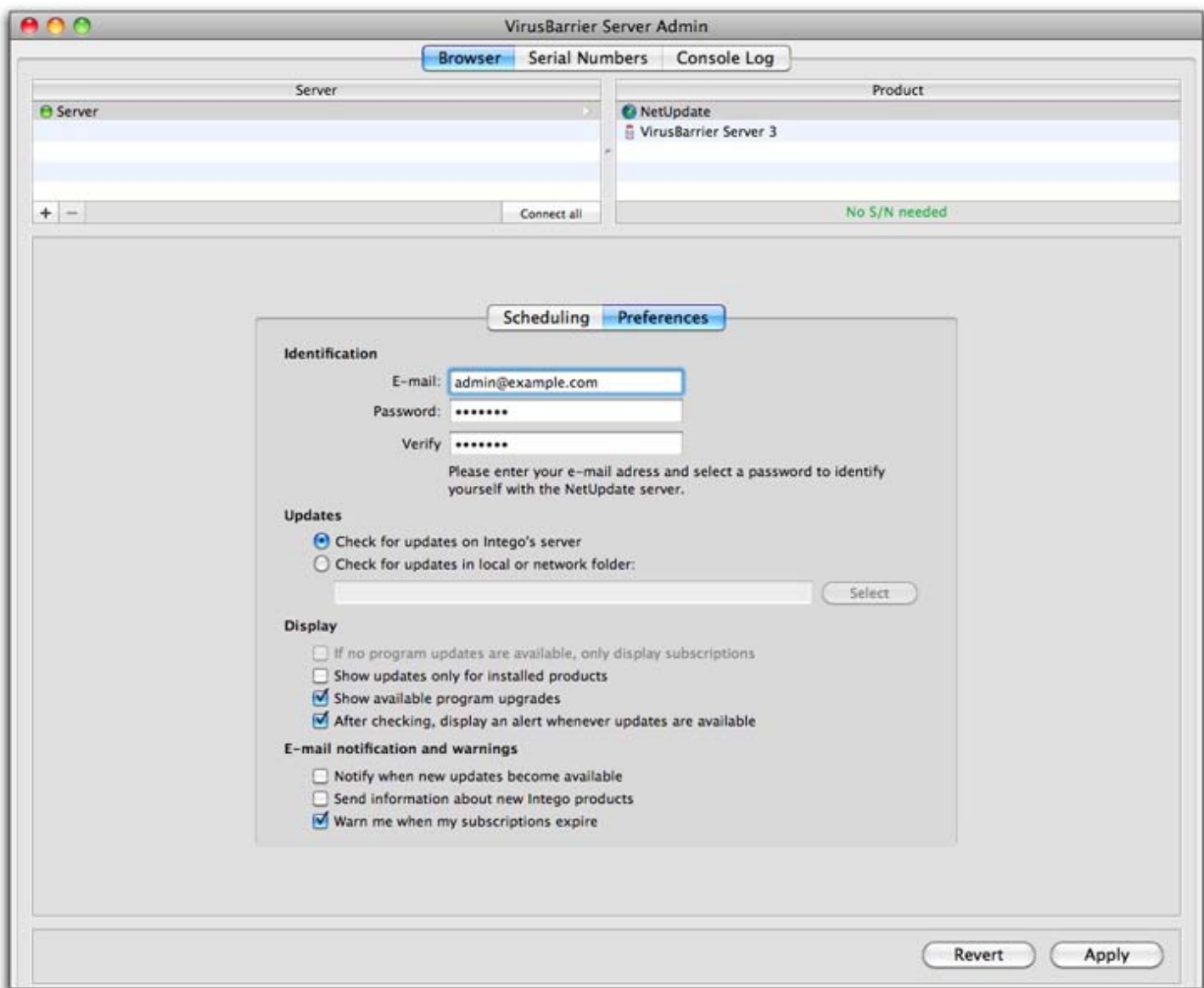
- **Automatically check for updates:** Tells NetUpdate to automatically connect to the Intego NetUpdate server to check for updates with the frequency you specify.

The pop-up menu lets you quickly set that frequency to **daily**, **weekly**, or **monthly**. (In each case, the period starts from when you select something from the pop-up menu. For example, if you were to select **daily** at 1 pm on a Tuesday, the next check would occur at approximately 1 pm on Wednesday.) Clicking the **Customize...** button lets you be more specific about when the check should occur.

If you do not check this option at all, you can manually check for updates by connecting to your server via Apple Remote Desktop or a VNC client, opening the NetUpdate application (in the Applications folder) and clicking the **Check now...** button.

- **Background update:** If you check this option, then when NetUpdate performs an update it will automatically quit any programs that need to be updated, and will restart your server if required.
- **Also process major upgrades:** If you check this option, NetUpdate will also install major upgrades if these upgrades are available to you free of charge. Note that you must have **Background update** checked in order to access this option.

The **Preferences** pane has the following controls:



- **Identification:** Enter an e-mail address and password to identify yourself with the NetUpdate server. If you need to change the e-mail address, you can do so here.
- **Updates:** You can have NetUpdate check for new software in two locations. The default choice, **Check for updates on Intego's server**, should be used in most cases. But if you are working on a network, and have multiple user licenses for Intego products, you can choose a NetUpdate folder anywhere on your network.

To do this, select **Check local or network folder:** and click the **Select** button to select a folder, or enter the folder's path in the text field. If you use a local NetUpdate folder on a remote volume, this volume must be mounted on each computer at check time to access the NetUpdate archives.

To use a local NetUpdate archive folder, first download update files to one computer. From NetUpdate on your server, select the update you want to download by checking it in the update list, then select **File > Download Item to...** and copy or move them to the NetUpdate archive folder you have set.

**Note:** when updating Intego software via update files located in a local NetUpdate folder, NetUpdate needs to check with the Intego server to verify the subscription rights of the program being updated. Computers updating Intego software in this manner therefore need to be able to access the Internet.

- **Display:** This section comprises four checkboxes:

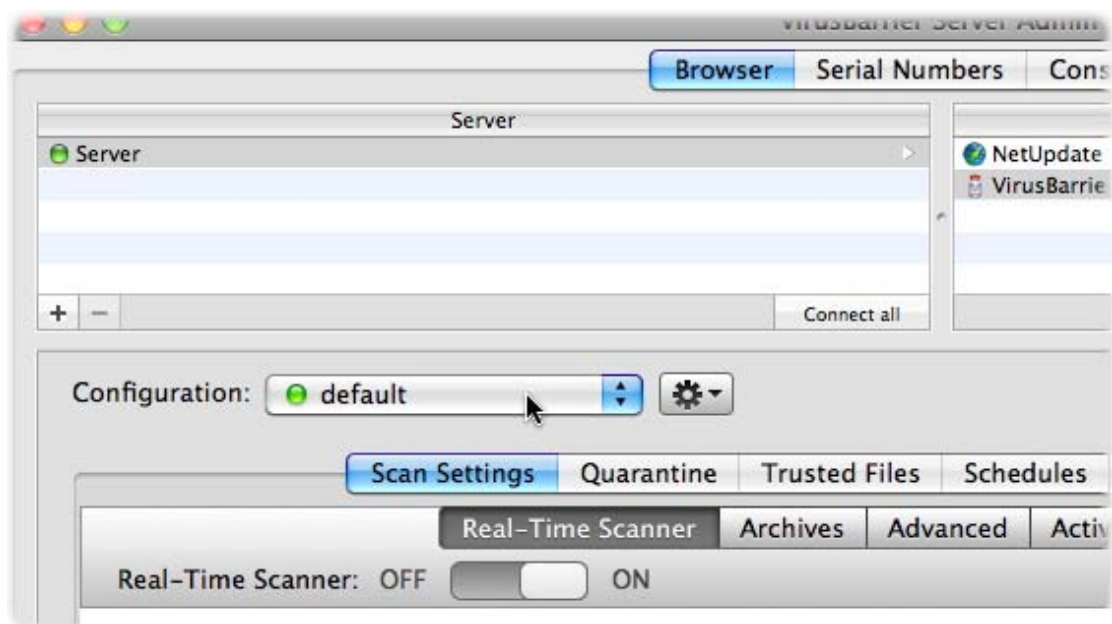


- **If no program updates are available, only display subscriptions:** If this is enabled, only subscriptions display in NetUpdate's window.
- **Show updates only for installed products** suppresses display of Intego products that you don't own.
- **Show available program upgrades** tells you when Intego has a version of the program that is substantially improved beyond normal updates, and requires a fee to perform the upgrade.
- **After checking, display an alert whenever updates are available** will display an alert in the NetUpdate window whenever an update is available for your Intego products.
- **Email Notification:** Three email notification options are available on this pane:
  - **Notify when new updates become available:** If you check this option, you will receive email messages whenever new updates to Intego products are released.
  - **Send information about new Intego products:** Checking this box means that you allow Intego to use the email address you register to send you occasional messages presenting its new products.
  - **Warn me when my subscription expire:** This setting helps you remember to renew your Intego subscription so you're never without the most up-to-date protection.

## Working with Configurations

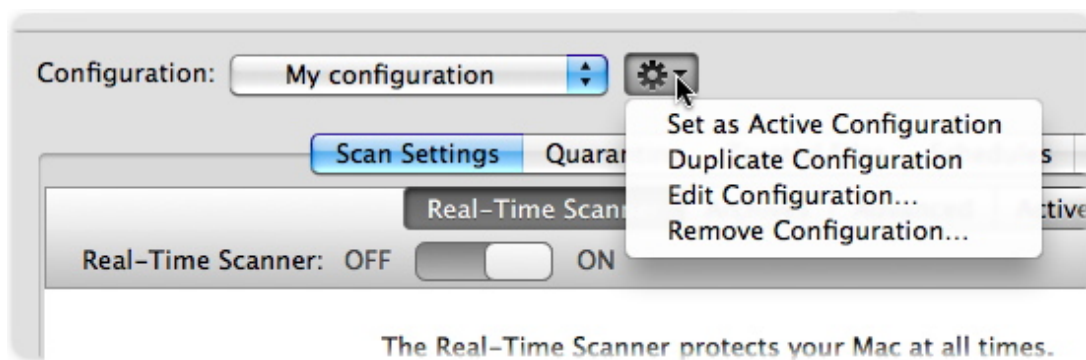
VirusBarrier Server 3 lets you save multiple configurations. Each configuration contains all the settings and preferences you have applied to VirusBarrier Server 3 in its different screens and preferences. You may also want a specific set for less protection when you are connected only to a local network, and additional protection when you're serving files to the Internet. You may want to have a configuration that sends you e-mail messages when any intrusions occur, for when you are not at your computer.

