# CORE FORCE User's Guide

# CORE FORCE User's Guide

# Table of Contents

# List of Figures

# Chapter 1. Getting Started

## Introduction

This section provides an overview of what CORE FORCE is, what you can do with it and a brief description of its architecture.

## What is CORE FORCE?

CORE FORCE is the first community oriented security solution for personal computers. CORE FORCE is free and can be installed in computers using Windows 2000 or Windows XP, and provides a framework than combines a host-based Intrusion Prevention System (H-IPS) with a powerful personal firewall. This security framework is leveraged by a community of security experts that share their security configurations for a growing list of programs. These security profiles can be downloaded by any user of CORE FORCE from the community website and they're also completely open so that they can be peer-reviewed to minimize security hazards. The community approach to endpoint security also allows end-users who are no security experts to work in a secure environment.

CORE FORCE can be used to:

- Protect your computer from compromise by worms, virus and email-borne malware
- Prevent you computer from being used as a staging point to amplify attacks and compromise others
- Prevent exploitation of known bugs in the operating system and applications running on your computer
- Prevent exploitation of unknown bugs (0-day) in the operating system and applications running on your computer.
- Detect and prevent execution of adware, spyware, trojan horses and other malware on you computer

The product provides inbound and outbound stateful packet filtering for TCP/IP protocols, granular file system and registry access control and programs' integrity validation. These capabilities can be configured and enforced system-wide or on a per-application basis for specific programs such as email readers, web browsers, media players, messaging software, etc.

## How does CORE FORCE works?

### Configuration

CORE FORCE enforces security settings independently of the operating system's own configuration.

Security permissions are configured using a configuration tool with a powerful graphical interface. They are stored on XML files, which allow the sharing of settings among users, and are accessed through a Windows Service. Permissions are enforced by custom device drivers running at kernel level.

Permissions can be configured for the entire operating system (System permissions) or on a per application basis by grouping them into application profiles (Program permissions).

They can include inbound and outbound network traffic restrictions, file system access restrictions to folders and files and registry access restrictions to registry keys and values.

Programs are identified by a cryptographically strong hash of the executable file's contents that is checked every time the program runs.

CORE FORCE can be configured to provide different security levels, so the user can decide how to run a program. The security configuration of a program can be easily changed by choosing a standard security level (High, Medium, Medium-Low, Low). The user can change this level at any time, according to the task he is performing: for example, if the user is about to open a suspicious mail attachment, he can raise the Security Level for the mail program and for the entire system. On the other hand, if the user is installing a new application, he can lower the Security Level to avoid unnecessary false alarms.

If none of the standard security levels suit the needs of the user, they can be customized by enabling and disabling individual *policies*. Each policy usually provides security configuration to enable a feature of a program (for example, *Allow opening attachments (confirmation required)*). With this configuration method, CORE FORCE releases the user from the task of dealing with files and registry permissions directly.

Finally, the user can configure permissions for specific files, registry keys and network connections. Several tools, such as log viewer, the Learning Wizard and confirmation popups aid the user on this task.

Authorized and unauthorized operations can by logged to a system wide or per application audit trail.

## CORE FORCE Architecture

CORE FORCE is implemented by security modules that provide different aspects of the security framework. These modules are implemented as system drivers that work in kernel mode to provide the highest level of protection to protected resources. A centralized administrative console allows users to configure all permissions for the computer and to interact with CORE FORCE Community to download security profiles and updates, and share them to other users too.

### Firewall

The firewall component of CORE FORCE is a Windows port of OpenBSD's PF, the open source, mature, server-level firewall (PF: The OpenBSD Packet Filter [http://www.openbsd.org/faq/pf/]). The PF functionality has been trimmed and tailored to make it suitable for desktop systems.

CORE FORCE support inbound and outbound stateful filtering with advanced settings such as TCP flags and ICMP type/code flags. It works on a per application basis, loading and unloading rules dynamically at application runtime and it can be configured to require runtime user confirmation on certain connections. It is implemented at kernel level as an intermediate driver that mediates communications between the network card drivers and the operating system's TCP/IP protocol stack, making it very difficult to bypass.

### Filesystem and Registry

The file system and registry access control component of CORE FORCE is implemented as a file system filter that mediates communication between the operating system and file-systems drivers.

The component runs at kernel level and captures file system and registry access operations performed by the rest of the operating system (user-level applications, services and kernel subsystems) and enforces permissions for create, read, write, execute, delete and list operations. Due to its location inside the operating system, it can traps calls to any filesystem, and even calls made by other kernel components. The filesystem permissions can be specified using wildcards and specifying whether a subfolder inherits the configuration from its parent.

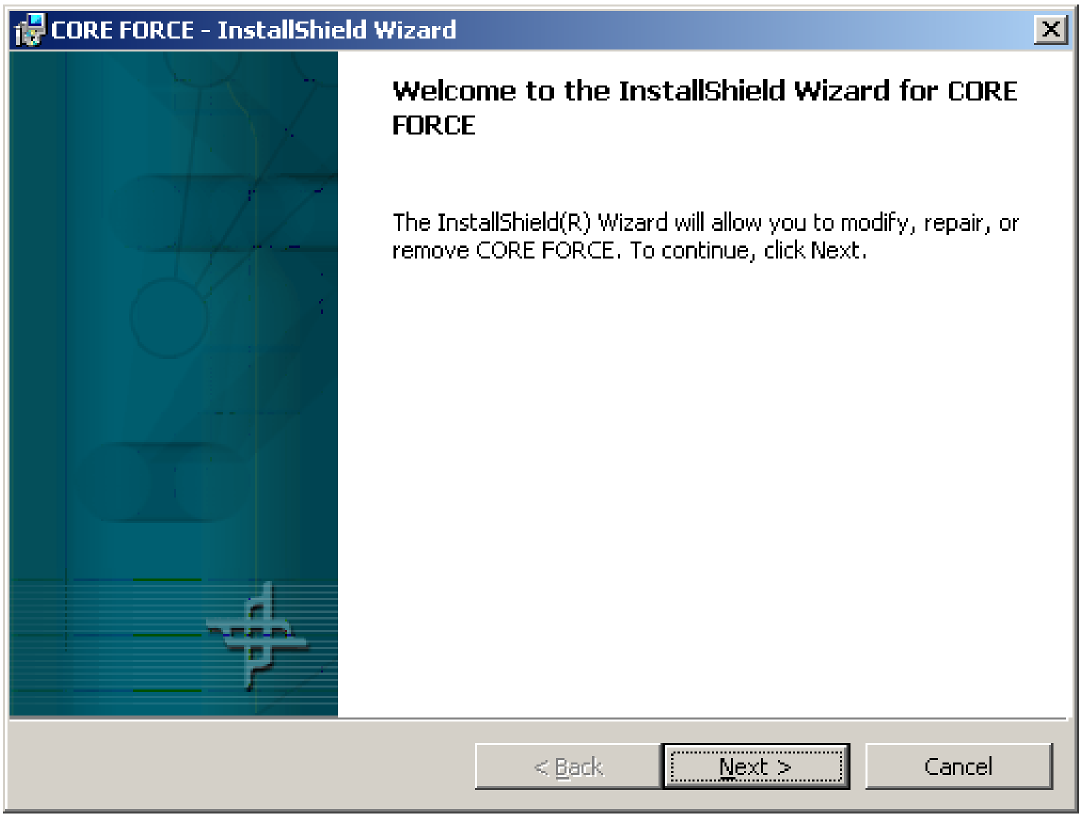
# Installation & Setup

## First time installation

CORE FORCE is distributed as a single executable file that installs and configures all required modules. To install the product, execute the file and follow the instructions of the Installation Wizard (see Figure 1.1, “Installation Wizard”).

### Note

You need administrative privileges to install CORE FORCE.



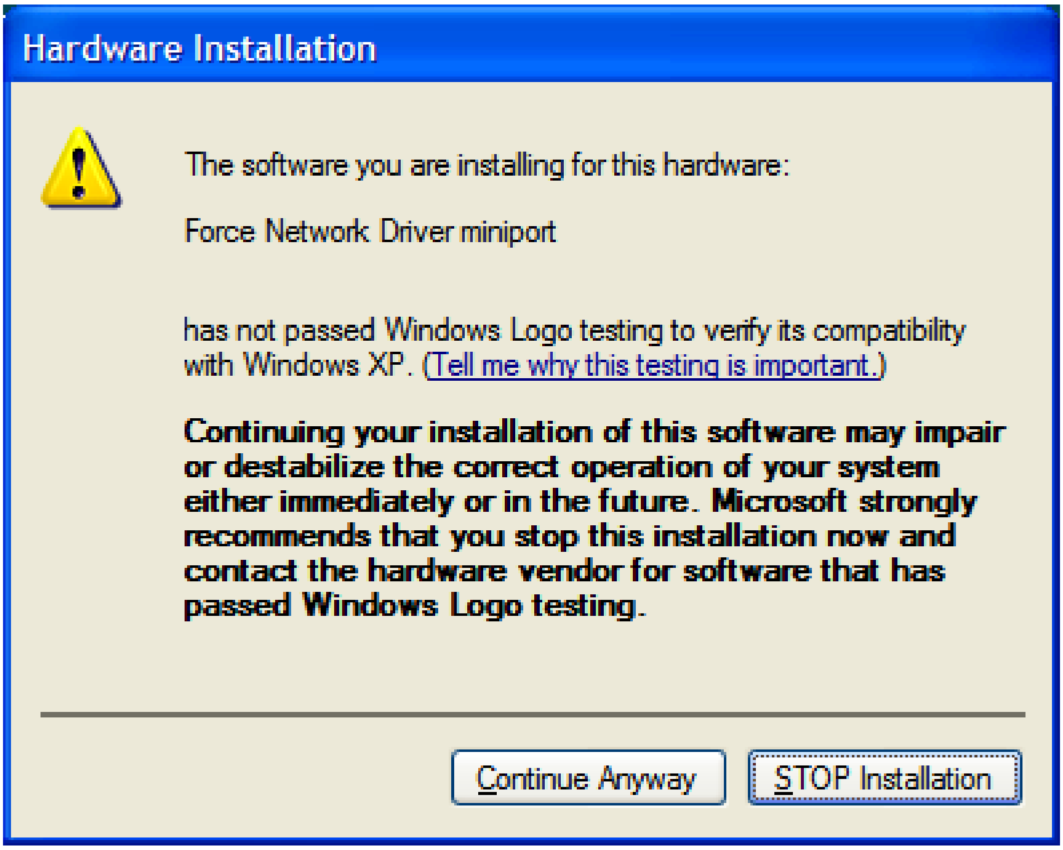
CORE FORCE - InstallShield Wizard

Welcome to the InstallShield Wizard for CORE FORCE

The InstallShield(R) Wizard will allow you to modify, repair, or remove CORE FORCE. To continue, click Next.

**Figure 1.1. Installation Wizard**

On Windows XP, you will be asked to accept the installation of new unsigned drivers (see Figure 1.2, “Confirm the installation of an unsigned driver”). This is normal behavior, please click the Yes button to continue.



Hardware Installation

The software you are installing for this hardware:

Force Network Driver miniport

has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

**Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.**

**Figure 1.2. Confirm the installation of an unsigned driver**

### Note

During the installation, your computer can be disconnected from the network.

To finish the installation process, you have to reboot your computer. Click Yes if you want to reboot inmediately, or click No if you plan to reboot later. Notice that CORE FORCE will not be activated until you reboot. To complete the configuration of the product, a Setup Wizard is launched the first time CORE FORCE is run (see next section).

After your computer is rebooted, CORE FORCE will be installed on your system. While the product is active, the Force icon () appears on the system tray. From this icon, you can activate or deactivate CORE FORCE and access the configuration interface. When Force is not active, the tray icon appears striked ().

## Setting up CORE FORCE: The Setup Wizard

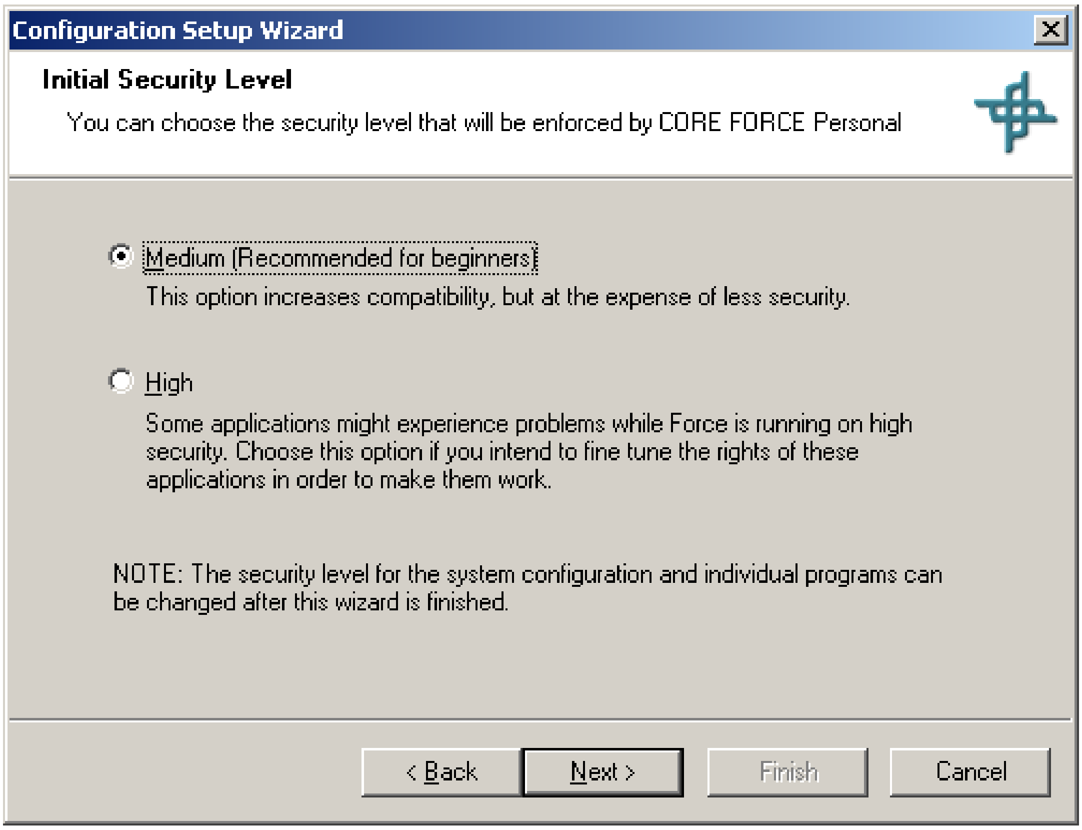
The Setup Wizard appears the first time you run CORE FORCE. This wizard will help you setup several network settings and import predefined application profiles for your programs.

### Note

The Setup Wizard can be launched again from the Tools menu in CORE FORCE's configuration interface.

All the options shown on this Wizard have appropiate default values. If you are not sure what to answer on some of these settings, just leave their default and click Next.

The first page of the Wizard (Figure 1.3, “Configuration of initial security level on the Setup Wizard”) configures the security level to be set for programs imported during this setup. The security level for a program defines which set of permissions are going to be applied while the program is running. If this is the first time you install CORE FORCE, it's recommended to start with the default security level (Medium) to avoid compatibility issues with your installed applications (You can always elevate the security level for configured programs after the Wizard is finished).



Configuration Setup Wizard

Initial Security Level

You can choose the security level that will be enforced by CORE FORCE Personal

● Medium (Recommended for beginners)

This option increases compatibility, but at the expense of less security.

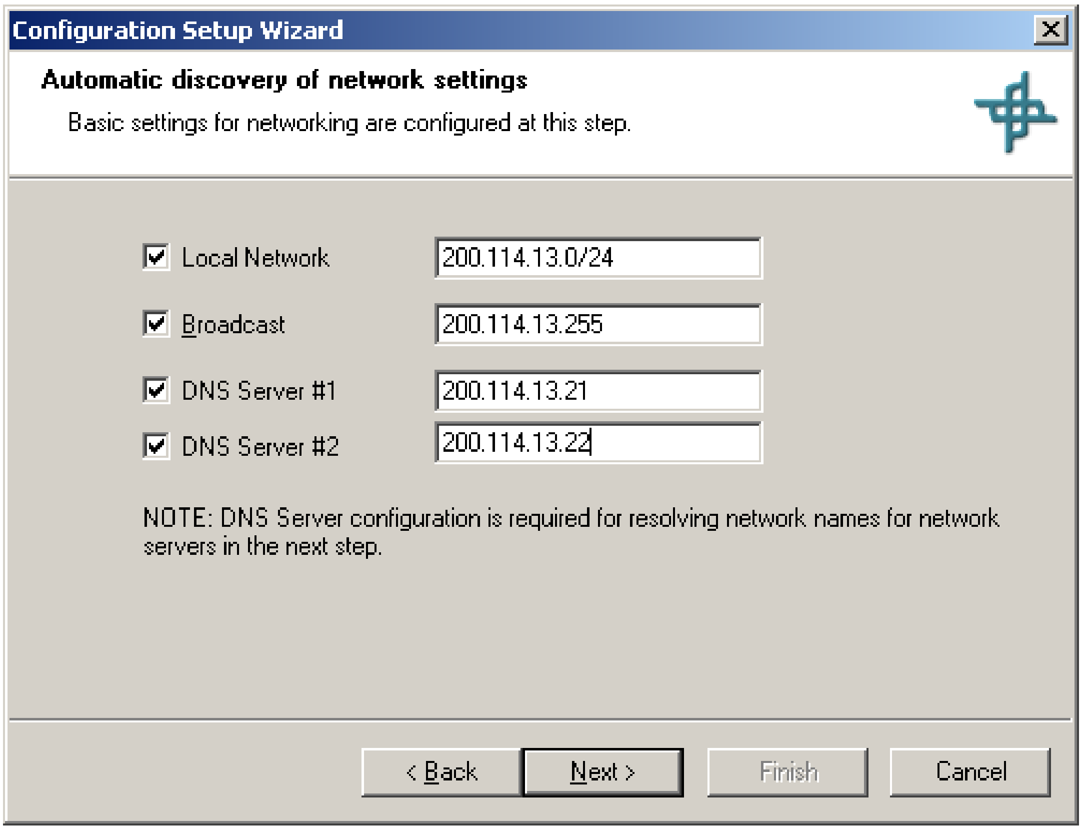
○ High

Some applications might experience problems while Force is running on high security. Choose this option if you intend to fine tune the rights of these applications in order to make them work.

NOTE: The security level for the system configuration and individual programs can be changed after this wizard is finished.

**Figure 1.3. Configuration of initial security level on the Setup Wizard**

In the following two pages of the Wizard, CORE FORCE will try to discover your computer's network settings automatically (see Figure 1.4, “Automatic Discovery of Network Settings on the Setup Wizard (Basic settings)” and Figure 1.5, “Automatic Discovery of Network Settings on the Setup Wizard (Common servers)”). CORE FORCE scans the configuration of network programs on your computer, such as Internet Explorer and Outlook Express, and collects all the relevant settings (mail server, web proxt, etc). You can change any of these options by replacing their default value. For network addresses you can enter: IPs (e.g. 216.239.41.104), host names (e.g. www.google.com) or network masks (e.g. 216.239.41.0/23). For ports, only numbers are allowed. When you're done, press the Next button.



Configuration Setup Wizard

**Automatic discovery of network settings**

Basic settings for networking are configured at this step.

☑ Local Network: 200.114.13.0/24

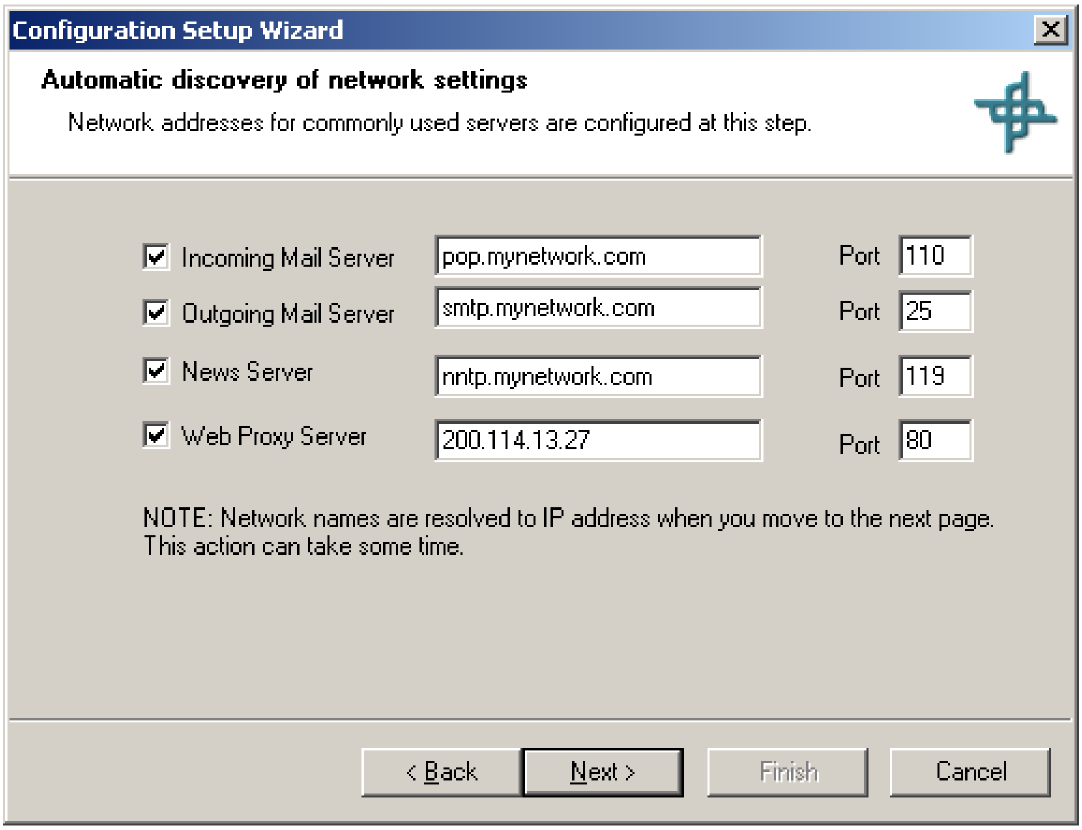
☑ Broadcast: 200.114.13.255

☑ DNS Server #1: 200.114.13.21

☑ DNS Server #2: 200.114.13.22

NOTE: DNS Server configuration is required for resolving network names for network servers in the next step.

