

User Guide

GeSWall 2.9 Professional Edition



GentleSecurity

Notice to User

Information in this manual may change without notice and does not represent a commitment on the part of GentleSecurity.

The software described in this manual is provided by GentleSecurity under a license agreement. The software may only be used in accordance with the terms of the agreement.

No part of this publication may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without the prior written permission of GentleSecurity.

GentleSecurity claims copyright in this program and documentation as an unpublished work, revisions of which were first licensed on the date indicated in the foregoing notice. Claim of copyright does not imply waiver of other rights by GentleSecurity.

Copyright 2005-2009 © GentleSecurity S.a.r.l.
All rights reserved.

GentleSecurity S.a.r.l.
66, Rue de Luxembourg
L-4221 Esch-sur-Alzette
Luxembourg

Email: gswsupport@gentlesecurity.com
Web: www.gentlesecurity.com

Published on: July 2009

Table of Contents

1	Introduction.....	4
1.1	Overview	4
1.2	Access Restriction Policy.....	7
2	Getting Started With GeSWall	8
3	Notifications	13
4	GeSWall's Labels	16
5	Application Instances.....	18
6	Application Wizard.....	20
6.1	Normal Mode.....	21
6.2	Expert Mode	23
7	Using the GeSWall Console.....	27
7.1	Security Levels	27
7.2	Resources.....	29
7.3	Applications.....	31
7.4	Resource Name Syntax	35
7.5	Network Access Restriction	39
7.5.1	How to deny network access for isolated applications.....	41
7.5.2	How to deny network access for all applications.....	42
7.6	Untrusted Files.....	43
7.7	Isolated Applications.....	45
7.8	Logs.....	47
8	Application Database Update.....	49
9	Windows Vista UAC (User Account Control).....	51
10	Licensing	53

1 Introduction

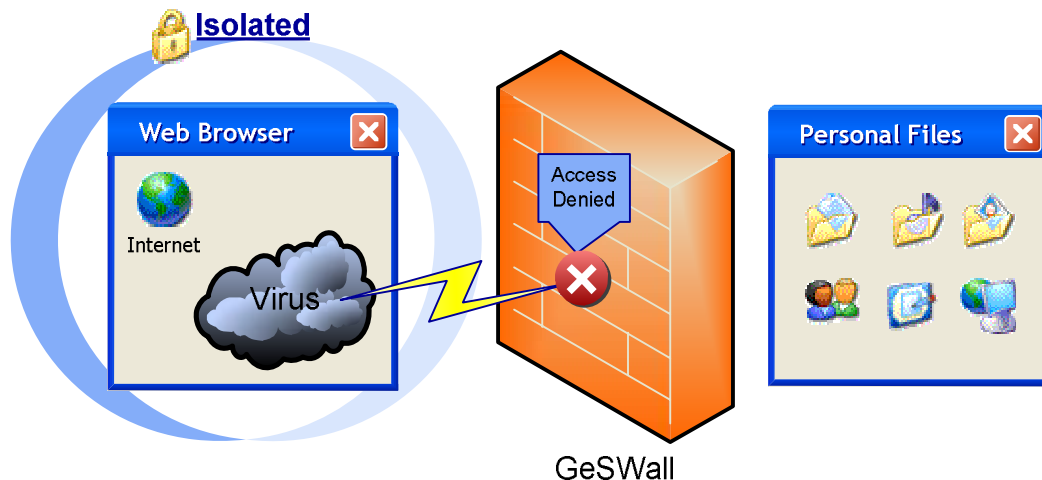
With GeSWall, you can securely surf the web, open e-mail attachments, chat, exchange files etc, regardless of the security threats posed by the internet. GeSWall prevents damage from malicious software and intrusions by isolating applications. Isolation applies an access restriction policy that effectively prevents different kinds of attacks, including:

- ✓ Rootkits, key loggers, backdoors
- ✓ Confidential file disclosure
- ✓ Intrusions
- ✓ Malicious software spreading

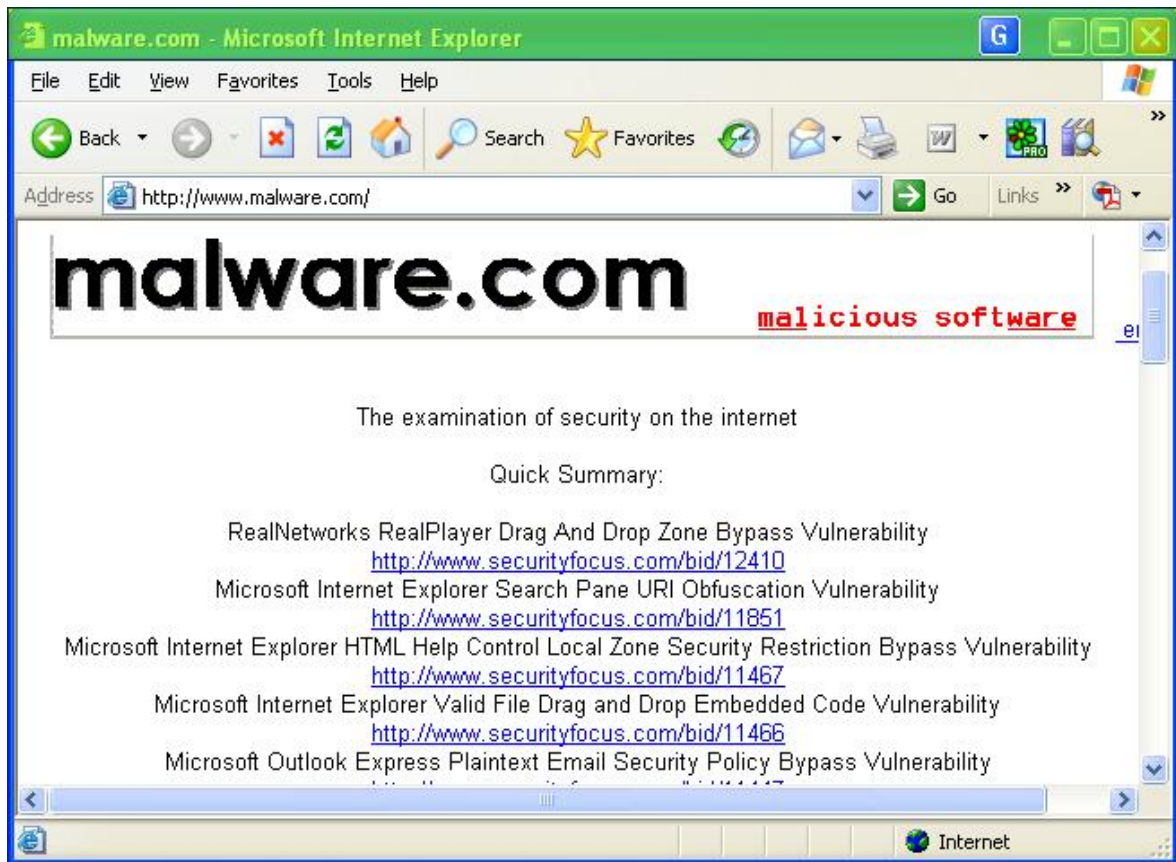
Though GeSWall does not require support or education to use, it provides powerful features to customize advanced settings. This manual will guide you through them.

1.1 Overview

Once installed, GeSWall dynamically isolates web browsers, e-mail, chat, P2P, IRC clients and other applications that may serve as entry points for malicious software or intrusions. Viruses, trojans, spyware and exploits cannot pass through an isolated application and so cannot cause any damage.

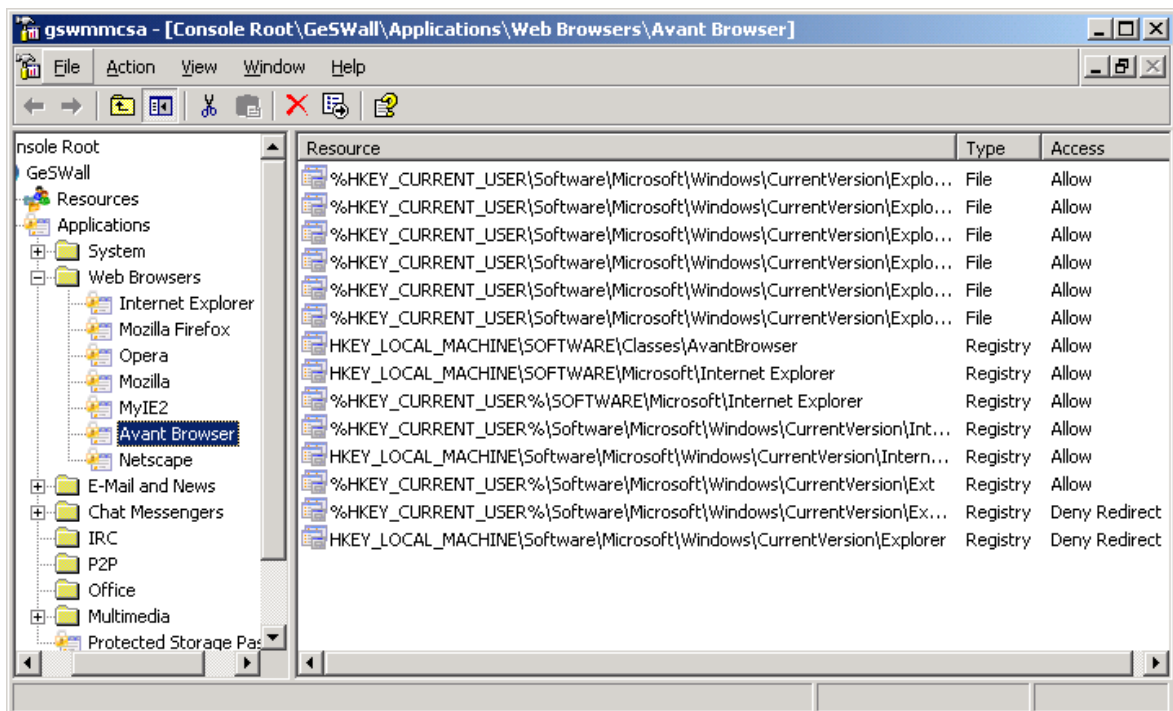


An access restriction policy prevents leaks of confidential documents and unauthorized modification of files, registry, etc., coming through an isolated application. These restrictions are unintrusive and do not disable important application functionality.



The technology used allows any application to be automatically isolated without configuration by a user. To make it even smoother and transparent, GeSWall applies specific access rules for most popular internet applications. Those specific rules come in an open Application Database. GentleSecurity staff regularly adds new applications to the database so you can get smooth support for more applications from the automatic update service.

With the GeSWall Console, advanced users may choose an appropriate security mode and create rules for applications which are not currently in the application database.