You see configurations when the Browser pane is active. VirusBarrier Server 3 comes with one configuration, called **default**. (You can't delete this configuration.)



The action button next to the list lets you duplicate, edit, remove and hide configurations.

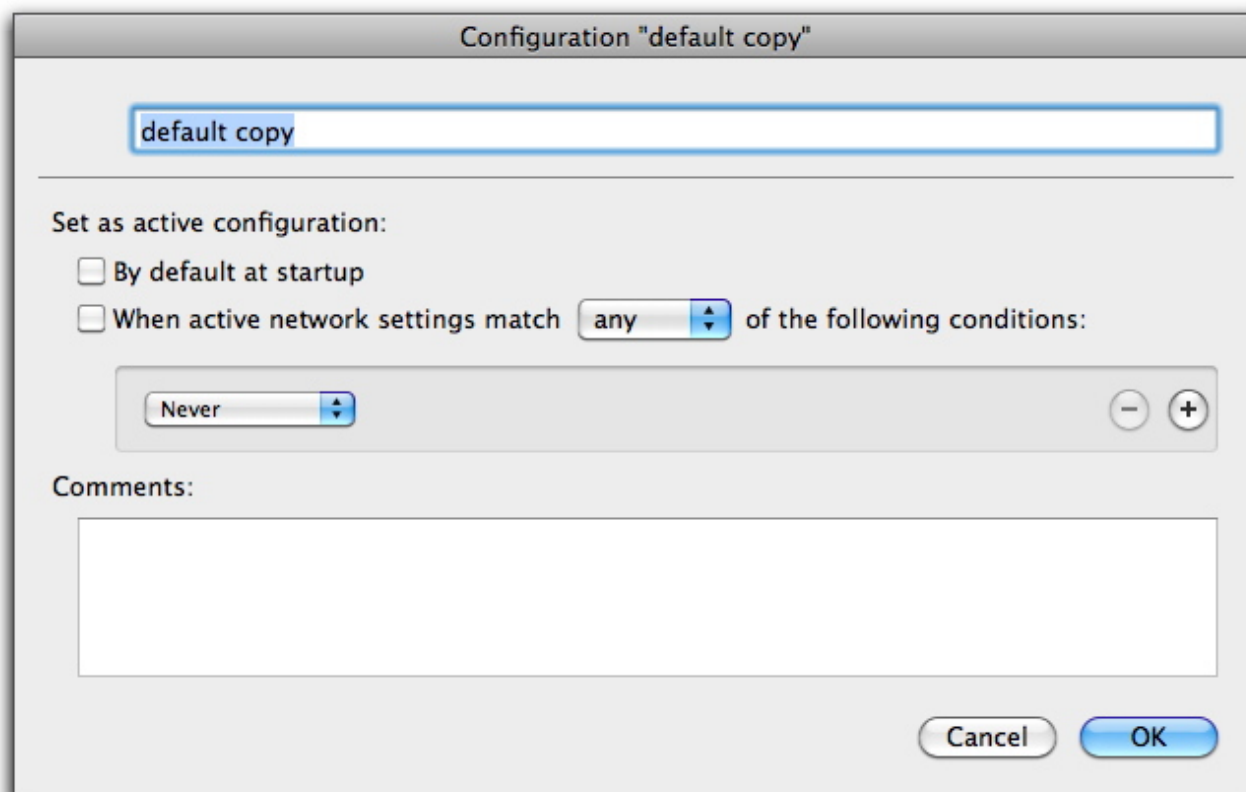




## Creating, Editing and Deleting Configurations

You create a new configuration by clicking the action button and selecting **Duplicate Configuration** from the pop-up menu that appears.

This new configuration has the same name as the one you duplicated, with the word "copy" appended. Rename it by clicking the action button and selecting **Edit Configuration** from the pop-up menu. A window appears.



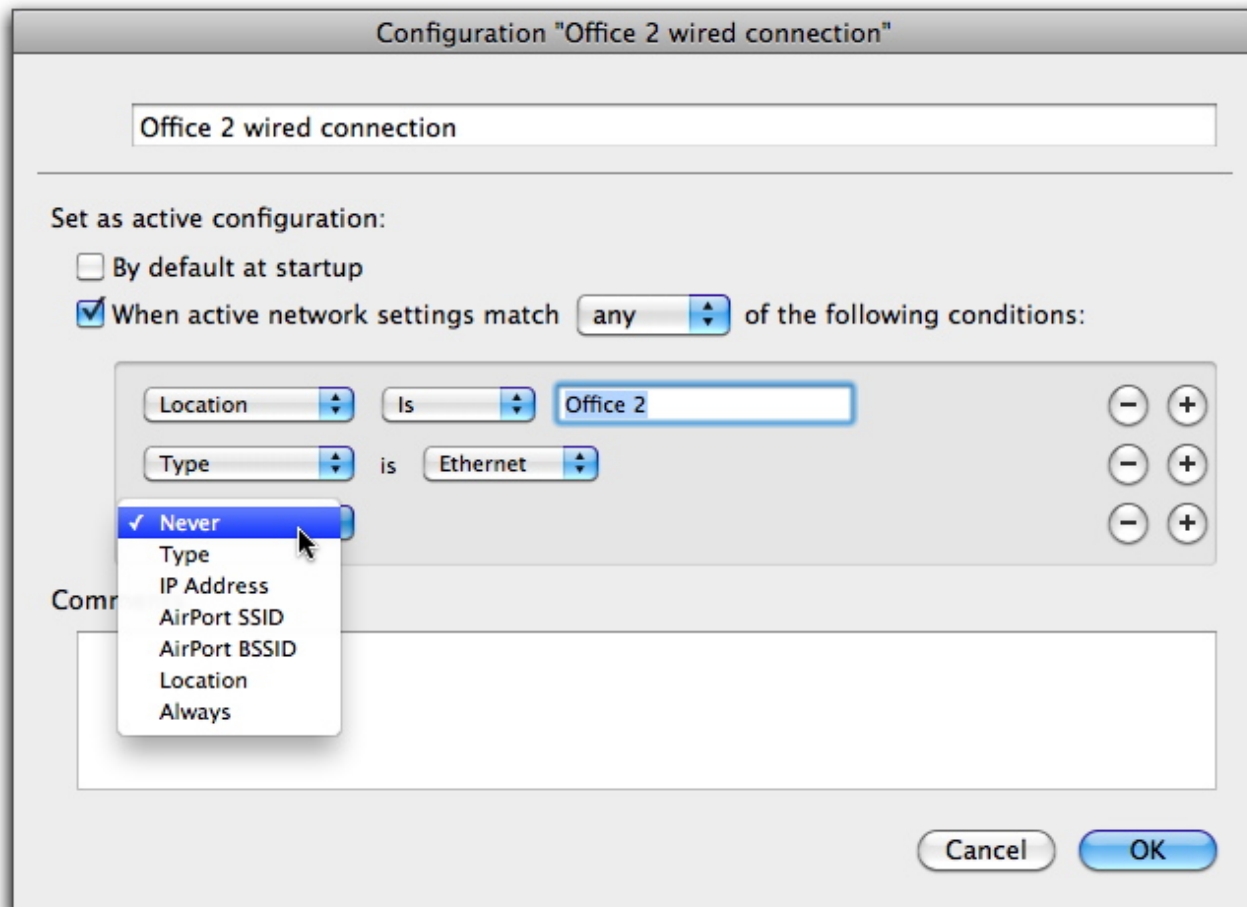
After the area where you can change the configuration's name follows the **Save as active configuration** section. By changing the two criteria in this section, you can determine when VirusBarrier Server 3 will automatically switch from one configuration to another. The options are:

- **By default at startup**, which takes effect when you restart your server.
- **When active network settings match...**, which lets you set conditions under which the configuration will change. checkbox it will automatically become active when any or all conditions you specify regarding the following networking criteria are true.
  - **Never**: This condition will never be true, so the configuration will never turn on automatically.
  - **Type**: Choices are Ethernet, AirPort, FireWire, PPP or Bluetooth.
  - **IP Address**: You can choose a specific IP address, or a range. A Current button identifies the IP address

your server has at the moment.

- **AirPort SSID:** The common name for a wireless network, such as "My AirPort". You can choose for this condition to be true when the SSID is, is not, or contains a text string you specify.
- **AirPort BSSID:** The MAC address of a wireless network connection point, expressed as a string of hexadecimal numbers.
- **Location:** The Location defined in your server's Network preferences.
- **Always:** The condition is always true.

You can add multiple criteria to this section by clicking the + sign to the right, or remove existing criteria by clicking the – sign.



The **Comments** field is a place for any description or notes you'd care to add: they don't affect operation of the configuration in any way.

To save your the changes you've made to the configuration, click the **Apply** button at the bottom-right of the VirusBarrier Server Admin window.

To make your new configuration become, active click the Action button and choose **Set as Active Configuration**.

You can now make any changes to VirusBarrier Server 3 that you want, and they are saved under the current configuration. To make another configuration active, simply switch to it using the pop-up menu, then choose **Set as Active Configuration** from the Action button. You can also select another configuration from the Configurations list in the Intego Menu, if you are working on the server whose configuration you wish to change. (For more information about the Intego Menu, see the [Intego Getting Started Manual](http://www.intego.com/manuals/en/vbs/6-Preferences-and-Configurations.html).)