**Figure 1.4. Automatic Discovery of Network Settings on the Setup Wizard (Basic settings)**



Configuration Setup Wizard

**Automatic discovery of network settings**

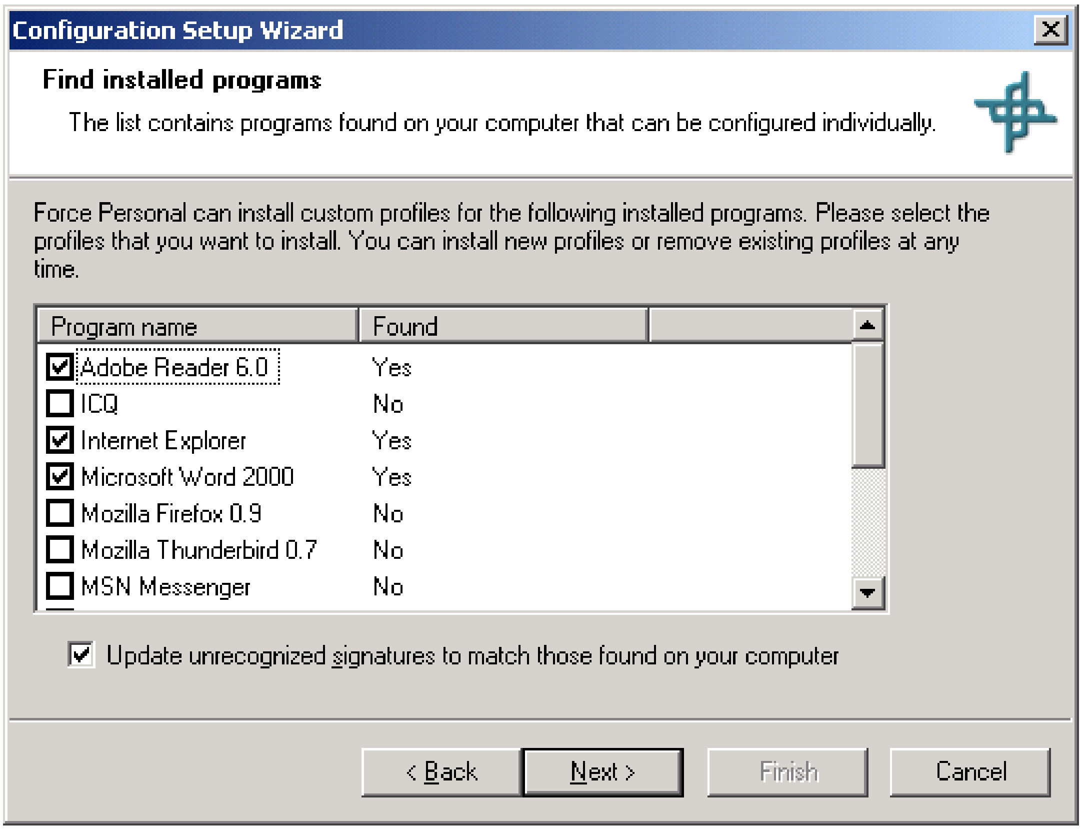
Network addresses for commonly used servers are configured at this step.

| | | | |
|---|---|---|---|
| ☑ Incoming Mail Server | pop.mynetwork.com | Port | 110 |
| ☑ Outgoing Mail Server | smtp.mynetwork.com | Port | 25 |
| ☑ News Server | nntp.mynetwork.com | Port | 119 |
| ☑ Web Proxy Server | 200.114.13.27 | Port | 80 |

NOTE: Network names are resolved to IP address when you move to the next page. This action can take some time.

**Figure 1.5. Automatic Discovery of Network Settings on the Setup Wizard (Common servers)**

The next page (Figure 1.6, “Find installed programs on the Setup Wizard”) displays a list of all program security configurations bundled with CORE FORCE. For each one of them, CORE FORCE searches your computer for the associated program. The column named found indicates whether the program is installed and has been located on your system. If the application was found, but its digital signature does not match the signature stored on the profile, then the message "Yes, but signature is invalid" is displayed. This can indicate that you have a different version of the product, you have installed a patch, or the program has been modified by a virus.



Configuration Setup Wizard

Find installed programs

The list contains programs found on your computer that can be configured individually.

Force Personal can install custom profiles for the following installed programs. Please select the profiles that you want to install. You can install new profiles or remove existing profiles at any time.

| Program name | Found |
|---|---|
| ☑ Adobe Reader 6.0 | Yes |
| □ ICQ | No |
| ☑ Internet Explorer | Yes |
| ☑ Microsoft Word 2000 | Yes |
| □ Mozilla Firefox 0.9 | No |
| □ Mozilla Thunderbird 0.7 | No |
| □ MSN Messenger | No |

☑ Update unrecognized signatures to match those found on your computer

**Figure 1.6. Find installed programs on the Setup Wizard**

By default, only found applications are installed, but you can include or exclude applications individually. If the signature of some profiles did not match, leave the checkbox "Update unrecognized signatures to match those found on your computer" checked, to avoid unnecessary false alarms. When you are done, click Next.

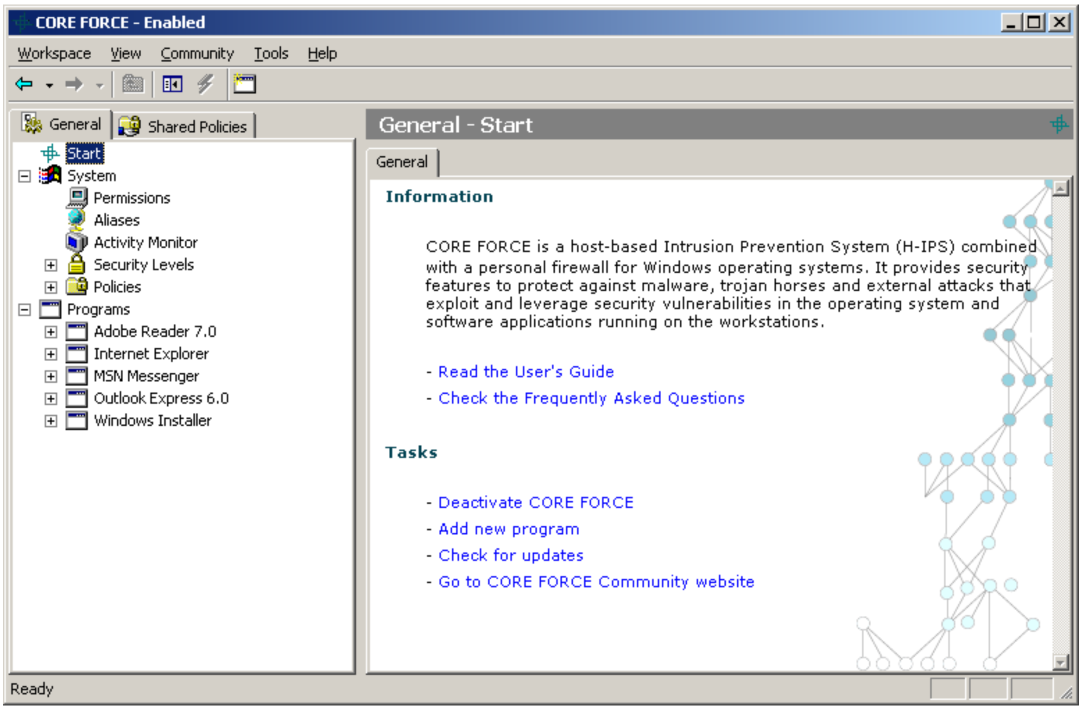
At this time, the profiles for the application that you selected will be installed. Notice that this operation can take a while, depending on the amount of profiles you choose to install. When all the profiles are installed, the Next button is enabled. Click on it to finish the wizard.

After the Setup Wizard is finished, your computer and all your applications will be secured by CORE FORCE.

# Introduction to the Configuration Interface

CORE FORCE provides a unified interface for configuration and monitoring. This interface is used to: create and customize program profiles, change global settings, view logs and monitor in real-time the activity of a program, among other tasks.

To open this interface, double-click the Core Force tray icon (⌖), or right-click the icon and select Configure. You can also launch the configuration interface from the CORE FORCE folder on the Programs start menu.



Information

CORE FORCE is a host-based Intrusion Prevention System (H-IPS) combined with a personal firewall for Windows operating systems. It provides security features to protect against malware, trojan horses and external attacks that exploit and leverage security vulnerabilities in the operating system and software applications running on the workstations.

- Read the User's Guide
- Check the Frequently Asked Questions

Tasks

- Deactivate CORE FORCE
- Add new program
- Check for updates
- Go to CORE FORCE Community website

### Figure 1.7. CORE FORCE configuration interface

Figure 1.7, “CORE FORCE configuration interface” shows the configuration interface layout. It is divided in two panes: the left pane is called workspace and the right pane, main window. The workspace displays a tree with configurable elements, such as applications and policies. The main window shows configuration options and details associated with the item selected on the workspace (either an element or a configuration category).

You can hide the workspace by clicking the hide/show workspace icon (◧) on the toolbar. The workspace selector (Figure 1.8, “Workspace selector”) allows you to change the current workspace. On the current version of the product, two workspaces are available:

### Figure 1.8. Workspace selector

| | |
|---|---|
| General | From this workspace you can access the system profile and global configuration options.<br>You can also create and customize application profiles, access activity logs (either historic and in real-time) filtered by application. |
| Shared Policies | Groups of permissions used as building blocks for the construction of application profiles. |

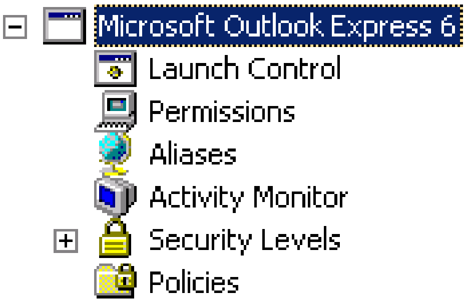


**Figure 1.9. Detail of workspace element**

You can expand an element in the workspace to see a list of configuration categories that apply to that element (see Figure 1.9, “Detail of workspace element”). The following list shows a brief description of the available categories.

Launch control

This option is only applicable to application profiles. It's used to configure the entry point of the secured program, i.e. the executable file that is used to launch the program. You can specify a path based on predefined folders (Program Files, Windows Directory, etc.), paths from a registry value, or custom aliases, so that the entry point can be defined indepdently of the location in a particular computer. Here you can also define the digital signature (hash) of the executable file, so that CORE FORCE can prevent you from executing tampered versions of the program.

Permissions

This option shows the complete set of permissions configured for the parent element, including file system and registry permissions, and firewall rules.

Aliases

You can define here filesystem and network variables, called aliases, that will be used to configure permissions for file system resources and to define firewall rules. For example, "Home Folder" or "Mail Server".

Activity Monitor

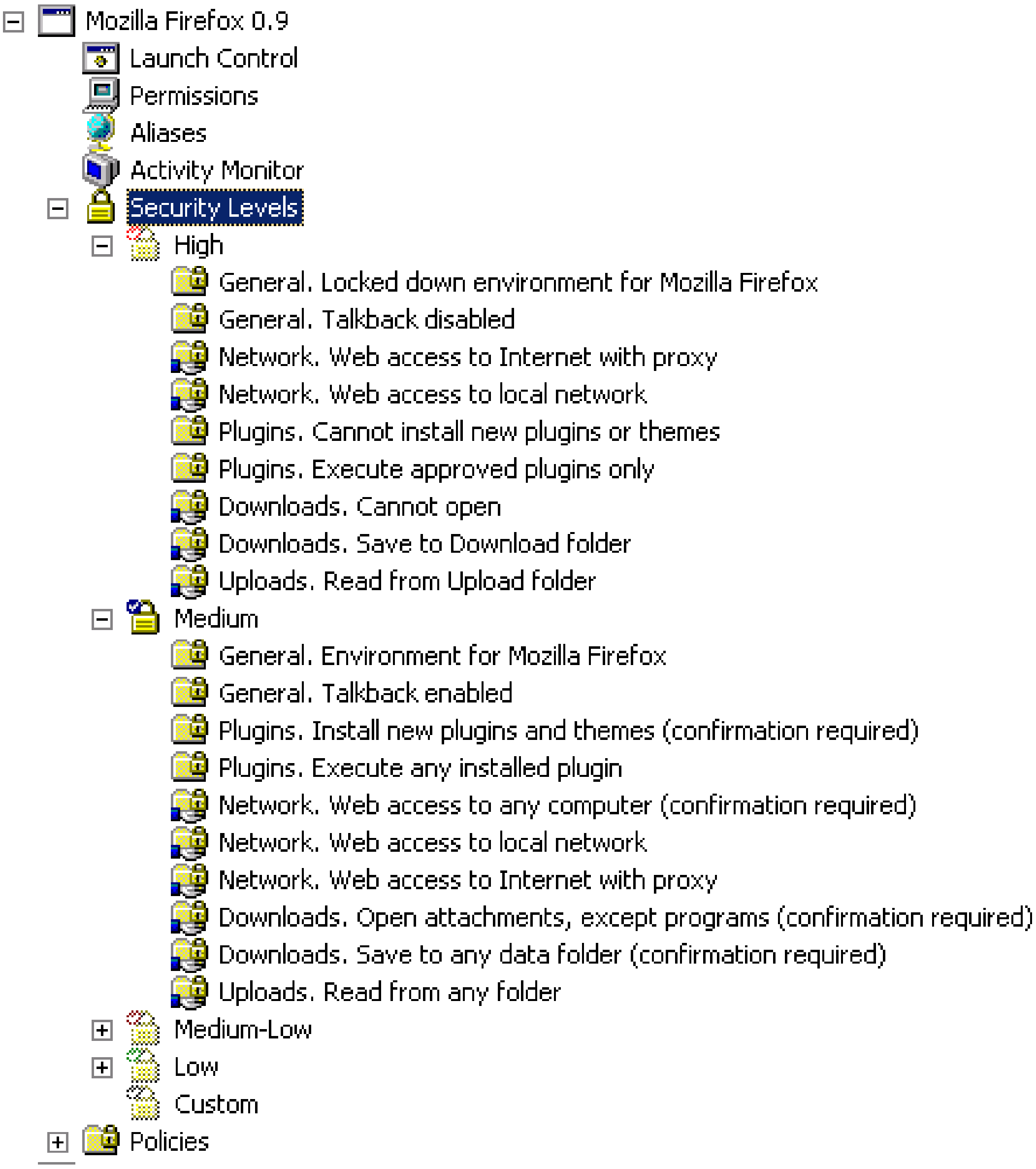
The activity monitor allows you to watch in real-time the logs generated by each application, with several filtering tools. You can also view the list of running processes and the security configuration being applied. This category is only available for application profiles or the system profile.

Security Levels

This element displays the policies, either shared or local (to the program configuration), assigned to each security level (Figure 1.10, “Security levels element on the workspace”). You can customize each security level by assigning and removing policies, or by enabling and disabling those that have already been assigned.

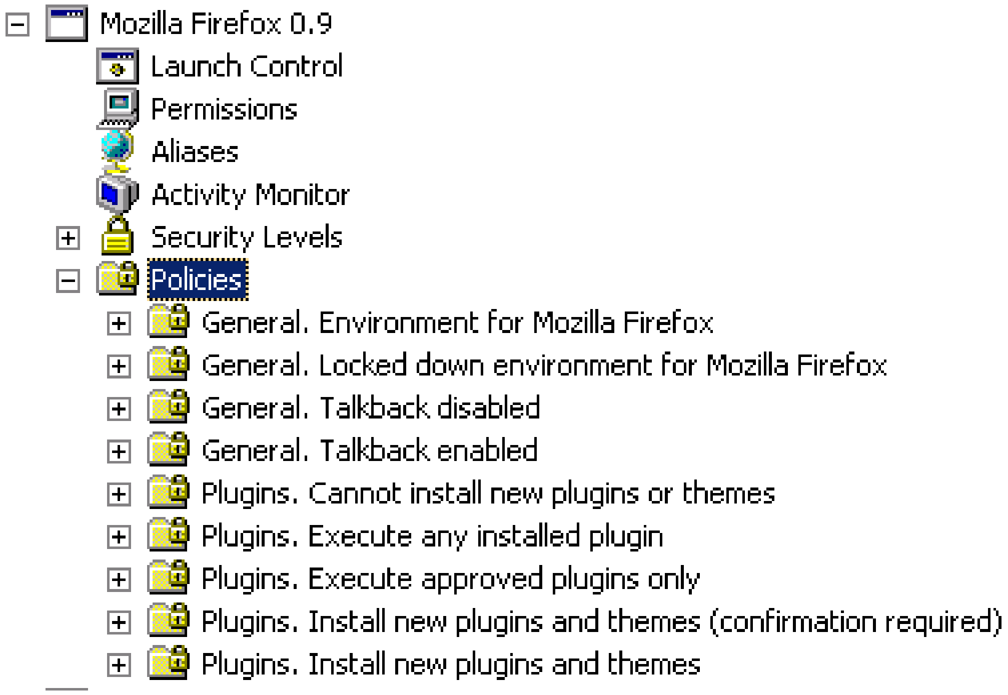
Policies

From this category, you can modify the access permissions defined for each local policy and create new ones (Figure 1.11, “Policies element on the workspace”).



- Mozilla Firefox 0.9
  - Launch Control
  - Permissions
  - Aliases
  - Activity Monitor
  - Security Levels
    - High
      - General. Locked down environment for Mozilla Firefox
      - General. Talkback disabled
      - Network. Web access to Internet with proxy
      - Network. Web access to local network
      - Plugins. Cannot install new plugins or themes
      - Plugins. Execute approved plugins only
      - Downloads. Cannot open
      - Downloads. Save to Download folder
      - Uploads. Read from Upload folder
    - Medium
      - General. Environment for Mozilla Firefox
      - General. Talkback enabled
      - Plugins. Install new plugins and themes (confirmation required)
      - Plugins. Execute any installed plugin
      - Network. Web access to any computer (confirmation required)
      - Network. Web access to local network
      - Network. Web access to Internet with proxy
      - Downloads. Open attachments, except programs (confirmation required)
      - Downloads. Save to any data folder (confirmation required)
      - Uploads. Read from any folder
    - Medium-Low
    - Low
    - Custom
  - Policies

**Figure 1.10. Security levels element on the workspace**



Mozilla Firefox 0.9
Launch Control
Permissions
Aliases
Activity Monitor
Security Levels
Policies
General. Environment for Mozilla Firefox
General. Locked down environment for Mozilla Firefox
General. Talkback disabled
General. Talkback enabled
Plugins. Cannot install new plugins or themes
Plugins. Execute any installed plugin
Plugins. Execute approved plugins only
Plugins. Install new plugins and themes (confirmation required)
Plugins. Install new plugins and themes

**Figure 1.11. Policies element on the workspace**

# Adding new programs

The first to step to secure a program is to create a new security profile. Right-click on the "Programs" item and select *Add new program...* (see Figure 1.12, “Adding a new program security configuration”).

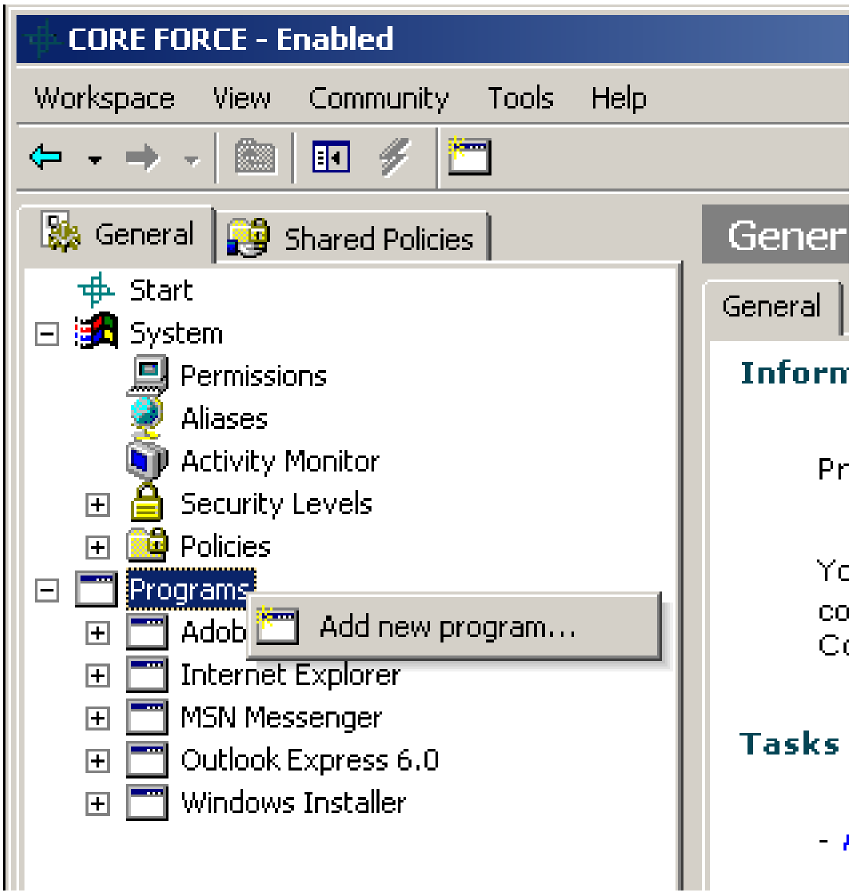
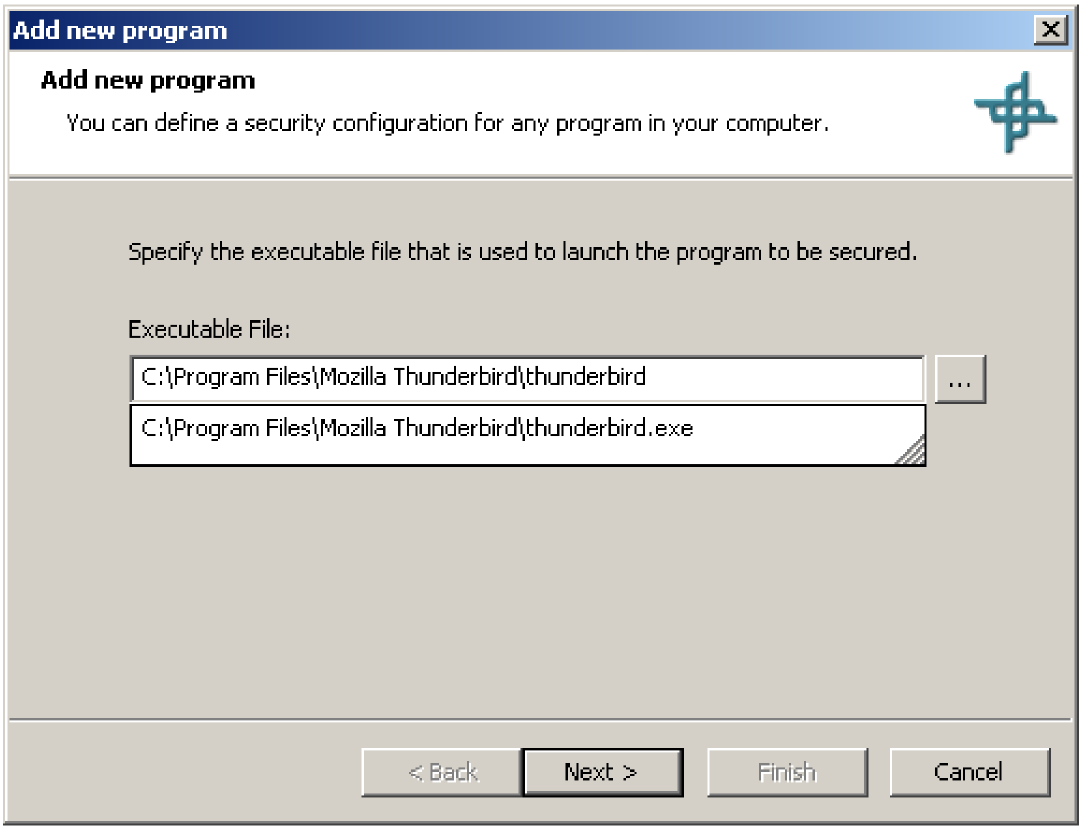


**Figure 1.12. Adding a new program security configuration**

This will start the *Add new Program* wizard, that will guide you through the necessary steps. In the first place, CORE FORCE requires you to identify the program's executable file (see Figure 1.13, “Adding a new program security configuration”). You can enter the complete path for the file (the edit box has auto-completion to ease the location of the file) or click the *+browse-button.png+* button and browse to locate it. We will use Mozilla Thunderbird to complete the information needed by the wizard.



Add new program

**Add new program**

You can define a security configuration for any program in your computer.

Specify the executable file that is used to launch the program to be secured.