1.2 Access Restriction Policy

The GeSWall access restriction policy determines how GeSWall will restrict access by applications to system resources. Resources are files, registry keys, processes etc. and all resources are categorized as either *untrusted*, *trusted* or *confidential*.

The access restriction policy is composed of both generic rules which apply to all applications and specific rules which apply to only one application.

The generic rules for an isolated application are that the application:

1. Can read but cannot modify trusted resources.
2. Cannot read or modify confidential resources.
3. Cannot log pressed keys also known as key-logging.
4. Cannot capture screen-shots of trusted application windows.
5. Cannot read clipboard data from trusted applications.
6. May create new untrusted resources, e.g. files.
7. May read or modify untrusted resources.

The only generic rule for a non-isolated application is that the application cannot load untrusted executables into its address space. All other resources access are allowed.

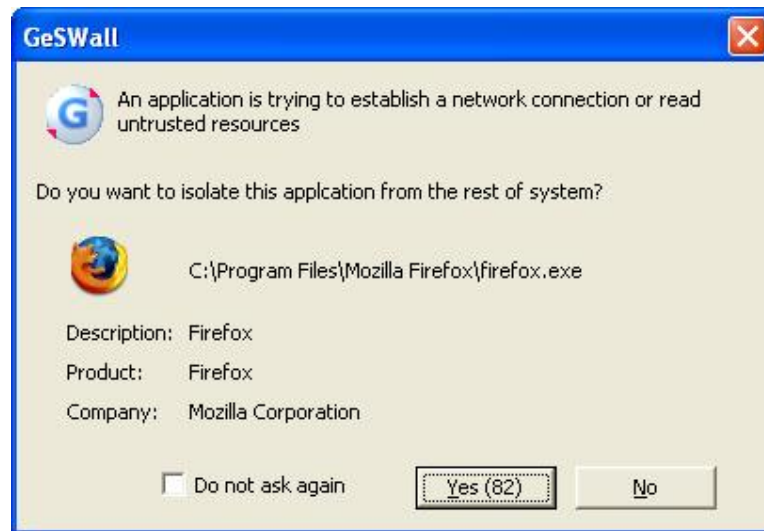
These generic rules are overridden by any application specific rules in the application database.

All resources are trusted except those created by isolated applications. Resources created by isolated applications are untrusted. Confidential resources are any resources, which are marked as confidential in the database. By default, any files in a user *My Documents\Confidential* folder are confidential. You may specify additional untrusted and confidential resources explicitly by their name or ownership.

The GeSWall policy model also reserves the notion of a *Jailed Application* - an application that has no permissions by default and may access only explicitly granted resources.

2 Getting Started With GeSWall

The installation procedure is very simple and does not require any user intervention. Just click on the downloaded *geswall.msi* and follow the instructions. After installation and reboot, GeSWall starts protecting your PC. Whenever you start a web browser or other internet application that GeSWall is aware of, it is isolated. Depending on settings, isolation happens automatically or you get a pop-up dialog request such as:



Depending on settings, the pop-up will appear as soon as an application tries to access an untrusted resource or as soon as it attempts to establish a connection to the internet.

To help you to make a choice, the dialog contains some information about the application.

Yes – isolate an application

No – let it run unisolated

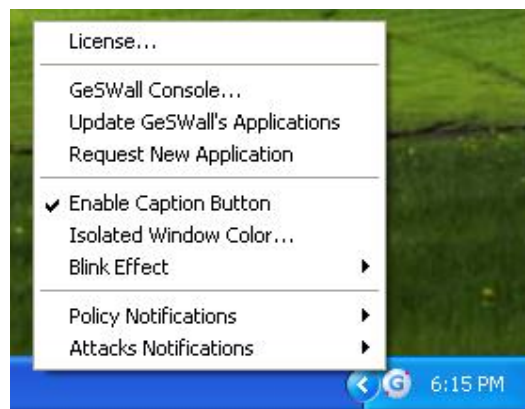
If you want to make the same choice every time you run this application then just check 'Do not ask again'. If you do not make any choice before the number on the "Yes" button has counted down to zero then the application will be isolated for you.

Usually you should always run an untrusted application in isolated mode. You may however occasionally want to run an untrusted application non-isolated if you want to allow it to modify trusted resources, e.g.: to install new software, ActiveX components, etc.

Once an application is isolated, GeSWall marks its active window caption with a special indicating color, so that you may easily distinguish isolated applications.



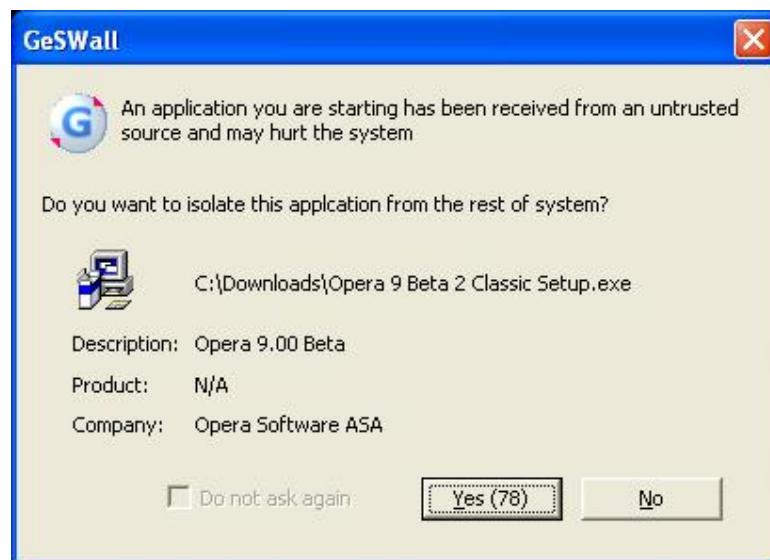
Clicking on GeSWall tray icon pops up a menu. With this menu, you may choose your favorite color and features for the isolated window caption, update Application Database, request support for new application.



Clicking on the caption 'G' button triggers a context GeSWall menu. You can use this menu to restart an application as non-isolated and customize isolated window color.



Files and registry keys created by an isolated web browser or other isolated application pose a risk as they may contain mal-ware. GeSWall treats all such files as untrusted and warns whenever an application is started from untrusted executables proposing to isolate it. In some cases, if you have downloaded a software installation package from a source that you trust then you may need to run it non-isolated.

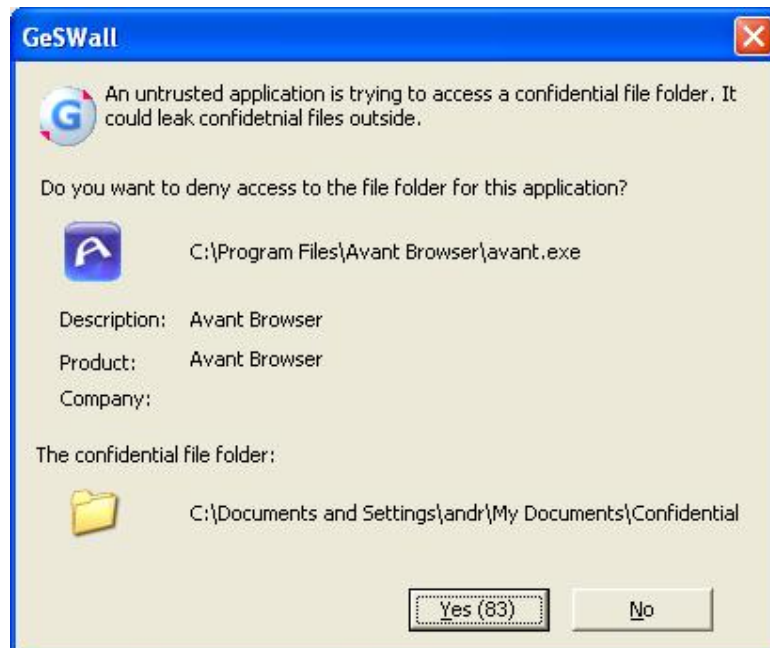


Usually installation programs (setups) may not proceed properly being isolated. It is recommended to run trusted setups as non-isolated. GeSWall assists in the process by warning on setups isolation.



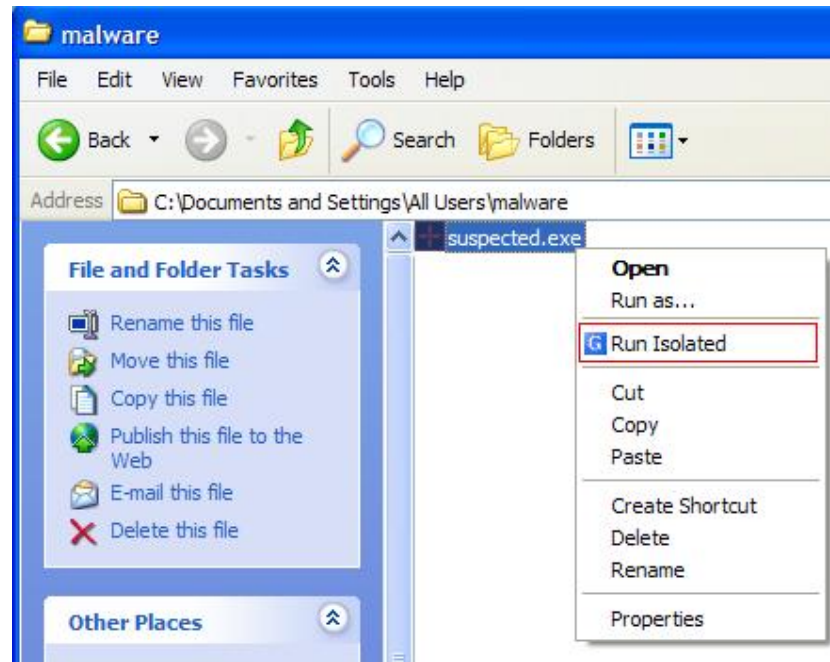
If you do not trust a setup and suspect a malicious activity then start it isolated. GeSWall used to prevent attacks that come via installed trusted applications, such as web browsers, messengers, mail, p2p clients and so on. The best option for an untrusted setup is fully virtualized environment, e.g. Virtual PC or VmWare.

When an isolated application is trying to access a confidential file, GeSWall shows the following warning.



In order to prevent confidential information disclosure, GeSWall will deny access to the file but you have an option to authorize it in certain cases, e.g. to attach a confidential document to an e-mail message.

You can start an application as isolated by Windows Explorer context menu. For that select a file, click right mouse button and execute “Run Isolated” item as shown on the figure below.



If a file is not an executable then GeSWall isolates an application associated with given file type. For example, “Run Isolated” on a .pdf file results in isolated Acrobat Reader opening that .pdf file.