To delete the active configuration, select **Remove Configuration...** from the pop-up menu. You'll see a dialog box that asks you to confirm the deletion. VirusBarrier Server 3 will switch to the **default** configuration after deletion of the

current one.

[« Using VirusBarrier Server 3 Monitoring Tools](#)

[Creating Custom Firewall Rules »](#)

© 2010 Intego. All Rights Reserved.



## Creating Custom Firewall Rules

- [Custom Firewall Rules](#)
- [Creating Rules with the Assistant](#)
- [Creating Rules Manually](#)
- [Working with Rules](#)

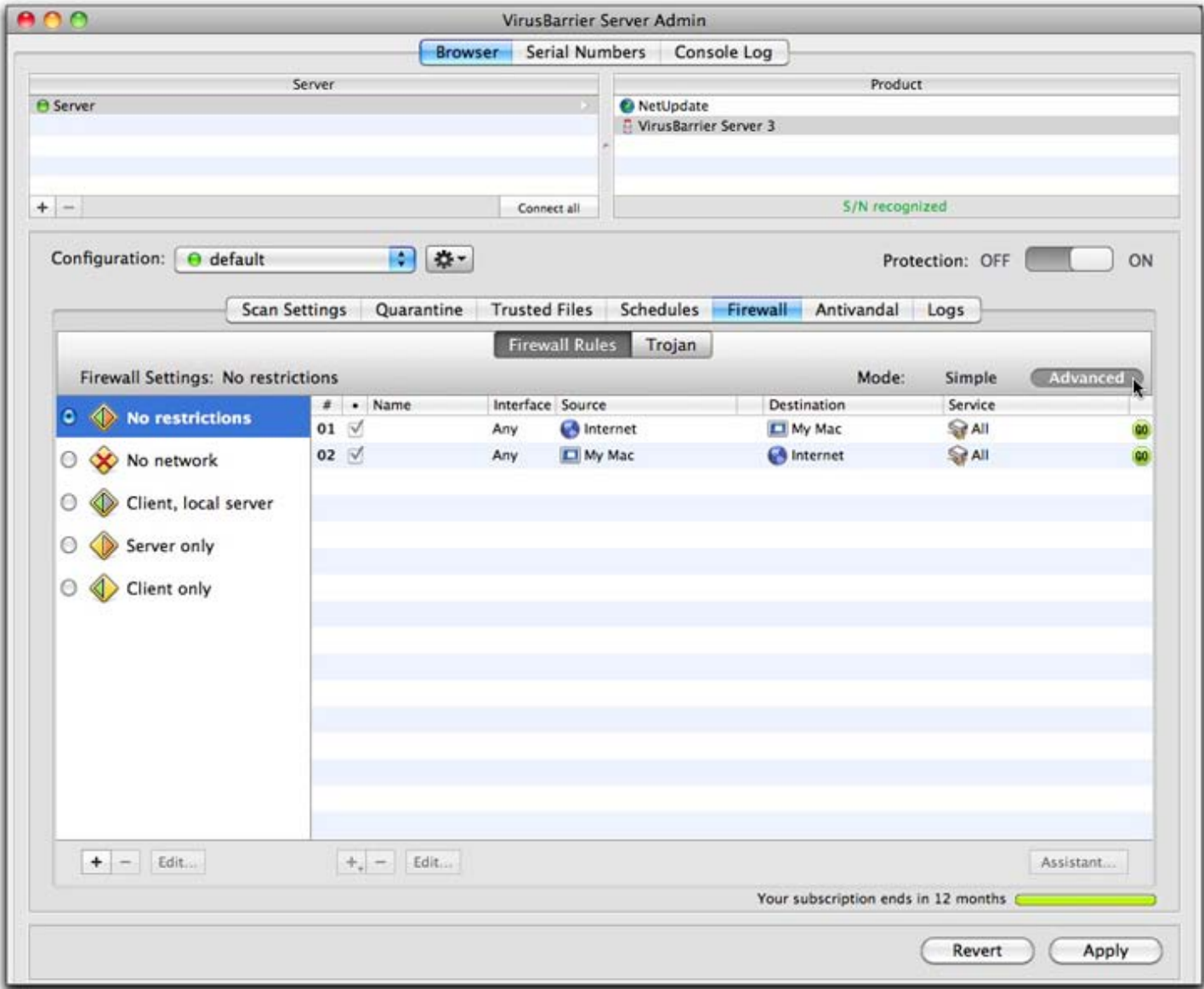
[Go to Main Table of Contents](#)

### Custom Firewall Rules

Each of the five firewall settings described in chapter 4, [Protecting Your Server from Network Attacks](#), is actually a collection of rules, each of which in turn is defined by naming permitted or forbidden sources, destinations, services and interfaces.

To see your Firewall rules, choose a server, click on **VirusBarrier Server 3**, then click on the **Firewall** tab.

By default you see the Simple mode, which doesn't permit you to change the rules or any of their parts. To do that, you need to enter the Firewall screen's advanced mode. To do so, click the **Firewall** tab and then click **Advanced**.



*WARNING: Changing these settings could dramatically affect your computer's ability to access local networks and the Internet. You should only use advanced mode if you fully understand its effects and how it functions.*

In simple mode, clicking any of the five preset firewall settings displays an animation; in advanced mode, you see the details of each setting's rules.

In addition, hovering the cursor over any of the preset settings for a few seconds displays a text that briefly describes what it does.

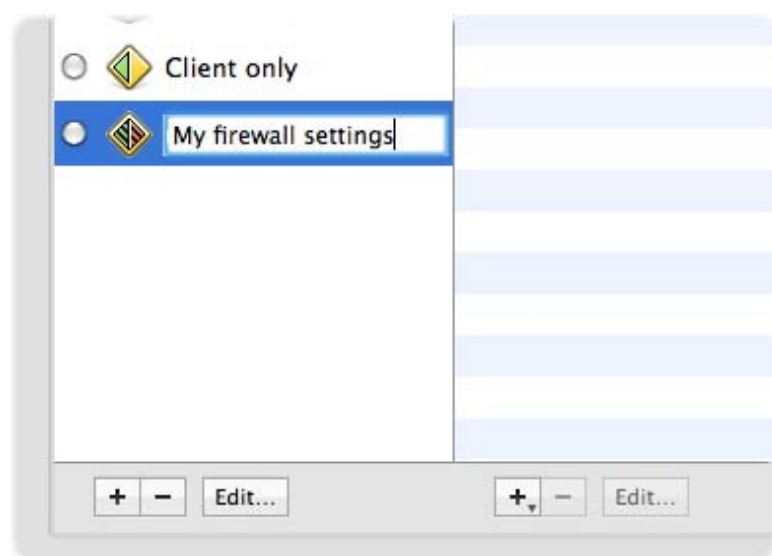


In this example, the **Client, local server** setting shown has four rules.

- The first allows the local network to access your server through all Connected Services – that is, TCP connections that involve back-and-forth communications, such as serving files from your server.
- The second rule, however, forbids such connections from the Internet at large, preventing your server from acting as a server to an unknown computer outside your local network.
- The third rule allows all other communications from the Internet to your server.
- The fourth rule allows all communications from your server *to* the Internet.

The five preset firewall settings are "locked" for convenience and stability: you can't change their rules, or the order in which they appear. But VirusBarrier Server 3 gives you two ways to create additional, customized settings: through the program's Firewall Assistant, and manually.

In either case, the first step is to click the + button below the list of settings. You'll see a new setting appear, named "untitled settings". Click it and type any name you prefer, then press Enter or Return to make the change permanent.



Note that you've only created this setting, but have **not** enabled it yet. It's a good idea to not enable firewall settings until you have finished adding all your rules. To make it the active setting, click the radio button to its left.

## Creating Rules with the Assistant

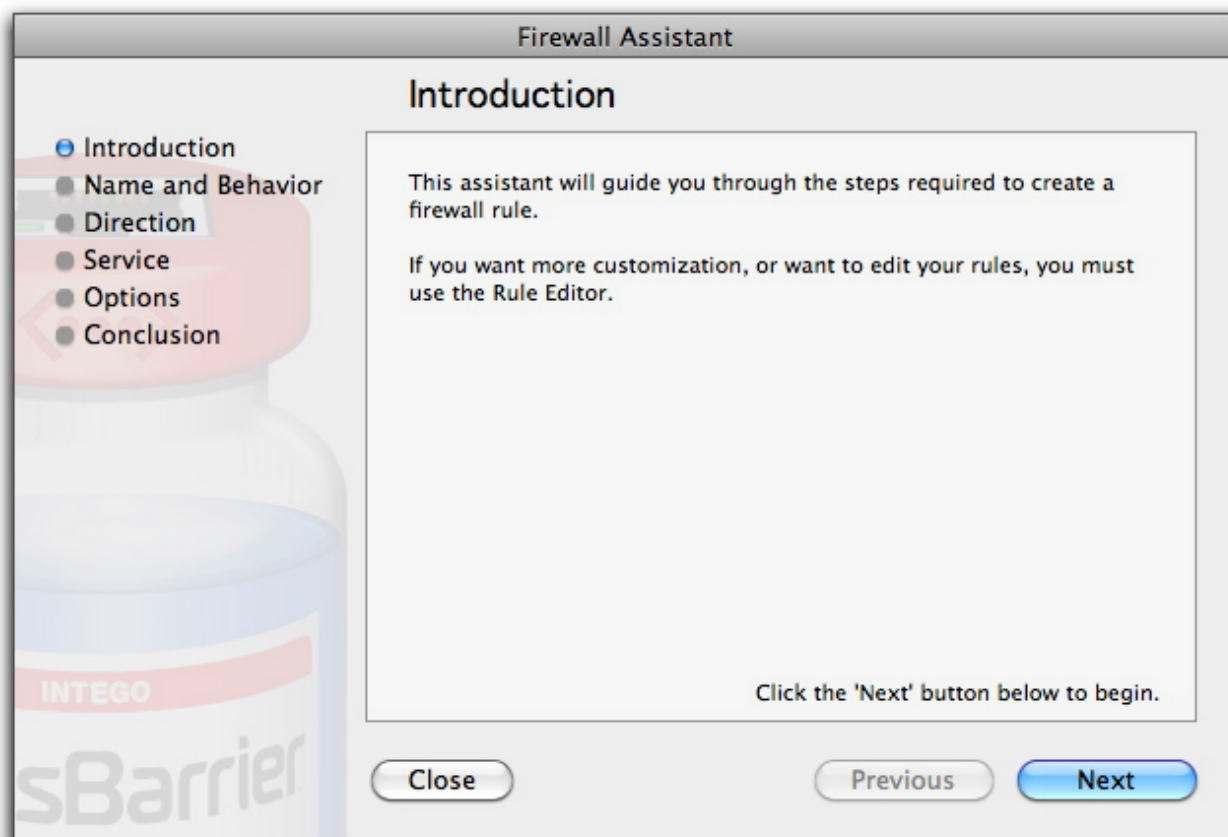
VirusBarrier Server 3 contains an assistant to help you create your own custom firewall rules. With this assistant, you can create your own rules with just a few mouse clicks. While not all of VirusBarrier Server 3's rule features are available when you create rules with the assistant, it can cover most of your needs. If you need more customization, you can edit rules manually after creating them with the assistant.

