Reference Guide

PortsLock®

SmartLine Inc

Contents

Using this guide....3

1. Overview 4

1.1 Introduction 4
1.2 General Information....4
1.3 Technical Data 5
1.4 Requirements....6
1.5 Main Purpose 6

2. Installation 7

3. Interface 9

2.1 General Information....9
2.2 Main Dialog 9

4. Principles of Packet Filtering 11

5. Principles of Packet Auditing....12

6. Setting Up Rules....15

6.1 Setting Up Security Rules....17
6.2 Setting Up Audit Rules 22

7. Batch Processing....24

8. Monitoring....26

9. Deployment Examples 29

Using this guide

This guide assumes you're familiar with basic functions like click, right-click and double-click, and that you're familiar with the basics of the operating system you're using. Also, we use the following conventions:

- *Italics* for file names, paths, buttons, menus, and menu items.
- ***Bold Italics*** for notes and comments.
- Keyboard keys with a plus sign separating keys that you press simultaneously. For example: press Ctrl+Alt+Del to restart your computer.

We strongly recommend to read this guide very carefully and thoroughly. It was designed around the understanding that its users already have basic network knowledge as well as the ability and know-how to install a Local Area Network (LAN).

1. Overview

1.1 Introduction

PortsLock® is a firewall with user-level access controls for Windows NT/2000/XP and Windows Server 2003. Once PortsLock is installed, administrators can assign permissions to TCP/IP connections, just as they would in managing permissions on an NTFS partition of a hard disk. It lets you control which users can access what TCP/IP based protocols (HTTP, FTP, SMTP, POP3, Telnet, etc.) on a local computer, depending on the time of day and day of the week. You can also set allowed/denied TCP/UDP ports and IP addresses for incoming and outgoing connections. PortsLock enhances access control possibilities for system administrators, helps them to build a more secure network environment, and protects corporate networks against attacks from the inside.

It is important to note that PortsLock works perfectly with other personal firewalls and routers installed on the same computer.

1.2 General Information

PortsLock operates at the transport (TDI) level. Data is only allowed to leave the local system if the PortsLock rules allow it. As packets arrive they are filtered by their type, source address, destination address, port information contained in each packet, and the security context. Unlike other personal firewalls, PortsLock's packet filtering is based not only on networking rules (such as source and destination addresses, ports, protocols, etc.) but also on the user's security context. It means that administrators can assign different filtering rules to different users or user groups and these rules will apply to network packets "on the fly", exactly like file permissions in an NTFS partition.

PortsLock is absolutely transparent to users. Users do not have to set up rules in their applications to use the network. Only administrators are allowed to set rules so users without administrative privileges cannot bypass the PortsLock security.

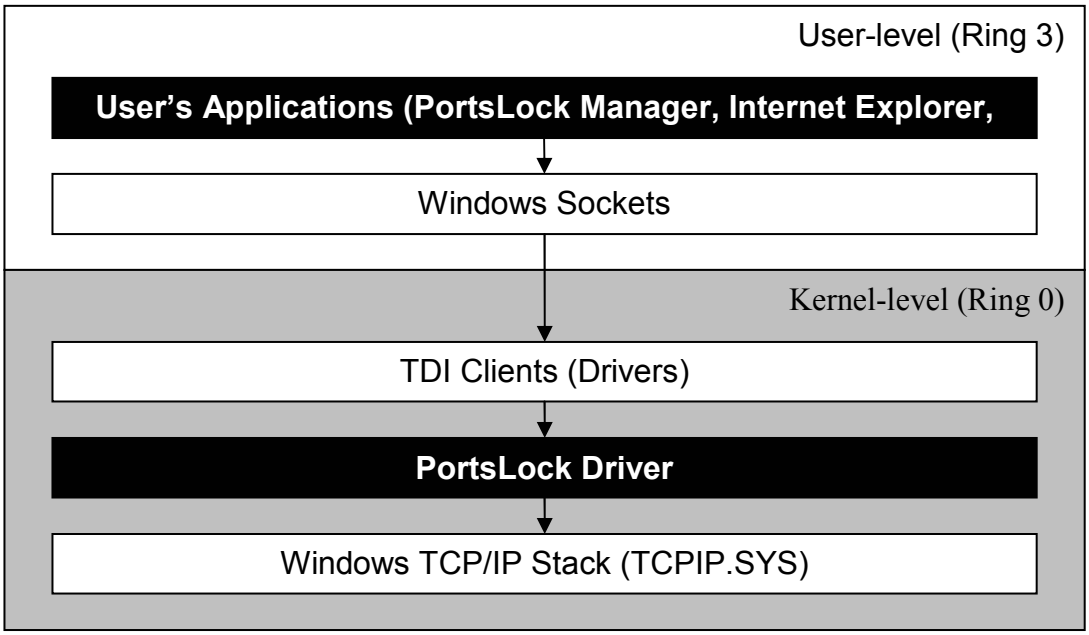
In addition to packet filtering, PortsLock adds the ability to audit network packets on a local computer. This packet auditing is also based on the user's security context and allows you to audit network packets that belong to a certain user or user group. PortsLock employs the standard event logging subsystem and writes audit records to the Windows event log so they can be read using any event viewer software (such as *EventViewer*, *Remote Task Manager*, etc.) as well as PortsLock's built-in *Audit Log Viewer*.

Moreover, PortsLock has a real-time monitor of TCP/IP network activity. PortsLock specifies which process and user are associated with what TCP/IP address and provides detailed information about every network activity.

1.3 Technical Data

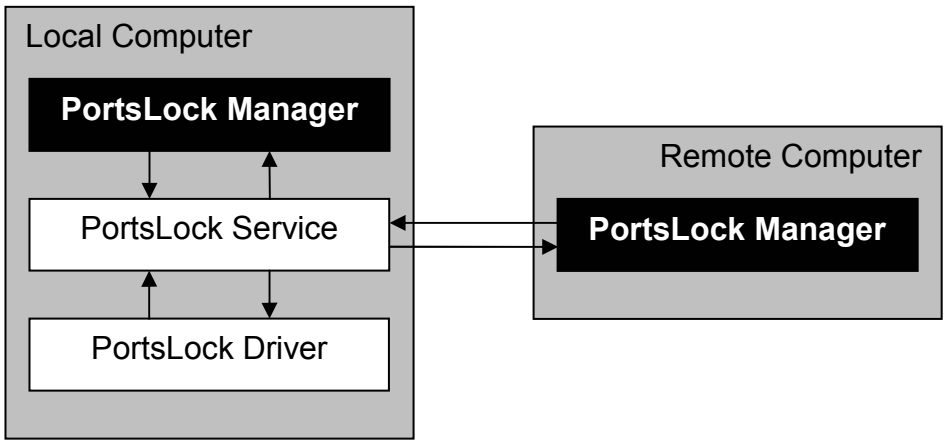
PortsLock consists of tree parts: PortsLock® Driver, PortsLock® Service (*plservice.exe*), and PortsLock® Manager (*plmanager.exe*).

PortsLock Driver is the core of PortsLock. It is implemented as a special low-level driver tightly integrated into the system kernel. This driver fully controls the system's driver *TCPIP.SYS*. Therefore, it has absolute control over all packets passing to *TCPIP.SYS* and is able to ensure complete protection of the system it is operating on.



PortsLock Service is installed on each client system that you want to protect. PortsLock Service runs automatically in the background and provides communication with PortsLock Driver.

PortsLock Manager is the control interface Systems Administrators use to manage each network computer that has PortsLock Service.



1.4 Requirements

PortsLock works on any computer using Windows NT/2000/XP and Windows Server 2003.

To use PortsLock, you must have a functioning TCP/IP network protocol.

1.5 Main Purpose

The following are a few examples of PortsLock uses:

- Blocking access to network resources (web sites, network services, LAN, etc.) for a particular user or user group.
- Controlling access to network resources, depending on the time of day and day of the week.
- Auditing network activity for a particular user or user group.
- Real-time monitoring of applications' network activities and discovery of malicious programs (viruses, Trojans, etc.).

2. Installation

To install PortsLock just run Setup (*setup.exe*).

PortsLock installs to the directory of your choice. Setup tries to find a PortsLock installation and, if one exists, Setup suggests you install PortsLock to the same directory. If a previous installation does not exist, Setup suggests you install PortsLock to the Program Files directory on the system drive (e.g. *C:\Program Files\PortsLock*). You can always select another directory for installation.