3 Notifications

GeSWall provides interactive notifications on its security policy events. There are two types of notifications:

- 1) Policy Notifications
- 2) Attacks Notifications

Policy Notifications inform about GeSWall's restrictions, such as prevented modifications to files/registry/processes/etc. For example, notification message:

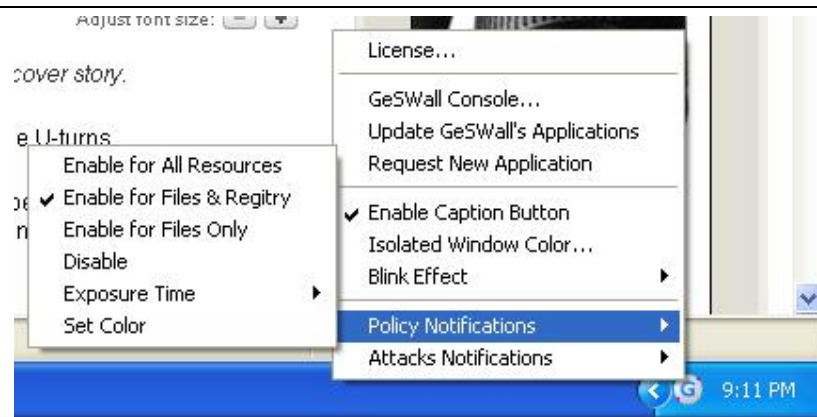


This means that GeSWall's security policy restricted access for Internet Explorer to the ShowCmd and WFlags registry values.

The Policy Notifications are useful for the first time to evaluate GeSWall's policy and watch what it does actually. Additionally, policy notifications are useful for troubleshooting, constructing the rules for new applications and testing malware or suspicious files.

In GeSWall's tray icon menu you can:

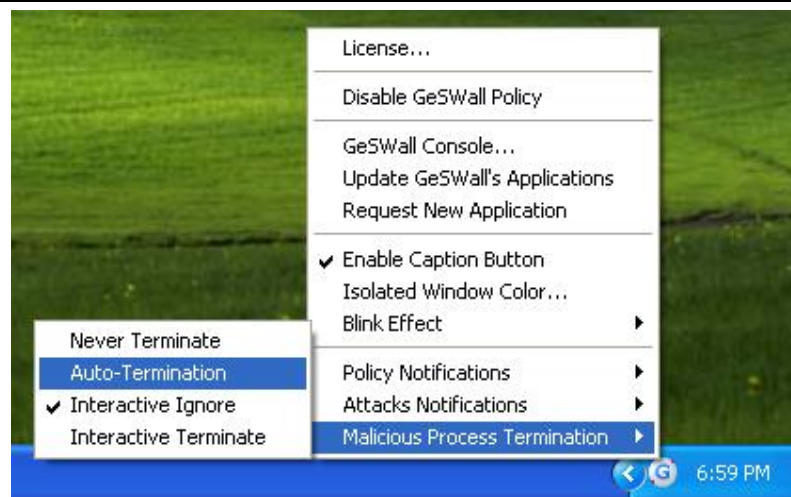
- Filter notification messages by resource type in order to reduce their amount
 - Enable for All Resources
 - Enable for Files & Registry
 - Enable for Files Only
- Disable all notifications
- Define message font color
- Set notification message exposure time



Attacks Notifications can be considered as filtered policy notifications. GeSWall looks over blocked resources for particular patterns which indicate a malware activity. Once a such activity is detected GeSWall notifies about prevented threat. While the policy notifications are useful on purpose, when you adjust application rules or test some malware. Attack's detection is for regular use as it provides lowest output and only when it is really something suspicious.



You have an option to terminate malicious application by clicking on 'Terminate' button. Additionally, you can adjust default termination behavior with 'Malicious Process Termination' menu item of GeSWall's tray icon.



- Never Terminate – disables termination option.
- Auto-Termination – automatically terminates application as soon as malicious activity is detected. When you see an attack notification, application is already terminated by GeSWall.
- Interactive Ignore (default) – an attack notification window has two buttons: ‘Terminate’ and ‘Ignore’. You can choose to terminate process by clicking on ‘Terminate’ button. If you don’t click on either ‘Terminate’ or ‘Ignore’ during the notification exposure time, then application will not be terminated.
- Interactive Terminate – the same as ‘Interactive Ignore’ but application is terminated if no choice taken during the notification exposure.

4 GeSWall's Labels

A file created or modified by isolated application is labeled as “untrusted”. If that file is:

- An executable - GeSWall classifies a process as posing threat and isolate it on execution;
- A driver or DLL - GeSWall prevents its loading into kernel and trusted processes;
- A script – script engine gets isolated on script translation.

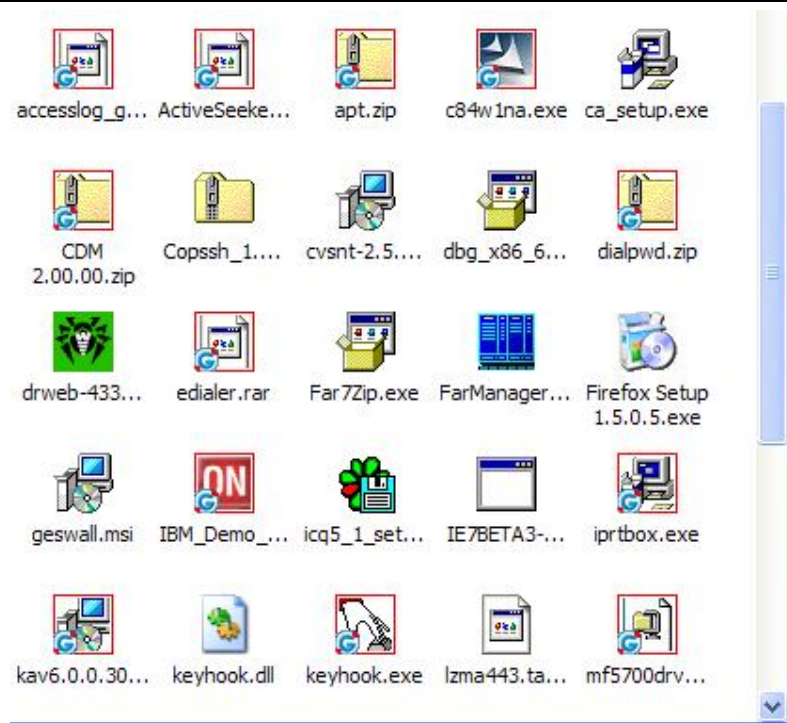
Additionally, GeSWall isolates an application when it is accessing an “untrusted” file. Note, the application must be “known” in this case. “Known” means an application has particular rules in the application database. The rules ensure non-intrusive application functionality.

GeSWall preserves the labels on files for their life time and in case of the following operations:

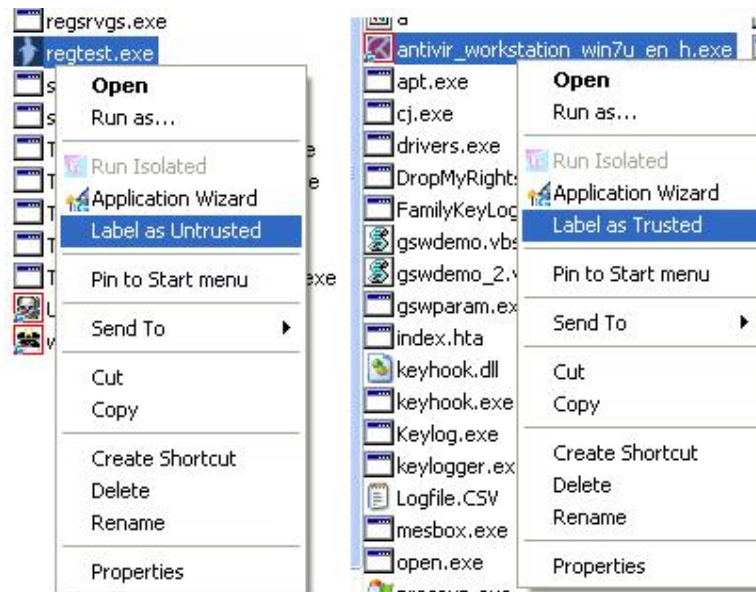
- file renaming
- moving file to the folder on the same volume

"Untrusted" labels are cleaned on a copy operation from non-isolated application, because a new copied file is created by non-isolated application, which performs this operation. The same semantic is applied to the windows file attributes. For example, an encrypted file can be stored unencrypted if copied to unencrypted folder.

GeSWall marks “untrusted” file icons with a red square and overlaid ‘G’ letter in the left bottom corner, as shown on the figure below.



You can label a file as trusted or untrusted by Windows Explorer context menu as shown on the screenshot.



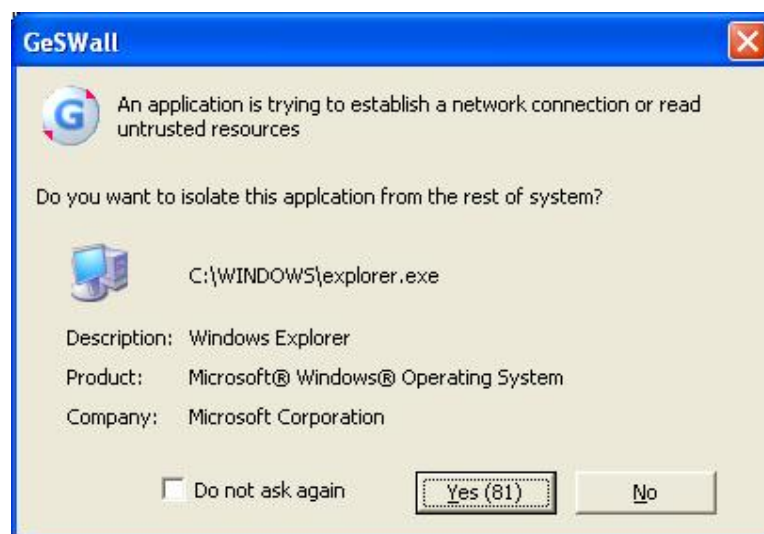
5 Application Instances

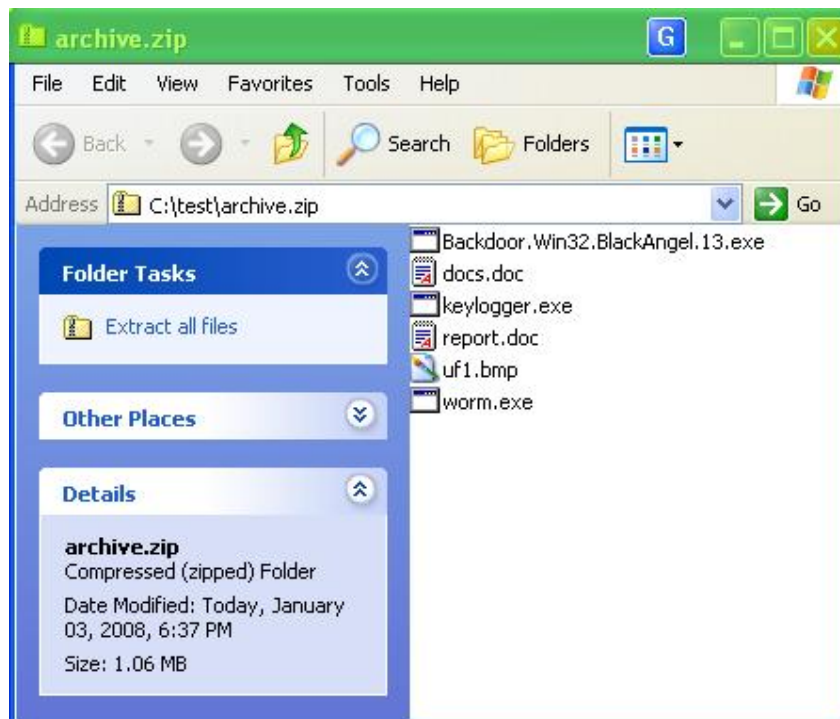
Application instances are also known as processes. An application may have several instances running at the same time, e.g. several processes of Internet Explorer. Each process might be isolated or not. Isolated processes could be recognized by colored caption or 'G' letter button.