The VirusBarrier Server 3 Assistant walks you through a series of steps to create your rule:

- **Introduction**
- **Name and Behavior**
- **Communication Direction**
- **Service**
- **Options**
- **Conclusion**

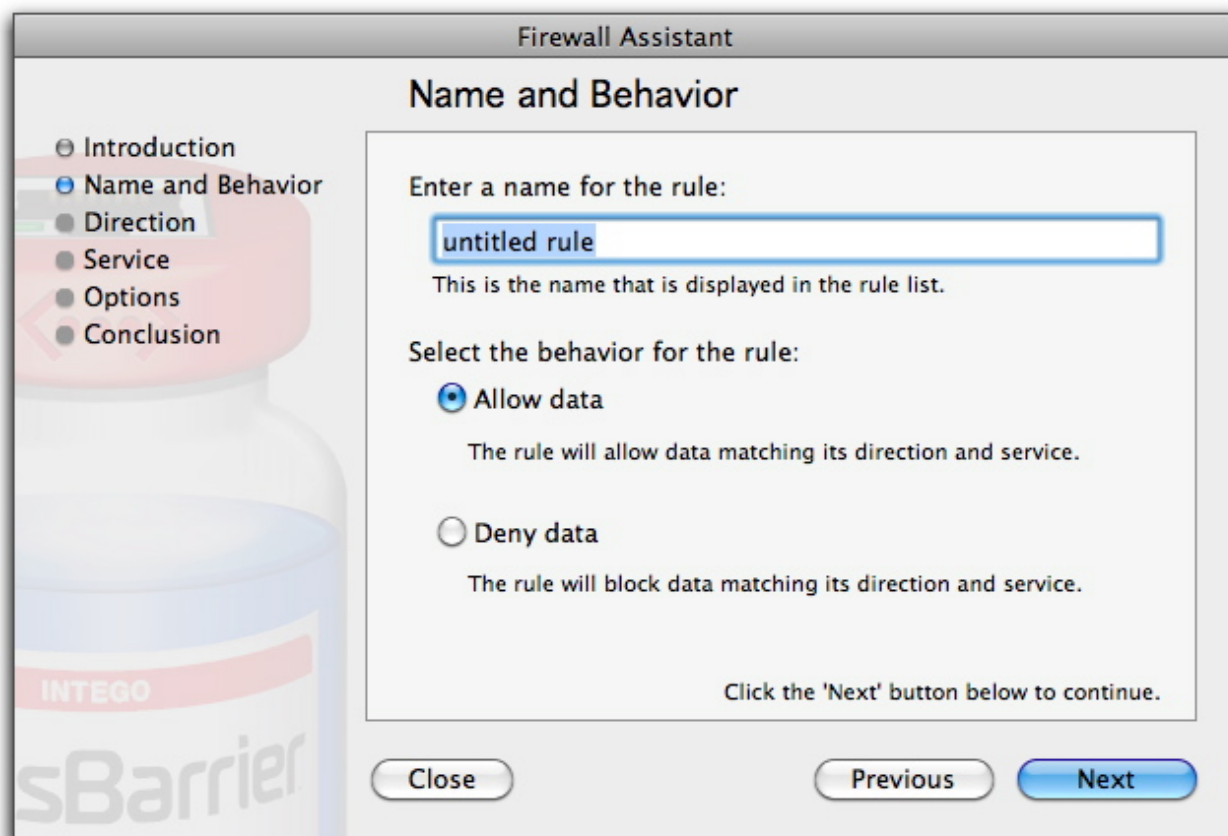
To create a new rule using the assistant, click the **Assistant** button in the bottom-right corner of the window.

The first assistant screen displays.



Click the **Next** button to begin creating a new rule. You can click the **Previous** button at any time to return to previous screens, or click Close to exit the Assistant.

## Name and Behavior

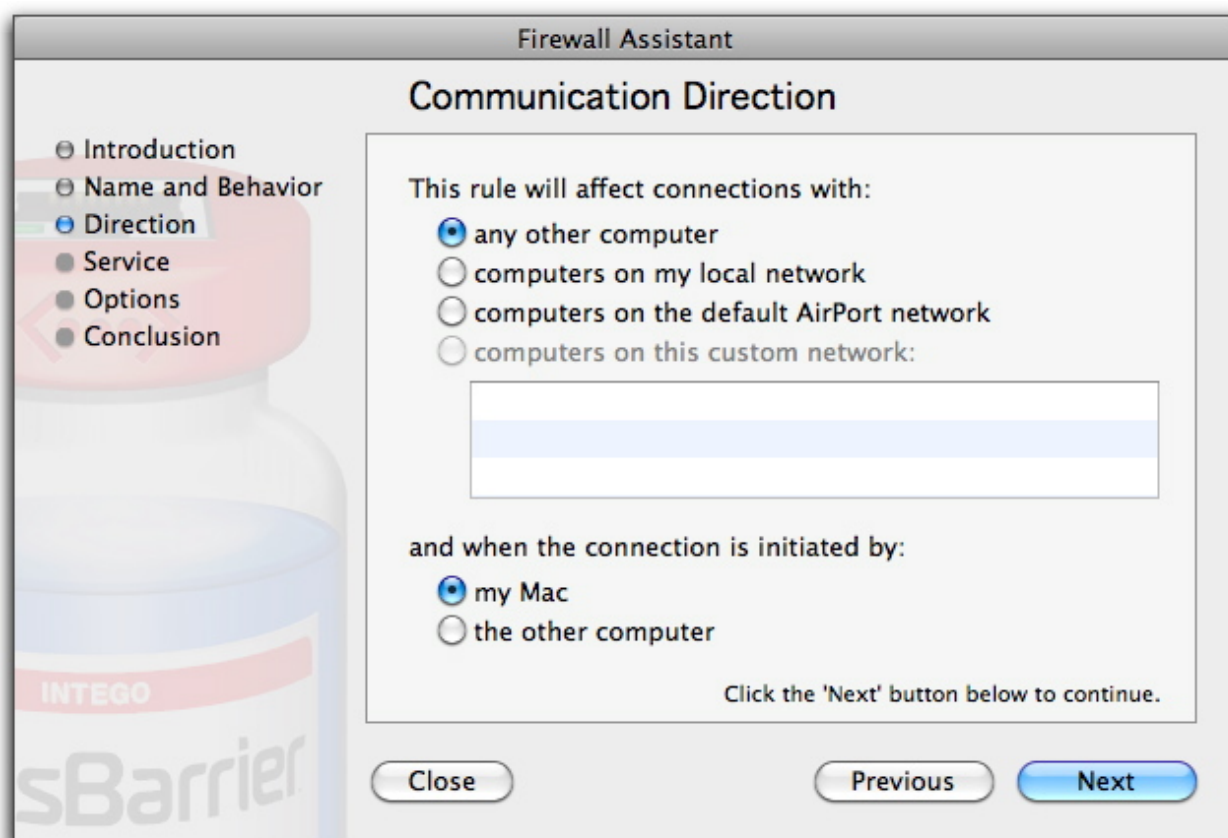


Enter a name for your rule in the name field, then select the behavior for the rule: **Allow data** or **Deny data**. If you select **Allow data**, the rule will allow data matching its direction and service to pass. If you select **Deny data**, the rule will block data matching its direction and service.

## Communication Direction

This screen lets you choose the communication direction and which host initiates the communication.