You have three choices: install both PortsLock Manager and PortsLock Service using Typical setup, install only PortsLock Manager using Custom setup, then selecting the *PortsLock Manager* component, or you can install only PortsLock Service using Custom setup, then selecting the *PortsLock Service* component.

Also, Setup supports unattended (silent) setups. This gives an install that can be used from within a batch file. If you want to install PortsLock without user intervention run Setup with the */s* parameter (e.g. *c:\setup.exe /s*). There is a special configuration file for silent setups — *portslock.ini*. *Portslock.ini* must be in the same directory where *setup.exe* is located. With this file, you can customize the installation parameters. For example, to install only PortsLock Service, *portslock.ini* should look like:

[Install]
Service = 1
Manager = 0
Documents = 0

If you have purchased a license for PortsLock, you can also specify the location of its registration file in the *portslock.ini* file so Setup automatically registers new versions of a PortsLock:

RegFileDir = C:\Directory

where *C:\Directory* is where your registration file is located.

You can also specify a destination directory for PortsLock:

InstallDir = C:\Program Files\PortsLock

If you want to run a program (e.g. batch file) after a successful install, you can specify the *Run* parameter:

[Misc]
Run = C:\mybatchfile.bat

PortsLock supports remote installation to help a Systems Administrator to set up a service on remote machines without ever having to physically go to them. If the PortsLock Service isn't installed on the remote system you are trying to connect to, PortsLock Manager will suggest that you install the service. Select the PortsLock Service executable file (*plservice.exe*) and PortsLock Manager will copy it to the remote computer. The PortsLock Service executable file will be copied to the Windows system directory (e.g. *c:\winnt\system32*) if this service doesn't exist on this system. If the service exists on this system but is too old, PortsLock Manager will copy the executable file to the directory of the old file and the old file will be replaced.

After a successful install, you can run PortsLock Manager by selecting the *PortsLock Manager* item from the *Programs* menu.

3. Interface

2.1 General Information

PortsLock Manager has a user-friendly, easy-to-use interface. All functions can be accessed with either a mouse or keyboard.

In any dialog you can press the *F1* button to get specific help.

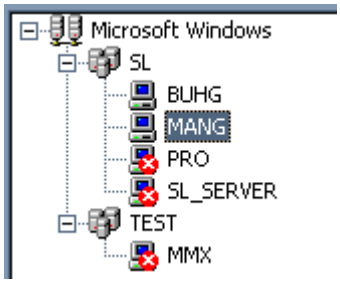
The main window of PortsLock Manager can be resized. PortsLock Manager saves its size and position, and restores these at its next startup.

PortsLock Manager has a menu at the top of its main window. Many functions are accessible through this menu.

You can select *Always on Top* from the *View* menu to keep the PortsLock Manager on top (above) any other applications.

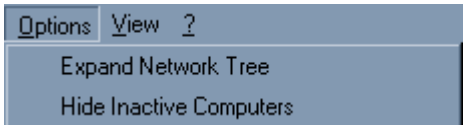
2.2 Main Dialog

When you start PortsLock Manager it displays its main dialog where you can select a computer to control.



The left side of the Main dialog shows a list of the computers available in your network. This listing is called the *computer tree*. Each computer that is running PortsLock Service has an icon of a computer. Each computer without PortsLock Service running on it has an icon of a computer overlaid by a red circle containing a white **X**, indicating the computer is inactive. A computer will also show as inactive if you do not have the system privileges to connect to it.

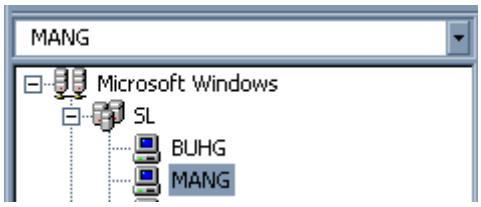
If you want a listing of only active computers — computers with running and accessible PortsLock Service — select *Hide Inactive Computers* in the *Options* menu. If you do not want the computer tree to expand automatically, unselect *Expand Network Tree* in the *Options* menu.



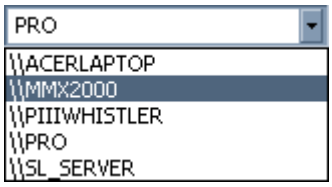
To refresh a list of computers, press F5 or select *Refresh Network Tree* from the *View* menu. Also, you can refresh the state (whether active or inactive) of a selected computer by pressing Shift+F5 or selecting *Refresh Selected Computer* from the *View* menu.

If your computer is not connected to a network, the list of computers will be empty or may contain only a single record — "Microsoft Windows Network" (or similar message).

To access a remote computer, it needs to have PortsLock Service installed and running, and it needs to have a connection to your computer. To access a remote computer, simply select it from the computer tree. PortsLock Manager automatically connects to the computer immediately after it has been selected. You can use a mouse to select the computer or you can use the keyboard's arrow keys and press Enter on a selected computer. Alternatively, you can type in the computer's name in the field above the computer tree, then press Enter.

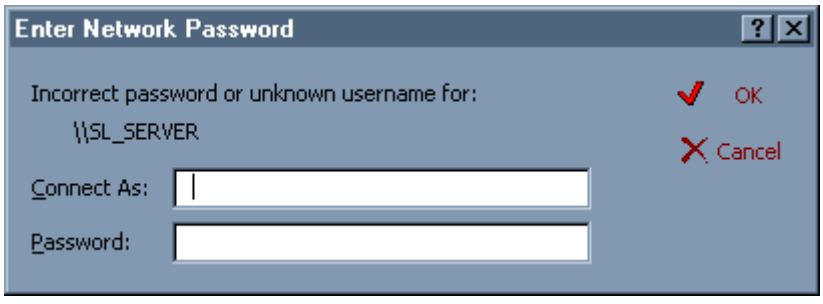


To connect to the local computer, do not specify a computer name. If *Connect to Local Computer at Startup* is enabled in the *Options* menu, PortsLock Manager automatically connects to the local computer each time it starts up.



All frequently used computers are added automatically to the most recently used (MRU) list so they can be easily accessed.

If you don't have administrative privileges on the selected computer, PortsLock Manager will show the **Enter Network Password** dialog and you'll be able to connect under the account of any other user. The **Enter Network Password** dialog appears when you attempt to connect to a computer, but the domain controller (DC) does not recognize the user account you have used to log on. This often occurs when you are logged on as the administrator of a local computer and attempt to access domain resources. To access the domain resources, you must provide a valid user account and password that the domain recognizes. User accounts are a domain name followed by a backslash (\) and the user name, e.g. *D1\John*.



If you successfully connect to a computer, its name appears in the status bar of PortsLock Manager. All major PortsLock Manager functions become available only if you are connected to a computer.

4. Principles of Packet Filtering

To achieve security, you need to define a set of security rules for PortsLock so it can determine if a packet should be allowed to pass or not. To do this, PortsLock looks through its set of security rules for a rule that matches the user who owns the packet and the contents of the packet's header. Once a match is found, the rule action is followed. The rule action could be to block (*Deny*) the packet or to forward (*Permit*) the packet. Only the first match counts, as the rules are searched in order.

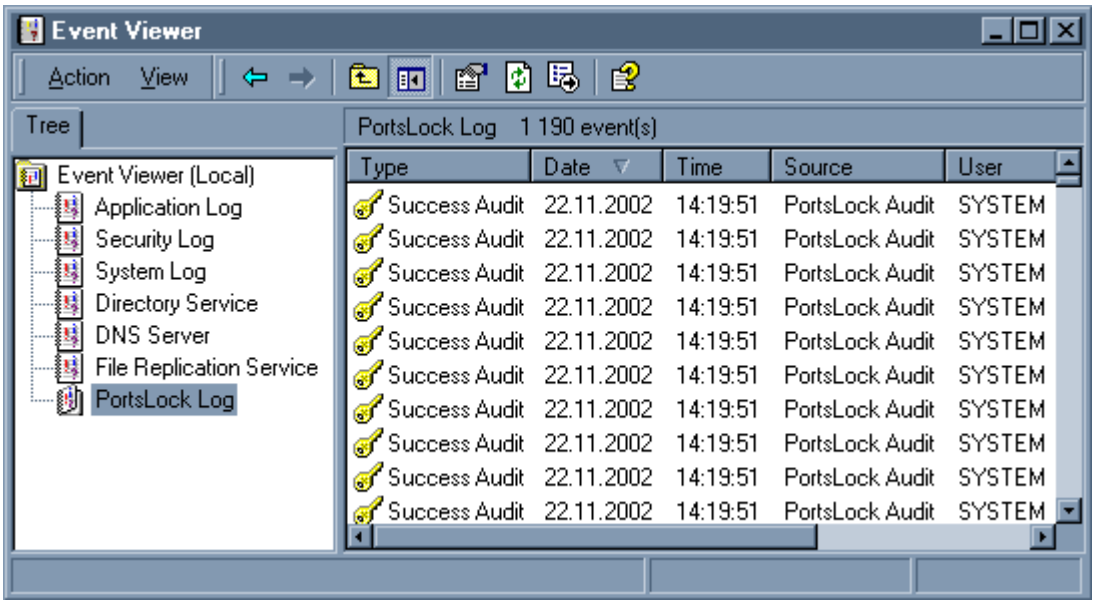
The packet matching criteria varies depending on the protocol. You can specify rules that depend on the source IP address of the packet, its destination IP address, the source port number, the destination port number (for protocols that support ports), the packet's direction (incoming or outgoing), the user or user group that owns the packet, and even the time of day and day of the week the rule is active. This wide range of matching criteria allows you to create a very flexible and secure network environment.