Executable File:

C:\Program Files\Mozilla Thunderbird\thunderbird

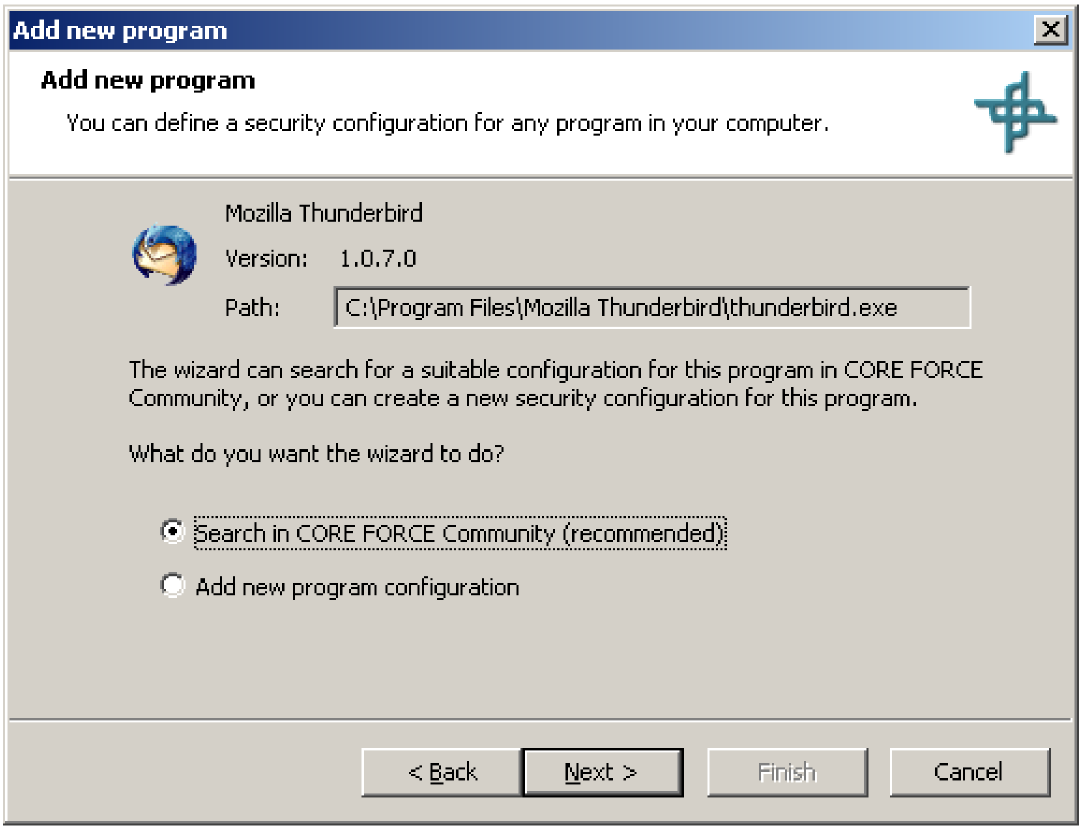
C:\Program Files\Mozilla Thunderbird\thunderbird.exe

**Figure 1.13. Adding a new program security configuration**

The following page shows basic information, if available, retrieved from the executable file (icon, revision and complete path) and gives two options to continue (see Figure 1.14, “The Add new program wizard can look in CORE FORCE Community for an appropiate security profile”):

Search in CORE FORCE Community (recommended)
: This option will search in CORE FORCE Community for appropiate security profiles for this program. These security configurations are shared and peer-reviewed by members of the community, which rate them so that the best profiles can be found by users (without trying or inspecting every one of them).

Add new program configuration
: Allows you to create a security profile from scratch. We will discuss this option later in article.



Add new program

**Add new program**

You can define a security configuration for any program in your computer.

Mozilla Thunderbird

Version: 1.0.7.0

Path: C:\Program Files\Mozilla Thunderbird\thunderbird.exe

The wizard can search for a suitable configuration for this program in CORE FORCE Community, or you can create a new security configuration for this program.

What do you want the wizard to do?

● Search in CORE FORCE Community (recommended)

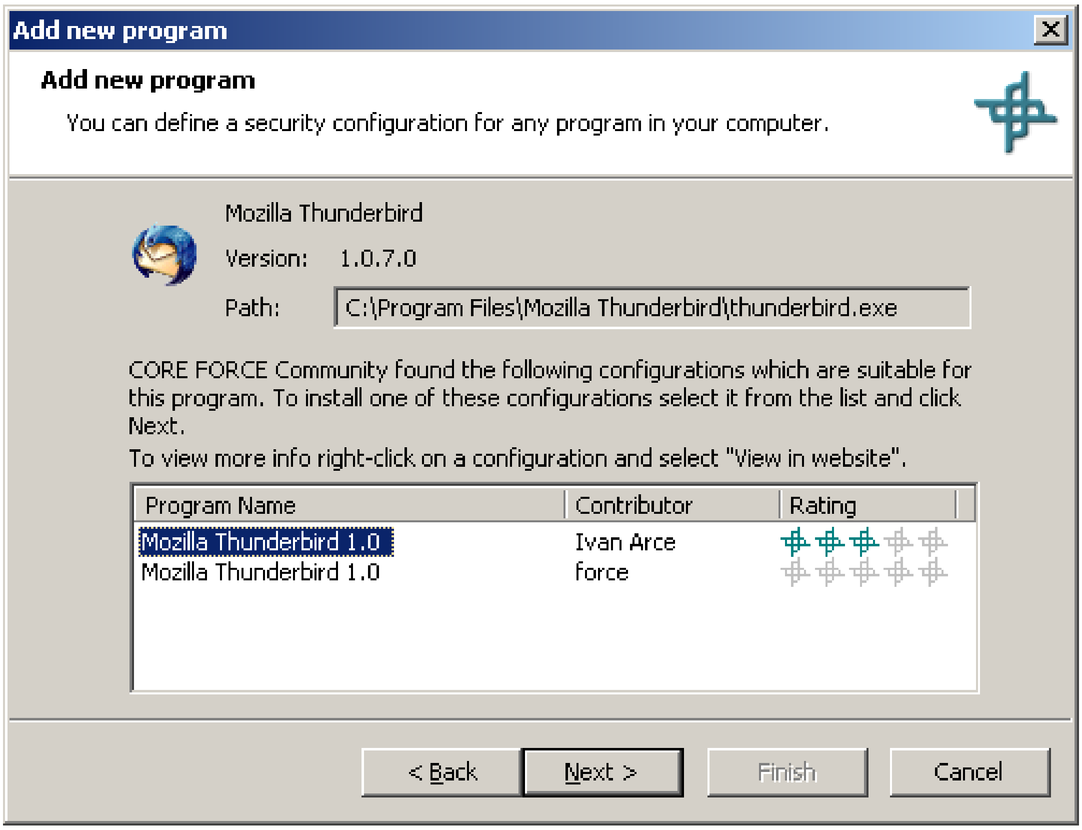
○ Add new program configuration

**Figure 1.14. The Add new program wizard can look in CORE FORCE Community for an appropiate security profile**

Once you have selected the first option and clicked *Next*, the wizard will contact CORE FORCE Community to retrieve available profiles for Mozilla Thunderbird. The community server will try to find security profiles matching the following criteria:

1. Signature: CORE FORCE calculates a digital signature (using a hash function) for the executable file used to launch the program to achieve unambiguous identification (This signature is also used to verify the integrity of a secured program. If the executable's program file changes, CORE FORCE will show a warning before running it).
2. The program's executable file name (in the example, thunderbird.exe) and version.
3. The program's executable file name.

The next page of the wizard will show all security profiles that have matched (See Figure 1.15, “Mozilla Thunderbird profiles in community website”).



Add new program

Add new program

You can define a security configuration for any program in your computer.

Mozilla Thunderbird

Version: 1.0.7.0

Path: C:\Program Files\Mozilla Thunderbird\thunderbird.exe

CORE FORCE Community found the following configurations which are suitable for this program. To install one of these configurations select it from the list and click Next.
To view more info right-click on a configuration and select "View in website".

| Program Name | Contributor | Rating |
|---|---|---|
| Mozilla Thunderbird 1.0 | Ivan Arce | ●●●○○ |
| Mozilla Thunderbird 1.0 | force | ○○○○○ |

## Figure 1.15. Mozilla Thunderbird profiles in community website

For every applicable security profile returned by CORE FORCE Community, the list shows:

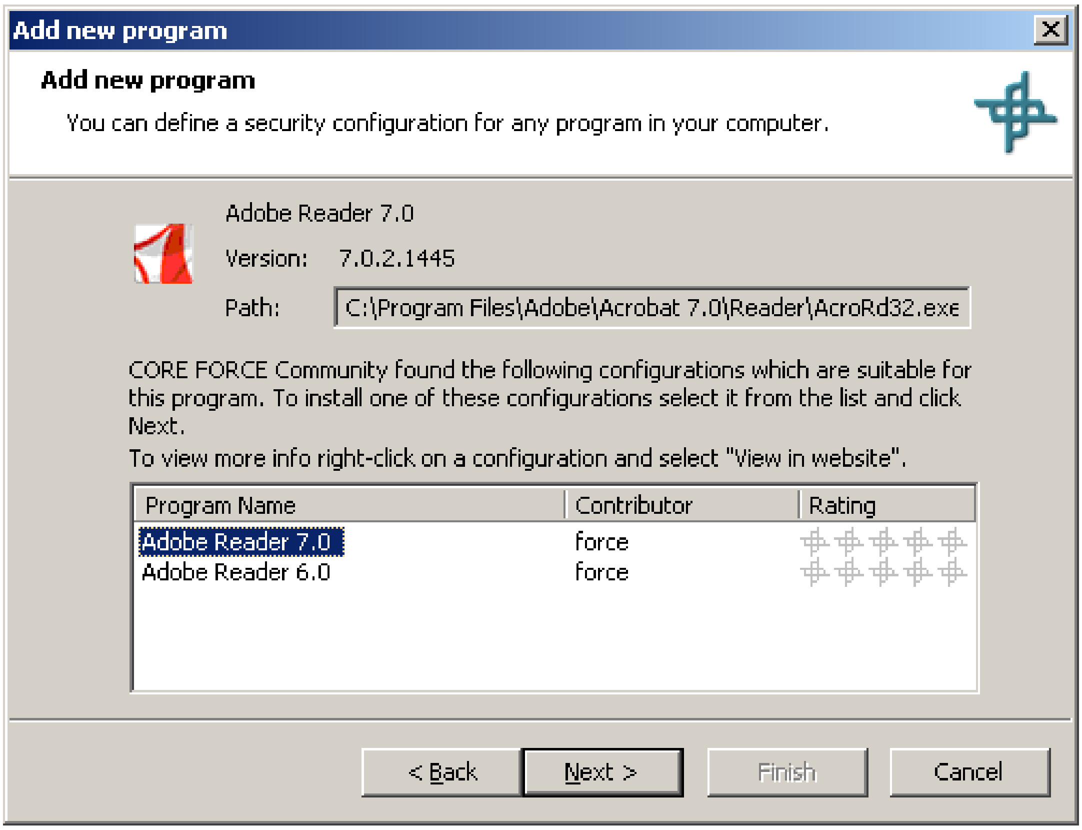
Program Name — This is the name of the security profile given by the Contributor.

Contributor — This is the user that submitted the profile to the community (Users must register in CORE FORCE website to be able to share security profiles. The registration to the community is free).

Rating — This is defined by votes from registered users in the CORE FORCE Community.

The security profiles in the list are sorted by the matching criteria listed above and their associated rating (In the example you can see that there are two security profiles available for Mozilla Thunderbird, and that the first one has a higher rating than the other). If you want to get more information about a profile before selecting it, right-click on the *Program Name* and select *View in Website*.

Another probable scenario is that CORE FORCE Community will report some security profiles that do not match your program's exactly. Figure 1.16, “Adobe Acrobat Reader profiles” shows two matching profiles for Adobe Acrobat Reader 7.0, the first item is shown above because it matches the executable's file signature (and the remaining profile is is returned based on the executable's file name).



**Add new program**

You can define a security configuration for any program in your computer.

Adobe Reader 7.0

Version: 7.0.2.1445

Path: C:\Program Files\Adobe\Acrobat 7.0\Reader\AcroRd32.exe

CORE FORCE Community found the following configurations which are suitable for this program. To install one of these configurations select it from the list and click Next.

To view more info right-click on a configuration and select "View in website".

| Program Name | Contributor | Rating |
|---|---|---|
| Adobe Reader 7.0 | force | ✚✚✚✚✚ |
| Adobe Reader 6.0 | force | ✚✚✚✚✚ |

**Figure 1.16. Adobe Acrobat Reader profiles**

Once you have selected the security profile to be installed, the wizard will download it from CORE FORCE Community and import it into your local security configuration.

## Creating a new security configuration for a program

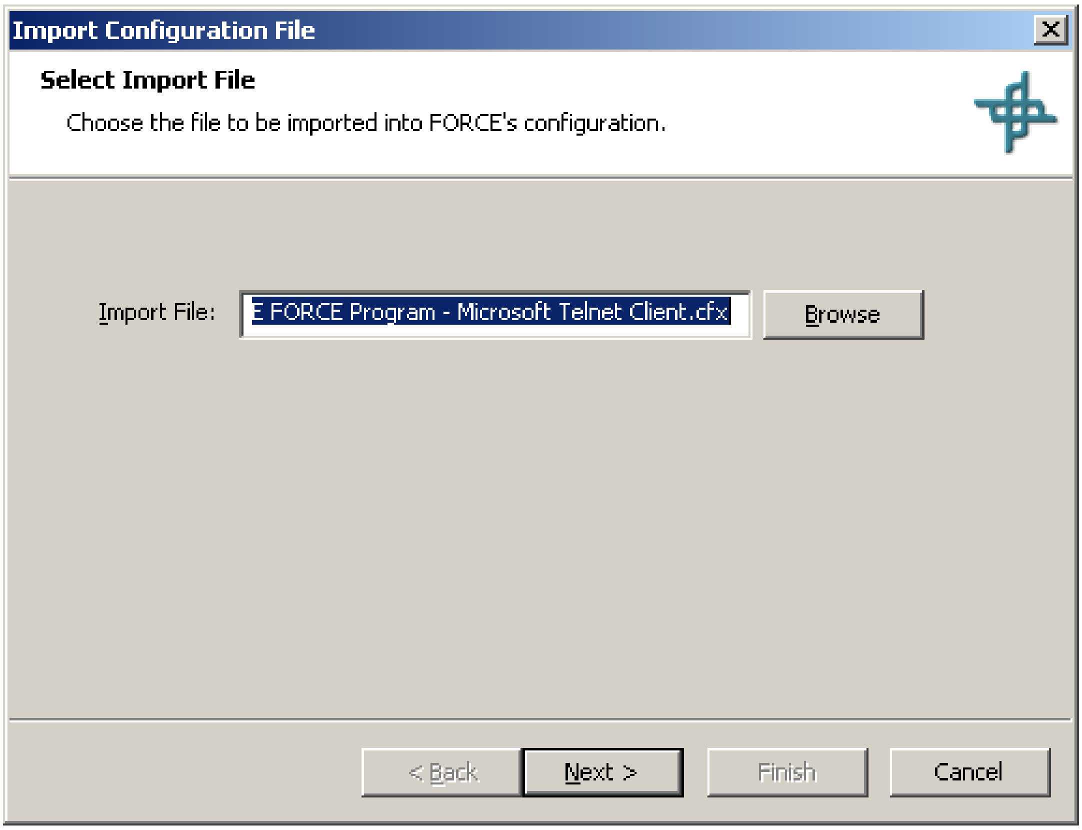
If you want to create a security profile for a program from scratch, you need to follow the first two steps described above and select *Add new program configuration* in the step shown in Figure 3. The wizard will then ask you for a name for the new security profile (it suggests a name based on the program's name and version retrieved from the executable's file).

If you're new to CORE FORCE, it's recommended that you read the chapter *Configuring application profiles*.

## Importing a security profile from a file

Security profiles can also be exported to files (to back them up or to use them in other computers without submitting them to CORE FORCE Community). To export a program's security configuration, right-click on the program's name and select *Export Configuration* from the pop-up menu.

An exported security profile can be imported back into CORE FORCE by selecting *Import Configuration* from the *Tools* menu (See Figure 1.17, “Import configuration”).



Import Configuration File

Select Import File

Choose the file to be imported into FORCE's configuration.

Import File: E FORCE Program - Microsoft Telnet Client.cfx

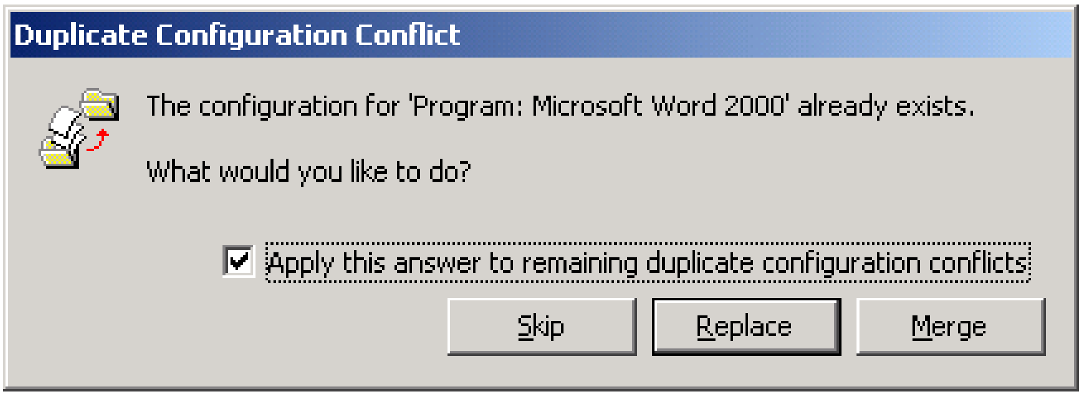
**Figure 1.17. Import configuration**

Every exported file contains, along with the program's security configuration, all the shared policies it references. If these policies are already installed on your system (they could have been included in the built-in database, or they could have been imported with another security profile), a confirmation dialog appears (See Figure 1.18, “Resolving a duplicate configuration conflict”). The available options are:

Skip
: Don't install the policy that comes inside the file and leave the policy on your system unmodified. Choose this option if you have modified the policy to best suit your system configuration.

Replace
: Override the policy installed on your system with the policy inside the file. Use this option if you have not modified the policy. This option will assure that the application you are installing will work exactly as expected and, when the policies are updated, you will update your installation accordingly.

Merge
: This option combine the policy on your system with the policy on the file. The permissions already installed have precedence over the new ones. In this way, the changes you have already made will remain, and the new elements of the profile will be incorporated. On some conditions, this option should produce contradictory policies that does not work as expected.



Duplicate Configuration Conflict

The configuration for 'Program: Microsoft Word 2000' already exists.

What would you like to do?

☑ Apply this answer to remaining duplicate configuration conflicts

**Figure 1.18. Resolving a duplicate configuration conflict**

# Chapter 2. Configuring application profiles

## Organization of a security profile

### Introduction

CORE FORCE has two sets of permissions that are applied to any program running in your computer. If a program has a specific security configuration installed in CORE FORCE, these are the set of permissions that are used to secure it. When there is no appropiate configuration for a program, the default set of permissions is applied, which are configured through *System* (See Figure 2.1, “Default security permissions (*System*) and configuration for specific programs”).

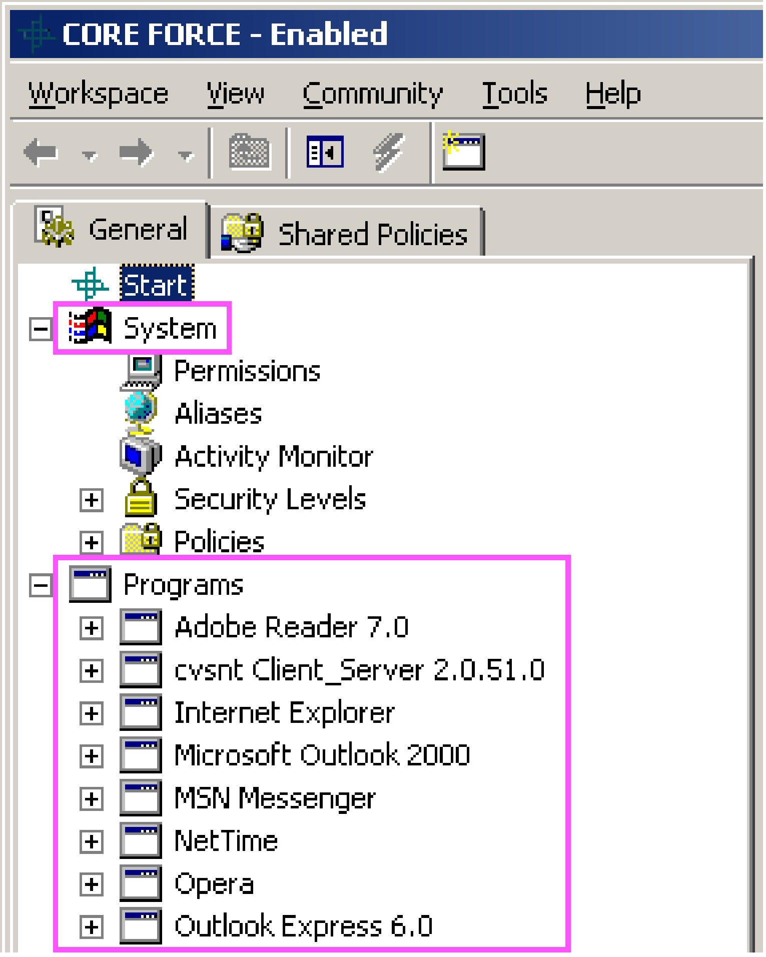


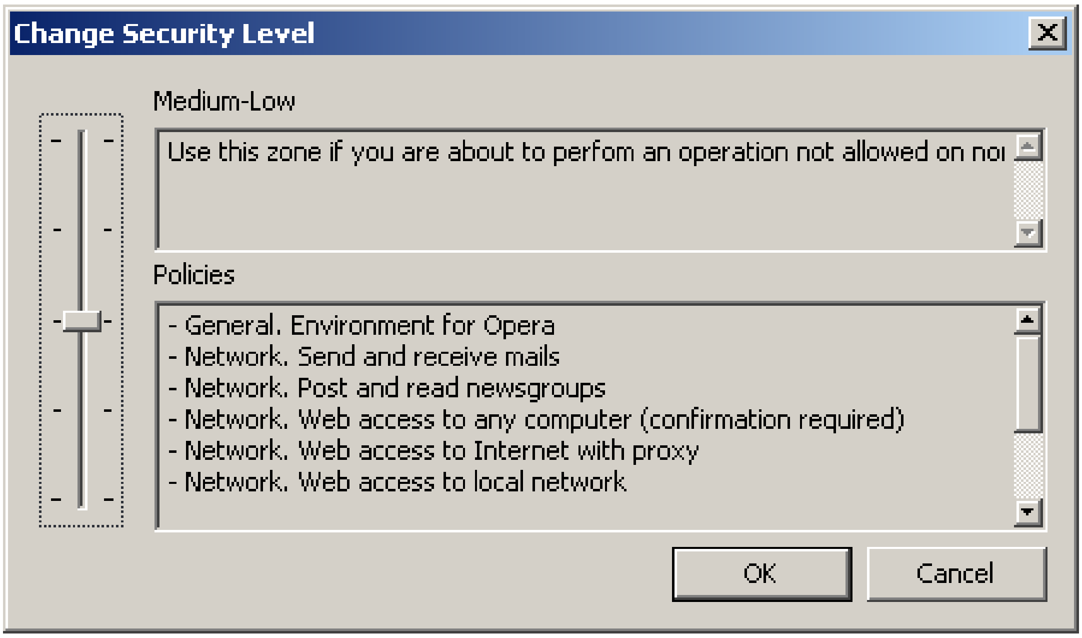
**Figure 2.1. Default security permissions (*System*) and configuration for specific programs**

These set of permissions are usually referred as security profiles, and they group detailed permissions for the program to run correctly and, at the same time, restricted to access appropiate resources only.

### Security Levels

Every security profile has a set of *Security Levels*: High, Medium, Medium-Low, Low and Custom. Each security level is configured by the developer of the profile, and they require a balance between features allowed to work in the program and how loose the security configuration becomes.

An end-user can decide the security level that he considers safe to run a particular program (See Figure 2.2, “Changing the security level of a program”). If at any time, the program requires a more permissive security level to perform a particular action, the program can be temporarily lowered to a new security level.