First, in the **This rule will affect connections with:** section, select a remote host. You have four choices for the remote host:

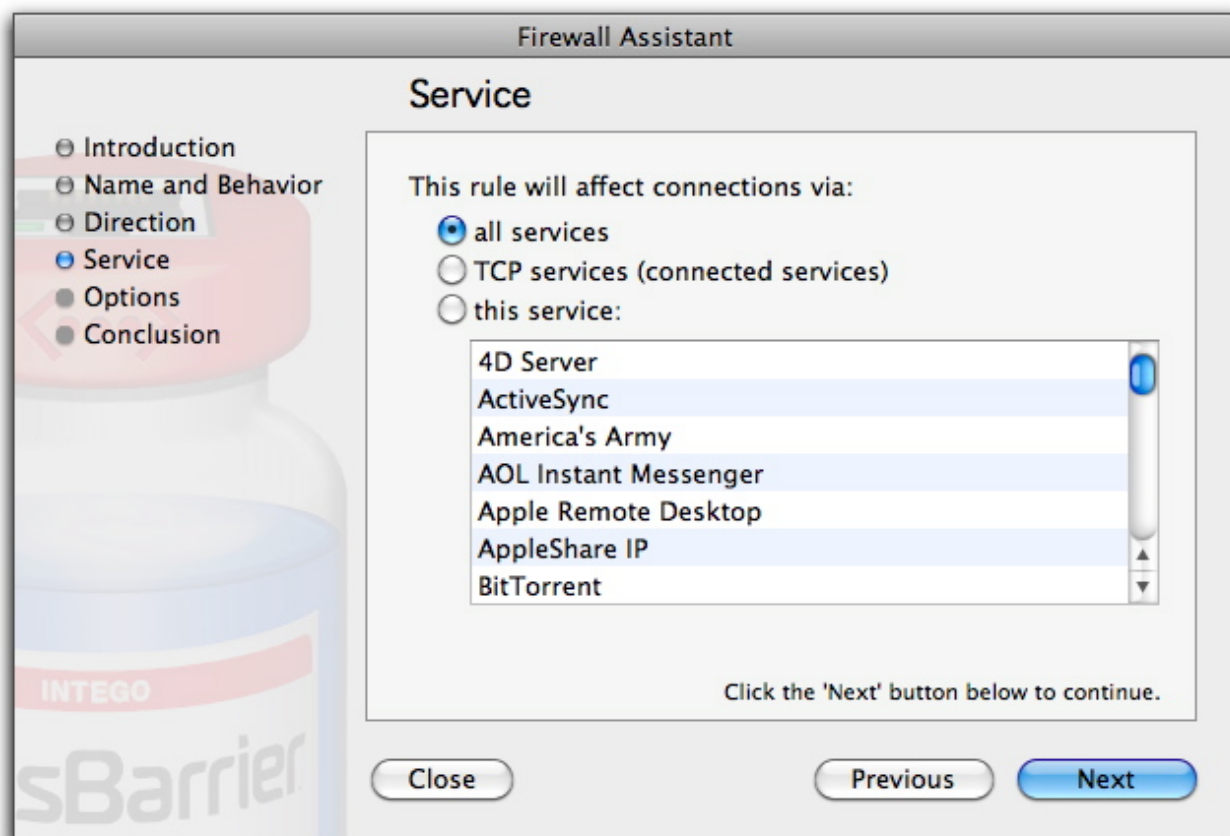
- **Any other computer:** Any computer other than your server.
- **Computers on my local network:** Any computer on the same local network as your server.
- **Computers on the default AirPort network:** Any computer on your default AirPort network, if you have one.
- **Computers on this custom network:** If you have created any custom networks using the standard rule editor, you can select one of them here. (See the ["Creating Rules Manually" section](#) to learn how to set up a custom network.)

Next, select the computer that initiates the connection:

- **My Mac:** The computer using this rule.
- **The other computer:** The remote host, as was defined in the first part of this screen.

## Service

This screen lets you choose the service that the rule affects.

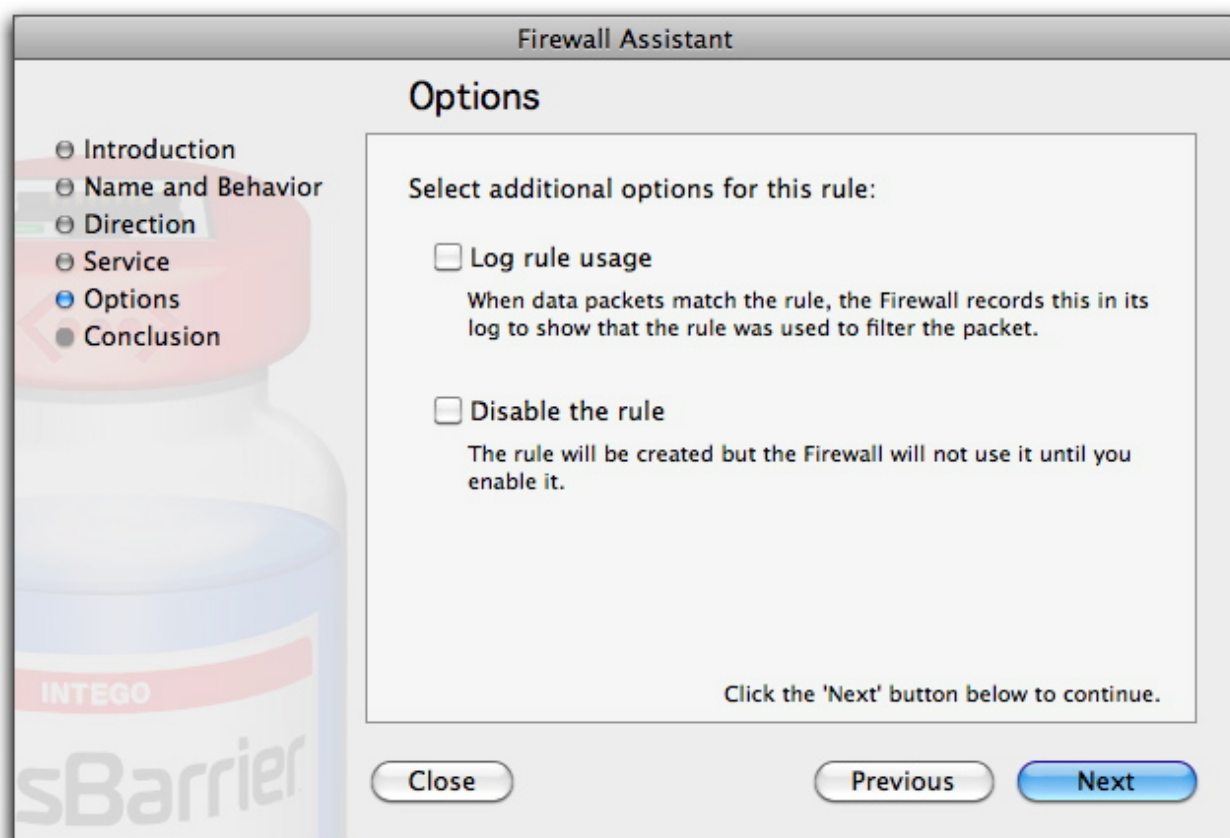


You can choose from three types of services:

- **All services:** All network services.
- **TCP services (connected services):** Services that require that a connection be open and maintained between two computers, such as HTTP, FTP, Telnet, SSH, POP3, AppleShare, etc. This covers all TCP connections.
- **This service:** You can choose from a list of services that correspond to popular applications and protocols. Select the service you want to use by clicking its name in the list.

## Options

This screen lets you choose additional options for your rule.

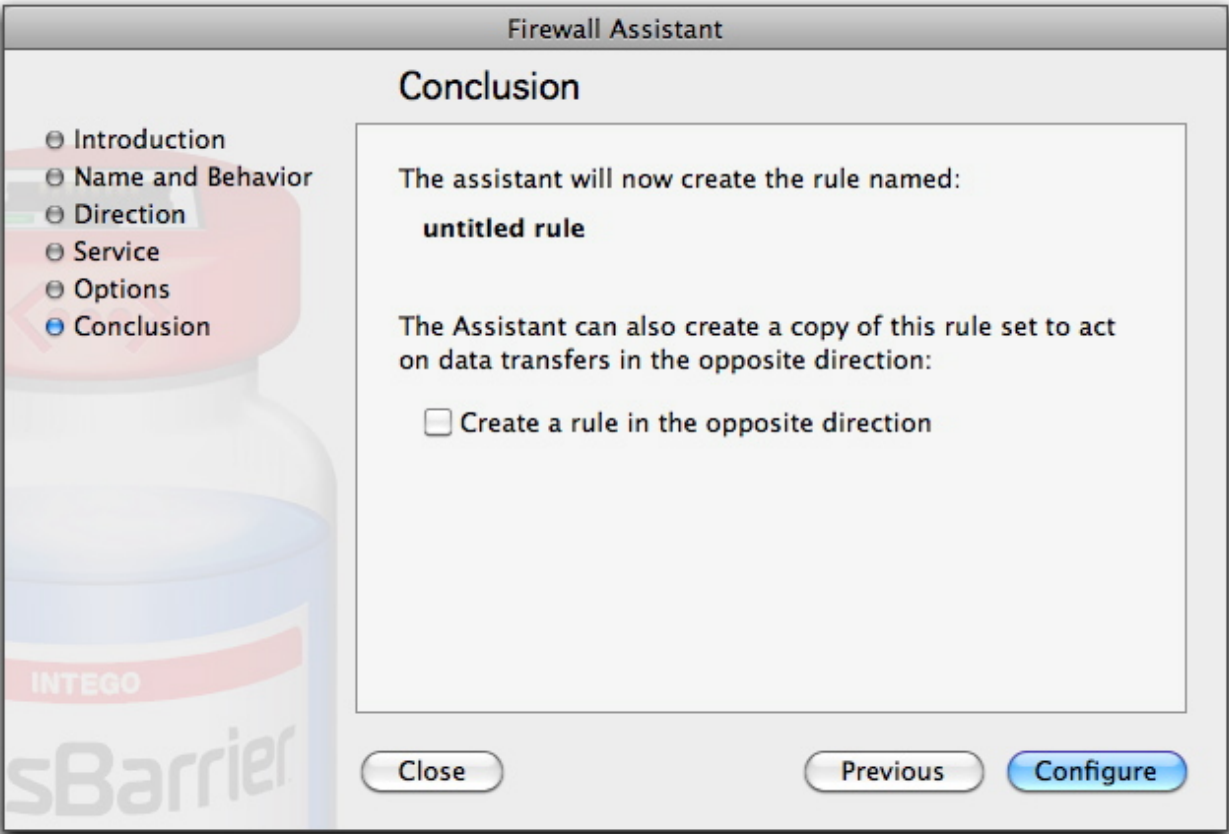


Two options are available on this screen:

- **Log rule usage:** The firewall records each time this rule is used in its log.
- **Disable the rule:** VirusBarrier Server 3 creates the rule but disables it. You can enable it manually.