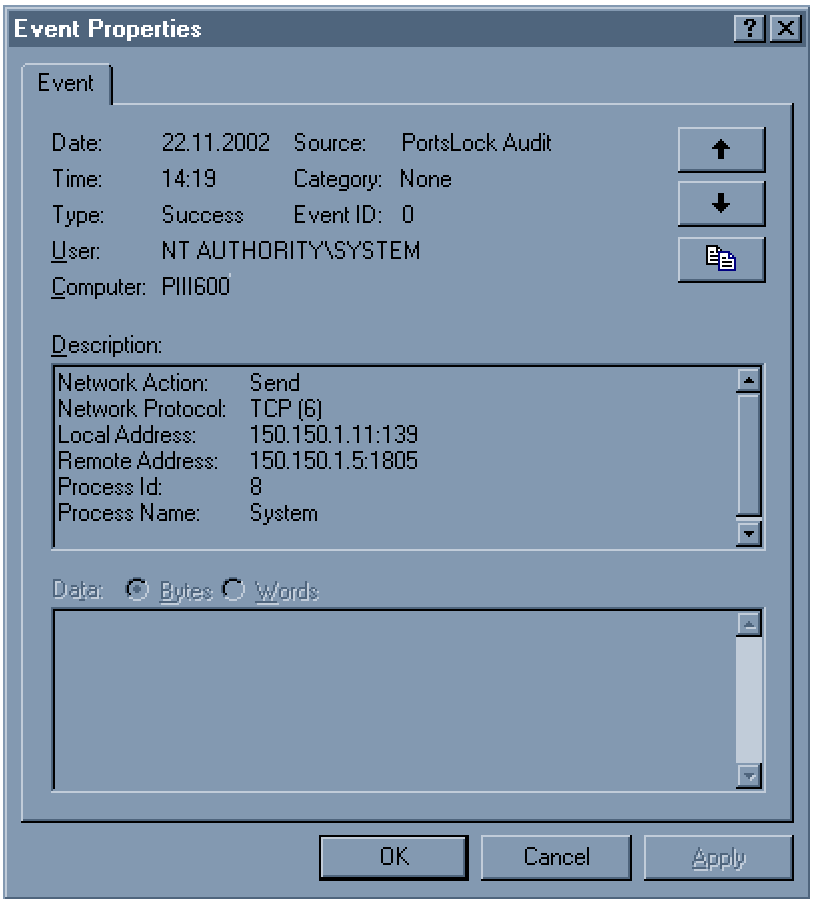
5. Principles of Packet Auditing

To audit a user's network activities, you need to define a set of audit rules for PortsLock so it can decide if information about a packet should be logged or not. To determine if a packet should be logged, PortsLock looks through its set of audit rules for a rule that matches the user that owns the packet and the contents of this packet's header. Once a match is found, the rule is applied. Only the first match counts, as the rules are searched in order.

The packet matching criteria is the same as for security rules (see the **Principles of Packet Filtering** section of this manual).

PortsLock uses the standard event logging subsystem to log a packet's information. It is extremely useful for system administrators because they can use any event log reading software to view the PortsLock's audit log. You can use the standard *Event Viewer*, for example.





PortsLock has its own built-in event viewer that represents information in a more convenient form.

Type	Date/Time	Local Address	Local Port	Remote Address	Remote Port	Protocol	Action
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Send
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Send
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Event Receive
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Send
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Event Receive
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Send
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Event Receive
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Send
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Event Receive
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Send
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Event Receive
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Send
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Event Receive
Success	22.11.02 14:19:51	150.150.1.11	139	150.150.1.5	1805	TCP (6)	Send

The columns in the audit log viewer are defined as follows:

- *Type* – the class of an event, either *Success* for allowed packets or *Failure* for denied packets.
- *Date/Time* – the date and the time when this event was received by the logging service.

- *Local Address* – the local IP address of the endpoint.
- *Local Port* – the local port of the endpoint, if applicable.
- *Remote Address* – the remote IP address of the endpoint, if applicable.
- *Remote Port* – the remote port of the endpoint, if applicable.
- *Protocol* – the protocol (*TCP*, *UDP*, *ICMP*, etc.) of the endpoint.
- *Action* – the network activity type. This can be *Connect*, *Listen*, *Accept*, *Disconnect*, *Send*, *Receive*, and so on.
- *User* – the name of the user that owns the endpoint.
- *PID* – the identifier of the process that owns the endpoint.
- *Process* – fully qualified path to the process executable file. In some cases, the process name may be displayed instead of the path.

6. Setting Up Rules

It is important to understand the internal logic of PortsLock's packet filtering and auditing before creating rules.

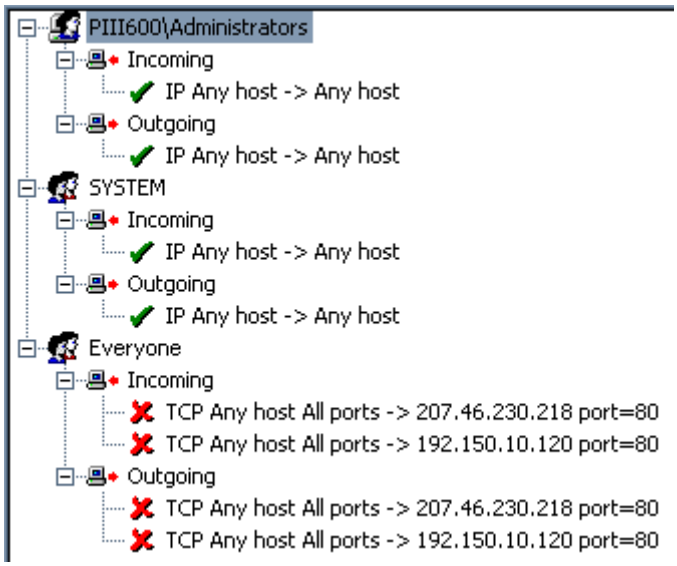
There are two types of rules in PortsLock – security and audit.

- Security rules are responsible for packet filtering. Each security rule follows one of two actions: *Permit* or *Deny*. If you choose to deny a packet, PortsLock will send back a response to the requesting application indicating that the connection attempt was refused. *Permit* simply allows the packet to be routed to its destination.

- Audit rules are responsible for packet auditing. Each audit rule can have one of two actions: *Active* or *Inactive*. *Active* means the rule takes effect on packet auditing. *Inactive* means the audit rule is to be ignored. You can audit allowed packets, denied packets or both types. If you choose to audit only allowed packets, PortsLock will write a record to the Event log each time a packet is routed to its destination. If you are auditing denied packets then PortsLock writes a record to the Event log only when the connection attempt is refused because of the matched security rule.

PortsLock can have separate rules for each user or user group on your computer. It means that you can assign different rules to different users working on a local computer. Moreover, you can audit packets that belong to particular users. This is possible because PortsLock was developed as a firewall with user-level access control and it is tightly integrated into the Windows security subsystem. PortsLock handles network packets and connection requests exactly as Windows handles requests to the files and folders on an NTFS partition.

Each rule belongs to a user or user group so together they form a tree. Please note that rules can be set for both incoming and outgoing traffic.