Usually there are no restrictions on the number of application processes. However, some applications work only with a single active instance by default. For example, all pdf files are opened within a single Acrobat Reader process, `acrord32.exe`. That leads to a problem when you need to open trusted and untrusted pdf files. In this case, both trusted and untrusted files are opened in the same process, which might be isolated or not. If untrusted file is opened by non-isolated process, then it may perform malicious activity without any restriction. Security border is enforced on per process basis and there is no way to safely open untrusted document in non-isolated application. In opposite, a trusted file opened by isolated application cannot be modified and saved properly.

To resolve the issue GeSWall forces certain applications, such as Microsoft office Word, Excel and Adobe Acrobat, to start new processes for opening associated files or documents. Whenever you click on a document associated with those applications it is opened in a separate process. The same happens when document is opened via reference link on the web page.

Additionally, GeSWall starts a new process of Windows Explorer for opening zip archives. An untrusted archive is opened in isolated Windows Explorer window.





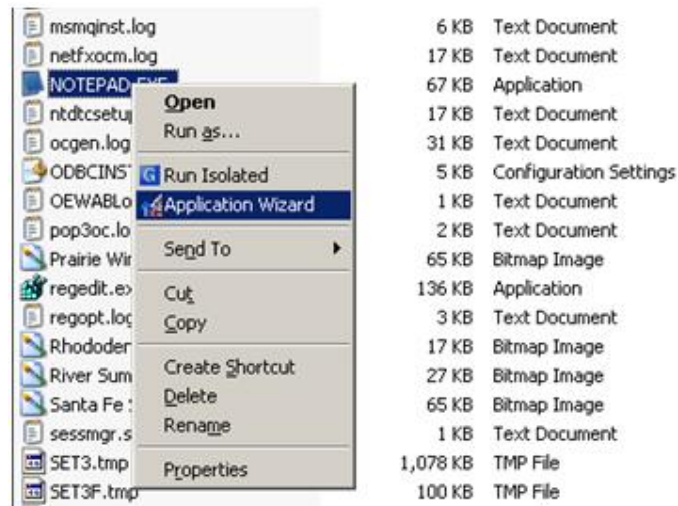
Files in isolated window are not labeled as untrusted, but effectively they are untrusted. Clicking on the files leads to opening them in isolated applications and extracted files are labeled as untrusted. Only copying operations do not preserve untrusted label.

Note, that enforcing separate processes described in this section is not supported in Windows Vista.

6 Application Wizard

A flawless execution of isolated application may require specific access rules. The rules describe important resources (files, registry, etc.) an application must have unrestricted access to. GeSWall has pre-configured rules for most popular internet applications: web browsers, e-mail clients, messengers, file sharing clients, office applications. etc. Those specific rules come with Application Database. GentleSecurity staff regularly adds new applications to the database which is received through the automatic update service. However, in some cases it is required to customize pre-configured rules or add support for new application. Application Wizard aims to automate and simplify the task.

Application Wizard can be launched from Windows Explorer's context menu, as shown on the screenshot below.



To start the Wizard, choose an application executable file, click on right mouse button and select 'Application Wizard' item. Please note, to use Wizard you must have administrative privileges or configure appropriate permissions for geswall.dat file placed into GeSWall's installation folder.

On the Wizard welcome screen you can choose an operation mode: normal or expert. Normal mode exposes only most important settings and hides advanced details. In expert mode you have an option to customize all settings generated by Wizard. Expert mode is recommended only for advanced GeSWall's users.

Normal mode is enabled by default. To continue Wizard in expert mode you set 'Expert mode' check box as shown on screenshot below.



Press 'Next' button to continue with chosen Wizard mode.

6.1 Normal Mode

In Normal Mode the Wizard has two pages. Configuration settings are filled automatically and an input is required only to adjust Wizard's defaults.

On the first page Wizard display basic application information and allows to define Display Name and Group. Display Name would be used in GeSWall notifications. Group is required for easier application classification in GeSWall Console.



Additionally, you can adjust processing time by corresponding slider control, Processing time is time used to automatic analysis of application behavior. Wizards starts given application isolated, checks what resources (files, registry, etc.) are accessed by that application and automatically constructs application specific rules.

Clicking on Next button starts analysis procedure. A completion status displayed by appearing progress bar as displayed on screenshot below.



You can disable automatic analysis by removing check from “Autofill rules for this application”. In that case Wizard skips analysis phase and switches to the final page.



At this point Wizard completed all required steps but not yet saved settings. Press on Finish button to save updated setting into Application Database.

6.2 Expert Mode

In Expert Mode you can adjust all Wizard's settings but defaults would be the same as in Normal Mode. This mode is particularly useful for troubleshooting, when isolated application is not functioning as expected.

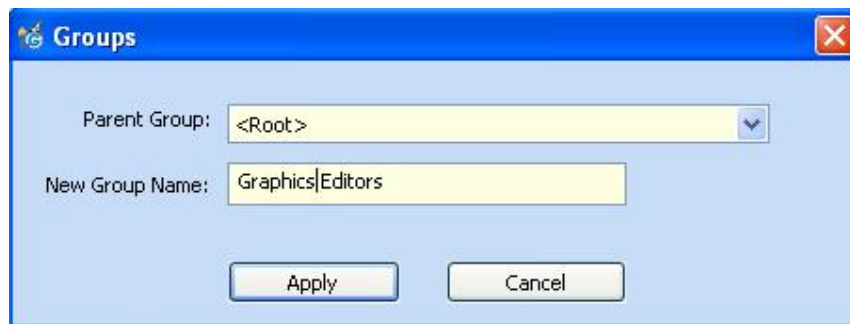
On the first pages Wizard displays basic application parameters:

- Application file path - used for identification by name
- Display Name - necessary for notifications and GeSWall Console
- Group - for application classification in GeSWall console
- Identification type
- Security Level

For more information on “Identification Type” and “Security Level” see “6.3 Applications” section.



If non of existing group fits the application category, you can create a new one by pressing on 'New Group' button.

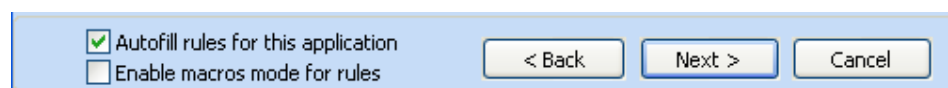


If application already exists in Application Database the Wizard displays corresponding message and retrieve all current settings from the database, as shown on screenshot below.



You have an option to delete such application by pressing on ‘cross’ button and start with clean settings.

Additionally, you can enable automatic analysis by checking “Autofill rules for this Application”.

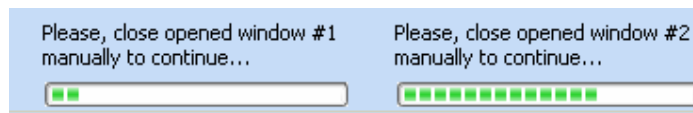


“Enable macros mode for rules” checkbox allows to automatically apply macro substitutes (see “6.4 Resource Name Syntax” for more details).

Press Next button to continue. If automatic analysis is enabled then Wizard performs these steps:

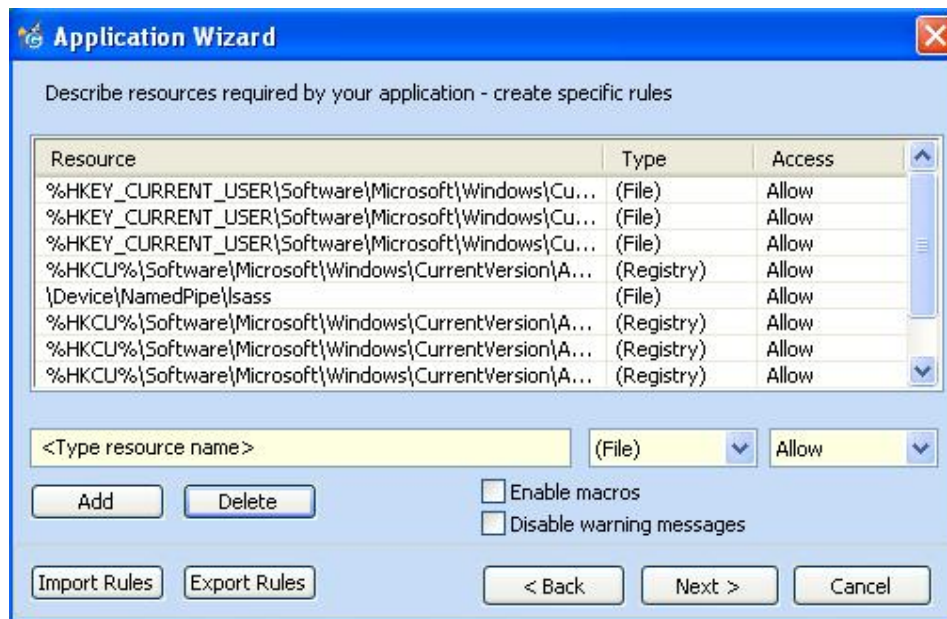
- launches given application as non-isolated and waits until you terminate that application;
- launches application as isolated and waits for your termination as well;
- determines specific rules based on access restrictions while application ran isolated.

The state of this process is displayed in appearing progress bar.



When Wizard launches application you should perform there some typical actions. For example in case of chat messenger (ICQ, Yahoo Messenger, Skype, etc.): logon to a server, type/send some messages, change profile settings and so forth. In case of troubleshooting, perform some particular actions that lead to a malfunction when application run isolated. GeSWall tracks access to all resources (files, registry, etc.) accessed by application during this procedure and determines what rules are required for that application.