## Conclusion

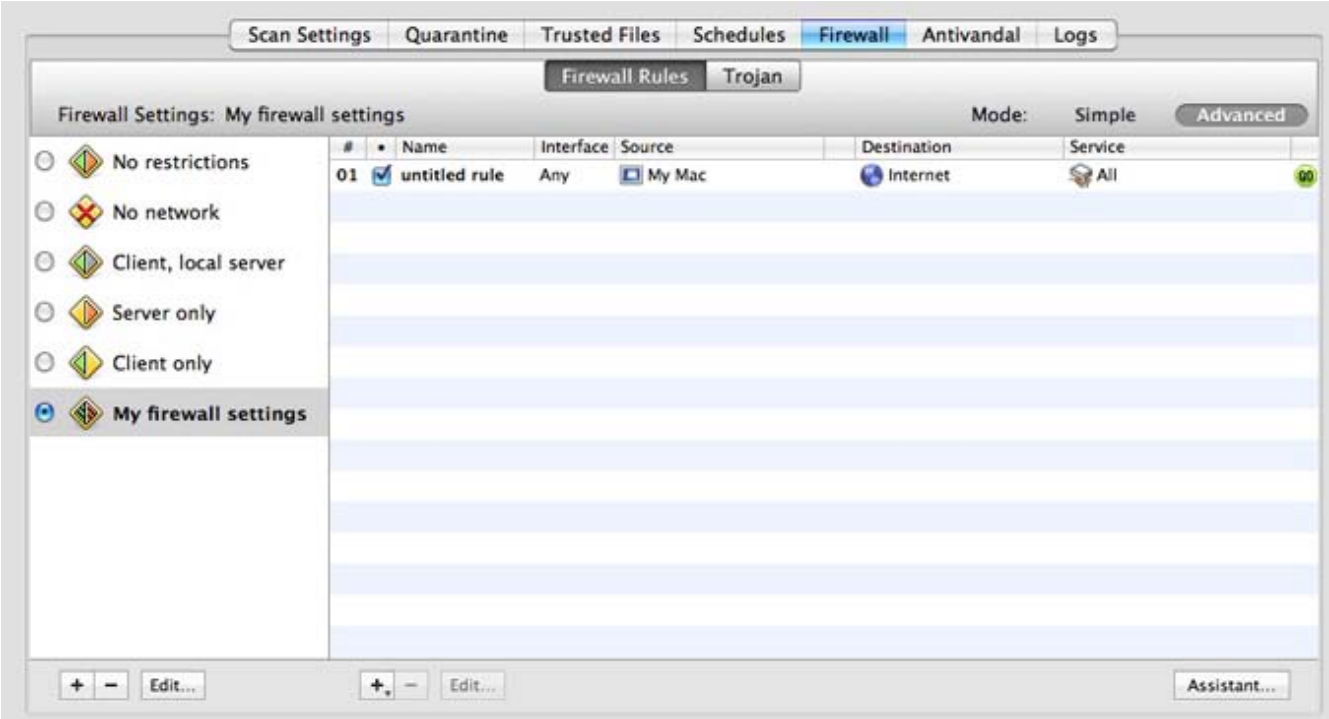
This screen creates the rule according to the settings you have selected in the assistant.



This screen offers one final option: if you check **Create a rule in the opposite direction**, the assistant creates a matching rule with the source and destination switched.

Click **Configure** to create your rule and exit the assistant.

When you have finished, you will see that your rule (or rules, if you checked **Create a rule in the opposite direction**) displays in the VirusBarrier Server 3 list of firewall rules.



If you wish to further customize the rule, or edit it, see the section "Editing Rules" in the [Working with Rules](#) section, below.

## Creating Rules Manually

You can quickly create a rule to control information to and from common services and programs. To do so, click the + button at the bottom of the Rule list and hold your mouse button down for a second. You'll be able to choose from a popup list of the most common services. A rule governing your selection then appears in the Rules list.



The Rule Editor lets you create rules of much greater variety and complexity. To see it, click the + button at the bottom of the list of rules.



VirusBarrier Server 3's Rule Editor allows network administrators to quickly and easily define and implement a

comprehensive security policy. It is extremely flexible, and allows you to define an unlimited number of rules in seconds. To create a rule, you need to specify details in six areas:

- **Rule Name, Logging, Evaluation and Schedule**
- **Rule Source**
- **Rule Destination**
- **Rule Service**
- **Rule Interface**
- **Rule Action**

## Rule Naming, Logging, Evaluation and Schedules

At the top of the Rule Editor is a field where you can name this rule. Just below it is the **Log** checkbox. If you check the **Log** box, an entry is added to the VirusBarrier Server 3 log any time this rule acts; a small red dot to the right of the rule's name in the Rules list indicates that the rule is logged. If this box is not checked, this rule is not logged.



The screenshot shows the Rule Editor interface. At the top, there is a text field labeled "Name:" containing the text "untitled rule 1". Below this, under the "Options:" section, there are two checkboxes: "Log" (unchecked) and "Stop Evaluating Rules" (checked). At the bottom, under the "Schedule:" section, there is a button labeled "Edit...".

If the Log checkbox is checked, the **Stop Evaluating Rules** checkbox will be available, and is checked by default. These two settings, in tandem, are a powerful way to troubleshoot a network without hampering its traffic.

***WARNING:** If you can't figure out why some of your rules aren't taking effect, look at the rules above it and ensure that the Stop Evaluating Rules checkbox is off for each of them.*

To edit the Schedule, click the **Edit...** button. The Schedule window displays.

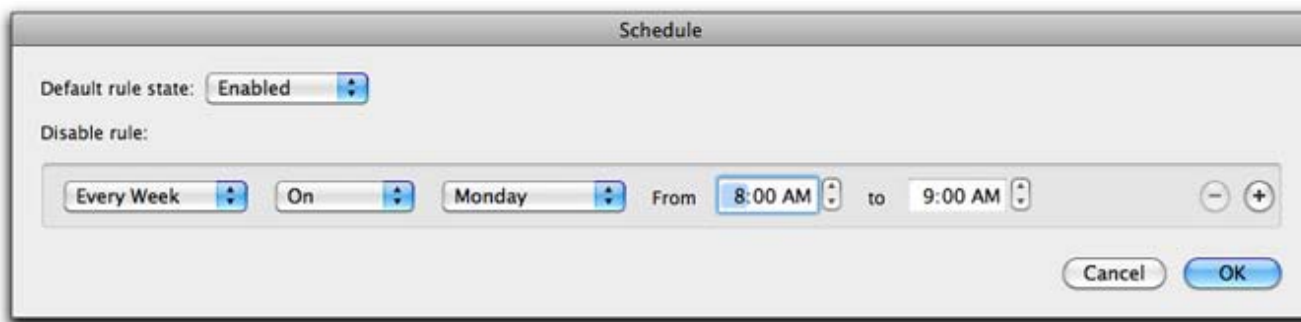


The screenshot shows the "Schedule" window. It has a title bar that says "Schedule". Inside, there is a section labeled "Default rule state:" with a dropdown menu set to "Enabled". Below this is a section labeled "Disable rule:" with a dropdown menu set to "Never". To the right of the "Disable rule:" dropdown are minus and plus buttons. At the bottom right of the window are "Cancel" and "OK" buttons.

The Default rule state is set to **Enabled**, which means that your rule is activated. If you set it to **Disabled**, VirusBarrier Server 3 does not use this rule. You may want to have certain rules active in one configuration, and not another. For more on using configurations, see the "Working with Configurations" section of Chapter 6, [Intego VirusBarrier Server 3 Preferences and Configurations](#).

If your default rule state is **Enabled**, you can set specific times for the rule to be disabled. If your default rule state is **Disabled**, you can set specific times for the rule to be enabled.

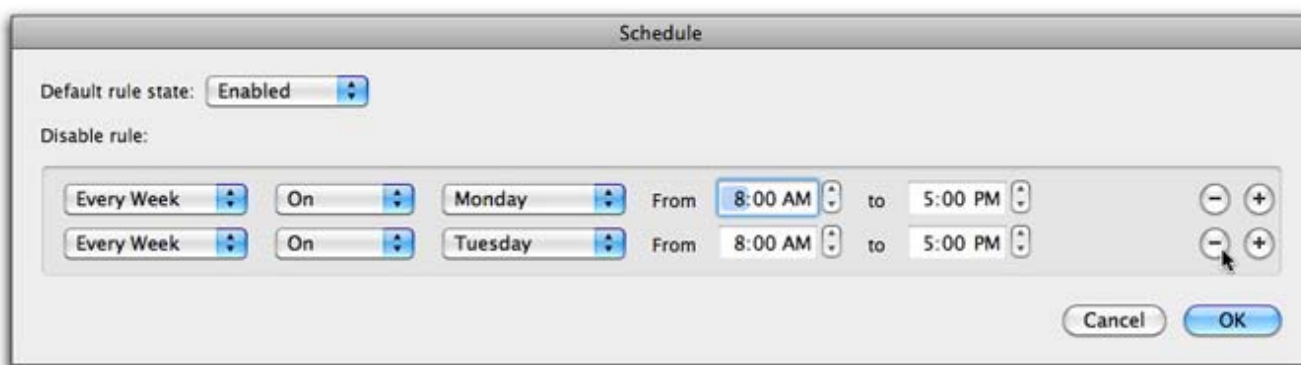
When you first create a rule, the rule will always be active. If you wish to have the rule enabled or disabled at certain times, select **Enabled** or **Disabled** from the popup menu and select one of the time intervals in the list.



Three options are available in addition to **Never**:

- **Every Week** allows you to change the rule's schedule so it is enabled at a fixed time every week, such as every Monday at 8:00 am.
- **Every Day** enables the rule at a specific time every day.
- **From** allows you to disable or enable the rule for a specific period of time by specifying the beginning and ending time.

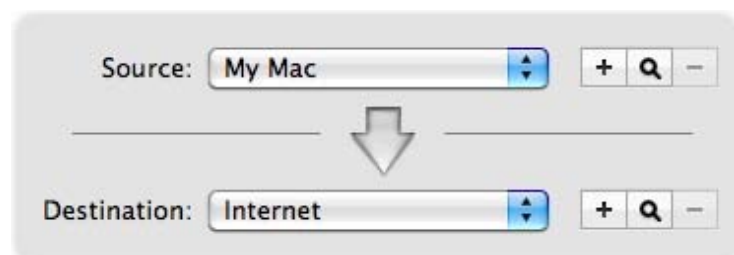
You can schedule additional times for rules to be enabled or disabled using the + button. For example, if you need a rule to be disabled only during office hours on Mondays and Tuesdays, you can set these two days in the Schedule window. To remove a scheduled time from the list, click the – button to the right of the item.