Users and rules are applied from top to bottom. When a packet reaches PortsLock, it is checked against the list of users and rules:

1. PortsLock looks at the top user or user group first, then goes down the list and finally checks the lowest user or user group.

2. If the packet's security context does not correspond to a user or user group then PortsLock continues down the list with each user or user group. If there are no more users or user groups on the list, PortsLock allows the packet to pass through without applying any rules to it.

3. If the packet's security context corresponds to a user or user group, PortsLock checks that user's or group's rules (see next).

4. PortsLock looks at the top criteria first and goes down the list checking to the lowest rule last.

5. If a packet meets the criteria of a rule, that rule is applied and the rest of the users and rules are ignored. For this reason, it is best to place all rules that allow at the top.

6. If a packet does not meet the criteria of a rule then PortsLock continues down the list taking each rule in sequence. If there are no more rules for the current user or user group, PortsLock takes the next user or user group.

Rules may apply to:

- Stand-alone IP hosts
- Range of IP addresses
- The whole subnet or network.

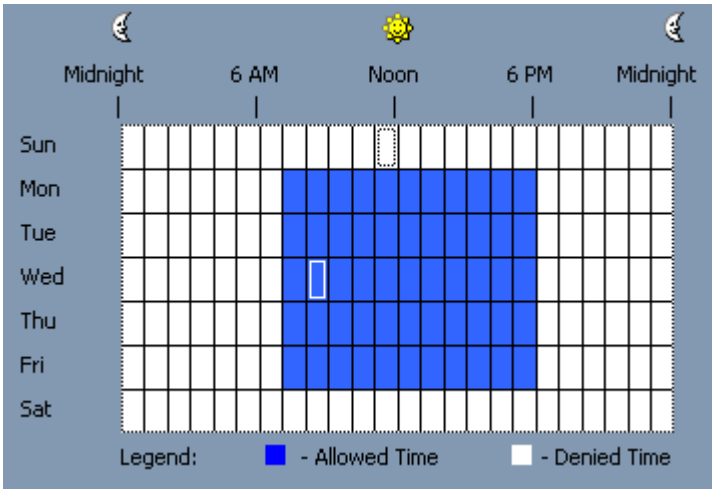
PortsLock supports these IP based protocols:

- *TCP*
- *UDP*
- *ICMP*
- *Raw IP*
- *Other (by protocol number).*

The ability to allow or deny a protocol by its number (*Other*) is extremely important to network administrators faced with a constantly growing list of application requirements to support. Granting this, PortsLock allows you to set rules even for new and unknown protocols.

For protocols that support ports (*TCP* and *UDP*), PortsLock can have rules that will contain not only IP addresses but also port numbers. It allows you to permit or block access to specific network services that reside at specific ports.

It is important to note that rules can be applied at predetermined time intervals. In some cases, it may be useful to apply particular rules during office hours and different criteria for after hour access.



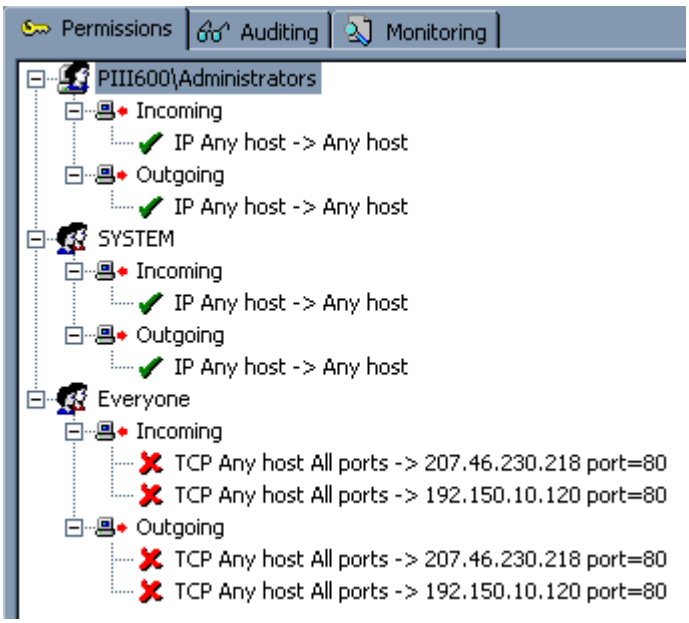
You can define an interval when a selected rule will *Permit* (for security rules) or is *Active* (for audit rules) and when this rule becomes *Deny* (for security rules) or *Inactive* (for audit rules). It means that the same rule can invert its type of action depending on the time of day and day of the week. Hence, there are three action types for rules:

- *Permit* or *Active*
- *Deny* or *Inactive*
- *Time-dependent*

6.1 Setting Up Security Rules

As noted above, security rules are responsible for packet filtering. It means that by using security rules you can permit or block a user's access to the network.

To manage security rules, select the *Permissions* tab.

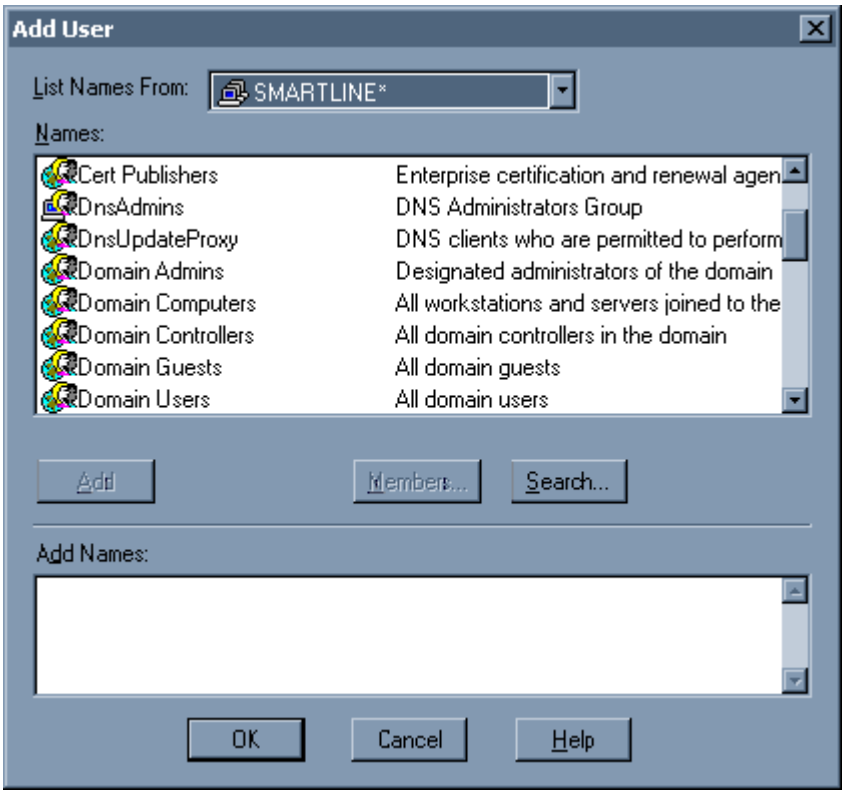


When you open the *Permissions* tab for the first time, the permissions list is empty, i.e. doesn't contain any users or user groups and their rules. An empty permissions list means that there are no rules to apply, so all network packets will be allowed to pass through.

There are a few simple steps to define permissions:

1. Add the user or user group.

   At first, you have to decide for which user or user group you would like to set rules. To add a new user or user group to the list, click on the *User* button. You can add several accounts simultaneously.



   To delete a user or user group from the list, highlight its record and press the *Delete* button.

   Users and user groups in PortsLock are searched on this list from the top down. To change the order of users and user groups on the permissions list, use the *Move Up* and *Move Down* buttons at the top right side of the *Permissions* tab.

> **!** If you add the Everyone user at the top of the list then all subsequent users and user groups will have no effect on packet filtering. For this reason, it is best to place the Everyone user at the end of the permissions list.