Medium-Low

Use this zone if you are about to perfom an operation not allowed on noı

Policies

- General. Environment for Opera
- Network. Send and receive mails
- Network. Post and read newsgroups
- Network. Web access to any computer (confirmation required)
- Network. Web access to Internet with proxy
- Network. Web access to local network

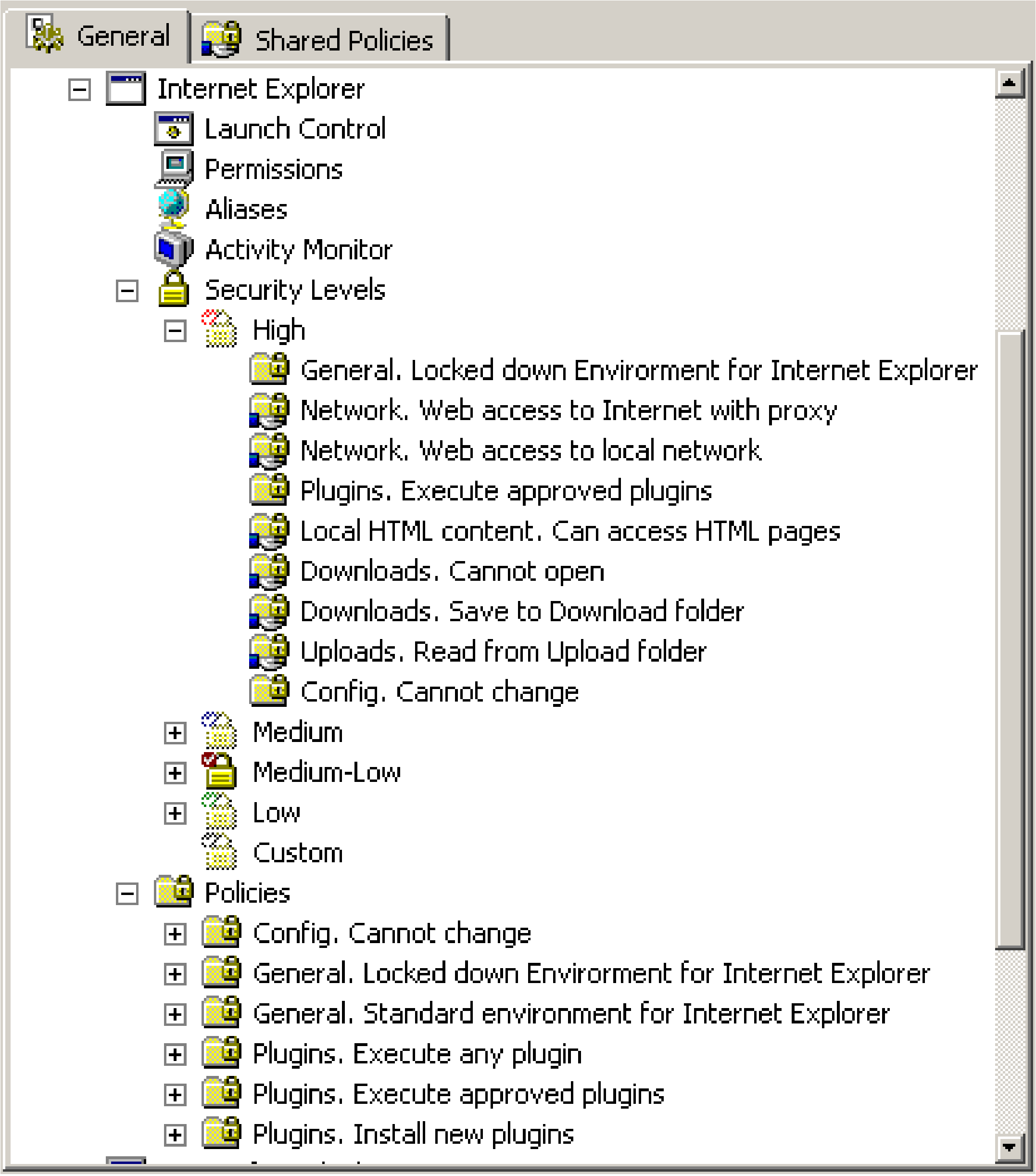
**Figure 2.2. Changing the security level of a program**

# Policies

The basic configuration unit in CORE FORCE is a permission. Permissions can be configured for network resources (with firewall rules), file system and registry objects. This level of detail provides the developer of a security profile with a powerful framework to secure program. At the same time, however, it could overwhelm the user and make the configuration impractical. CORE FORCE provides organizational features that solve this problem by enabling the developer to group permissions in reusable blocks, called *Policies*.

A policy is usually associated with features enabled in a program by the group of permissions it contains. These blocks can then be used throughout the configuration of a program to develop other policies or define a program's security levels. The security profile for MSN Messenger shipped with CORE FORCE, for example, defines a policy named *Network. Web access to Messenger Network* with a set of firewall rules to allow the program to connect with the MSN Messenger network (usually through the port 1863).

Every security profile can define its own collection of policies. These policies are used to establish the set of features that have been configured to run safely. The developer of a security profile then needs to assign policies he has already defined to the security levels where he wants them to be applied (See Figure 2.3, “Policies assigned to security level High in Internet Explorer”).



General | Shared Policies

- Internet Explorer
  - Launch Control
  - Permissions
  - Aliases
  - Activity Monitor
  - Security Levels
    - High
      - General. Locked down Envirorment for Internet Explorer
      - Network. Web access to Internet with proxy
      - Network. Web access to local network
      - Plugins. Execute approved plugins
      - Local HTML content. Can access HTML pages
      - Downloads. Cannot open
      - Downloads. Save to Download folder
      - Uploads. Read from Upload folder
      - Config. Cannot change
    - Medium
    - Medium-Low
    - Low
    - Custom
  - Policies
    - Config. Cannot change
    - General. Locked down Envirorment for Internet Explorer
    - General. Standard environment for Internet Explorer
    - Plugins. Execute any plugin
    - Plugins. Execute approved plugins
    - Plugins. Install new plugins

**Figure 2.3. Policies assigned to security level High in Internet Explorer**

In order to define a policy, the developer needs to create it and assign it a name (which should describe the functionality enabled by the associated set of permissions). The permissions applied by the policy can be configured by selecting the *Permissions* item it contains (See Figure 2.4, “Configuration options of a policy”), which shows the editors to define firewall, file system and registry permissions. Additionally, the user can reuse other policies in order to define a new set of permissions by linking them through the *Assigned Policies* item.

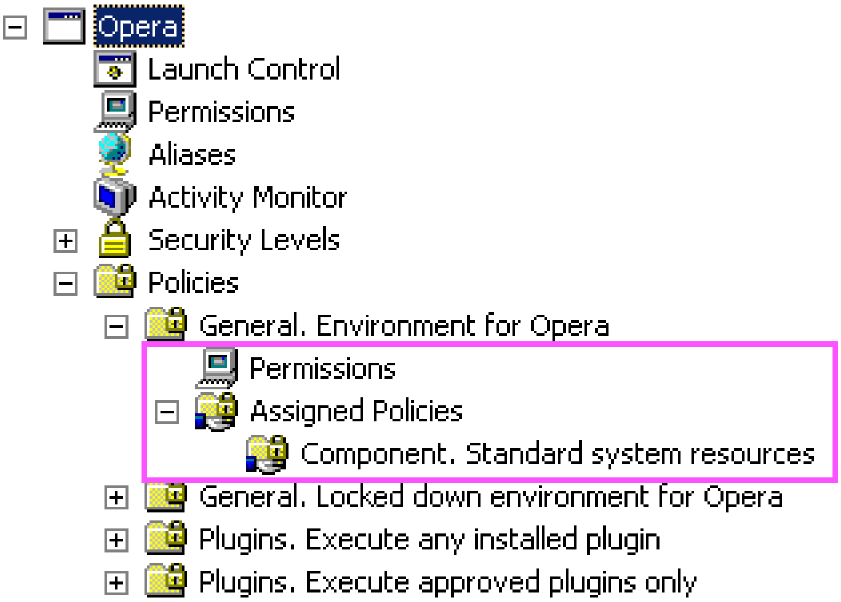
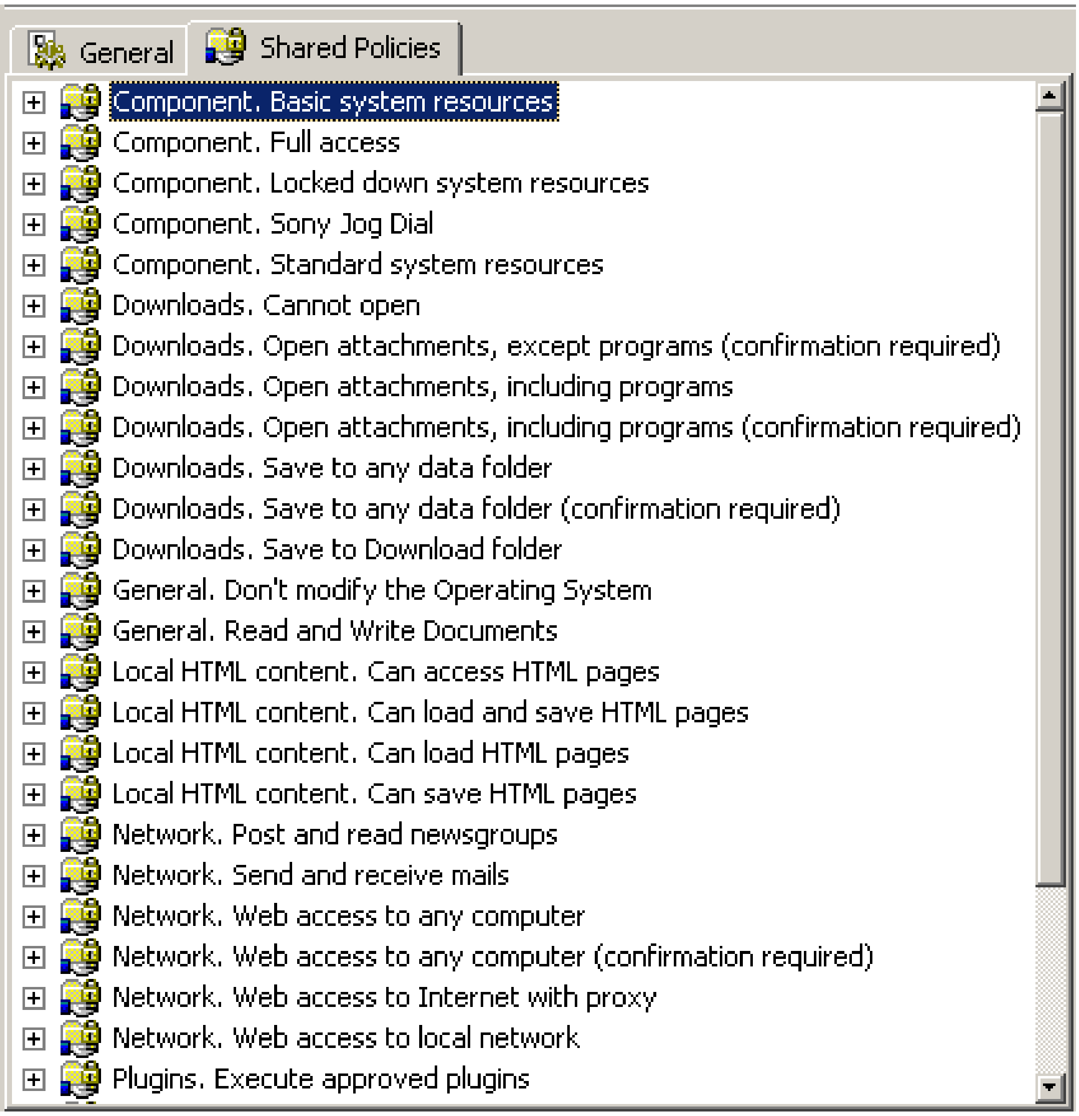

Opera
Launch Control
Permissions
Aliases
Activity Monitor
Security Levels
Policies
General. Environment for Opera
Permissions
Assigned Policies
Component. Standard system resources
General. Locked down environment for Opera
Plugins. Execute any installed plugin
Plugins. Execute approved plugins only

**Figure 2.4. Configuration options of a policy**

Policies that can be used in more than one program are created as *Shared Policies*, and can then be assigned to any program's security levels. The policy *Enable web connections to the intranet* is a good example of a Shared Policy, because it can be assigned to a large number of applications, and its permissions can be applied to all of them. On the other hand, a policy called *Disable logging* may not be useful as a Shared Policy if every program requires different permissions to write their logs. Figure 2.5, “Shared Policies shipped with CORE FORCE” shows some Shared Policies that are shipped with CORE FORCE.



- Component. Basic system resources
- Component. Full access
- Component. Locked down system resources
- Component. Sony Jog Dial
- Component. Standard system resources
- Downloads. Cannot open
- Downloads. Open attachments, except programs (confirmation required)
- Downloads. Open attachments, including programs
- Downloads. Open attachments, including programs (confirmation required)
- Downloads. Save to any data folder
- Downloads. Save to any data folder (confirmation required)
- Downloads. Save to Download folder
- General. Don't modify the Operating System
- General. Read and Write Documents
- Local HTML content. Can access HTML pages
- Local HTML content. Can load and save HTML pages
- Local HTML content. Can load HTML pages
- Local HTML content. Can save HTML pages
- Network. Post and read newsgroups
- Network. Send and receive mails
- Network. Web access to any computer
- Network. Web access to any computer (confirmation required)
- Network. Web access to Internet with proxy
- Network. Web access to local network
- Plugins. Execute approved plugins

**Figure 2.5. Shared Policies shipped with CORE FORCE**

# Priority and override of permissions

As explained above, the security configuration is defined a three different levels (which are visually represented by the configuration interface), as shown in Figure 2.6, “Organization of a security profile”

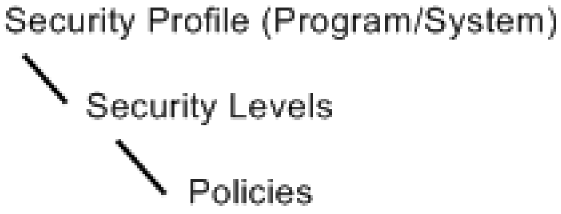


**Figure 2.6. Organization of a security profile**

Permissions have been shown to be configured only in Policies, that are then assigned to appropiate security levels. If two policies assigned to a security level provide a permission to the same object, the last referenced policy overrides the previous one. This is generally used to define a restrictive set of permissions (for example, blocking all network access and changes to the file system and registry), that is then relaxed by additional policies that enable a program's features. To change the order of policies assigned to a security level, select a policy and use the ↑ ↓ buttons in the toolbar.

Finally, a user may require some minor tweaks for a security profile to work correctly in his machine (for example, to enable a program's access to another local network, or to allow a program to write to additional file system folders). This configuration is usually placed in the *Permissions* item inside a security profile (See Figure 2.7, “Permissions for a security profile”).

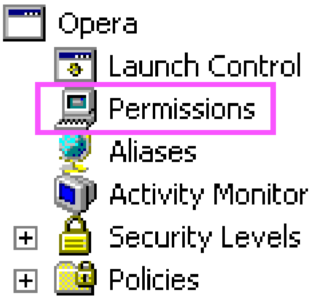


**Figure 2.7. Permissions for a security profile**

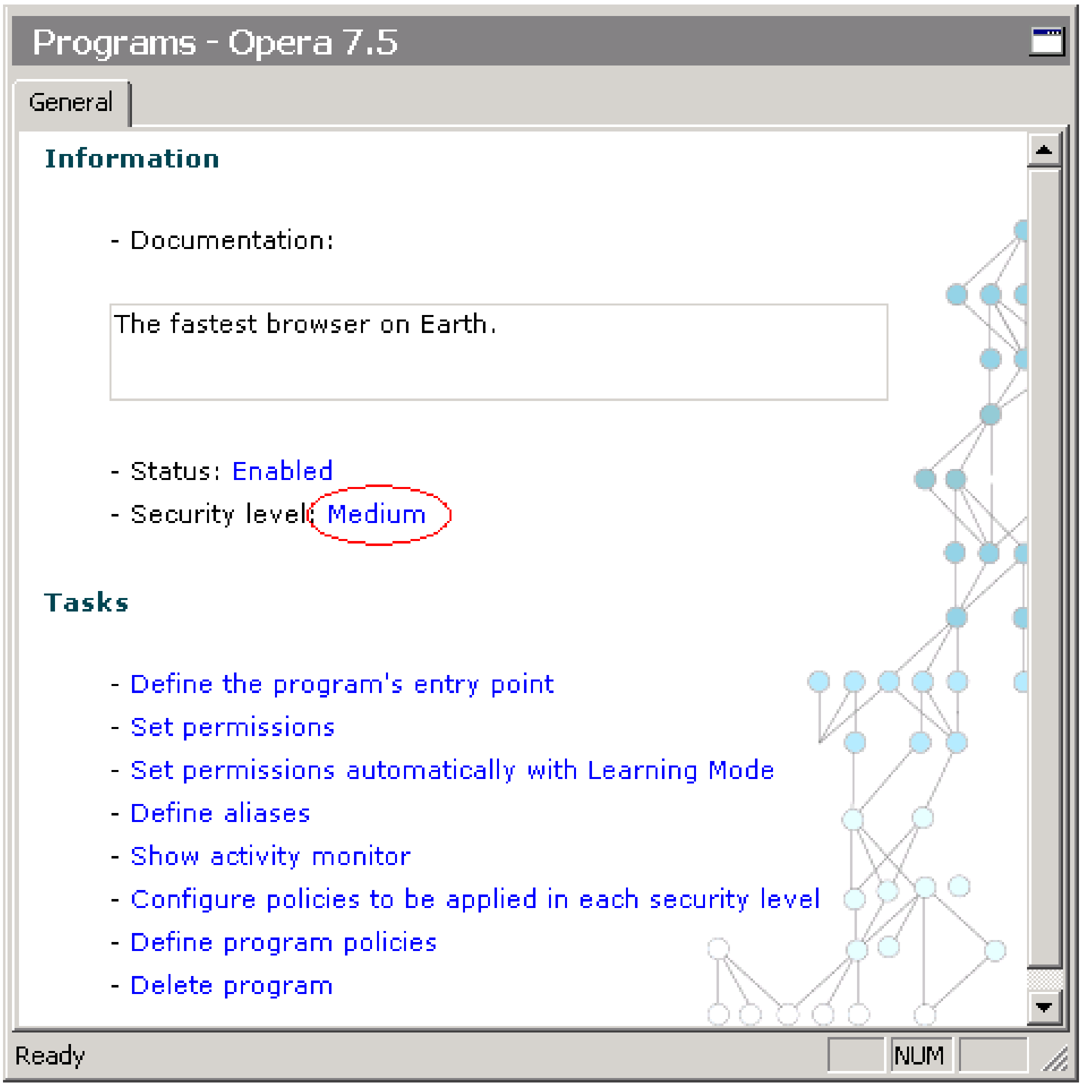
Permissions configured there have higher priority than those from the current security level and thus override them. Additionally, this item can be used to view all permissions being applied (from all policies assigned to the current security level).

# Using security levels and policies

Security levels are the simplest method to change the configuration settings of an application. It allows to assign a complete security environment all-at-once with a single click. On this section, you will see how to change the security level of an application, how to create a new level for specific tasks and how to modify the standard security levels to best suit your needs.

## Selecting a security level

When you select an application from the workspace, the main window displays, among other details and common tasks, the active security level for the application (Figure 2.8, “Information pane and common tasks for an application profile”). To change it, simply click the name of the active level (displayed in blue). A dialog box will appear containing information about the available security levels (Figure 2.9, “Change security level wizard”). Use the slider bar to select the desired level, and a brief description of the settings associated with the selected level will be displayed.



**Information**

- Documentation:

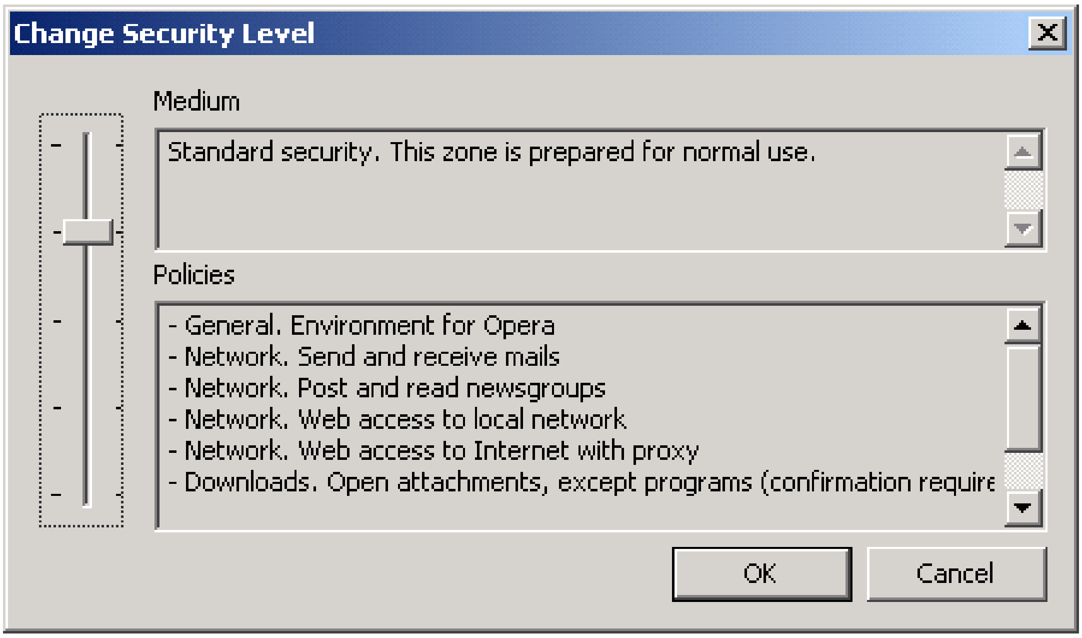
The fastest browser on Earth.

- Status: Enabled
- Security level: Medium

**Tasks**

- Define the program's entry point
- Set permissions
- Set permissions automatically with Learning Mode
- Define aliases
- Show activity monitor
- Configure policies to be applied in each security level
- Define program policies
- Delete program

**Figure 2.8. Information pane and common tasks for an application profile**



Medium

Standard security. This zone is prepared for normal use.