Scheduled rules are displayed with a calendar icon in the rule list.

## Rule Sources and Destinations

When defining rules, the Source is the entity that sends data; the Destination is where the data goes. You can choose from a list of four sources and destinations for any rule. However, VirusBarrier Server 3 will not allow you to choose the same source and destination for a given rule. (If you try, VirusBarrier Server 3 will correct the error.)



These four Sources and Destinations are available by default:

- **My Mac**: Your computer.
- **Local Network**: A local network that your computer is connected to.

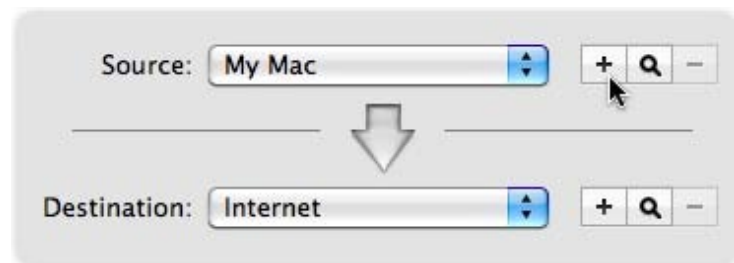


**AirPort Network:** A wireless AirPort network that your computer is connected to.

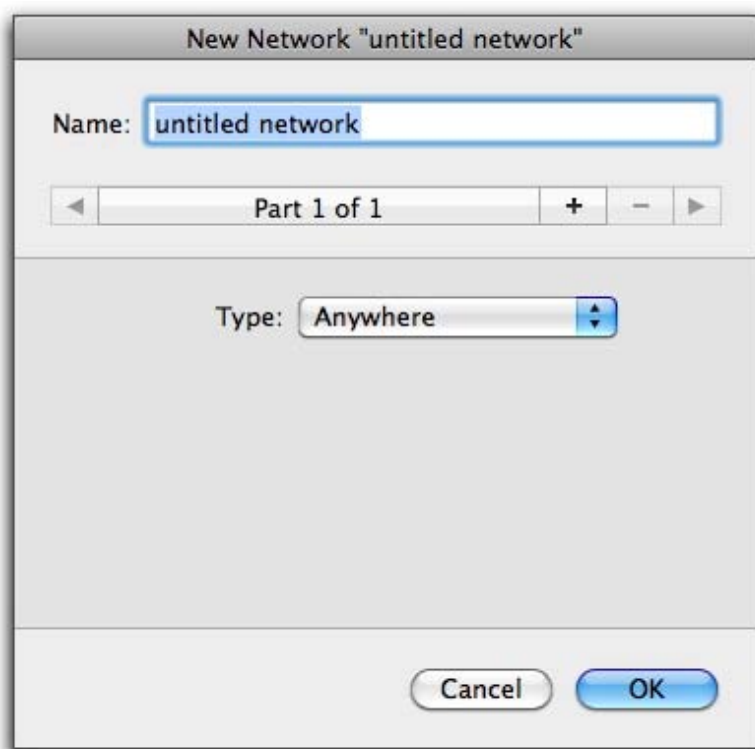
- **Internet:** The Internet, in addition to any local network you may be connected to; effectively, all networks.

You can create new sources and destinations to use in your rules. This allows you to specify exactly which computers you wish to have your server communicate with.

To create a new source, click the + button to the right of the Source or Destination popup menu. In our example, we'll create a new Source; however, once it's created, it will also show up in the list of possible Destinations.



The New Network editor displays.



Enter a name that will help you remember the network. If, for example, you're blocking IP addresses whose last octet is in the range of 100–155, you might name the Source/Destination "IPs from 100–155".

The pop-up menu offers a selection from seven types of network.





Name	Definition	Address Type
Anywhere	Any network.	None, as this source covers all networks.
My Mac	Your computer.	The IP address(es) of your server displays in the Address field, and cannot be changed.
My local network	The local network your computer is connected to.	The IP address(es) of your server and subnet mask of your local network display in the Address field, and cannot be changed.
Machine	A specific IP address.	Any IP address. If you enter a domain name, VirusBarrier Server 3 will resolve it to a single IP address.
Network	A specific network.	Any Subnet IP address and Subnet mask. As above, VirusBarrier Server 3 will resolve domain names to a single IP address.
Address Range	A group of IP addresses.	Beginning and ending addresses. VirusBarrier Server 3 will resolve domain names to a single IP address.
Ethernet ID	A single device connected to the network by Ethernet.	An Ethernet ID, as six two-character hexadecimal numbers.

Rule Services

"Service" refers to a combination of protocol type, port (or ports) used, and protocol-specific criteria. These items, taken together, typically describe a program or class of program that sends and receives information. For example, information sent by the TCP protocol over port 80 using HTTP would be a Web service.

VirusBarrier Server 3 comes with over 50 common services preprogrammed so you can easily stop (or allow) traffic that appears to be of a specific type.



While most preprogrammed Services clearly map to a specific program, some selections in this list such as "Web" pertain to a class of communications instead. Here are some of those non-specific Services:

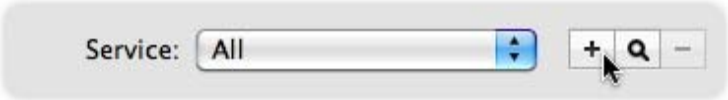
Name	Description	Settings
All	All communications, regardless of protocol or port.	All protocols, on all ports.
Apple Remote Desktop	A program that allows an administrator Mac to control another Mac over a network connection.	Port 3283 over UDP.
Connected Services	All TCP communications. A TCP session maintains a connection between computers, so it's always clear that it was initiated by the Mac and can therefore be trusted. By comparison, a UDP session is a series of communications without a "memory" of who initiated it.	All TCP communications, on any port.
FTP	File Transfer Protocol.	TCP, ports 20 or 21.
iChat AV	An instant messaging program with video and sound.	Port 5060 over UDP.
IRC	Internet Relay Chat.	TCP on port 194 for IRC, and all TCP traffic between ports

		6665 and 6669, inclusive.
iTunes Music Sharing	A way to share your iTunes music library over your local network.	Port 3689 over TCP.
Mail	E-mail communications.	TCP port 25 for SMTP, port 110 for POP3, port 143 for IMAP4, port 220 for IMAP3 port 389 for LDAP, and port 587 for message submission.
NTP	Network Time Protocol.	UDP on port 123.
SSH	Secure Shell.	TCP on port 22 using SSH.
Telnet	Remote login.	TCP on port 23 using telnet.
VNC	Virtual Network Computing, a graphical remote-control system.	TCP on ports 5900-5999.
Web	Web browsing, for example through a browser such as Safari.	TCP on ports 80 and 8080 through HTTP, and on port 443 on HTTPS.
Well-Known Ports	A large range of ports with long usage traditions in network communications.	TCP and UDP on all ports from 0 to 1023.

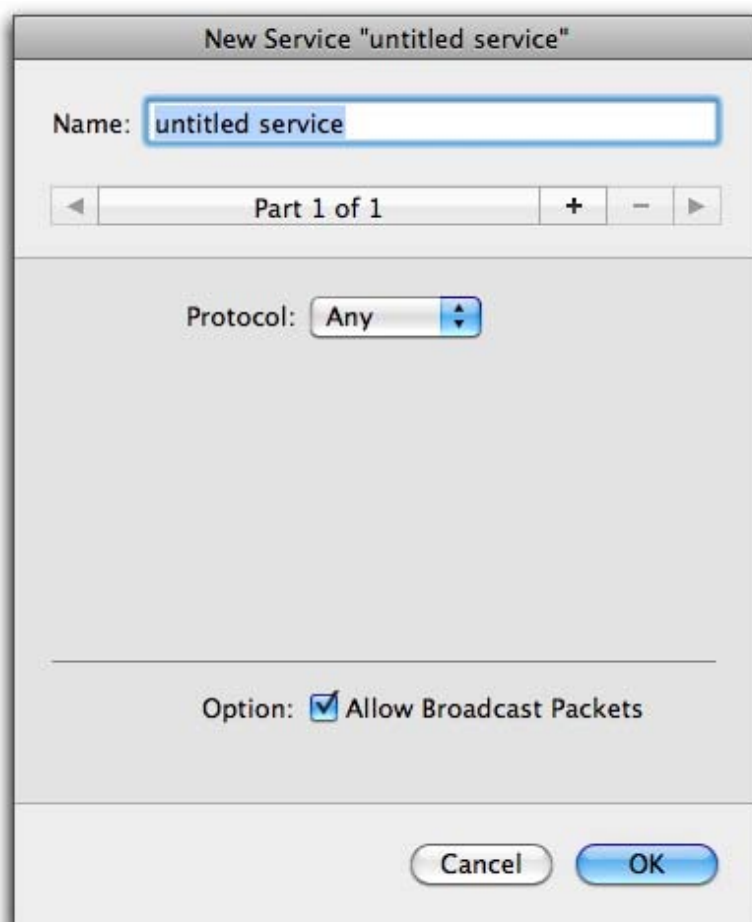
The remaining services are for specific programs or protocols.

Be careful when creating rules for specific services. When you select a service for a specific program, it is possible that this program uses the same port as another program or service. Blocking or authorizing a specific service may conflict with other, more general rules. For example, if you wish to block ICQ traffic, selecting ICQ as a service will also block AOL Instant Messenger traffic since both programs use the same port. Other programs may also share the same ports. If you find that you cannot connect to a given service, or send or receive traffic, try deactivating your rules one by one to see if there is a conflict.

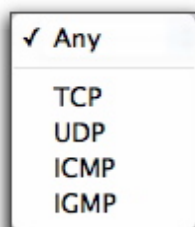
To create a new service, click the + button next in the Service section.