2. Add or edit the rule.

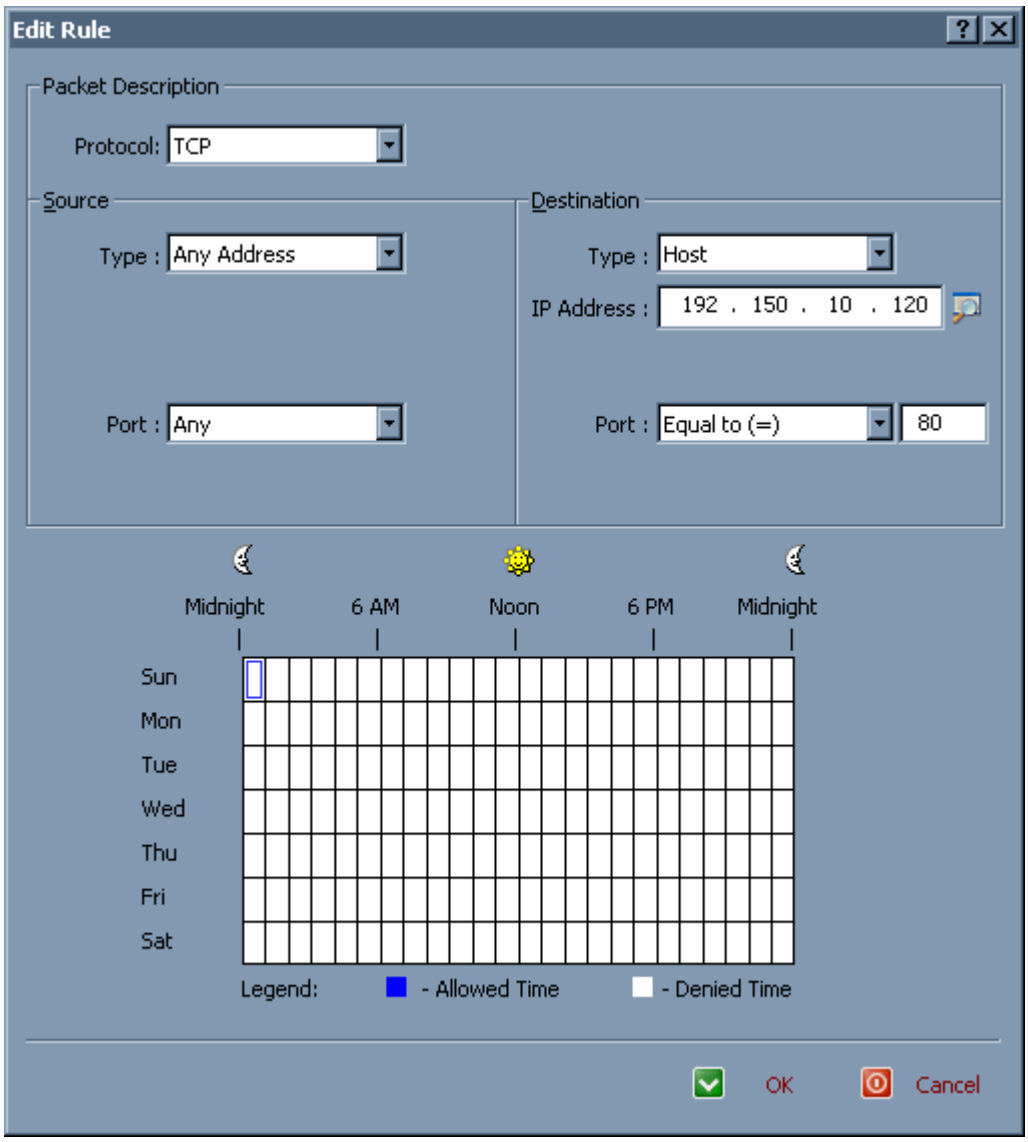
   To enable packet filtering it is not enough to just add the user or user group. You should also specify the rules that will be used to filter all packets for that user or user group.

   Different rules can be set separately for incoming and outgoing traffic:

   - *Incoming* – all network packets that are coming to the local computer from outside. By defining incoming rules, you can deny applications on a local computer to receive data from any source.

   - *Outgoing* – all network packets that are going from the local computer to outside. By defining outgoing rules, you can deny applications on a local computer to send data to any source.

   To add either an incoming or outgoing rule, press the *Rule* button. To edit a rule, either double-click it or select it and press the *Edit* button.



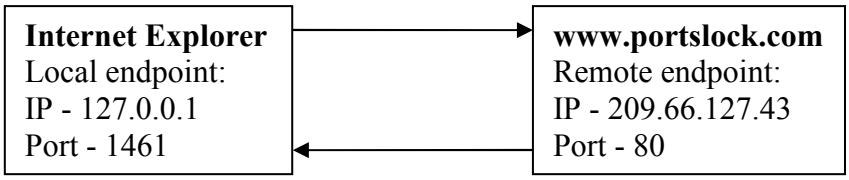
The first step is to describe the packet you wish to be filtered by this rule.

One of the main packet's description parameters is its protocol. Please note that PortsLock supports only TCP/IP based protocols (for more information please see the **Setting Up Rules** section of this manual). Select the protocol from the *Protocol* combo box at the top, left side of the dialog.

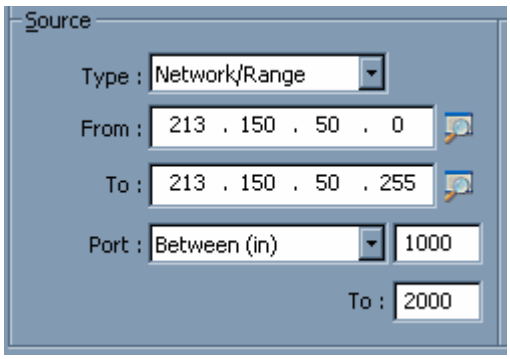
If you select the *Other* protocol then you have to enter its protocol's number in the editbox. For example, some protocols, such as *IPSec*, work over IP protocols 50 and 51, so it is only possible to filter them by their numbers.

> **!** Note that the *IP* protocol includes all other protocols. It means that if there are two rules: a rule for the *IP* protocol at the top of the list and below it is a rule for any other protocol (*TCP*, *UDP*, *ICMP* or *Other*) then the packet will be filtered by the first rule and the second one will be ignored even if the packet contains a protocol that is obviously specified in the second rule. For this reason, it is better to place rules with the *IP* protocol at the bottom of the user rule list.

The next step of describing the packet is defining its local endpoint and remote endpoint. ***It is very important to clearly understand what local and remote endpoints are. For example:***



For each rule, set a source IP address. It can be specified as:



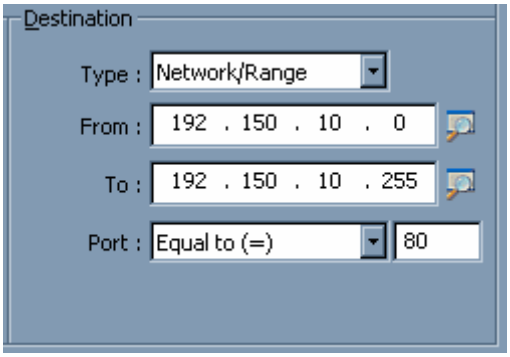
- *Any Address* – any IP address.
- *Host* – a particular IP address.
- *Network/Mask* – an entire sub-network.
- *Network/Range* – an IP address range.

Also, for *TCP* and *UDP* protocols it is necessary to set a source port. Possible options are:

- *Any* – any port.
- *Equal to* – a port that is identical to the defined value.
- *Greater than* – all ports that are greater than the defined value.
- *Less than* – all ports that are less than the defined value.
- *Not Equal to* – all ports that are different from the defined value.
- *Between* – all ports that are between the two defined values.
- *Not Between* – all ports that are outside of the two defined values.

Typical settings for a packet's source are: "Any host All ports".

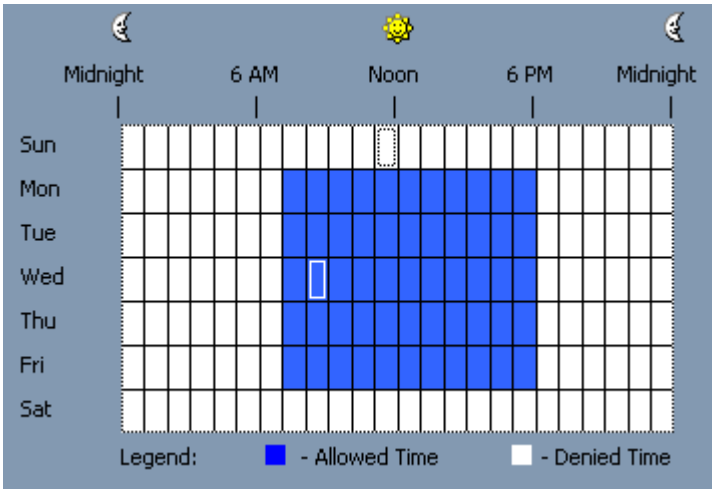
In exactly the same way as defining a packet's source you have to define its remote endpoint.