When automatic analysis is disabled or completed, Wizard switches to the rules page.



The page lists all specific rules and provides interface to add new ones or delete existing (see “6.3 Applications” section for more details on specific rules). The list contains both existing rules (if any already configured for the application) and automatically generated. To add new rule: type resource name, select resource type, set access permission (typically allow) and press ‘Add’ button.

Resource name must comply with Name Syntax described in “6.4 Resource Name Syntax” section. Additionally, you can check “Enable macros”. In this case Wizard tries to apply most often macro substitutes for all resource names you enter.

To delete rule, select a rule in the list and press ‘Delete’ button.

Additionally, you can import a list of rules from a file by pressing on ‘Import Rules’ button. Imported rules will be added to the current ones. A file for import contains list of rules that were previously exported by mean of ‘Export Rules’ button. Import/Export functions are useful for rules templates which could be applied for many applications.

When you complete with rules configuration press ‘Next’ button to switch on final page.



Once you click on ‘Finish’ button, all configuration settings would be stored into Application Database. Pressing ‘Cancel’ button undo all Wizard’s changes.

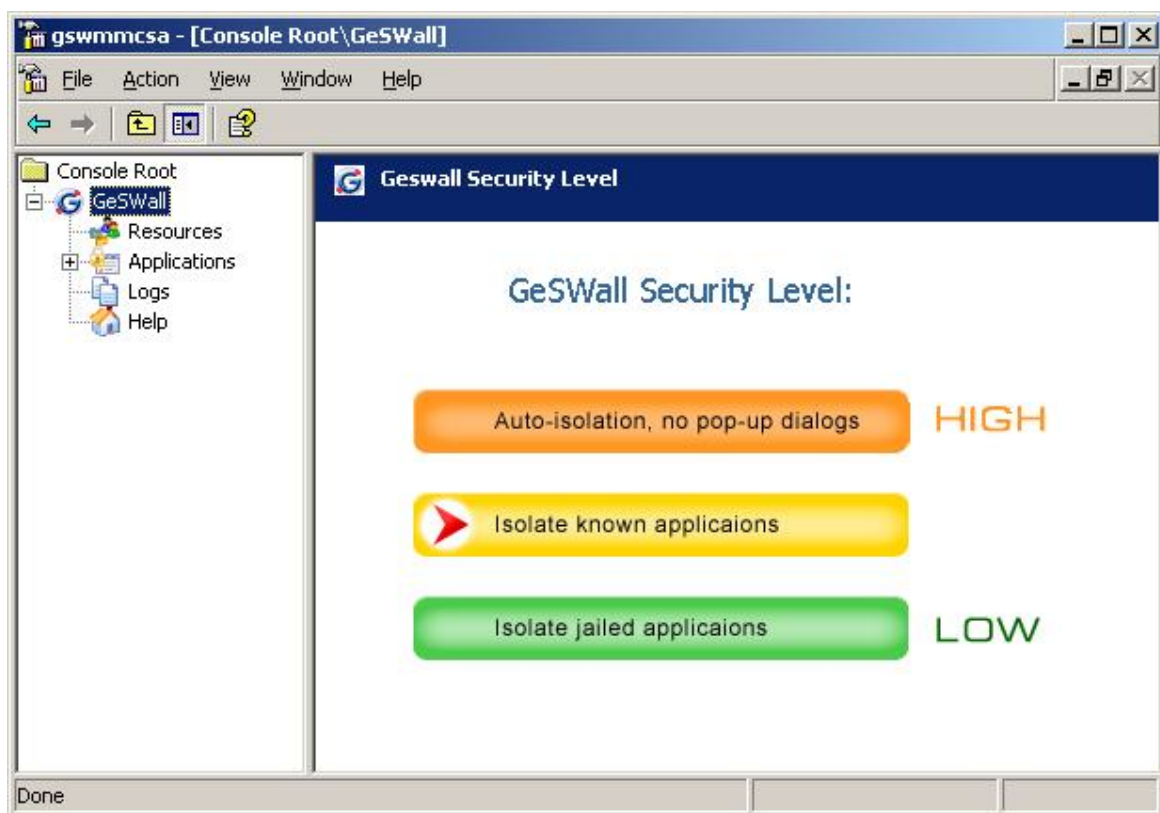
7 Using the GeSWall Console

The GeSWall Console is not required to use GeSWall but it serves as a tool for advanced users to add or change specific application rules or to configure some settings that affect the way that GeSWall behaves. The Console is an MMC (Microsoft Management Console) snap-in, which can be started through a shortcut in the GeSWall menu: Start/Programs/GeSWall/GeSWall Console.

Note: to run the Console you must be a member of the local administrators group.

7.1 Security Levels

GeSWall supports four security policy templates named Security Levels. Switching between security levels changes GeSWall behavior and should be done with due caution. To choose a level, select the GeSWall root folder, as shown on the picture.



The current Security Level is marked by a red tick. Clicking on a different level triggers a level change, which is applied immediately (no reboot or other actions are required). Levels are ordered by the amount of security that they provide from Low at the bottom to High at the top.

Isolate jailed applications

GeSWall isolates only Jailed Applications (see Access Restriction Policy). All other applications are never isolated.

Isolate known applications

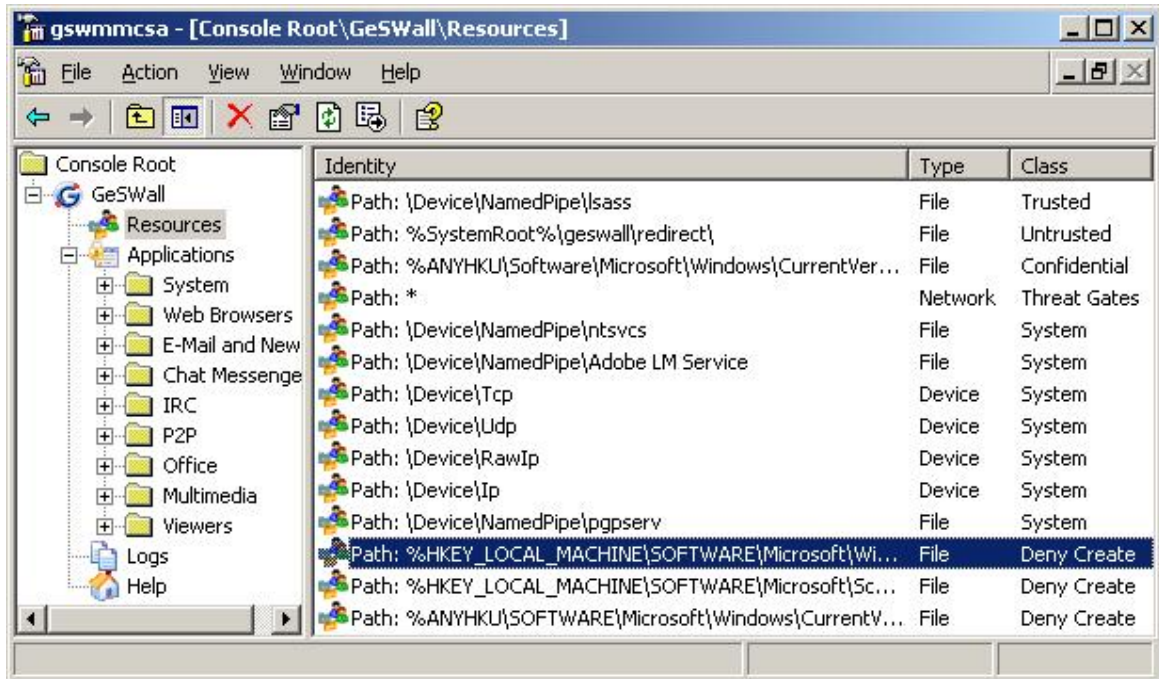
GeSWall only isolates applications, which have particular rules in the application database. The rules ensure non-intrusive application functionality. This is the default security level.

Auto-isolation, no pop-up dialogs

This level is similar to 'Isolate known applications' but it suppresses any pop-up dialogs. GeSWall applies the default actions without asking a user, so it automatically isolates known or untrusted source applications and denies access to confidential files. While this level is more secure because it does not rely on the user making correct decisions, it may cause undesirable restrictions.

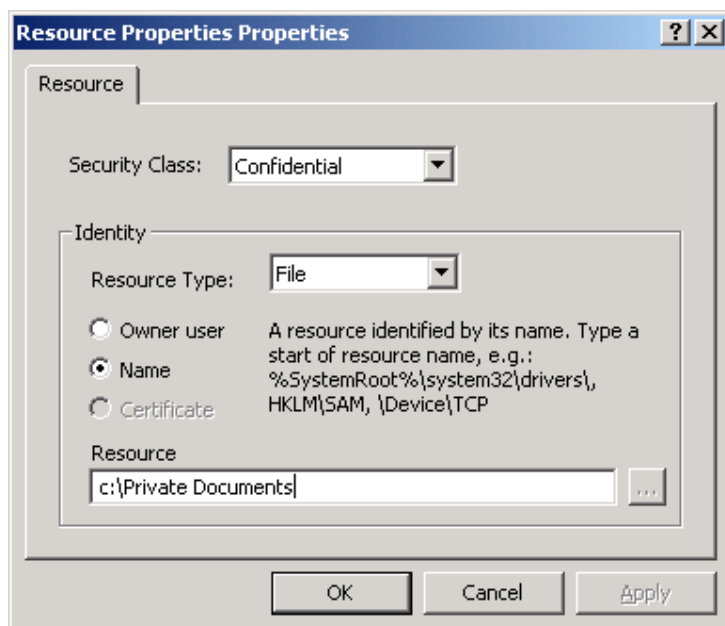
7.2 Resources

The 'Resources' folder contains definitions of trusted and untrusted resources. The Access restriction policy uses these definitions for isolating applications.



The default list of resources is required for GeSWall functionality and it is not recommended that you modify these however, you may add your own resource definitions, e.g. define additional file folders for confidential documents, or certain untrusted files.

To create a new resource definition, choose Action\New\Add Resource... from the main menu (alternative – mouse right click on the Resources folder in the right pane). A Resource Properties dialog will open.



The Security Class combo-box specifies the security class of the resource. It can be one of:

Trusted	A resource is trusted and an isolated application cannot modify it (read is allowed), unless it is explicitly enabled by a specific application rule. Note, that by default all resources are trusted.
Confidential	A resource is confidential and an isolated application can neither read nor modify it. By default, GeSWall defines all users' My Documents\Confidential folders as confidential. Therefore, you may either create that folder and copy your private documents there or define another file folder, which stores your confidential data.
Deny Create	The definition prevents an isolated application creating resources inside the specified path. For example, if "Deny Create" for "c:\windows\system32\" denies creating any new files inside c:\windows\system32\ path. Note that by default GeSWall allows isolated applications to create new files and folders without restriction but disallows the creation of new registry keys.
Untrusted	A resource is not trusted, this means an isolated application may modify it as well as read it.
Threat gates	Reserved for internal GeSWall use.
System	Reserved for internal GeSWall use.
Restricted for Trusted	Resource cannot be modified even by trusted (non-isolated) applications. This is useful to deny access for all applications and grant it only to particular applications by specific access rules. The security class is supported only for Network-type resources.