The New Service editor displays.



Four different protocol suites are available from the Protocol pop-up menu: TCP, UDP, ICMP and IGMP. You can also select Any, which covers all protocols.



When you select one of these protocol suites, additional options display in the bottom section of the panel, with a list of services that you can select from. The options depend on the protocol you selected.

**TCP or UDP** have the following options:

- **Any port:** Affects all ports.
- **Single Port:** Lets you specify a single port either by typing its number or by selecting from over a hundred options in the popup menu. (VirusBarrier Server 3 automatically fills in the correct number when you select from the popup menu.)
- **Range of Ports:** Lets you enter the beginning and ending port numbers that define a range.

**ICMP or IGMP** have the following options:

- **Any:** Affects all types.
- **Specific Type:** Lets you specify a single value either by typing its number or by selecting from over twenty options in the popup menu. (VirusBarrier Server 3 automatically fills in the correct number when you select from

the popup menu.) You can also specify a Code number, if necessary.

For each of these, an option is available to **Allow Broadcast Packets**. If checked, packets sent to all computers on a local network are included in this service.





Options: ☒ Allow Broadcast Packets  
☒ Destination Port

**Destination Port** is a final option, available only for services utilizing the UDP protocol. If it is checked, packets are filtered according to the function of the Destination Port. If left unchecked, packets are filtered according to the function of the source Port.

## Rule Interfaces

The Interface is the network adapter that the data passes through. This can be an Ethernet card, a wireless AirPort card, or any other type of network interface.

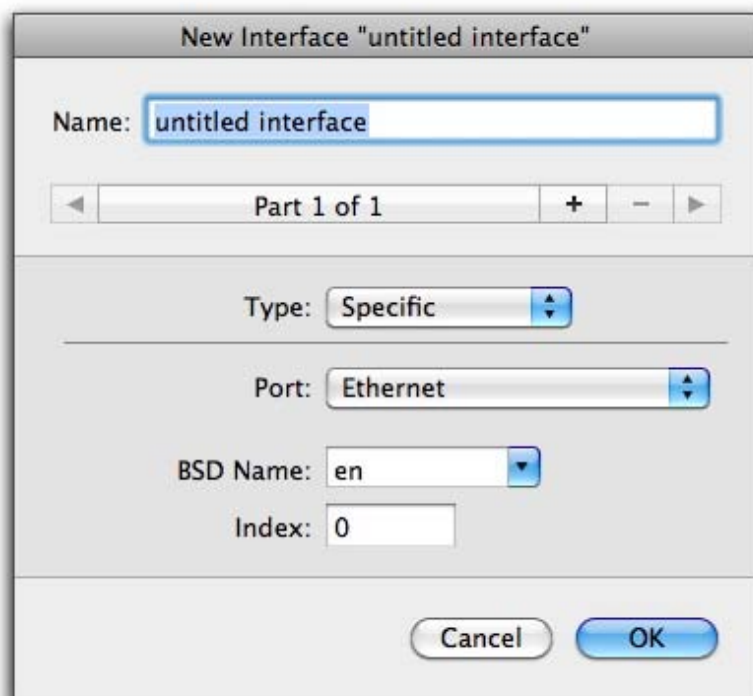
You can choose from a list of preprogrammed interfaces that exist on your computer, or you can create your own interfaces by clicking the + button.

Interface: Any    

The New Interface editor displays.



The Type pop-up menu has two options. The first, **Any**, uses all available network interfaces. The second, **Specific**, lists those interfaces that are available to you, depending on your computer's hardware and software, and gives you some additional options.



Typical interfaces are:

- **Airport:** Wireless networking
- **Built-in Ethernet:** Wired interface commonly used for networking
- **Built-in FireWire:** Wired interface commonly used for peripherals, such as a hard drive, but which can also be used as a network interface

The BSD Name and Index number are the identifiers used by the Unix layer of Mac OS X. You can set these manually, if you need to. (You probably won't have to, and shouldn't change them if you don't understand what they are.) If other interfaces are present in your server, an **Other** option will also be available.

## Rule Actions

Two actions are possible for any rule: Allow or Deny. Select the action you wish to use for your rule by checking the appropriate radio button, at the bottom of the Rule Editor window.

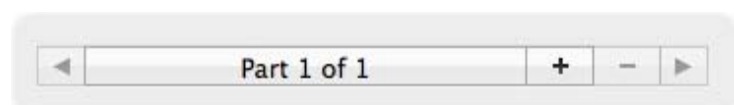


Finally, click **OK** to add this rule to your VirusBarrier Server 3 firewall rules.

## Multi-Part Sources, Destinations, Services and Interfaces

Rule sources, destinations, services and interfaces can have several parts. You can, for example, dictate that traffic from several specific IP addresses be banned, listing each one separately in a given Source.

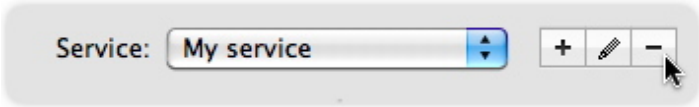
When you create or edit a source, destination, service or interface, you see a bar at the top of the window that looks like this:



- **Create a new part:** Click the + button.
- **Move among parts:** Click the arrow icons. Note that the text in the middle will tell you where you are, and how many parts exist in total. When you reach the last part, clicking the right arrow takes you back to the first one.
- **Delete a part:** To delete a part, it must be visible. Click one of the arrow icons until the part you wish to delete is displayed. Click the – button, then confirm the deletion in the dialog box that follows.

### Deleting Sources, Destinations, Services and Interfaces

You can delete any sources that you have created. To do so, select the source, and then click the – button.



A dialog box displays, asking if you really want to remove that network. Click Remove to delete the source network, or Cancel if not.

### Working with Rules

#### Rule Order

Rules you add to VirusBarrier Server 3's firewall are applied from first to last, so you need to make sure that your rules are in the correct order to function properly.

#	Name	Interface	Source	Destination	Service	
01	<input checked="" type="checkbox"/> Input	Any	Internet	My Mac	All	STOP
02	<input checked="" type="checkbox"/> Output	Any	My Mac	Internet	All	GO
03	<input checked="" type="checkbox"/> Network	Any	Local Network	My Mac	All	GO

In this example, the first rule blocks data coming from the Internet (which includes all networks, even a local network). Rule 3 allows traffic from a local network; but since it's in 3rd position, it is not applied; the 1st rule takes precedence. For rule 3 to be applied, it needs to be moved to the top of the rule list. To do this, select the rule and drag it to the appropriate position.

#	Name	Interface	Source	Destination	Service	
03	<input checked="" type="checkbox"/> Network	Any	Local Network	My Mac	All	GO
01	<input checked="" type="checkbox"/> Input	Any	Internet	My Mac	All	STOP
02	<input checked="" type="checkbox"/> Output	Any	My Mac	Internet	All	GO
03	<input checked="" type="checkbox"/> Network	Any	Local Network	My Mac	All	GO

#### Editing and Deleting Rules

To edit a rule, select the rule by clicking it, then click the button with the pencil icon at the bottom of the list. The Rule Editor will open, and you can make any changes you want to this rule. When you have finished making changes, click OK to save your changes. If you decide you do not want to save the changes, click Cancel.

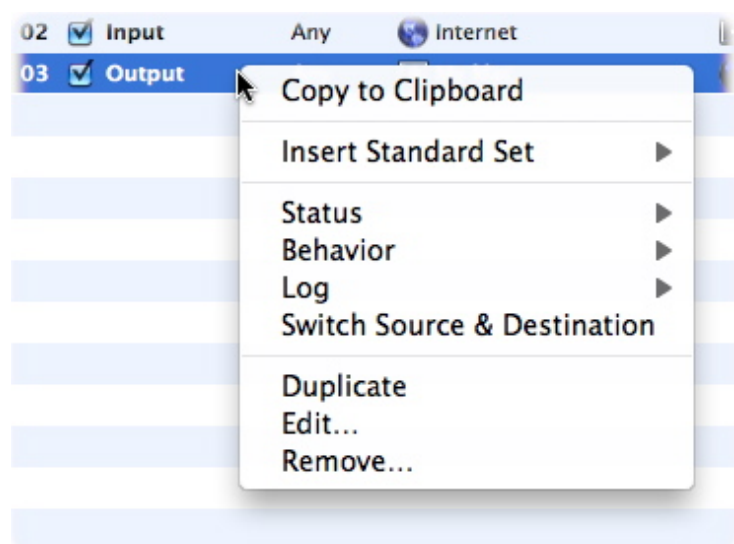
To delete a rule, click the rule in the list of rules, then click the – button at the bottom of the list.

#### Using the Rule Contextual Menu



VirusBarrier Server 3 lets you make changes to Firewall Rules quickly through a contextual menu. You can use this contextual menu to add new rules, to edit existing rules, or to change rule characteristics on the fly.

To see this contextual menu, right-click on a rule.



The menu offers the following options:

- **Copy to Clipboard:** Copies the contents of a Rule to the Mac's Clipboard in plain-text format. You can then paste the rule into a document, where it will look something like this: "#02/ON/Input/Any/Internet -> My Mac/All/Deny" (where slashes are tabs).
- **Insert Standard Set / Add Standard Set:** Insert or add a standard set of rules, from the same selection as is found in simple mode: No restrictions, No network, Client, Local Server, Server only, or Client only.
- **Status:** You can toggle the state of a rule, turning it On or Off. If the rule is scheduled to run at certain times, a check mark is displayed next to Scheduled in the submenu.
- **Behavior:** Toggle the behavior of a rule between Allow or Deny traffic.
- **Log:** Toggle whether the rule records traffic information in the log.
- **Switch Source & Destination:** "Reverses" a Rule, exchanging the source and destination.
- **Duplicate:** Makes a new copy of the Rule.
- **Edit...:** Opens the Rule Editor for the indicated Rule.
- **Remove...:** Deletes the Rule.

[« VirusBarrier Server 3 Preferences and Configurations](#)