Set a destination IP address and port. There is no difference in the process of defining a packet's source and destination, so all parameters have the same meanings.

By defining the protocol, source and destination, you are completely describing the packet, but there remains the final step of setting up a rule – defining its time interval.

Using special time controls you can define a time when the rule will act as a *Permit* rule and when it will act as a *Deny* rule. "Time control" appears at the bottom of the dialog. Use the left mouse button and select the allowed time. To select a denied time, use the right mouse button. You can also use the keyboard to set times, the arrow keys for navigation and the spacebar to toggle an allowed/denied time.



That's all there is to it. Now you can arrange the rules in the order that best suits your needs. Don't forget that rules are processed from the top of the list to the bottom (see the **Setting Up Rules** section of this manual). To change the order of rules, use the *Move Up* and *Move Down* buttons at the top, right side of the *Permissions* tab.

Please note that rules take effect immediately as they are added to the list.

! There are several potentially dangerous security rule settings that could make a local computer inaccessible from the network. We recommend that you:

1. Add the SYSTEM user and the Administrators group to the top of the list and allow them all IP traffic in both directions ("*IP Any host -> Any host*"). This will allow the local system and administrators to work normally.

2. Do not add the *Everyone* user with any *Deny* rule at the top of the list. It could block ALL network packets and a local computer will be completely inaccessible from the network.

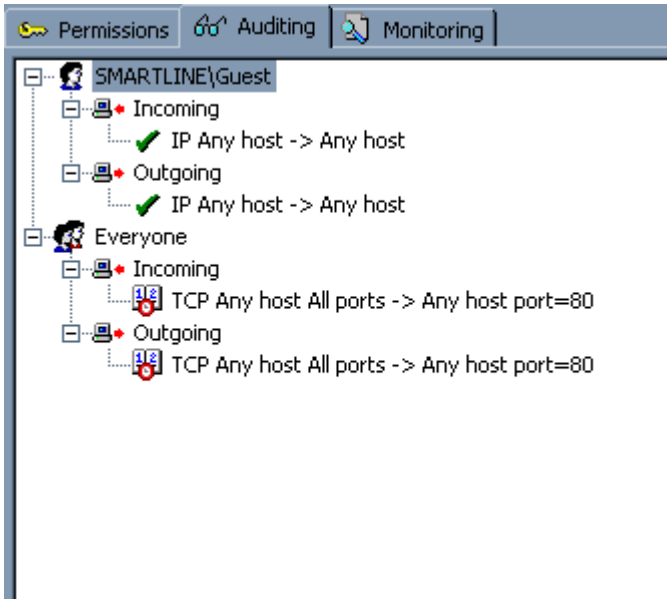
3. Do not block the TCP port 139 and UDP ports 137,138 for users or user groups that should be able to access the local network's resources (printers, shares, etc.).

4. Do not block TCP ports above 1024 for users or user groups that should be able to use PortsLock Manager and other remote management tools (such as *Remote Task Manager*, *DeviceLock Manager*, etc.).

6.2 Setting Up Audit Rules

As noted above, audit rules are responsible for packet auditing. This means that by using audit rules you can audit a user's access to the network.

To manage audit rules, select the *Auditing* tab.



There is not much difference between setting up audit and security rules so read the **Setting Up Security Rules** section of this manual before defining audit rules.

You can audit two types of packets:

- *Allowed* – all packets that were permitted by PortsLock, i.e. packets were routed to their destination.

- *Denied* – all packets that were blocked by PortsLock, i.e. packets were refused because of the matched security rule.

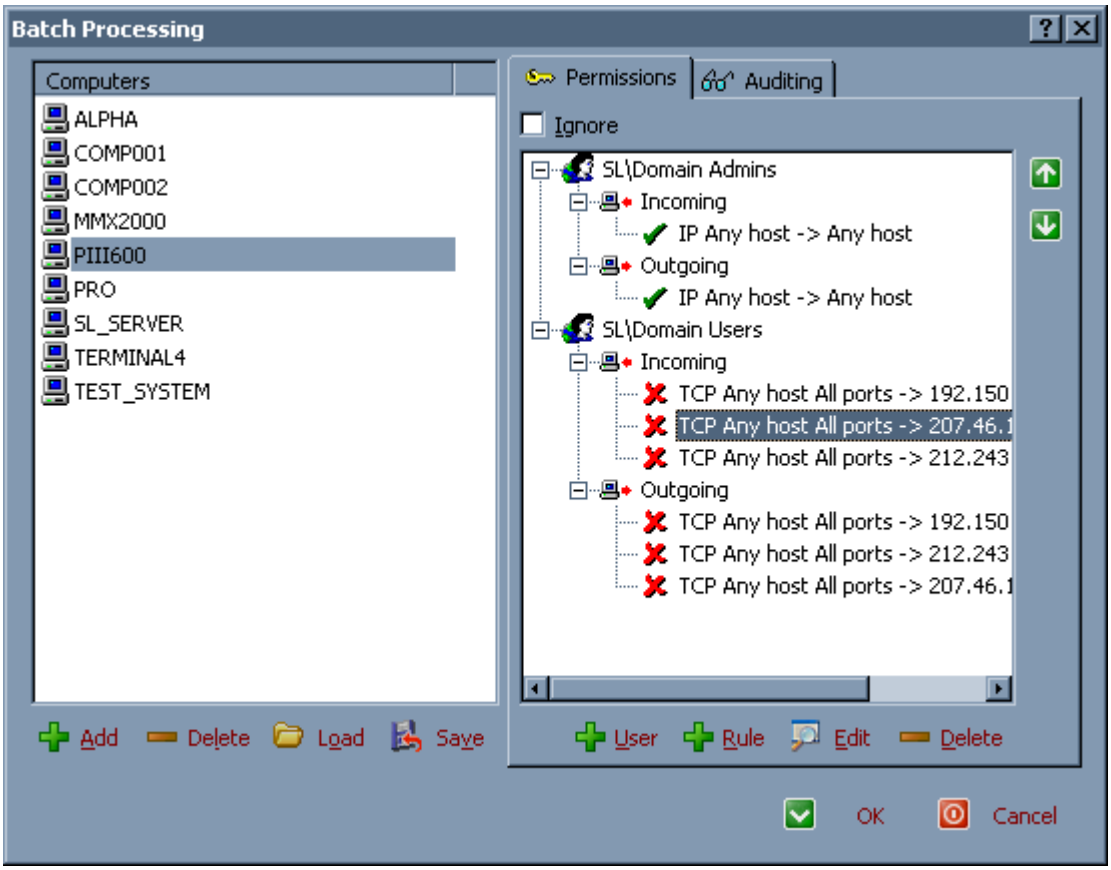
To enable logging for one or both of these packet types, check *Audit Allowed* and/or *Audit Denied* at the bottom of the *Auditing* tab.

Please note that until either Audit Allowed or Audit Denied is checked, logging is disabled in spite of defined audit rules.

7. Batch Processing

Batch Processing is one of the most powerful and useful functions of PortsLock. Usually, midsize and large networks contain many computers that should be configured equally. Using *Batch Processing* network administrators can set security and audit rules for every computer in the network very quickly.

To access *Batch Processing*, select the *Batch Permissions* item from the *File* menu or press Shift+F2.



First, you need to select the computers that you want to include in the batch processing. To add computers to the list, press the *Add* button. This opens a dialog with the computer tree where you can select any computer that is available on your network. Double-click on the computer name in the computer tree to add a computer or type the computer's name manually and press the *OK* button to include the selected computer(s) to the list.

You can also load computers from an external file. Press the *Load* button and select a file that contains the list of computers. Two file formats are supported – text file (.txt) and Comma Separated Values (.csv). A text file must contain computer names separated by tabs. Computer names in a .csv file must be separated by commas or semicolons. To save a computer listing to an external file, press the *Save* button. Select the type of the file – .txt or .csv.