The rest of the dialog specifies identification parameters of the resource. It includes resource and identification types. The 'Resource Type' combo-box chooses the Windows native type of the resource:

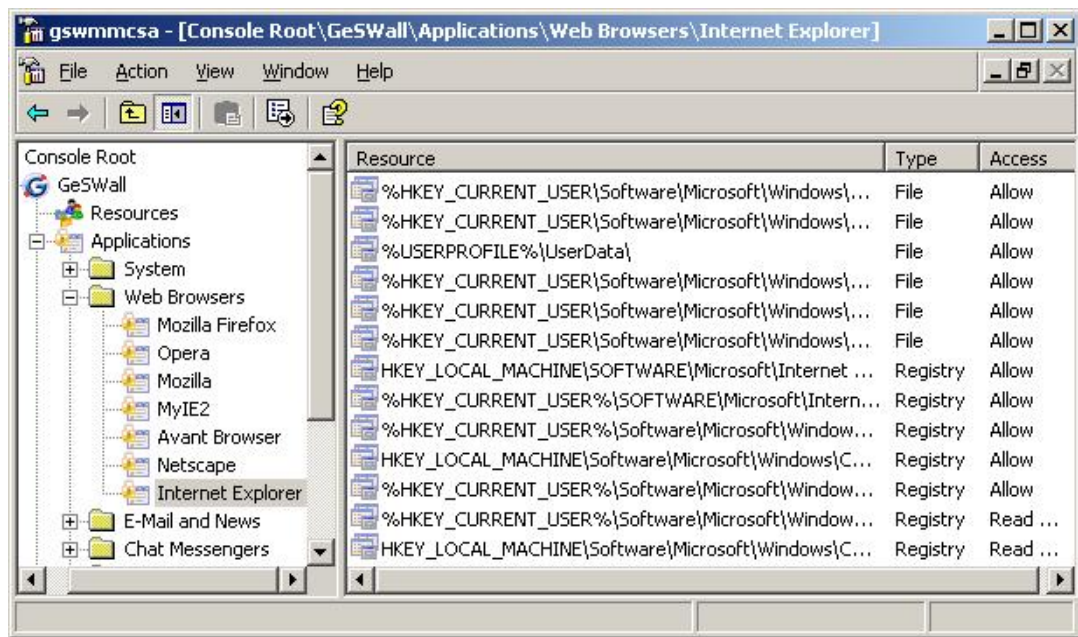
- file – file or file directory
- registry – registry key
- device – device object exposed by Windows kernel, e.g. \Device\Tcp (exposed by tcpip.sys driver to implement tcp networking), \Device\Cdrom (usual name of cdrom drives)
- system object – an object representing particular windows service, e.g.: SAM_DOMAIN\%MACHINENAME% - represent SAM database interface for given machine
- section – memory section, e.g. \KnownDlls\kernel32.dll
- network – network access via TCP/IP protocol, e.g:
 - update.microsoft.com
 - www.cnn.com:80
 - 192.168.1.1/24
 - *
- any – includes all possible resource types, not recommended

GeSWall identifies resources by owner user and name.

- Owner user – a user specified as owner in the Windows Security Descriptor. In the Resource edit-box you should type a user name or choose a user by the standard 'Select Users or Groups' dialog. By default, GeSWall has two definitions: Any resources owned by the local administrators group and local system are trusted, unless they are created by an isolated application.
- Name – a resource name prefix, e.g. c:\Program Files, %SystemRoot%\system32. The name may contain macro substitutions that must follow Resource Name Syntax.

7.3 Applications

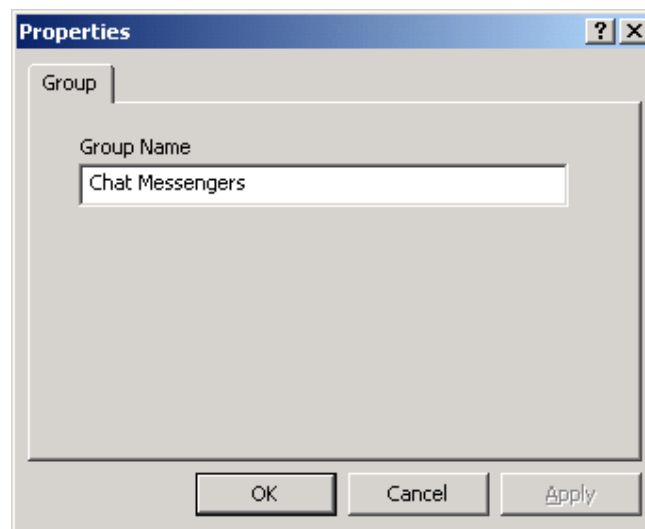
The 'Applications' folder contains known application definitions together with specific rules, which comprise the application database. For easy browsing applications are organized into logical groups, according to the application category.



The default application database has the following groups:

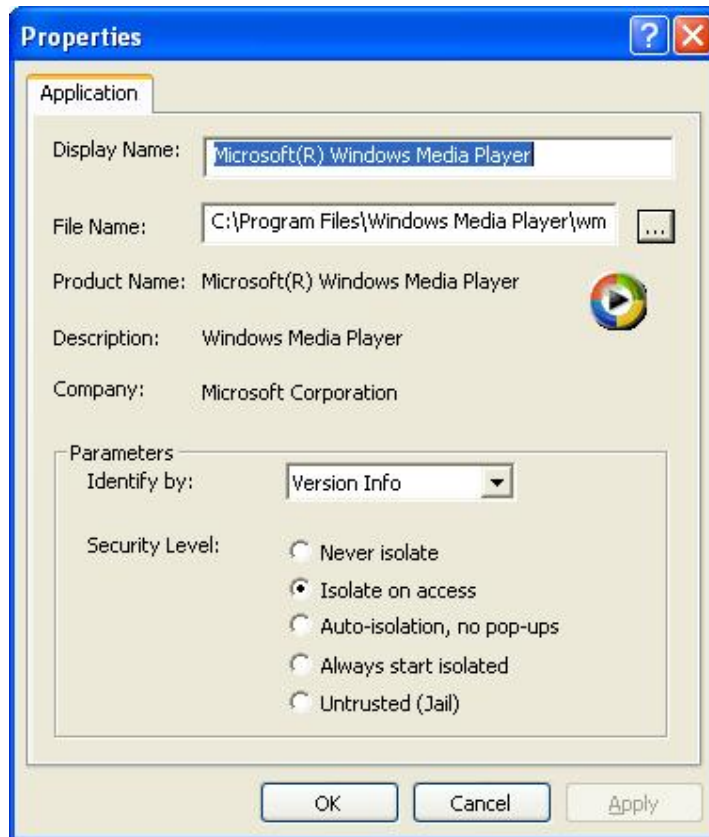
- System – Windows system and GeSWall components
- Web Browsers
- E-Mail and News clients
- Chat Messengers
- IRC clients
- P2P sharing applications
- Office applications, e.g. Microsoft Office components
- Multimedia, e.g. media players

You may create a new group by ‘Action\Add Group...’ item of main menu, which shows a dialog.



By ‘Action\Properties’ you may change the name of an existing group. An empty group can be deleted by ‘Action\Delete’.

‘Action\Add Application..’ of the main menu creates a new application definition in the chosen group.



The name specified in the ‘File Name’ field must be the name of an existing executable file. You may choose a name using the standard Open Dialog or type the name using standard Resource Name Syntax. Once an existing file name has been chosen, the dialog automatically fills in the rest of the parameters and you may press OK to proceed with the creation of application specific rules.

GeSWall can identify an application by Version Information or Name.

Version Information is a selection of certain parts of the file content provided by the application vendor. GeSWall checks version information only for trusted executable files because it cannot rely on untrusted content. This method allows an application to be identified regardless of its language localization, fix update, version or file path. This is the preferable way to identify trusted applications which have valid version information.

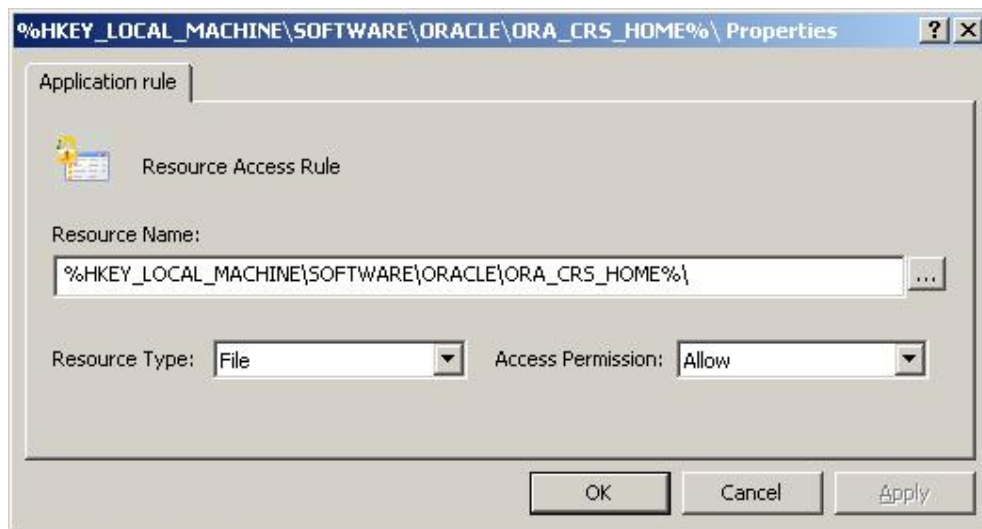
Name is the name of an application executable file following Resource Name Syntax. This method is useful for untrusted applications or applications without valid version information.

By default, the dialog sets the ‘Security Level’ of an application to ‘Trusted’, which you may decide to change. Available options are:

- **Never isolate** – means that the application is trusted and must not be isolated, no pop-up dialogs suggesting application isolation will be shown, see “Getting Started with GeSWall”. Prior GeSWall 2.7 the level is known as “Always trusted”.
- **Isolate on access** –application is trusted but once it tries to establish a network connection or access untrusted resources, a pop-up dialog to isolate the application appears, see Getting Started with GeSWall. Prior GeSWall 2.7 the level is known as “Trusted”.
- **Auto-isolation, no pop-ups** – the same as “Isolate on access” but isolation enforced automatically without pop-up dialogs. Additionally no dialogs appears on access to confidential resources. The effect of this application security level is similar to “Auto-isolation, no pop-up dialogs” GeSWall security level defined at the root console folder (see “Security Levels” section).
- **Always start isolated** – application is isolated on start, no pop-up dialogs are displayed. Prior GeSWall 2.7 the level is known as “Trusted, auto isolation”.
- **Untrusted (Jail)** - means Jailed Application, - an application that has no permissions by default and may access only explicitly granted resources.