Policies

- General. Environment for Opera
- Network. Send and receive mails
- Network. Post and read newsgroups
- Network. Web access to local network
- Network. Web access to Internet with proxy
- Downloads. Open attachments, except programs (confirmation require

**Figure 2.9. Change security level wizard**

# Modifying a security level

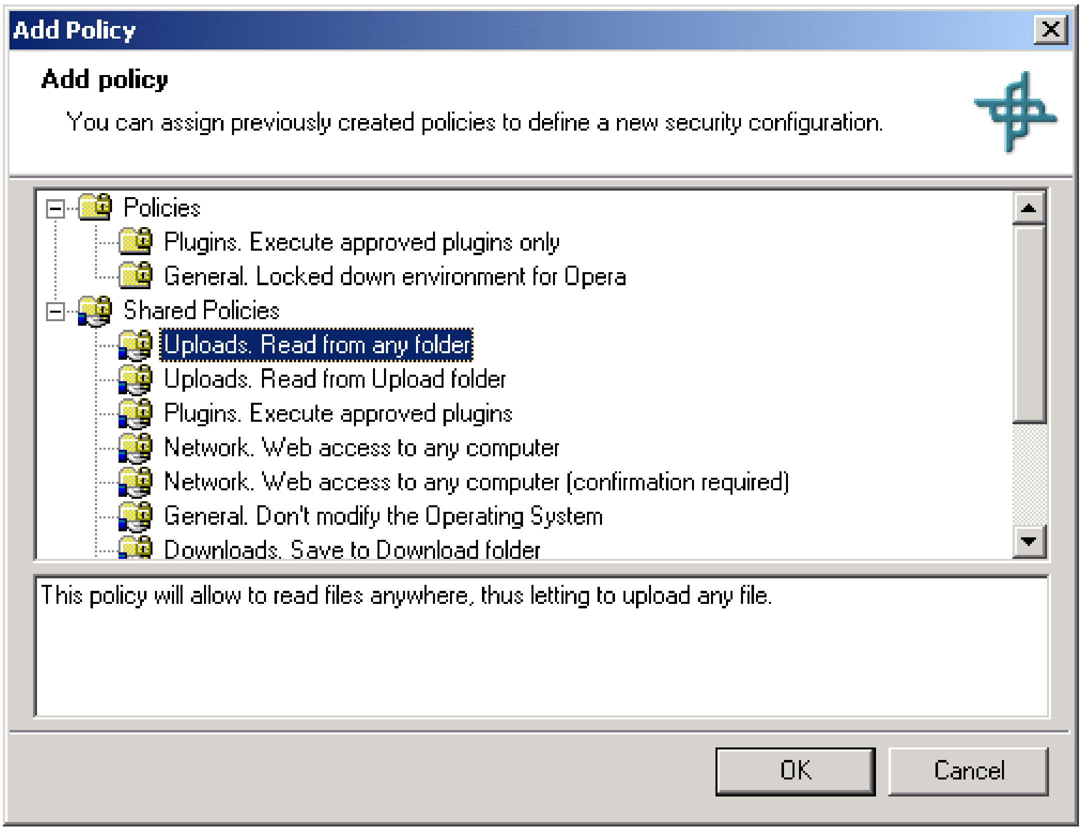
Security levels are composed of a group of policies, either shared and non-shared. When a security level is activated, the permissions contained inside these policies are enforced, along with those directly defined on the program. You can also temporarily enable/disable individual policies inside the security levels, and change the order of evaluation.

The standard security levels (High, Medium, Medium-Low and Low) are defined by the author of the profile and intended to reflect increasing levels of security. Another level, named Custom, is included on each profile (on the change security level dialog, it appears at the bottom of the list). You can use this level to define permissions that need to be used on special occassions. For example, when using Internet Explorer to access the Windows Update service.

If you need to make permanent changes for a profile, we suggest that you modify High, Medium, Medium-Low or Low security levels instead of using the level Custom.

To change the list of policies assigned to a security level, follow these steps:

1. Select the application you want to modify from the workspace
2. Click Configure Security Levels and then the security level you want to modify, or direcly select the security level inside the subtree of the application from the workspace.
3. To add a new policy for the level, click Add policy or the Add policy icon on the toolbar (✚). The Add policy dialog will appear (Figure 2.10, “Add Policies wizard”). Select a policy from the list to view a brief description of it.
4. To remove a policy, expand the level's subtree in the workspace and select the policy you want to remove. Then, click Remove policy or the Remove policy button in the toolbar (✕).



Add Policy

Add policy

You can assign previously created policies to define a new security configuration.

- Policies
  - Plugins. Execute approved plugins only
  - General. Locked down environment for Opera
- Shared Policies
  - Uploads. Read from any folder
  - Uploads. Read from Upload folder
  - Plugins. Execute approved plugins
  - Network. Web access to any computer
  - Network. Web access to any computer (confirmation required)
  - General. Don't modify the Operating System
  - Downloads. Save to Download folder

This policy will allow to read files anywhere, thus letting to upload any file.

**Figure 2.10. Add Policies wizard**

The permissions of the policies are applied sequentially from top to bottom: if two policies define permissions for the same item, those defined on the last one will be applied. The permissions defined inside the application are applied at the end, and so they have precedence. You can change the order of the policies by clicking move up and move down buttons on the toolbar ( ↑ and ↓ ).

# Creating new policies

If you want to add new permissions to a profile, we strongly recommend that you create a new policy. In this way, your profile will be more usable by others and clearer to understand and modify.

### Note

If the policy you are about to create could be used in other applications, you should create a *Shared Policy*.

To configure access permissions for the new policy you can: set specific network, files and registry permissions, or include other policies.

To create a new local policy for the application, follow these steps:

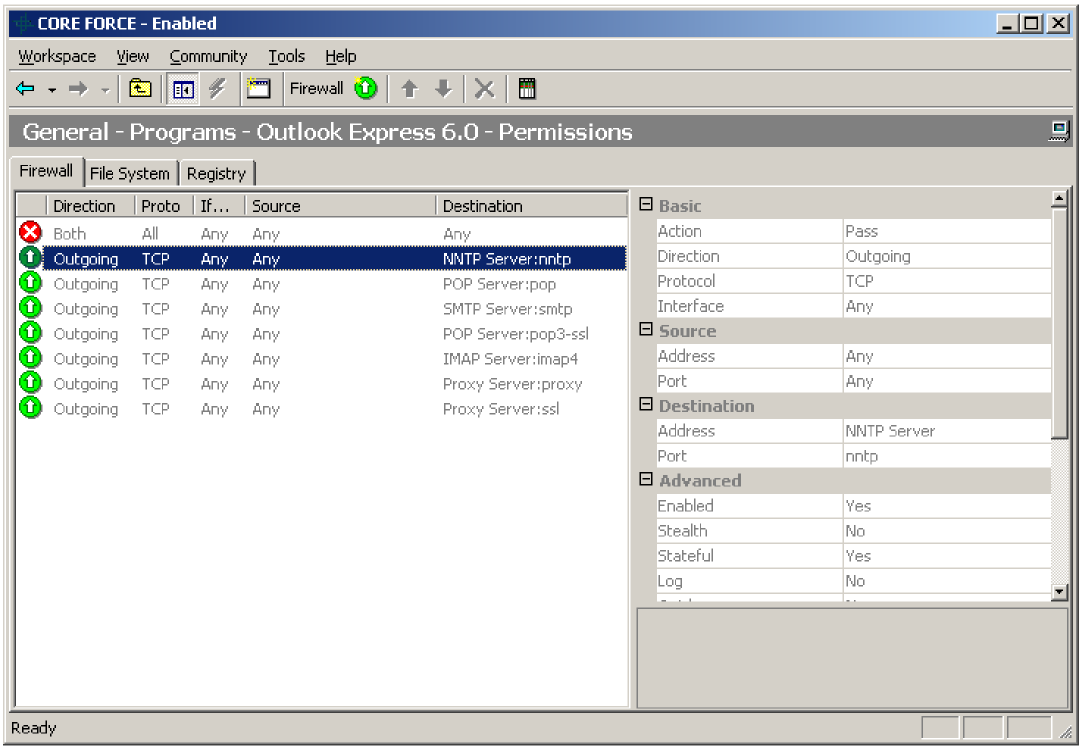
1. In the workspace, select the *Policies* item inside the application where the policy will reside.
2. Click on Create policy, or click on the Create Policy button on the toolbar (📁).
3. Write the name of the new policy and click Finish

# Customizing network permissions

Network permissions for an application or for the entire system are specified by a list of rules. The rules are consist in a *filter* and an *action*. The filter defines what connections (and individual network packets) will be processed, and the action dictates what to do with them. If a given connection matches more than one rule, the action associated with the last matching rule will be applied.

There are three possible actions: *block*, *pass* and *ask*. Ask allows the user to decide what to do when a matching connection is established by an application. For the definition of the filter, several options are available for either beginners and proffesional users, ranging from source and destination host/port to specific TCP flags and ICMP codes.

The network permissions are accessed by selecting the *firewall* subcategory on the *permissions* category. The window layout is shown on Figure 2.11, “Firewall permissions view”. On the left, a list of rules is shown. Selecting a rule shows on the right the customization options for that rule.



| | Direction | Proto | If... | Source | Destination |
|---|---|---|---|---|---|
| ✗ | Both | All | Any | Any | Any |
| ⬆ | Outgoing | TCP | Any | Any | NNTP Server:nntp |
| ⬆ | Outgoing | TCP | Any | Any | POP Server:pop |
| ⬆ | Outgoing | TCP | Any | Any | SMTP Server:smtp |
| ⬆ | Outgoing | TCP | Any | Any | POP Server:pop3-ssl |
| ⬆ | Outgoing | TCP | Any | Any | IMAP Server:imap4 |
| ⬆ | Outgoing | TCP | Any | Any | Proxy Server:proxy |
| ⬆ | Outgoing | TCP | Any | Any | Proxy Server:ssl |

| | |
|---|---|
| **Basic** | |
| Action | Pass |
| Direction | Outgoing |
| Protocol | TCP |
| Interface | Any |
| **Source** | |
| Address | Any |
| Port | Any |
| **Destination** | |
| Address | NNTP Server |
| Port | nntp |
| **Advanced** | |
| Enabled | Yes |
| Stealth | No |
| Stateful | Yes |
| Log | No |

**Figure 2.11. Firewall permissions view**

# Manipulating the rules

To create a rule, right-click on the list of rules and choose new, or click the New button from the toolbar (⬆). A new rule is created and stored at the end of the list.

A rule can be removed from the list by clicking the Remove button on the toolbar (✗), or by selecting it and pressing the **Delete** key.

To specify the order of evaluation, use the move down and move up options on the context menu, or the corresponding buttons on the toolbar ( ↑ and ↓ ).

# Specifying connections based on destination address

# and port

Most of the regular connections can be defined by specifying the protocol, the destination host and the destination port. A simple rule is obtained by leaving all the other options at their default values.

To make the configuration more flexible and understandable, and allow the portability of the profiles, host addresses and ports are defined indirectly through *aliases*. The content of the alias can be modified at any time to reflect changes in the network (for example, a change on the IP of the mail server).

To create a new basic rule, follow these steps:

1. Create a new rule by right-clicking on the list of rules and choosing *new*.
2. Choose the protocol. The option is located on the *basic* section of the Properties control.
3. Write the destination address. You can specify the address in several ways (see next paragraph). If the address exists and can be used, the IP number will appear on the section Information, at the bottom of the property control.
4. Write the destination port number or the port name. Notice that this option is active if the protocol is either *TCP* or *UDP*. If the number is valid, or the name was already defined, it will appear on the Information section.

As stated previously, CORE FORCE provides several ways to specify host addresses and ports. For addresses, the options are:

### Note

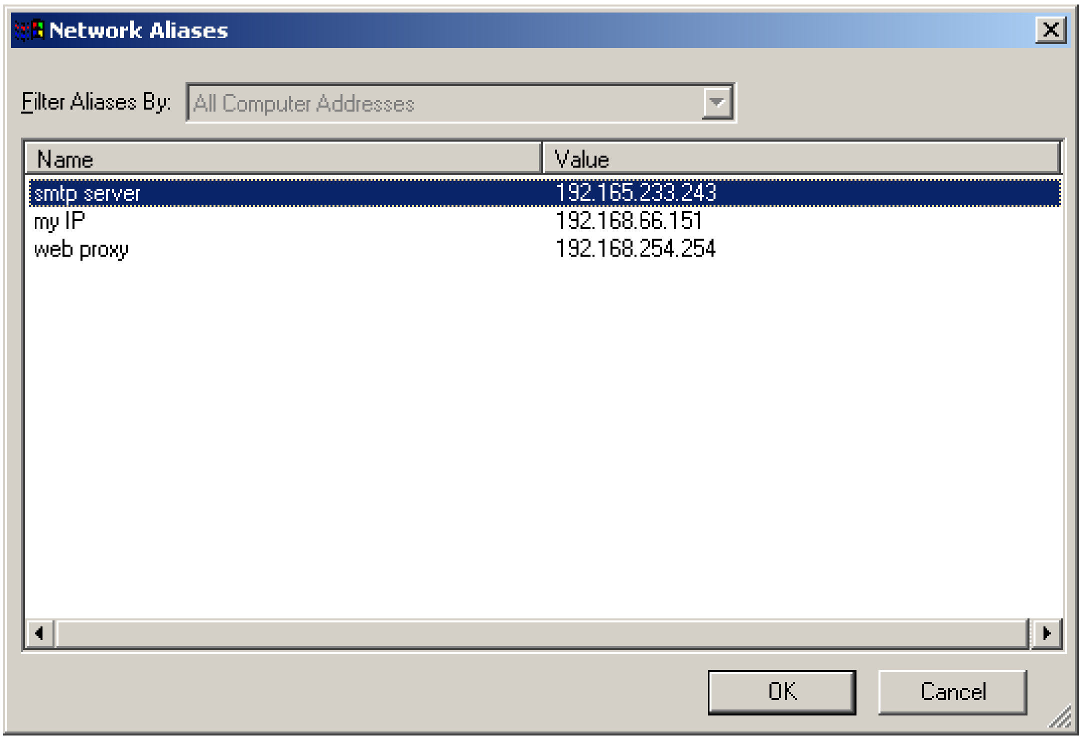
To modify a global alias, go to the Aliases element on the System Workspace.

- Choose a predefined alias (either local to the application or global) from the list of aliases. To choose a predefined alias, select <specific...> from the drop-down list. The alias selection dialog will appear (see Figure 2.12, “The network address aliases dialog”). This list displays the name of the alias on the left and the IP address on the right. The global aliases are displayed grayed and cannot be modifed from this dialog. The local aliases (those defined for the application being configured) can be modified by selecting an alias and choosing Edit from the context menu. To choose an alias for the rule, select it from the list and click OK. The name of the alias will be displayed on the address field, and the IP address in the Information section.
- Write the name of a predefined alias. This option is useful if you already know the name of the alias you want to use (notice that you have to spell it correctly).
- Write the name of the host (for example, `www.google.com`). If the host name can be resolved, an local alias will be created. The name of the alias will be the name of the host, and its address will be resolved. If the host is invalid, the field will not be changed.
- Write the IP address of the host. In this case, a new alias will be created. The name of the alias will be the IP address.

For ports, the options are:

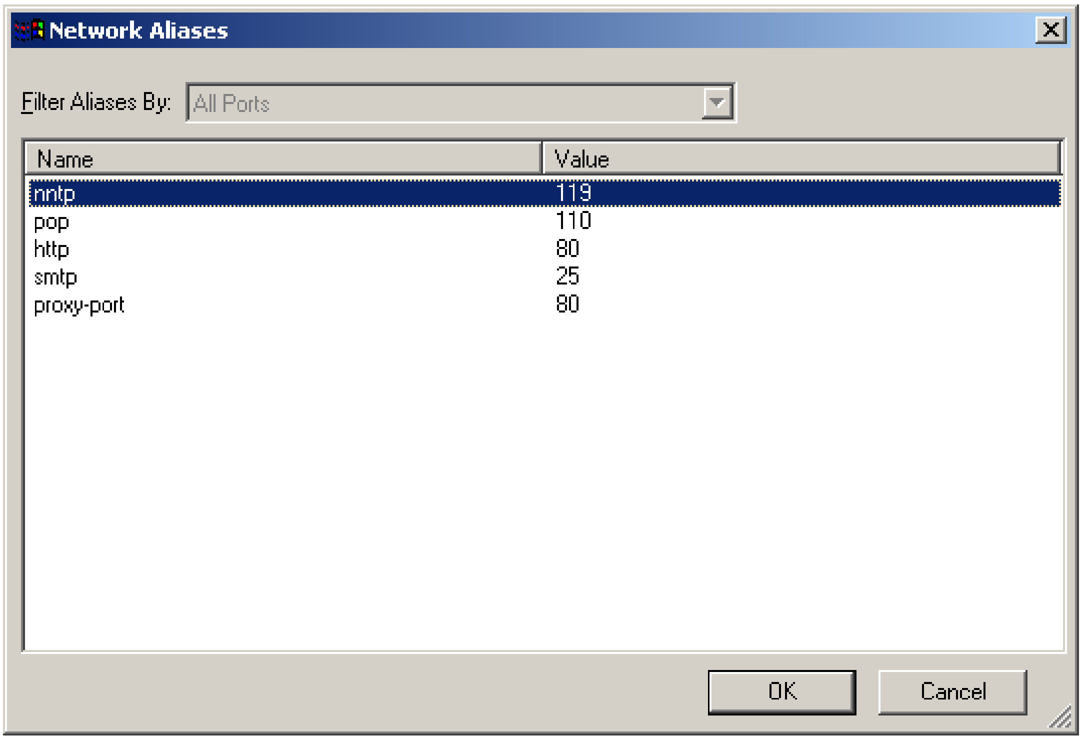
- Choose a predefined alias from the list of aliases (see Figure 2.13, “The network port aliases dialog”). The port number will be displayed in the Information section.
- Write the name of a predefined alias. This option is useful if you already know the name of the alias you want to use (notice that you have to spell it correctly).

- Write the port number directly. In this case, a new alias will be created. The name of the alias will be the port number.



| Name | Value |
|---|---|
| smtp server | 192.165.233.243 |
| my IP | 192.168.66.151 |
| web proxy | 192.168.254.254 |

## Figure 2.12. The network address aliases dialog



| Name | Value |
|---|---|
| nntp | 119 |
| pop | 110 |
| http | 80 |
| smtp | 25 |
| proxy-port | 80 |

## Figure 2.13. The network port aliases dialog

# Advanced options

The firewall component of CORE FORCE is based on the firewall of OpenBSD, PF (see PF: The OpenBSD Packet Filter [http://www.openbsd.org/faq/pf/]). As such, it has advanced features only found in full-blown, commercial firewalls and not in personal firewalls.

Some of the advanced options are:

Stateful

If a packet matches a rule with this option turned on (the rule includes the keywords keep state), CORE FORCE creates a state for this connection and automatically passes all subsequent packets belonging to the connection.

Stealth

In general, the response given by a system is different if it is protected with a firewall that if it is not. Because of this, an attacker can detect the presence or absence of a firewall. If the stealth option is turned on for a given rule, the system act as if the firewall were not present. This is done by answering all the external packets instead of silently dropping them.

IP Options

By default, network packages with IP options are discarded automatically. To accept this kind of packets, create a rule with this option turned on.

TCP Flags

This option allows the user to specify which flags should be turned on and which flags should be turned off for a given TCP packet in order to be handled by the rule.

You can use this option to identify the first packet of an outgoing connection (SYN flag turned on and ACK flag turned off), packages accepting connections (SYN and ACK flags turned on) and packages that abort connections (RST flag turned on), among others.

Using this option along with stateful option, you can permit connections that have been established normally only.

ICMP Options

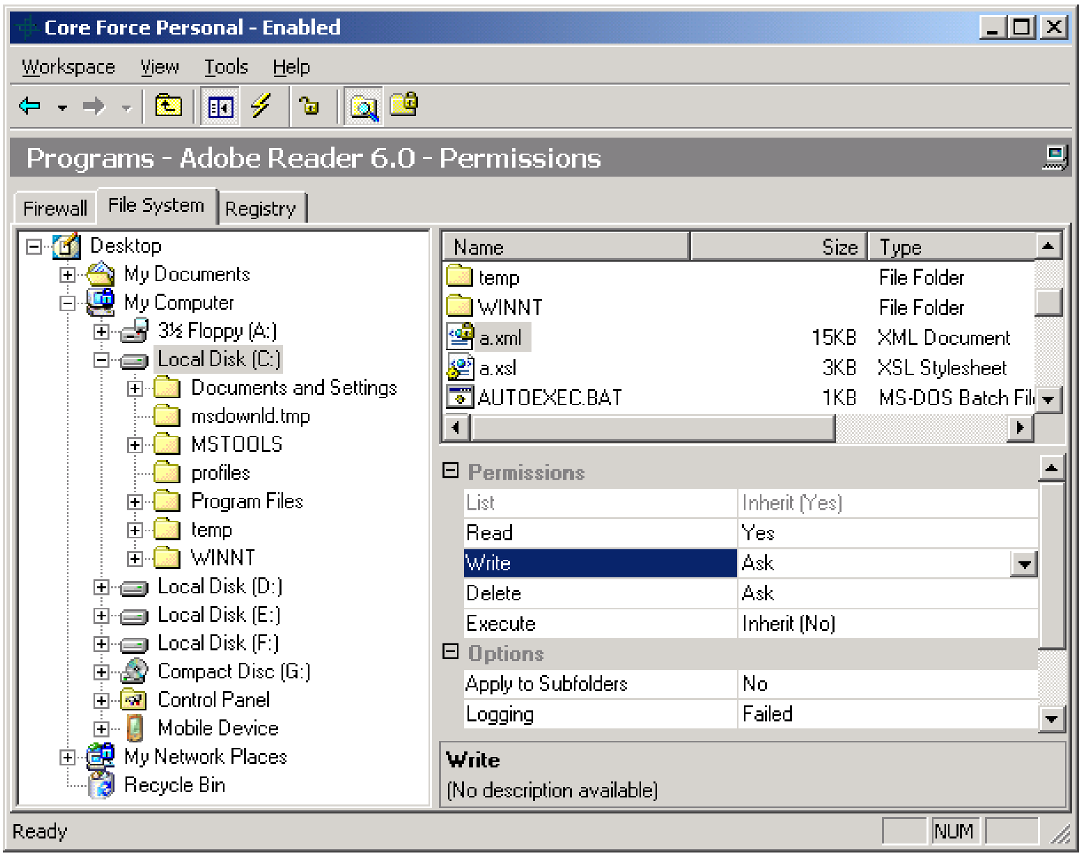
The ICMP protocol is used with very different purposes. This option allows you to specify exactly what ICMP packages you want to block or accept. For example, you can block *ping* requests (type *echoreq*), but permit unreachable reports (type *unreach*).

# Customizing file and registry permissions

The permissions category holds all the options related to the customization of individual items. It is divided in three subcategories: File System, Registry and Firewall. Each subcategory is activated by clicking on the respective tab at the top of the main window.

The File System and Registry subcategories are very similar in terms of window layout and configuration options, and will be described on this section. In the next section we will describe the Firewall subcategory, which stores the rules that specify network permissions.

There are two different views for File System and Registry: the *explorer view* (Figure 2.14, “File System Explorer View”) and the *resources view* (Figure 2.15, “File System Resources View”). The former, displays all the files and folders stored on your computer, and allows to secure them in-place. This view is the preferred method for creating new profiles and defining access rights for the first time. The latter, displays a virtual tree that contains only the customized items and general rules, replacing real file names and folders by aliases and regular expressions when possible. This view is used for generating general rules (such as those based on regular expressions), for cleaning up a malfunctioning profile or simplifying a bloated one, and for preparing a profile for deployment on other computers. To switch the view, use the buttons on the toolbar: 🔍 and 🔐.