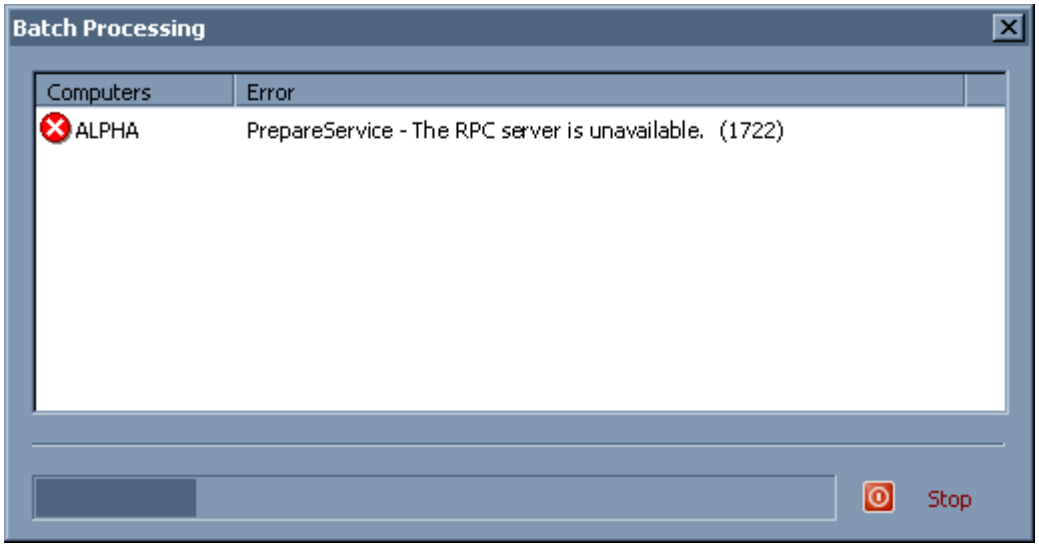
You then define the rules (security and/or audit) to be applied to the selected computers. Rules are defined in the **Setting Up Security Rules** and **Setting Up Audit Rules** sections of this manual.

If you want to define only security rules and do not want to change existing audit rules or vice versa, you have to check the appropriate *Ignore* checkbox on the *Permissions* or *Auditing* tab:

- If *Ignore* is checked on the *Permissions* tab then security rules will not be changed for selected computers.
- If *Ignore* is checked on the *Auditing* tab then audit rules will not be changed for selected computers.
- If *Ignore* is checked on both tabs then neither security nor audit rules will be changed for selected computers.

Also, if *Audit Allowed* and/or *Audit Denied* checkboxes on the *Auditing* tab are in the intermediate (grayed) state it means that the appropriate audit parameters will not be changed for selected computers.

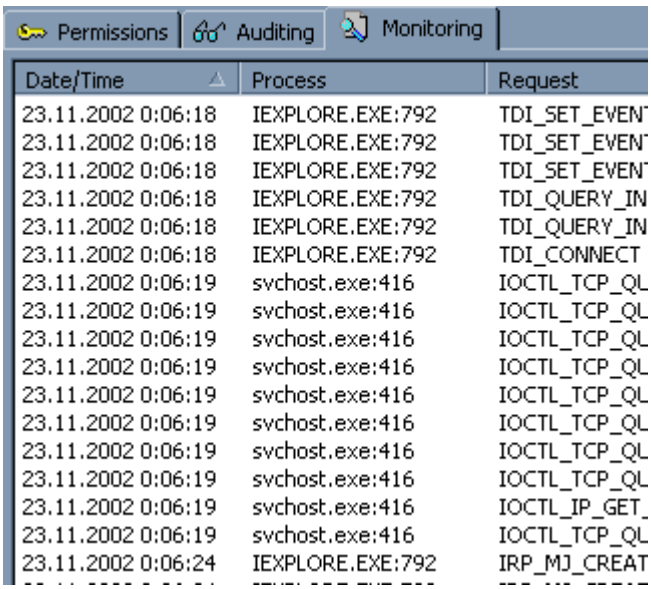
To start batch processing, press the *OK* button. You can abort processing at any time.



8. Monitoring

PortsLock adds the ability to monitor TCP/IP network activity in real-time. It shows you which process is associated with each connection endpoint, making it easy to determine what application and user are responsible for specific connections and activity.

To watch network activity in real-time, select the *Monitoring* tab.



Each line (message) in the monitoring list represents a different event and the information that PortsLock shows for the event includes the date and the time of the event, the event type (send, receive, etc.), the event's status, the local and remote address/port pairs of the endpoint on which the event took place, the number of bytes sent or received, and more.

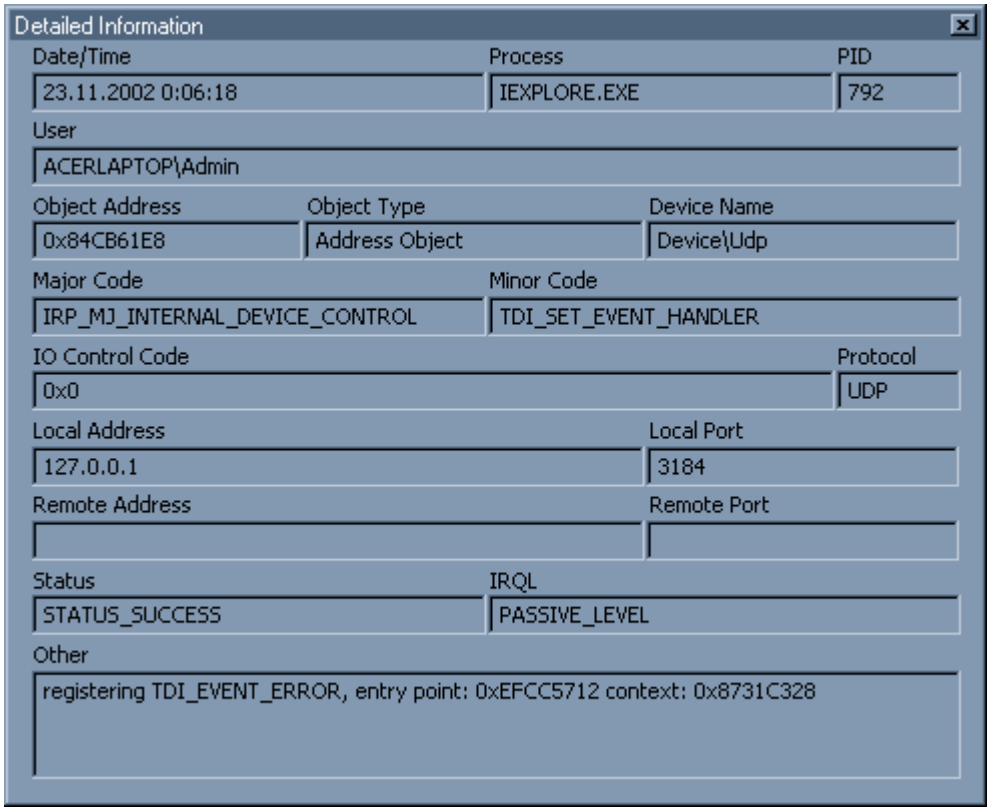
The columns in the monitoring list are defined as follows:

- *Date/Time* – the date and the time when this event was received by the PortsLock Driver.
- *Process* – the name and identifier of the process that owns the endpoint.
- *Request* – the request code (*TDI_CONNECT*, *TDI_SEND*, etc.) that has been sent to the TCP/IP driver.
- *Local Address* – the protocol (*TCP*, *UDP*, *ICMP*, etc.) of the endpoint and the local IP address/port-pair of the endpoint.
- *Remote Address* – shows the remote IP address/port pair of the endpoint, if applicable.

- *Status* – the result code (*STATUS_SUCCESS*, *STATUS_PENDING*, etc.) of the processed request.
- *User* – the name of the user that owns the endpoint.
- *Device Name* – the name of the TCP/IP's device (*Device\Tcp*, *Device\Udp*, *Device\RawIp*, *Device\Ip*, etc.) that should receive the request.
- *Other* – other request-specific information for the event, such as the number of bytes sent or received, connection flags, and so on.

To toggle the display of resolved names, click *Resolve Addresses*. If *Resolve Addresses* is checked, PortsLock tries to resolve IP addresses and ports to their name (*DNS*) versions, otherwise it shows their numeric representation.

If you wish to see more detailed information about an event, double-click on its record.



For more information about request and status codes, please see Microsoft's documentation for device driver developers – *Device Driver Kit (DDK)*.

By default, the monitoring list scrolls so that it always shows the most recent event. To disable auto-scrolling, uncheck the *Keep Last Message in View* item from the *Monitoring* menu.