The ‘Action\Properties’ menu item lets you modify Security Level after an application definition is created.

With an existing application definition, you may create specific access rules. An access rule specifies resource identification and permissions for that resource. A new rule is added by the ‘Action\Add Rule..’ menu item of an application context menu.



A resource is identified by its type and name according to Resource Name Syntax. The 'Access Permission' combo-box contains the following options:

Allow	Application may modify and read resource
Redirect	Application may read resource but once it tries to modify it, GeSWall creates a local copy of the file or registry key, which is modified instead. That allows the application to work smoothly and at the same time prevents modification of trusted resources. The local copy is not permanent. It is erased on application termination.
Read Only	Whenever an isolated application tries to modify a trusted resource, which is not described by a specific rule, GeSWall applies 'Redirect' permission. You may change that behavior by setting Read Only permission.
Deny	Deny any access to the resource.

Rules are applied on the application start, so an application re-start is required in order to enforce updated or new rules.

Note, that specific application rules have the highest priority. This means that an application will have the access specified in the rule regardless of any generic Access Policy rules.

7.4 Resource Name Syntax

Resource Name Syntax allows the identification of universal resource names that are valid in any environment. For example, instead of an exact folder name "C:\Program Files\MYIE2\Config\"

you may specify

`%HKEY_CURRENT_USER\Software\MYIE2\Folder%\Config`

This example uses macro-substitution that reads the `HKEY_CURRENT_USER\Software\MYIE2\Folder` registry value. This is where the MyIE browser stores its install folder name. Such notation is not environment specific and provides the correct name regardless of the software installation folder.

The structure of a name depends on the resource type.

Files and file directories are represented by usual names with macro-substitution, e.g. three variants of the same name

1. C:\Program Files\ICQ
2. %ProgramFiles%\ICQ
3. %HKLM\SOFTWARE\Mirabilis\ICQ\ICQPro\DefaultPrefs\ICQPath%

Registry key and value names are in regedit.exe format notation starting with the root-predefined keys, e.g.:

```
HKLM\SOFTWARE\Opera Software\Opera
%HKEY_CURRENT_USER%\Software\Skype
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
```

Resource name syntax also supports well-known acronyms for root-predefined keys.

Predefined key	Acronym
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_CLASSES_ROOT	HKCR
HKEY_CURRENT_CONFIG	HKCC
HKEY_PERFORMANCE_DATA	HKPD

Device names are Windows native names, which usually follow prefix \Device\, e.g.:

```
\Device\Tcp
\Device\CdRom
\Device\Floppy
```

Macro-substitutions are enclosed within percent signs (%) and expanded by GeSWall according to its meaning. The table below describes all supported macro-substitutions.

%EnvironmentVariable%

Application environment variable, which is expanded according to actual values, e.g.: %SystemRoot%, %HOMEPATH%, %TEMP%

%ANYUSERPROFILE%

Returns a list of user profile folders (%USERPROFILE%) that exist on a given system, e.g.

%USERPROFILE%\My Documents expands to the set:

```
C:\Documents and Settings\Administrator\My Documents
C:\Documents and Settings\test\My Documents
C:\Documents and Settings\LocalService\My Documents
C:\Documents and Settings\NetworkService\My Documents
```

%HKEY_CURRENT_USER% **%HKCU%**

Return HKEY_USERS\S-1-... registry key for actual user. This is the same as HKEY_CURRENT_USER, but macro-substitution must be used because

HKEY_CURRENT_USER is just a link to the corresponding HKEY_USERS sub-key and depends on the user who started an application.

%ANYHKU%

Returns a list of all HKEY_USERS\S-1-... registry keys, in fact all possible HKEY_CURRENT_USER, e.g.

HKEY_USERS\S-1-5-18

HKEY_USERS\S-1-5-19

HKEY_USERS\S-1-5-20

HKEY_USERS\S-1-5-21-813958858-572454927-963639892-1004

Registry value

A string value from the registry, e.g.

%HKLM\Software\Company\Software\InstallDir% - expands to InstallDir value content

%HKCU\Software\Winamp% - expands to the key default value content. Note, in that case HKCU must be used without % signs.

ANYHKU registry value

Returns a list of string registry values for all users who have a profile on a system, e.g.

%ANYHKU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal%

expands to the set of Personal registry value contents, which is My Document folder paths:

C:\Documents and Settings\Administrator\My Documents

C:\Documents and Settings\test\My Documents

C:\Documents and Settings\LocalService\My Documents

C:\Documents and Settings\NetworkService\My Documents

%getdir%() function

Function to extract directory name from full file name, e.g.:

%getdir%(%SystemRoot%\system32\msdtc.exe) expands to c:\windows\system32

Usually it is used to handle registry values.

%shortname%() function

Function to get a short 8.3 name from given file name, e.g.

%shortname%(%ProgramFiles%\Internet Explorer\IEXPLORE.EXE)

expands to c:\PROGRA~1\INTERN~1\ IEXPLORE.EXE

%longname%() function

Function to get a long name from parameter's file name, e.g.

%longname%(c:\PROGRA~1\INTERN~1\ IEXPLORE.EXE)

expands to c:\Program Files\Internet Explorer\IEXPLORE.EXE

%readfile% () function

`%readfile%` (`full_path_to_file`, `type_of_file`) returns string of data from given file.

The function has two parameters:

`full_path_to_file` – full path to the file. The parameter can be a macro-substitution as well.

`type_of_file` – type of file: `wchar` – unicode file, `char` – ascii file.

Samples:

```
%readfile%(c:\test, wchar)
```

```
%readfile%("%readfile% (c:\\test, wchar)", wchar)
```

```
"%readfile%(%HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Explorer\\Shell Folders\\AppData%\\Mozilla\\Firefox\\profiles.ini, char)"
```

%regexp_parse% () function

`%regexp_parse%` (`regex_pattern`, `data`) searches and returns substring according to given regexp pattern. The function has two parameters:

`regex_pattern` - regex pattern to search

`data` – data to search in. The parameter can be a macro-substitution.

Sample:

```
%regexp_parse% (\s*Path\s*=\s*([^\r\n]*), "%readfile%
(%HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Shell
Folders\\AppData%\\Mozilla\\Firefox\\profiles.ini, char)") – returns Firefox profile
path defined in profiles.ini file.
```

%regexp_parse_x% () function

`%regexp_parse_x%` (`regex_pattern`, `data`) is the same as `%regexp_parse%` but returns a set of found substrings. There are two parameters:

`regex_pattern` - regex pattern to search

`data` – data to search in. The parameter can be a macro-substitution.

Note, macro-recursion is not supported, so you cannot use one macro-substitution within another one. However, macro-substitution is allowed as a parameter for a macro-substitution function.

7.5 Network Access Restriction

GeSWall may restrict TCP/IP network traffic similar to network firewall functionality. You may configure application specific rules that deny or grant access to particular hosts, subnets at specified TCP/UDP ports. The rules are the same as those described in sections “7.2 Resources” and “7.3 Applications” but with ‘Network’ for Resource Type. Resource Name is an address of destination network hosts and subnets according to the following syntax.

Host[:Port][/Subnet]

Host is a mandatory field that represents DNS name or IP address of the target host, e.g.:

update.microsoft.com

192.168.1.17

Symbol ‘*’ should be used to apply rule to all network hosts.

:Port is an optional field specifying TCP or UDP port numbers as described here http://wikipedia.org/wiki/TCP_and_UDP_port. The ports identify specific network service, such as web and e-mail.

Please refer http://wikipedia.org/wiki/TCP_and_UDP_port for the list of known ports.

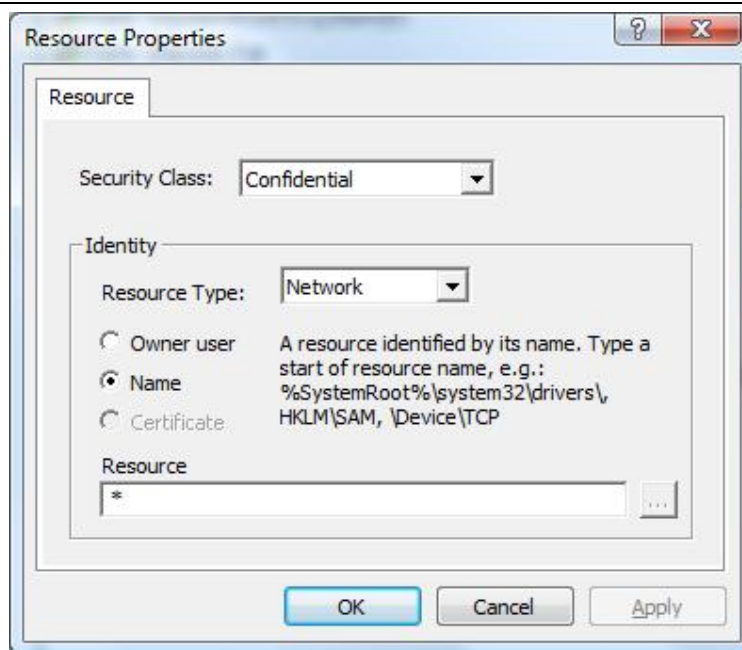
If the port is not specified then rule is applied to communications at all ports.

/Subnet is an optional field that defines network mask in CIDR notation as described here <http://wikipedia.org/wiki/Subnetwork>, e.g.:

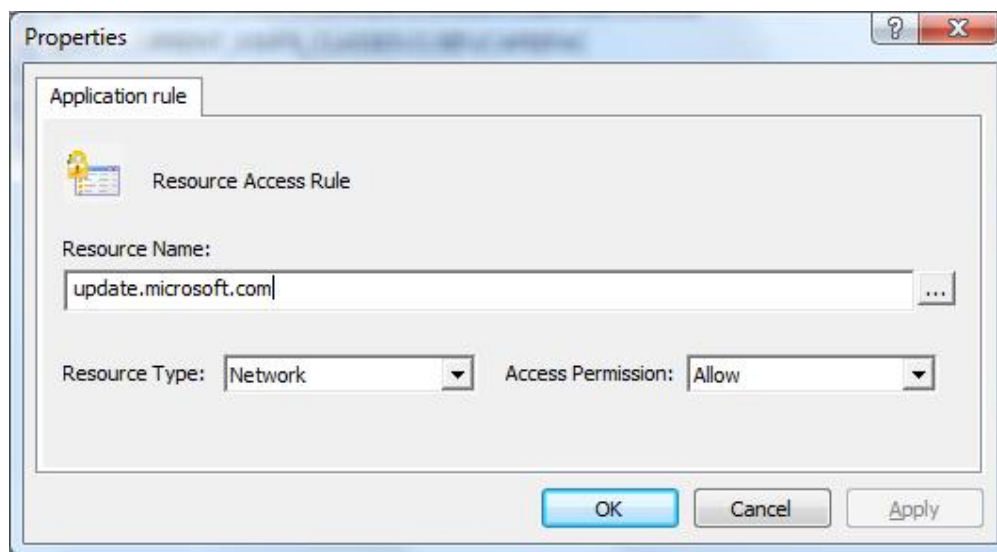
/Subnet	Network Mask	Hosts
/16	255.255.0.0	65,024
/24	255.255.255.0	254
/28	255.255.255.240	14

If subnet mask is not specified then rule is applied only to a single host.