Programs - Adobe Reader 6.0 - Permissions

- Desktop
  - My Documents
  - My Computer
    - 3½ Floppy (A:)
    - Local Disk (C:)
      - Documents and Settings
      - msdownld.tmp
      - MSTOOLS
      - profiles
      - Program Files
      - temp
      - WINNT
    - Local Disk (D:)
    - Local Disk (E:)
    - Local Disk (F:)
    - Compact Disc (G:)
    - Control Panel
    - Mobile Device
  - My Network Places
  - Recycle Bin

| Name | Size | Type |
|---|---|---|
| temp | | File Folder |
| WINNT | | File Folder |
| a.xml | 15KB | XML Document |
| a.xsl | 3KB | XSL Stylesheet |
| AUTOEXEC.BAT | 1KB | MS-DOS Batch Fil |

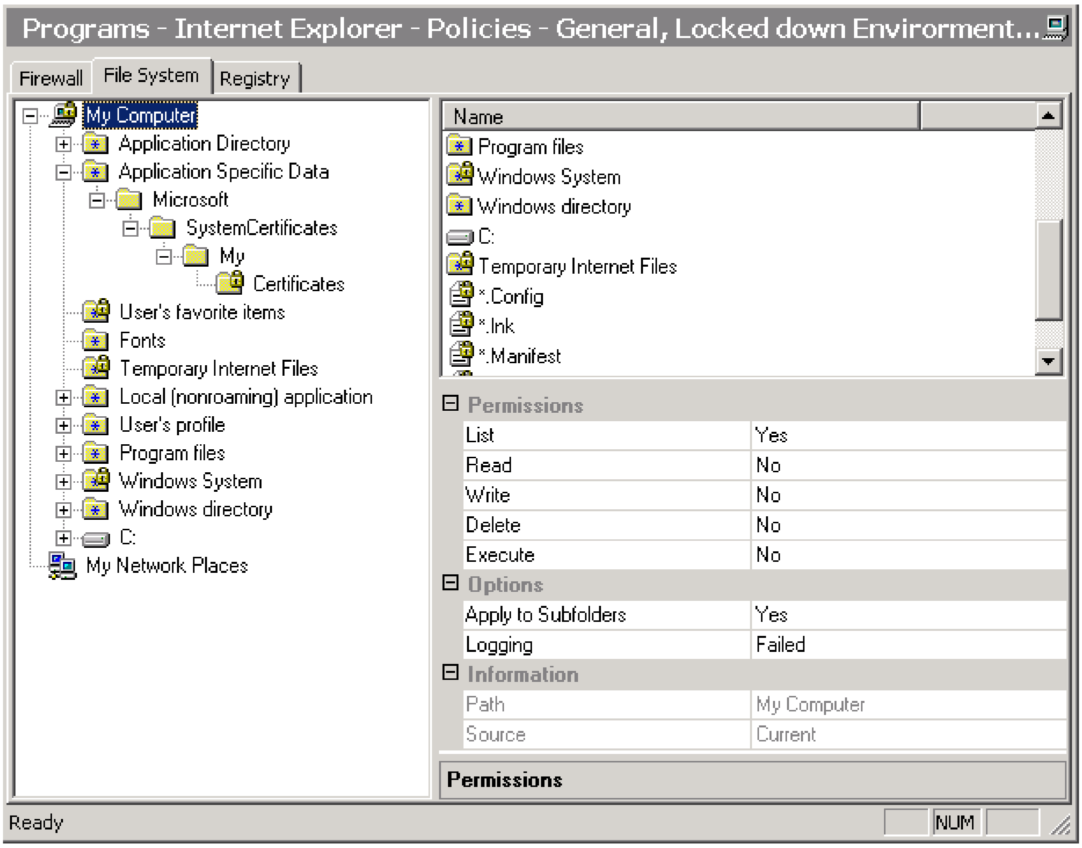
| Permissions | |
|---|---|
| List | Inherit (Yes) |
| Read | Yes |
| Write | Ask |
| Delete | Ask |
| Execute | Inherit (No) |
| **Options** | |
| Apply to Subfolders | No |
| Logging | Failed |

**Write**

(No description available)

Ready

## Figure 2.14. File System Explorer View


Programs - Internet Explorer - Policies - General, Locked down Envirorment...

- My Computer
  - Application Directory
  - Application Specific Data
    - Microsoft
      - SystemCertificates
        - My
          - Certificates
  - User's favorite items
  - Fonts
  - Temporary Internet Files
  - Local (nonroaming) application
  - User's profile
  - Program files
  - Windows System
  - Windows directory
  - C:
- My Network Places

| Name |
|---|
| Program files |
| Windows System |
| Windows directory |
| C: |
| Temporary Internet Files |
| *.Config |
| *.lnk |
| *.Manifest |

| Permissions | |
|---|---|
| List | Yes |
| Read | No |
| Write | No |
| Delete | No |
| Execute | No |
| **Options** | |
| Apply to Subfolders | Yes |
| Logging | Failed |
| **Information** | |
| Path | My Computer |
| Source | Current |

**Permissions**

Ready

**Figure 2.15. File System Resources View**

# Setting permissions for specific files and folders

You can use the explorer view to specify access rights for existing files and folders on your computer. To do that, after selecting the application profile you want to customize on the programs workspace, follow these steps:

1. Select the Set permissions link in the main window. Alternatively, you can select the permissions category on the workspace pane.

2. Activate the File System subcategory if another is active, by clicking on the respective tab at the top of the main window.

3. Browse your computer's file system in the tree view, and select the folder you want to configure. If you want to configure a file, select the containing folder first, and then select the file from the file list.

4. Change the permissions for the file or folder in the properties control. You will see a lock icon ( 🔒 ) over the icon of the file or folder to indicate that the item was secured.

An item can be customized for a subset of access types only: the options that you don't change remain as inherit, meaning that the actual permission will be deduced from parent folders and general rules. As a hint, when interit is set for an option, the value shown between parenthesis is calculated on-the-fly and represents the permissions that are currently applied to the item.

The Apply to subfolders option is applicable either to directories and files, but the meaning is different, depending on the item's type. For directories, if this option is turned on, the permissions for that item apply to all the files hierarchy rooted at that directory. If it is turned off, the permissions apply to all the files of the directory, but not to the subdirectories and their files. For file items, if the option is turned on, the permissions apply to items with the same name but stored anywhere on the file hierarchy rooted at the same directory of the configured item. with the same name stored on any subdirectory of the but located on any directory that has the same ancestor down from the directory where the file is stored.

# Configuring logging options

When configuring the permissions for files and folders, you can also specify logging option for the item. This option defines what type of information CORE FORCE will store when the application try to access the item. The options are:

- none: no information is stored.

- failed: a log message is generated when CORE FORCE blocks an access to the item

- all: a log message is generated when the application accesses the item, no matters what the result was.

Notice that the logging options apply to secured access types only, and not to access types marked as inherit. For example, if you configure read access to `*.doc` with logging options set as None, and delete access to `persdata.doc` with logging options set to All, no log message will be generated when the file `persdata.doc` is open for reading.

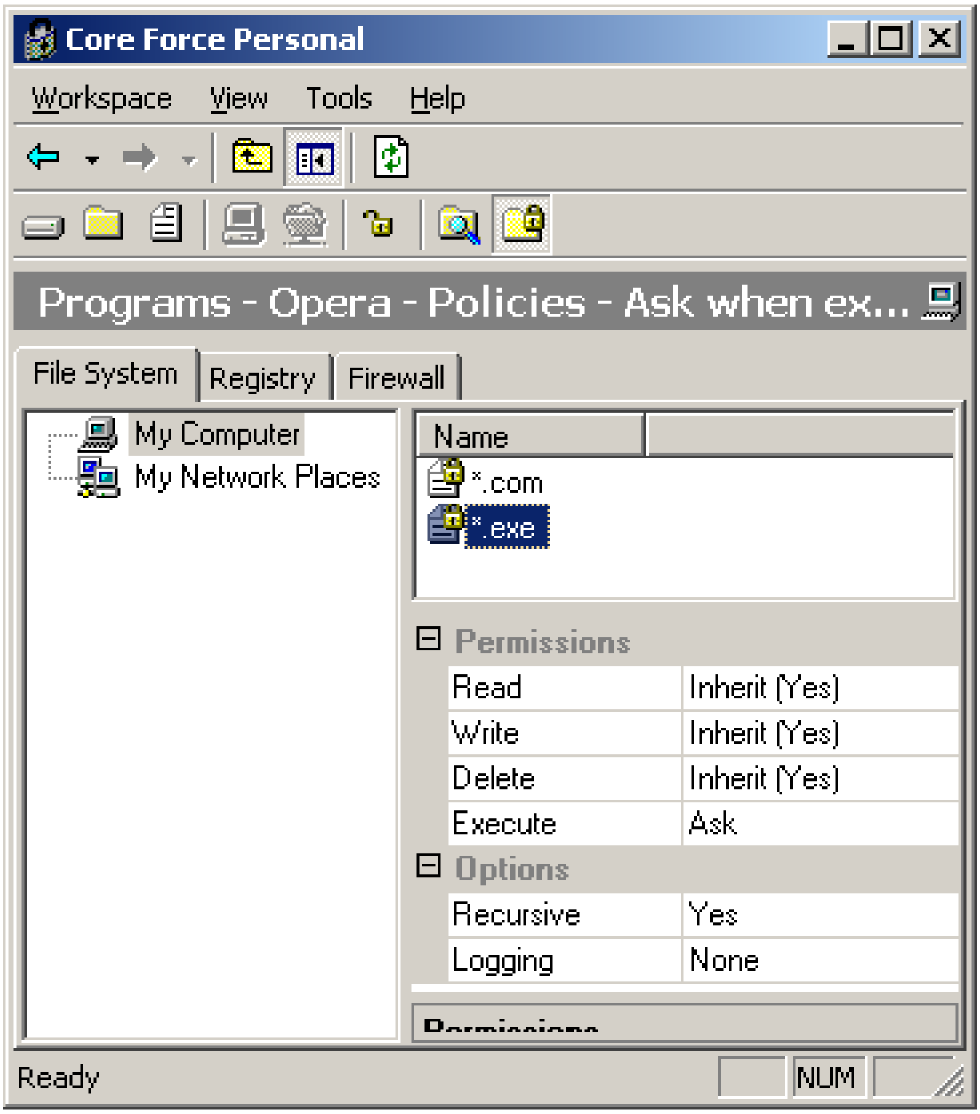
# Regular expressions and wildcards

We have seen how to define permissions for files residing on your computer by browsing the file system and selecting individual files. We have also seen how to specify permissions for a complete subtree using the *Apply to subfolders* option. CORE FORCE gives also the ability to specify access rights based on regular expressions.

In the current version, a regular expression is a string containing any number of wildcard characters. These wildcard characters include: a quotation mark (?), that represents any character, and an asterisk (*), that represent any number of characters, or the empty string. Notice that, due to the way Windows handles the file access, the file names (and as a consequence, the regular expressions) are case insensitive.

The permissions defined by wilcards are always entered and displayed on the *Resources view* (see Figure 2.16, “Using wildcards in permissions for files”). To specify permissions for files based on wildcards, select the application profile on the applications workspace and follow these steps:

1. Select the Set permissions link on the main window. Alternatively, you can select the permissions category on the workspace pane.
2. Activate the Resources View by clicking on the Resources View icon ( ).
3. On the tree view, browse to the folder where the files defined by the regular expression will reside. If you want to apply the permissions to files on any folder, select My Computer
4. Right-click on the folder you have selected and choose New/File. If you want to configure permissions for folders, choose New/Folder instead.
5. Enter the regular expression and press Enter. This operation will create a new item with the expression you have entered as its name.
6. Configure permissions for this item as previously explained.



| Permissions | |
|---|---|
| Read | Inherit (Yes) |
| Write | Inherit (Yes) |
| Delete | Inherit (Yes) |
| Execute | Ask |
| **Options** | |
| Recursive | Yes |
| Logging | None |

**Figure 2.16. Using wildcards in permissions for files**

You can activate the Apply to subfolders option for regular expressions too. If this option is set to Yes, permissions are applied to all the files that match the regular expression and are located on the subtree rooted at the folder containing the regular expression.

Notice that the permissions that you specify with wildcards are NOT shown on the Explorer View, and are NOT used to estimate inherited values. For example, if you deny read access to `*.doc`, if you specify inherit on read for the file `c:\hello.doc`, the value shown between parenthesis will not be the actual permission applied to the file.

# Advanced use of aliases

The concept of *alias* is used extensively by CORE FORCE to hide configuration details and allow the sharing of profiles. For example, if you are configuring your mail client, you will probably need a rule to allow the program to communicate with the mail server, for example, `mail.acme.com`. Now, if you want to share this profile with your friends, it will probably not work, because the mail server will be different. To ease the solution of these kind of problems, all network addresses, ports and most filesystem folders are encapsulated in *aliases*, which are named variables. In this way, the new user only needs to change the contents of the alias to use the profile developed by you, and do it only once and not for every new application.

The aliases can be local to an application or global. They are accessed from the workspace through the Aliases category of each application or the system configuration. The aliases stored on the system configuration are considered global, and can be used by any application.

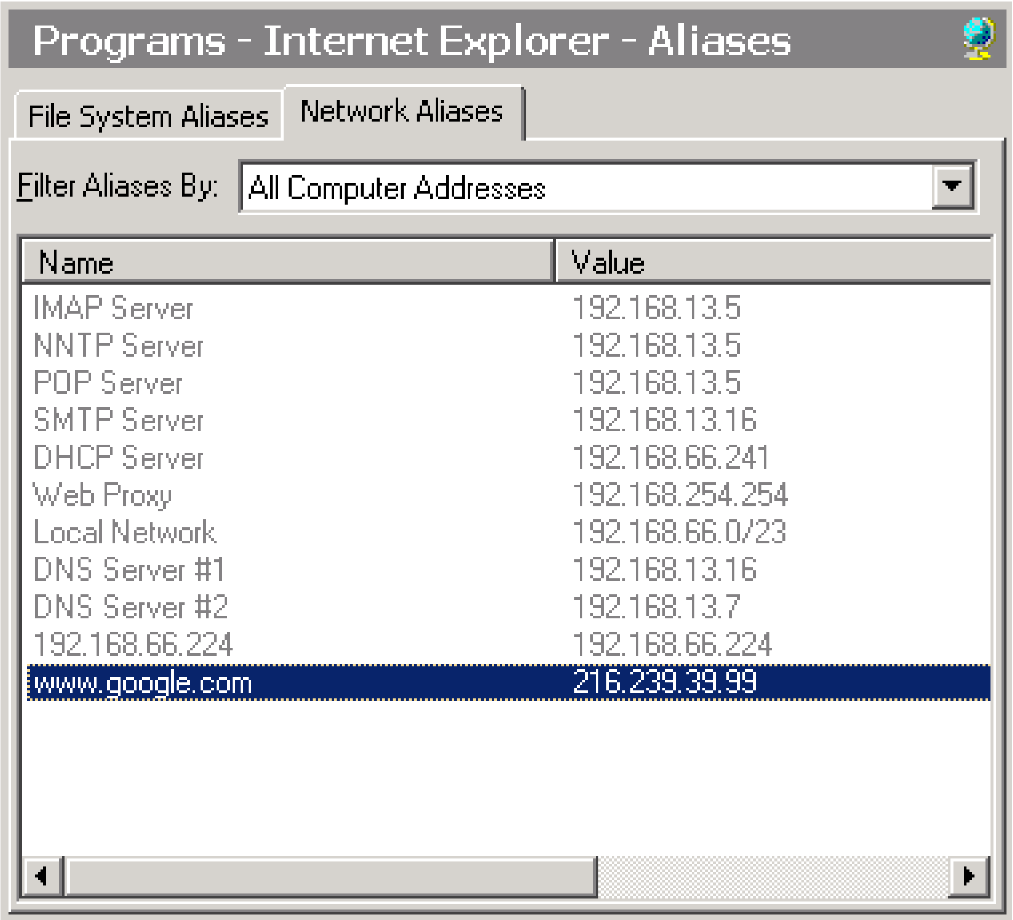
To create a new alias, you can use the context menu or the toolbar. The icon associated with this action is different depending on the type of alias you want to create. You can also delete or rename an alias. When you rename an alias, all their references are updated too.

### Note

Aliases are represented internally by unique identifiers, that are independent of their name. Once you delete an alias, all their references will remain orphan, even if you create a new alias with the same name.

## Network aliases

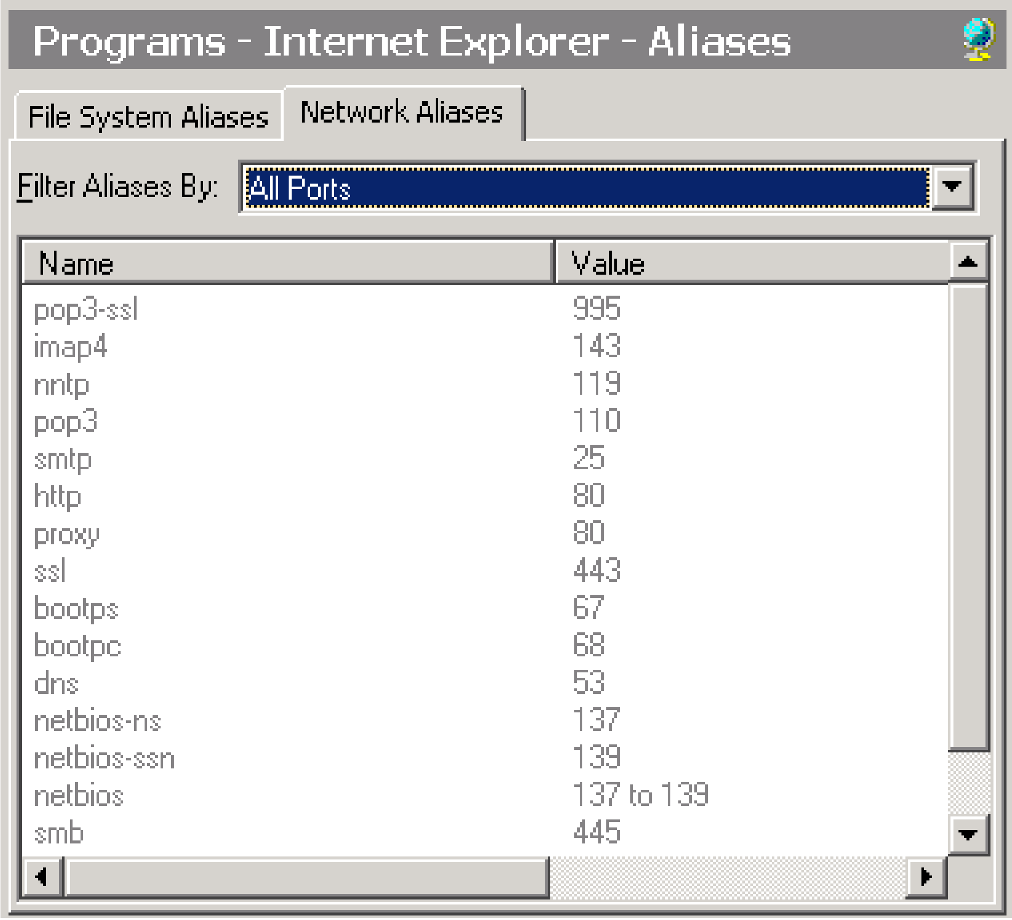
You can define two kinds of network alias: address aliases and port aliases. The former are bound to computers that you access often. They can represent one computer (for example, the mail server) or an entire network (for example, the local network). See Figure 2.17, “Network addresses aliases”. Port aliases are bound to network ports used by different protocols. These are numbers that are usually fixed and well-known, but they can change from network to network. See Figure 2.18, “Network ports aliases”. An alias can be edited by right-clicking on it and choosing edit from the context menu.



Filter Aliases By: All Computer Addresses

| Name | Value |
|---|---|
| IMAP Server | 192.168.13.5 |
| NNTP Server | 192.168.13.5 |
| POP Server | 192.168.13.5 |
| SMTP Server | 192.168.13.16 |
| DHCP Server | 192.168.66.241 |
| Web Proxy | 192.168.254.254 |
| Local Network | 192.168.66.0/23 |
| DNS Server #1 | 192.168.13.16 |
| DNS Server #2 | 192.168.13.7 |
| 192.168.66.224 | 192.168.66.224 |
| www.google.com | 216.239.39.99 |

**Figure 2.17. Network addresses aliases**

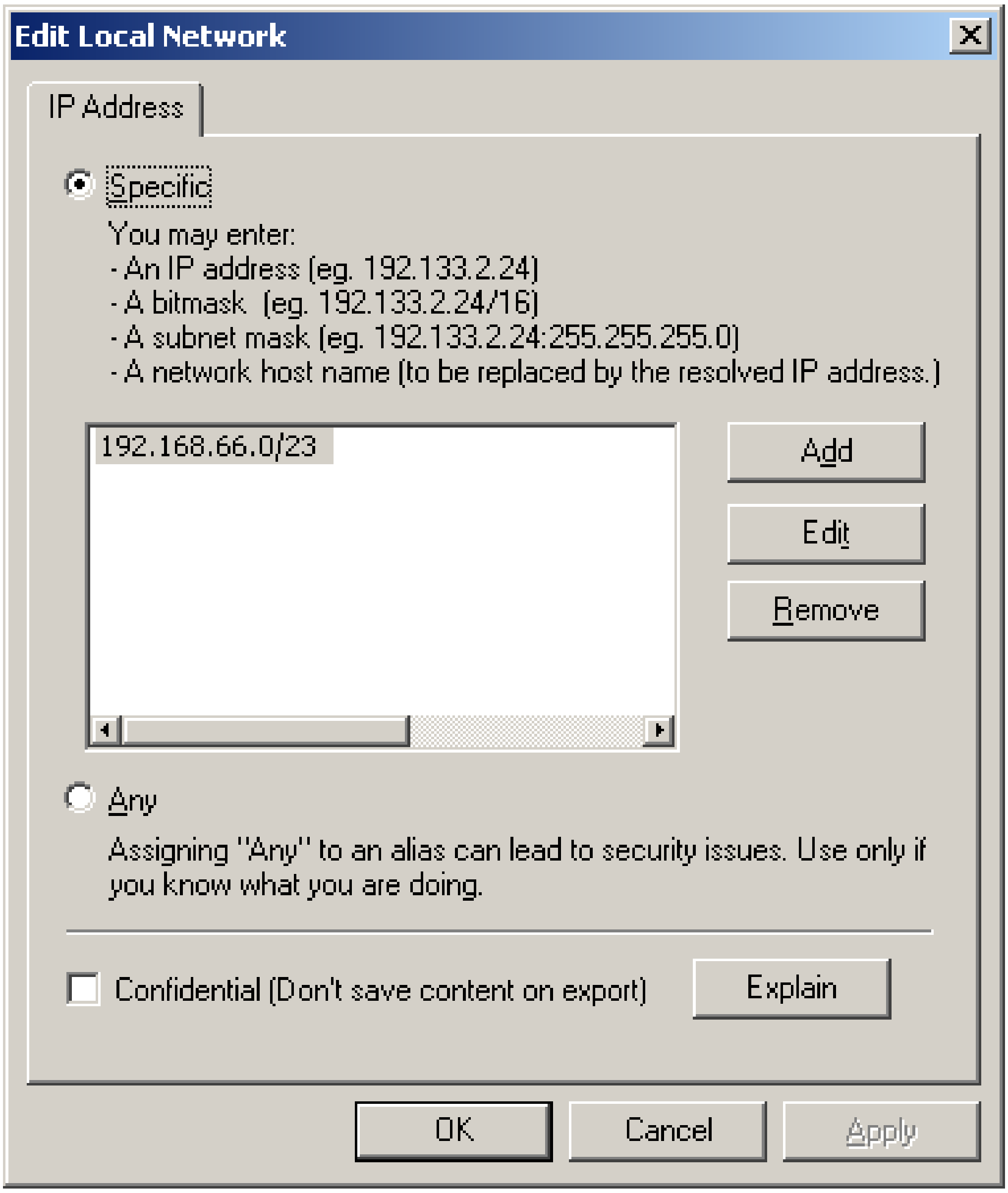


Filter Aliases By: All Ports

| Name | Value |
|---|---|
| pop3-ssl | 995 |
| imap4 | 143 |
| nntp | 119 |
| pop3 | 110 |
| smtp | 25 |
| http | 80 |
| proxy | 80 |
| ssl | 443 |
| bootps | 67 |
| bootpc | 68 |
| dns | 53 |
| netbios-ns | 137 |
| netbios-ssn | 139 |
| netbios | 137 to 139 |
| smb | 445 |

**Figure 2.18. Network ports aliases**

Figure 2.19, “Editor for aliases of Network Addresses” shows the alias editor for network addresses.



● Specific

You may enter:
- An IP address (eg. 192.133.2.24)
- A bitmask  (eg. 192.133.2.24/16)
- A subnet mask (eg. 192.133.2.24:255.255.255.0)
- A network host name (to be replaced by the resolved IP address.)

192.168.66.0/23

○ Any

Assigning "Any" to an alias can lead to security issues. Use only if you know what you are doing.

□ Confidential (Don't save content on export)

**Figure 2.19. Editor for aliases of Network Addresses**

Addresses can be defined in three different ways:

Fixed

This option is used to specify a unique address. Addresses can be written as IP addresses or host names. Host names are resolved when changes are saved. If the host name cannot be translated, an error message is displayed. In this way, address aliases always refer to unique IP addresses.