You can limit the number of records the monitoring list retains by setting the maximum number of messages with *Set Message Count* from the *Monitoring* menu. The number you specify determines the maximum number of records that PortsLock will maintain in its buffer at any given time. After a defined number of lines have accumulated, the oldest records become unavailable.

To clear all records from the monitoring list, select *Clear All Messages* from the *Monitoring* menu. ***Please note that once records are erased, they cannot be recovered.***

To save all the records currently in the monitoring list to a text file, select *Save* from the *Monitoring* menu. PortsLock then copies all the currently available events to the file that you specify. You can save either a brief or detailed log.

PortsLock can automatically refresh the contents of the monitoring list. To change the refresh rate use *Update Speed* from the *Monitoring* menu. To completely disable automatic refreshing, select the *Paused* menu item. At any time you can refresh the monitoring list manually by pressing the *Refresh* button on the *Monitoring* tab. If the *Always Active* menu item is checked, then PortsLock refreshes the monitoring list even if the *Monitoring* tab is not active (i.e. the *Permissions* or *Auditing* tab is selected).

PortsLock offers powerful filtering option so that you can narrow the output down what interests you. To filter records, use *Filter* from the *Monitoring* menu.

9. Deployment Examples

Following are several examples of configuring PortsLock's rules that may help you deploy PortsLock on your computers.

Please read the **Setting Up Security Rules** and **Setting Up Audit Rules** sections of this manual before defining any rules.

a) To allow for all users in the *Domain Users* group to access the Internet only from Monday till Friday and between 12pm and 5pm, allow them to access the local network at any time, and allow any traffic for *Administrators*:

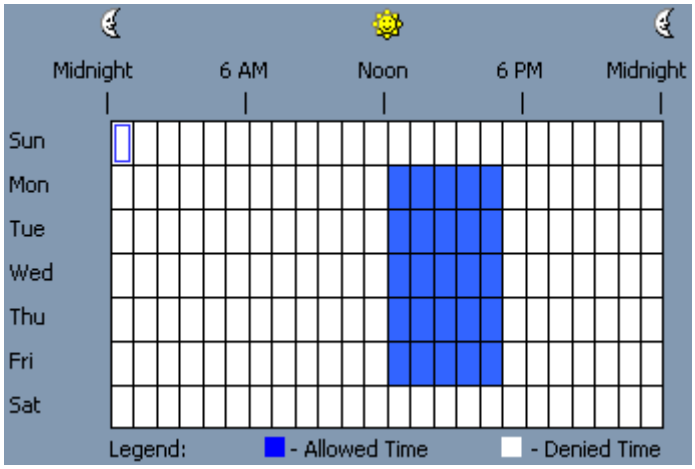
   Add *Administrators* to the top of the security rule list (the *Permissions* tab) and add two equal rules for *Incoming* and *Outgoing* with these settings:

   - Protocol: *IP*
   - Source Type: *Any Address*
   - Destination Type: *Any Address*
   - Time: *the allowed time for all periods*

   Add *Domain Users* below *Administrators* and add two rules for *Outgoing* with these settings:

   - Protocol: *IP*
   - Source Type: *Any Address*
   - Destination Type: *Network/Mask, LAN_IP_ADDRESS/LAN_MASK* *
   - Time: *the allowed time for all periods*

   - Protocol: *IP*
   - Source Type: *Any Address*
   - Destination Type: *Any Address*
   - Time: *as shown on the picture below*



* - you must substitute *LAN_IP_ADDRESS/LAN_MASK* with the real IP address and the network mask from your local network.

b) To prevent *Guest* from accessing *microsoft.com* at any time:

Add *Guest* to the top of a security rule list and add a rule for *Outgoing* with these settings:

- Protocol: *IP*
- Source Type: *Any Address*
- Destination Type: *Host*, IP Address: *207.46.249.27*
- Time: *the denied time for all periods*

c) To prevent *Guest* from accessing www.*microsoft.com* (HTTP on port 80) and *ftp.microsoft.com* (FTP on port 21) at any time:

Add *Guest* to the top of a security rule list and add two rules for *Outgoing* with these settings:

For www.*microsoft.com*

- Protocol: *TCP*
- Source Type: *Any Address*, Port: *Any*
- Destination Type: *Host*, IP Address: *207.46.249.27*, Port: *Equal to 80*
- Time: *the denied time for all periods*

For *ftp.microsoft.com*

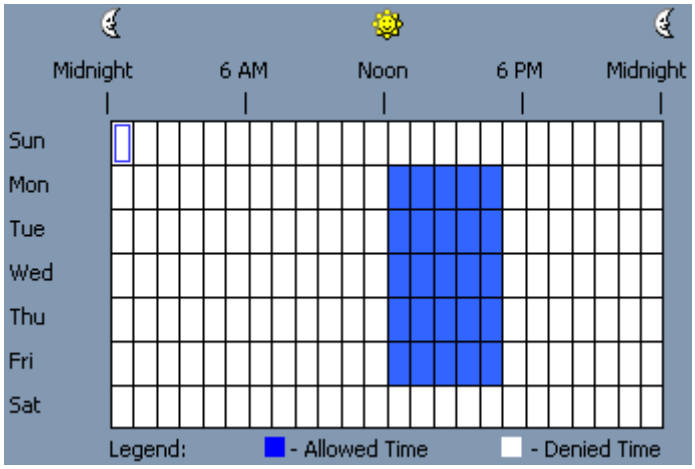
- Protocol: *TCP*
- Source Type: *Any Address*, Port: *Any*
- Destination Type: *Host*, IP Address: *207.46.249.27*, Port: *Equal to 21*
- Time: *the denied time for all periods*

d) To prevent *Guest* from accessing *microsoft.com* at any time but allow it to access www.*microsoft.com* (HTTP on port 80) only from Monday till Friday and between 12pm and 5pm:

Add *Guest* to the top of the security rule list. At the top of its rule list add a rule for *Outgoing* with these settings:

- Protocol: *TCP*
- Source Type: *Any Address*, Port: *Any*

- Destination Type: *Host*, IP Address: *207.46.249.27*, Port: *Equal to 80*
- Time: *as shown on the picture below*



Below the previous rule add another rule for *Outgoing* with these settings:

- Protocol: *IP*
- Source Type: *Any Address*
- Destination Type: *Host*, IP Address: *207.46.249.27*
- Time: *the denied time for all periods*

e) To prevent *John* from accessing the network at all, allow *John Group*, to which *John* belongs, to access only *TCP* ports 80 and 110, allow for all users in the *Domain Users* group to access only TCP ports 80, 110 and 21 (FTP), and allow any traffic for *Administrators*:

Add *Administrators* to the top of the security rule list and add two equal rules for *Incoming* and *Outgoing* with these settings:

- Protocol: *IP*
- Source Type: *Any Address*
- Destination Type: *Any Address*
- Time: *the allowed time for all periods*

Add *John* below *Administrators* and add two equal rules for *Incoming* and *Outgoing* with these settings:

- Protocol: *IP*
- Source Type: *Any Address*
- Destination Type: *Any Address*
- Time: *the denied time for all periods*

Add *John Group* below *John* and add three rules for *Outgoing* with these settings:

- Protocol: *TCP*
- Source Type: *Any Address*, Port: *Any*
- Destination Type: *Any Address*, Port: *Equal to 80*
- Time: *the allowed time for all periods*

- Protocol: *TCP*
- Source Type: *Any Address*, Port: *Any*
- Destination Type: *Any Address*, Port: *Equal to 110*
- Time: *the allowed time for all periods*

- Protocol: *IP*
- Source Type: *Any Address*
- Destination Type: *Any Address*
- Time: *the denied time for all periods*

Add *Domain Users* below *John Group* and add four rules for *Outgoing* with these settings:

- Protocol: *TCP*
- Source Type: *Any Address*, Port: *Any*
- Destination Type: *Any Address*, Port: *Equal to 80*
- Time: *the allowed time for all periods*

- Protocol: *TCP*
- Source Type: *Any Address*, Port: *Any*
- Destination Type: *Any Address*, Port: *Equal to 110*
- Time: *the allowed time for all periods*

- Protocol: *TCP*
- Source Type: *Any Address*, Port: *Any*
- Destination Type: *Any Address*, Port: *Equal to 21*
- Time: *the allowed time for all periods*

- Protocol: *IP*
- Source Type: *Any Address*
- Destination Type: *Any Address*
- Time: *the denied time for all periods*