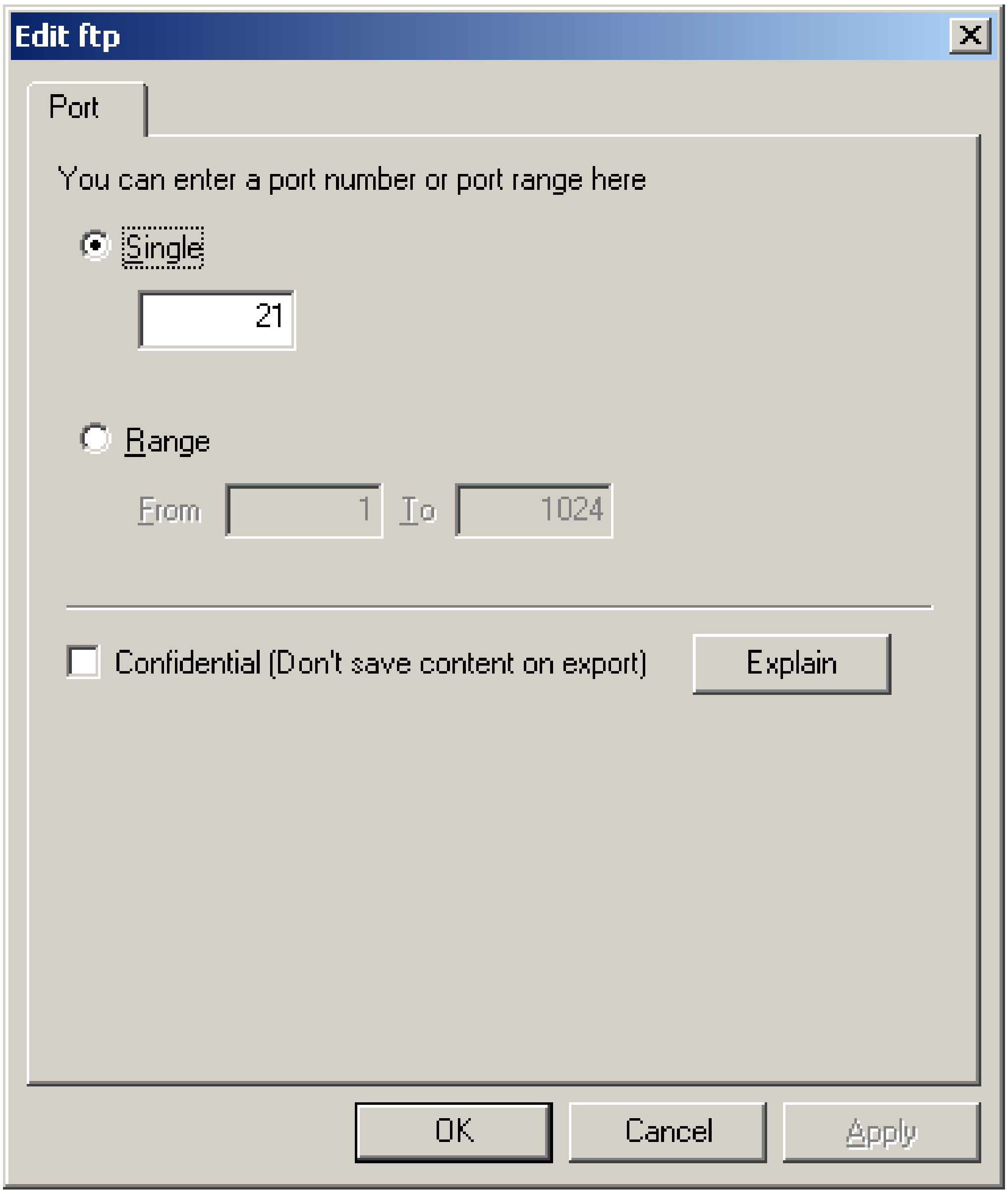
Bitmask form

This method is used to specify a range of addresses. The ranges have to be defined by the IP base and a number of bits of the IP that will be fixed. For example, to specify the range 192.168.33.0 - 192.168.33.255, you will have to enter: 192.168.33.0/24.

Any

Represents any host. This option is useful if you are not sure what address this alias refers to, or if the host is not available.

The network ports are numbers used by programs to communicate. Usually, each protocol has its own unique, known port. Nevertheless, these ports can be modified on certain occassions. To prevent profiles from not working on those situations, the network ports are also specified as aliases. Additionally, ports for the network rules can be defined with port ranges. Figure 2.19, “Editor for aliases of Network Addresses” shows the alias editor for network ports.



Edit ftp

You can enter a port number or port range here

● Single: 21

○ Range — From: 1 To: 1024

□ Confidential (Don't save content on export)

**Figure 2.20. Editor for aliases of Network Ports**

For this editor, the available options are:

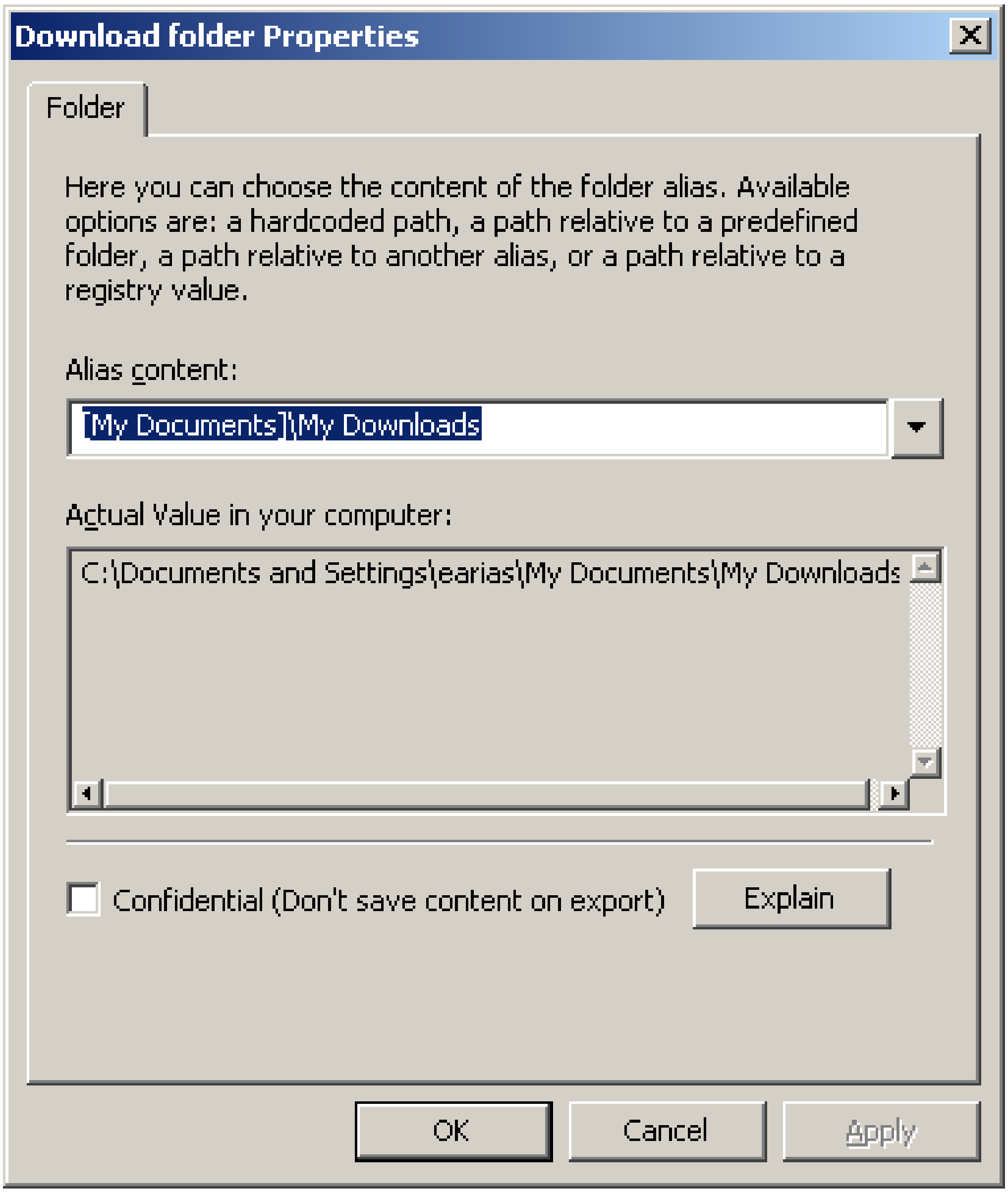
Single A single port number.

Range Allows the definition of ranges of ports. Both ends of the interval are included.

# File System aliases

File System aliases represent folders that are meaningful for an application or for the entire system and can be located at different paths for different users or computers (for example, My Documents).

The alias editor for the File System is the most advanced: aliases can be based on other aliases, on predefined folders or extracted from the registry. Figure 2.21, “Editor for aliases of Filesystem folders” shows the file system alias editor.



Here you can choose the content of the folder alias. Available options are: a hardcoded path, a path relative to a predefined folder, a path relative to another alias, or a path relative to a registry value.

Alias content: [My Documents]\My Downloads

Actual Value in your computer: C:\Documents and Settings\earias\My Documents\My Downloads

□ Confidential (Don't save content on export)

**Figure 2.21. Editor for aliases of Filesystem folders**

The dialog has two fields: Alias content and Actual value in your computer. As you build the alias content in the first field, the second field displays the actual location of the folder in your computer. For example, if your alias is based on the My Documents special folder, the second field expand the real path of that folder. To build aliases, you can use several elements, accessed by pressing the down arrow button ( ▼ ). You can also mix several elements, or mix variable parts with fixed ones.

The elements used to build aliases are:

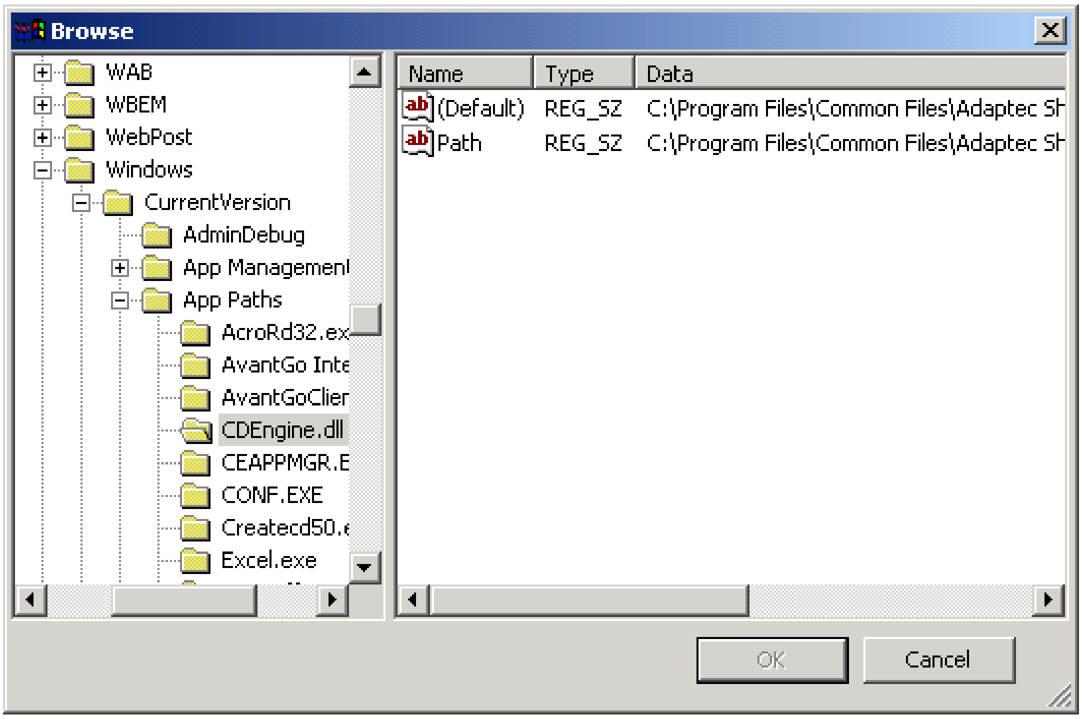
Browse... Allows you to select a specific folder by browsing your files.

Registry...
: Several programs store their paths in special keys on the registry. With this option, you can insert the content of a registry value inside the path you are building. When you select this option, a registry browser appears (see Figure 2.22, “Registry browser from the filesystem alias editor”).

Alias...
: You can use an alias to construct another alias. For example, you can define an alias for Home Folder and then create several subdirectories and define a different alias for each one. The alias selection dialog shows the list of available aliases, either local to the application or global (see Figure 2.23, “Alias Selection dialog from the filesystem alias editor”).

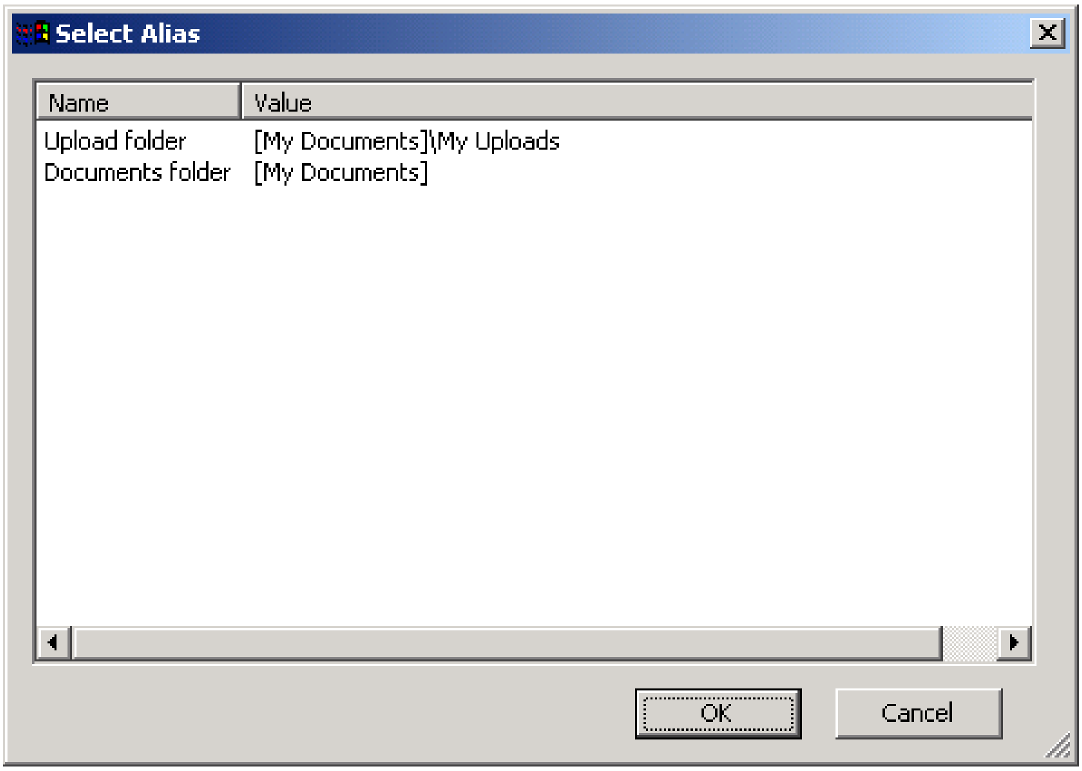
Predefined folder...
: Finally, an alias can be based on a predefined folder. Predefined folders are special directories set up by Windows that reflect the current installation. Examples of predefined folders are: My Documents, Windows System, etc.

Notice that if you use Browse or you type an absolute path, CORE FORCE replaces, whenever possible, any part of the path by predefined folders and/or aliases. The replacement is done to help you develop a configuration that can be used by multiple users or in other computers.



| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | C:\Program Files\Common Files\Adaptec Sh |
| Path | REG_SZ | C:\Program Files\Common Files\Adaptec Sh |

**Figure 2.22. Registry browser from the filesystem alias editor**



Select Alias

| Name | Value |
|---|---|
| Upload folder | [My Documents]\My Uploads |
| Documents folder | [My Documents] |

**Figure 2.23. Alias Selection dialog from the filesystem alias editor**

# Using Ask Dialogs

When you specify access rights for an object, either a file, directory or network connection, you have tree options for the action: Allow, Deny or Ask. Ask allows the user to decide what to do when a matching connection is performed/created by the application.

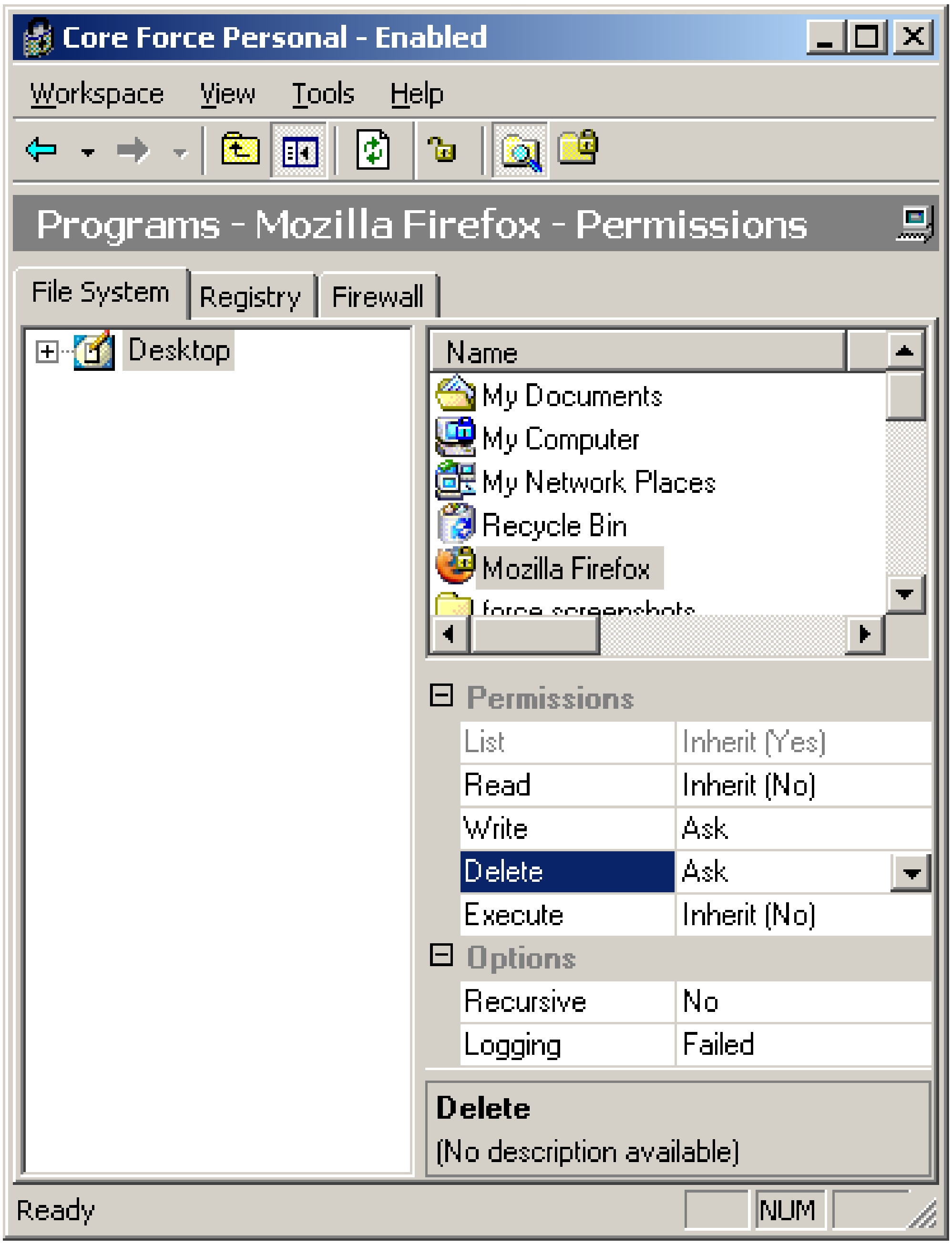
Despite the aparent simpleness of this option, it should be used with care, because it can be confusing at first: Some programs try to access files that they actually don't need (for example, open a file with "full access" when read-only is needed, or open the directories of a given path one by one), or make the same operation several times. In the former case, you would be asked for resources that are unnecessary for the application (and can be potentially harmful if you grant access to them permanently). In the latter case, you would be asked for the same resource several times.

While the dialog is displayed, CORE FORCE reacts in different ways, depending on the type of resource being asked for:

- *File system and registry:* The application is blocked until the dialog box is dismissed.
- *Network:* All the corresponding packages are dropped until the dialog box is dismissed. In this case you don't have the option to allow or deny the connections selectively (i.e. without making the change permanent).

## Asking for files and directories

To control the access to files and directories interactively, you have to select *ask* on an access type for an item (see Figure 2.24, “Select ask action for files”). You can choose *ask* for some types (for example, write and delete), and *yes*, *no* or *inherit* for others. The ask action is inherited as usual. In this way, you can define an ask permission and make it applicable to all the files and directories of a given subtree by enabling Apply to Subfolders.



Permissions

| | |
|---|---|
| List | Inherit (Yes) |
| Read | Inherit (No) |
| Write | Ask |
| Delete | Ask |
| Execute | Inherit (No) |

Options

| | |
|---|---|
| Recursive | No |
| Logging | Failed |

**Delete**

(No description available)

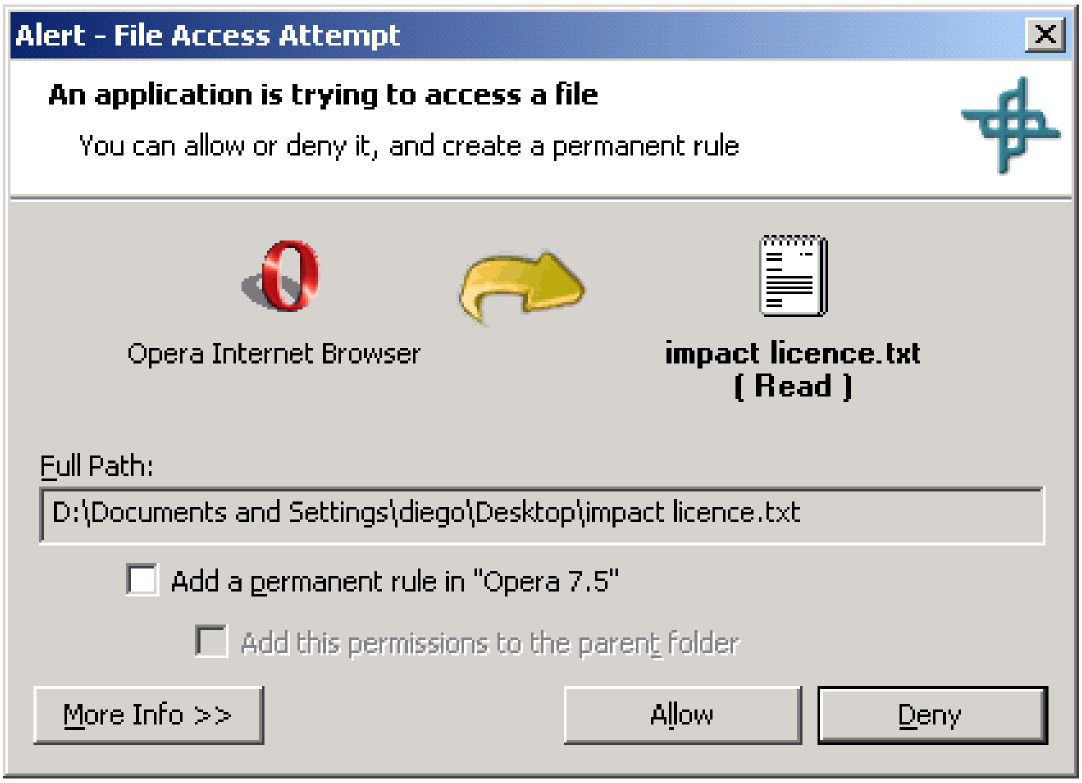
**Figure 2.24. Select ask action for files**

When the program tries to access a resource marked with ask, the file ask dialog is shown (see Figure 2.25, “Ask dialog for files”). The dialog contains the following elements:

- The name and icon of the program, or "system" if the program is not identified.
- The name and icon of the file or folder being accessed
- The operation requested (read, write, delete, create or execute)
- The full path of the file or folder folder being accessed

The dialog is dismissed by clicking on any of the two buttons: Allow or Deny. Additionally, the action can be customized by two modifiers:

- *Add a permanent rule in ...:* If this option is turned on, the application profile will be updated with your answer. The same answer will be applied in the future without asking again.
- *Add these permissions to the containing folder:* If this checkbox is turned on, your response will be applied to all items located on the same folder as the item being asked. This option is not applicable to directories. This option is enabled if the previous checkbox is set.



Alert - File Access Attempt

**An application is trying to access a file**

You can allow or deny it, and create a permanent rule

Opera Internet Browser

**impact licence.txt**
**[ Read ]**

Full Path:

D:\Documents and Settings\diego\Desktop\impact licence.txt

□ Add a permanent rule in "Opera 7.5"

□ Add this permissions to the parent folder

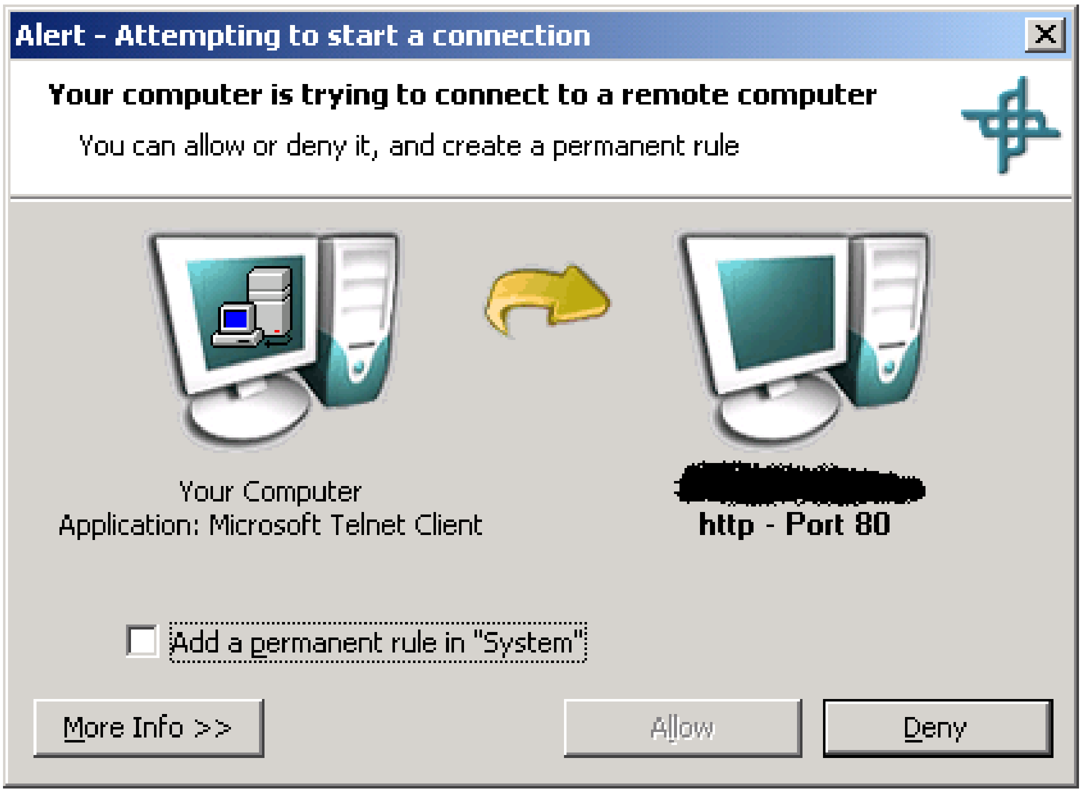
**Figure 2.25. Ask dialog for files**

Notice that, if the option *added permissions permanently* is turned on, your response will be added as a new permission in the application profile that is enforced for that program. For example, if you execute the Notepad application inside Internet Explorer and you don't have an application profile for Notepad, if it triggers an ask dialog, the permission will be added to Internet Explorer. This behavior is potentially dangerous if the application is not running inside its own profile: in this case the permission will be added to the global profile, and hence applicable to any nonconfigured program.

For registry keys and values, the dialogs are exactly the same, except that the name of the value or key is displayed, and the option *Apply these permissions to the containing folder* refers to the containing key.

## Asking for network connections

For network connections, the asking mode is activated by choosing *ask* for a given rule. When a network packet matches the conditions of the rule, a popup dialog appears (see Figure 2.26, “Ask dialog for network connections”).



Alert - Attempting to start a connection

Your computer is trying to connect to a remote computer

You can allow or deny it, and create a permanent rule

Your Computer
Application: Microsoft Telnet Client

[redacted]
http - Port 80

□ Add a permanent rule in "System"

**Figure 2.26. Ask dialog for network connections**

This popup dialog displays the following information:

- The name and icon of the program trying to make the connection, or "system" if the program is not identified.
- The direction of the communication (outgoing or incoming arrow).
- The name or the IP address of the remote computer.
- The name and number of the remote port.

Additionally, you can access the More information section by pressing More Info >> button. This section contains:

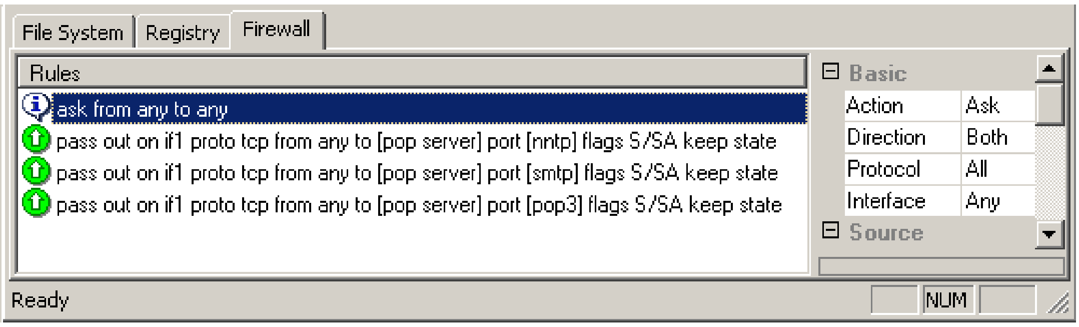
- The name of the network interface
- The name of the protocol
- The window title and the application path

The dialog is dismissed by clicking on any of the two buttons: Allow or Deny. If CORE FORCE is not able to block the application that is generating the network connection, Allow is not enabled (the packets generated by the program are dropped while the ask dialog is not answered).

The rule created by this dialog (if the option is enabled) tries to capture the semantics of the connection, in an effort to cover all similar connections. The rule will include?

- The information displayed in the dialog (protocol, source or destination host, known ports)
- For *pass* rules, *stateful* option turned on.
- For TCP connections, the flags S/SA, which indicates the packet for the connection request.
- For *block* rules, *stealth* option is turned on.

Figure 2.27, “Rule created automatically from the ask dialog” shows a set of rules created automatically by the ask dialog



```
ask from any to any
pass out on if1 proto tcp from any to [pop server] port [nntp] flags S/SA keep state
pass out on if1 proto tcp from any to [pop server] port [smtp] flags S/SA keep state
pass out on if1 proto tcp from any to [pop server] port [pop3] flags S/SA keep state
```

| | |
|---|---|
| Action | Ask |
| Direction | Both |
| Protocol | All |
| Interface | Any |

## Figure 2.27. Rule created automatically from the ask dialog

# Chapter 3. Creating new application profiles

In this chapter, you will see how you can create application profiles for new applications. CORE FORCE provides several tools to aid in the development of new profiles, such as Learning Wizard, Log Viewer and Shared Policies.

## The Learning Wizard

To build an effective profile for a given application, you need certain knowledge of what the application does and which resources it needs in order to work properly. The *log* option for files, registry and network rules along with the *Activity monitor* allows the registration of the resources an application uses.

For example, specifying the following permissions, you will obtain a complete trail of the activity of an application:

- In the File System section of Permissions, select My Computer and turn on the logging option for all the permission access types you want to be logged.
- Repeat the procedure for My Computer item on the registry tab.
- Create a network rule with log option turned on, and pass action (pass log from any to any).

If you want to build a profile based on the activity of an application, a more automatic alternative is to use the ask dialog, and activate the option Add these permissions permanently. This procedure works fine when a limited number of permissions need to be set: if the list is large, the popup dialogs easily becomes annoying.

The Learning Wizard allows the automatic creation or customization of a profile based on the activity of the application. Basically, this wizard generates permissions for all the files, registry keys and network resources accessed while you normally use the program. To use the *Learning Wizard* for building an application profile from scratch based on the execution of an application, click the Learning Wizardlink on the task list for the application and follow the instructions.

### Note

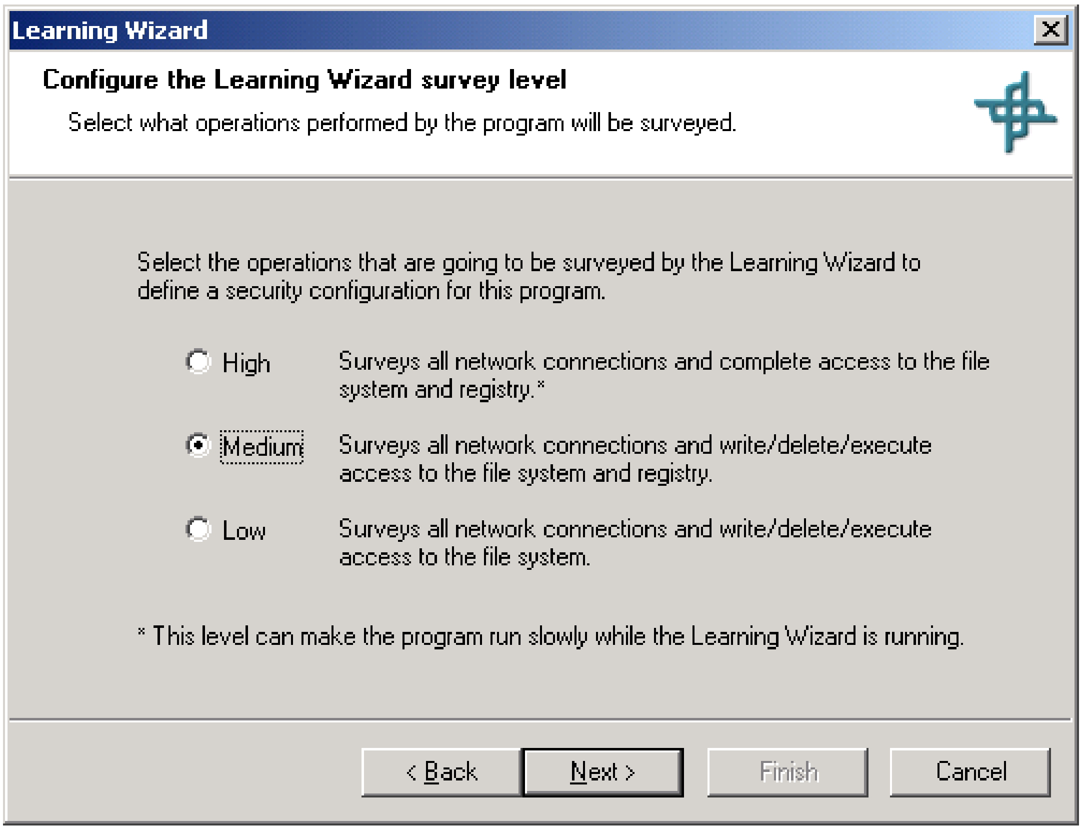
The Learning Wizard cannot be used if CORE FORCE is not activated or the application is disabled. Also, it is recommended to close all instances of the application being learned before starting the Learning Wizard.

Before starting the Wizard, you have to choose the ammount of information you want to gather during the learning (see Figure 3.1, “Learning Wizard. Choosing the gathering level”). The options are:

High This option instruct the Wizard to gather all network activity and all accesses to files, folders, registry keys and values, either list, read, write, delete and execute. Notice that this option can make the program run extremelly low and is not recommended, at least for the creation of a profile from scratch.

Medium This is the recommended option. If this option is chosen, the Wizard will record all network connections and write, delete and execute access to files, folders, registry keys and values. If needed, you can set other permissions manually after running the Wizard.

Medium This option is similar to the previous one, except that registry accesses are not recorded.



Learning Wizard

Configure the Learning Wizard survey level

Select what operations performed by the program will be surveyed.

Select the operations that are going to be surveyed by the Learning Wizard to define a security configuration for this program.

○ High — Surveys all network connections and complete access to the file system and registry.*

● Medium — Surveys all network connections and write/delete/execute access to the file system and registry.

○ Low — Surveys all network connections and write/delete/execute access to the file system.

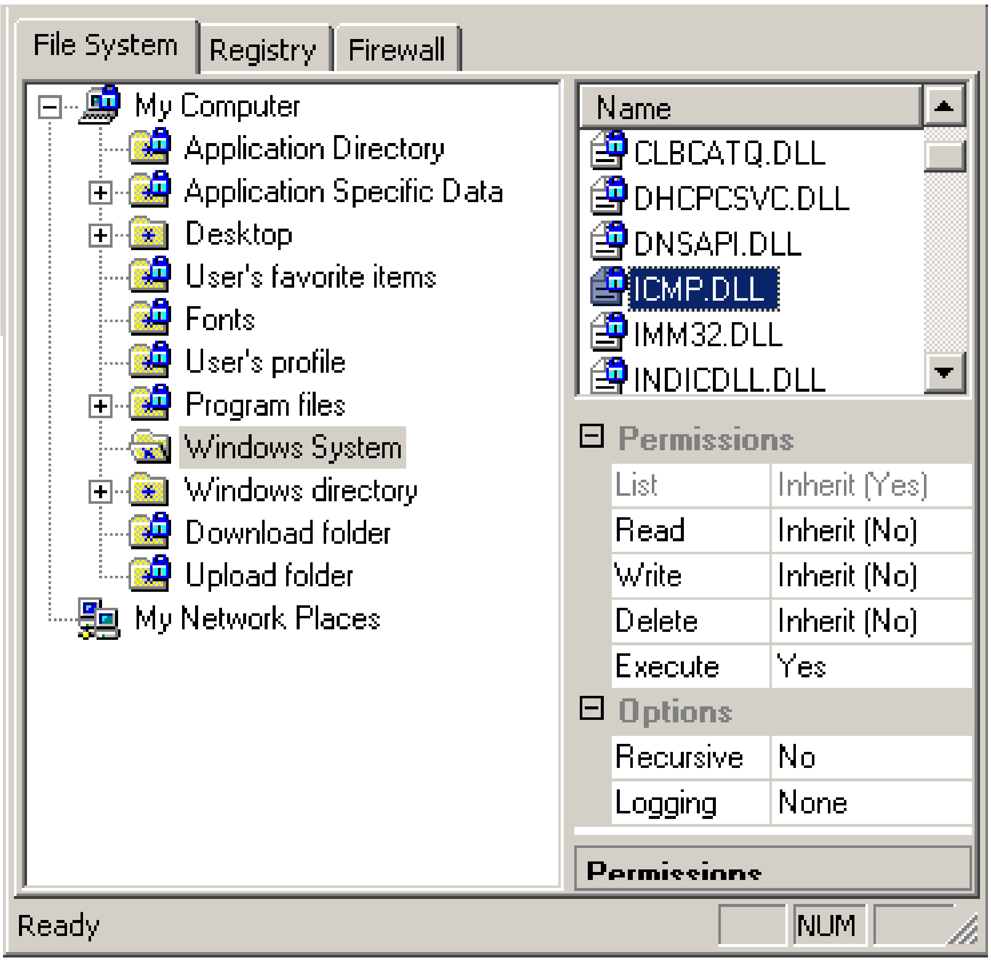
* This level can make the program run slowly while the Learning Wizard is running.

### Figure 3.1. Learning Wizard. Choosing the gathering level

After choosing the gathering level, click Next. At this moment, you have to run the program (the Wizard can run it for you if you click the Run button). Click Next to start the Wizard.

When executing the application, try to use as much of the functionality as possible, to force the application to access all the resources it needs. Avoid using features that wouldn't be accepted on normal use (for example, installing new plugins).

After a while, return to the Learning Wizard dialog and click Finish. The wizard will close and the profile for the application will include all the resources the application has used (see Figure 3.2, “Profile created by the Learning Wizard”). Only the type of permissions needed by the application are set, while the others will remain as inherit.



| | |
|---|---|
| **Permissions** | |
| List | Inherit (Yes) |
| Read | Inherit (No) |
| Write | Inherit (No) |
| Delete | Inherit (No) |
| Execute | Yes |
| **Options** | |
| Recursive | No |
| Logging | None |

**Figure 3.2. Profile created by the Learning Wizard**

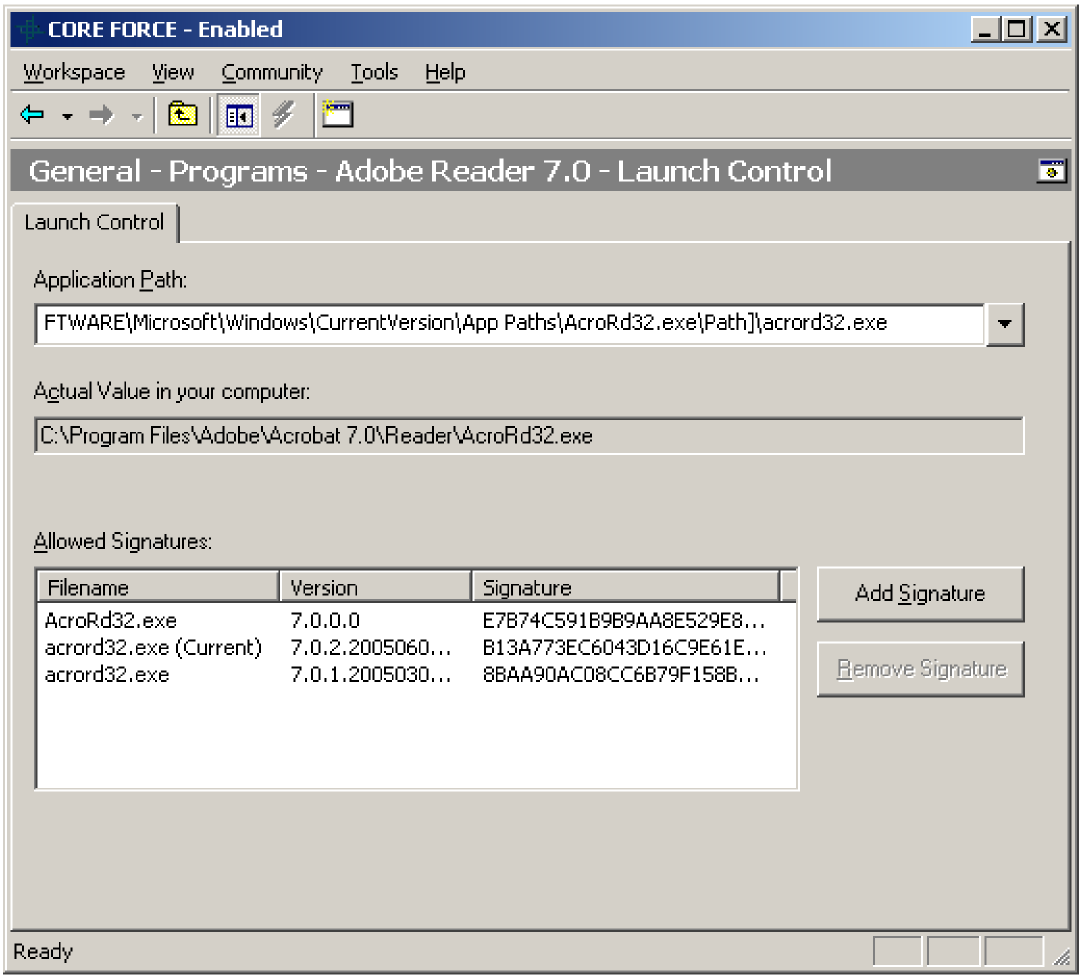
Notice that the Learning Wizard is a powerful tool to obtain a tight profile for an unknown application from scratch, but it is very likely that you should have to customize it in order to make it useful. For example, you should probably have to replace the permissions for individual temporary files (created by the Learning Wizard) by a permission for the `temp` directory. Force provides two actions for doing this. Both are accessed from the context menu (by right-clicking an item) on the Resources View only:

Get subitem's permissions
: This action generates on a directory the minimum set of permissions that covers all the permissions currently set for the subitems. For example, if you have a directory with some files that need read access and other files that need execute access, this action will provide read and execute access for the folder.

Unsecure subitems
: This action is used in conjunction with the previous action. It recursively unsecures all the items from the subtree rooted at the current item.

# Specifying the executable files of an application

Usually, applications are launched by executing a program file. The most common extensions for program files are *EXE* and *COM*. To bind an application to its application profile, you have to specify an entry-point. The entry-point can be identified by an absolute path, a path built from registry values, and by a hash. The latter option allows the identification of applications independently of their location, and is used in profiles made for deployment. See Figure 3.3, “Launch Control for applications”. To specify an entry-point for an application, follow these steps:



Application Path: FTWARE\Microsoft\Windows\CurrentVersion\App Paths\AcroRd32.exe\Path]\acrord32.exe

Actual Value in your computer: C:\Program Files\Adobe\Acrobat 7.0\Reader\AcroRd32.exe

Allowed Signatures:

| Filename | Version | Signature |
|---|---|---|
| AcroRd32.exe | 7.0.0.0 | E7B74C591B9B9AA8E529E8... |
| acrord32.exe (Current) | 7.0.2.2005060... | B13A773EC6043D16C9E61E... |
| acrord32.exe | 7.0.1.2005030... | 8BAA90AC08CC6B79F158B... |

**Figure 3.3. Launch Control for applications**

1. On the applications workspace, select the application you want to customize.
2. Click the link Define the program's entry point, or click the Launch Control subitem on the workspace. The main window will display the launch control pane.
3. Click the down arrow button on the right of the application path field ( ▼ ) and choose Browse.... A browse dialog will appear.
4. Use the browse dialog to select the executable file that defines the entry-point, and click Open. The path entered will be displayed in the field named Actual Value in your Computer. The field named Application Path will display the same path, but with directory names replaced by aliases and special folders when possible. On the Allowed Signatures list, a new entry will appear, with information extracted from the file you have selected.

# Glossary

Application profile

An application profile is a set of permissions that apply to a given application and to all the programs that the application executes. Every application on the system that needs special permissions or restrictions must have its own profile.

Application profiles can be downloaded or created from predefined templates, and customized by enabling and disabling security policies or individual rights.

System profile

The system profile, also known as the global profile, defined the permissions that apply to applications that don't have their own profile.

Application profiles also uses the system profile as the *default* for undefined permissions.

Entry Point

When defining an application profile, an entry point is a reference to an executable file that is used to run the application. CORE FORCE keeps a signature of that file to ensure that it wasn't changed, and to detect the execution of an application independently of the file's location.

Alias

If you want to share your profile, or use profiles made by others, chances are that other people have the programs installed in different directories, use different mailing and web servers and have other network adapters.

Aliases and special folders are used by Force to isolate as much as possible an application profile from the customizations of the computer where the profile were built. When you install a new profile, by specifying the location on your computer of the filesystem aliases and the addresses of the network aliases, you can tailor the profile to your computer.