The addresses might be specified in resource definition



or in application specific rule.

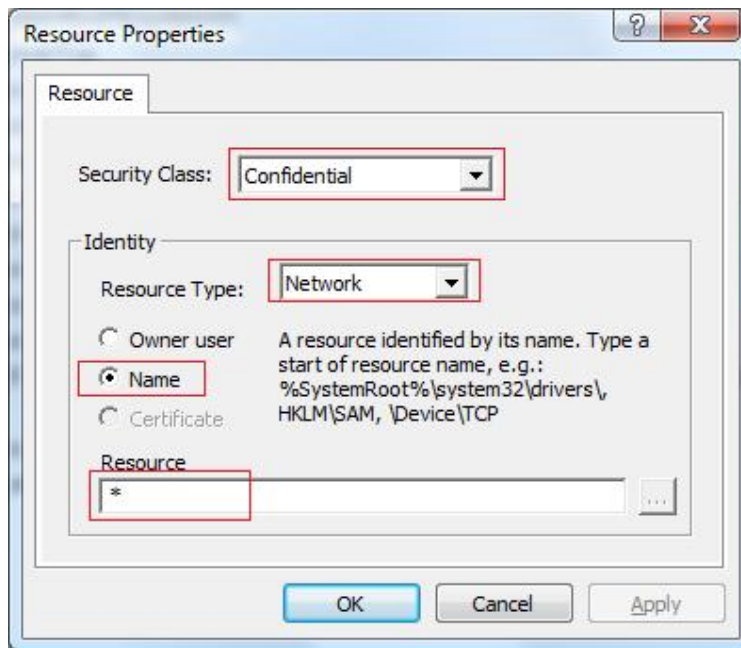


Please note that 'Resource Name' defines destination host address. Source host address and transport protocol, such as TCP, UDP, ICMP and etc, are not specified and could be any.

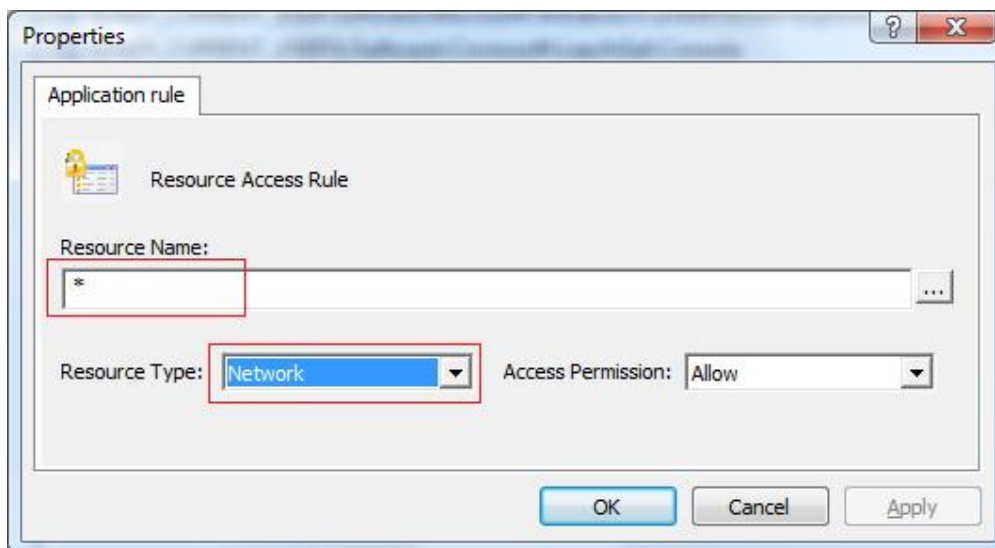
Also note, GeSWall controls IP protocol network traffic recognized and handled by Windows core. GeSWall doesn't control non-IP protocols, such as IPX, and does not control raw traffic prior its handling by Windows core. It means GeSWall cannot be used for screening network traffic from Windows core itself, but from applications.

7.5.1 How to deny network access for isolated applications

You may apply default network restrictions for all isolated applications. For that you need to add a confidential resource definition as shown on the figure.

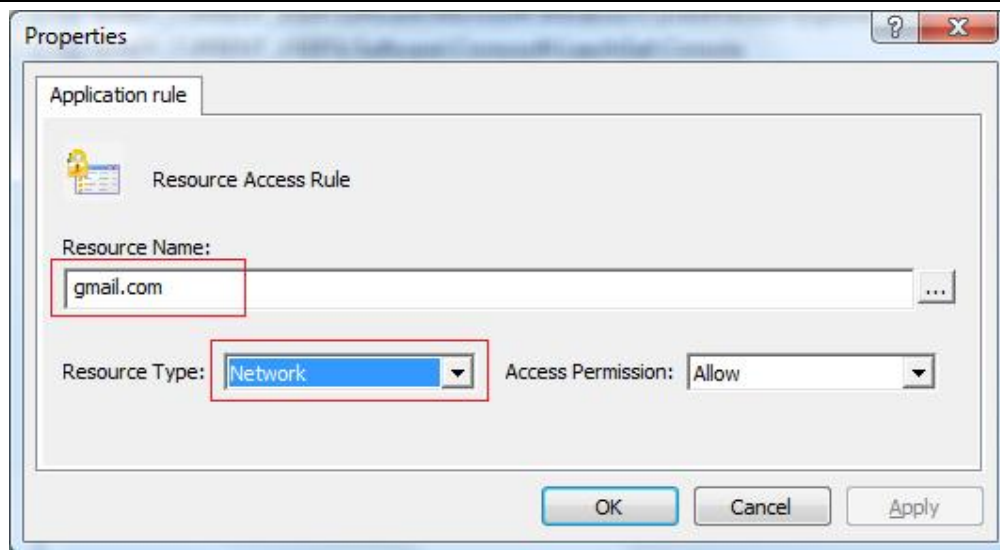


Once the resource definition is entered, isolated applications could not access network unless there are specific application rules that grant the access. For example, you could create such rule for a web browser:



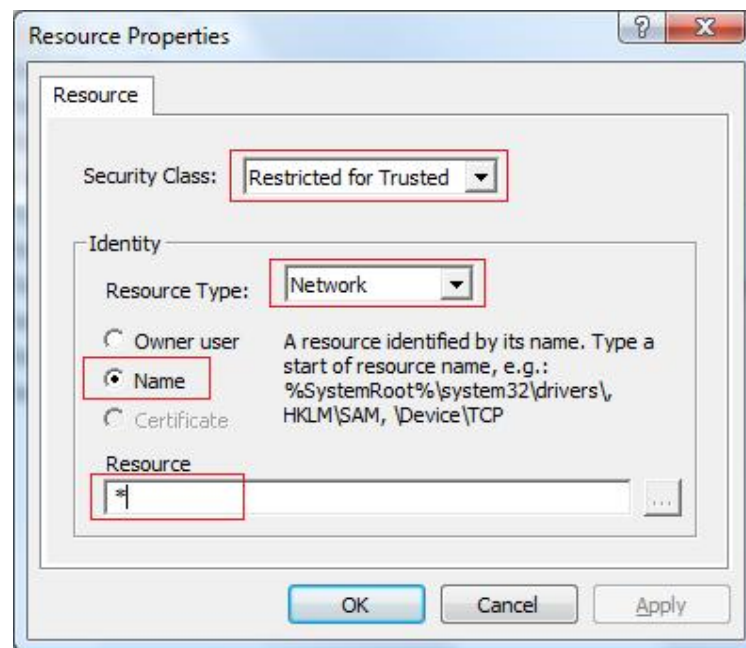
The rule grants access to all network hosts or web sites.

For an isolated e-mail client there could be a rule granting access only to e-mail server as illustrated on the figure:



7.5.2 How to deny network access for all applications

GeSWall might be configured to restrict network access for all applications including trusted. Such configuration enables using GeSWall as a firewall.



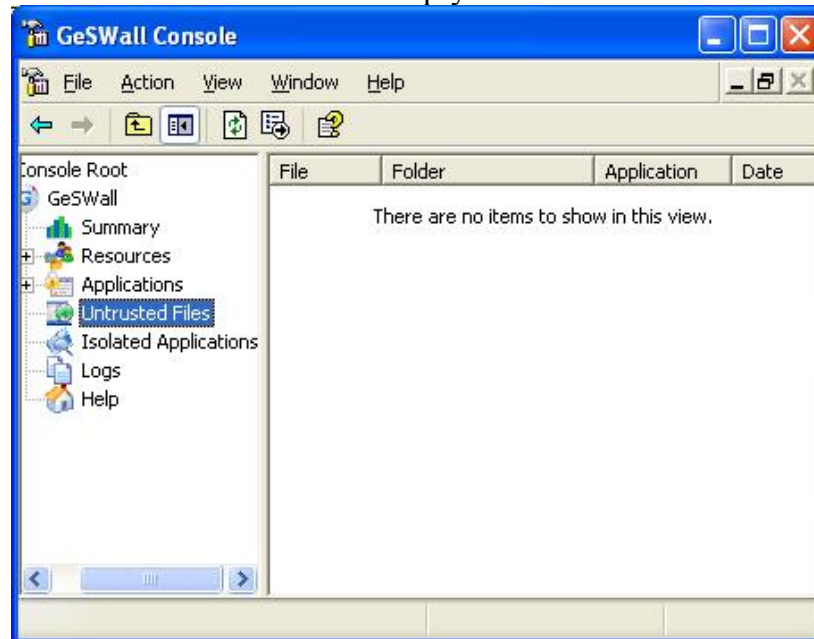
Once the resource definition is applied, network access is blocked for entire system and you should grant it specifically for individual applications including trusted.

System, services.exe, svchost.exe, lsass.exe and winlogon.exe are exclusions. The applications always have unrestricted access regardless the rules. That is required to provide core networking services such as DHCP client, DNS client and so on.

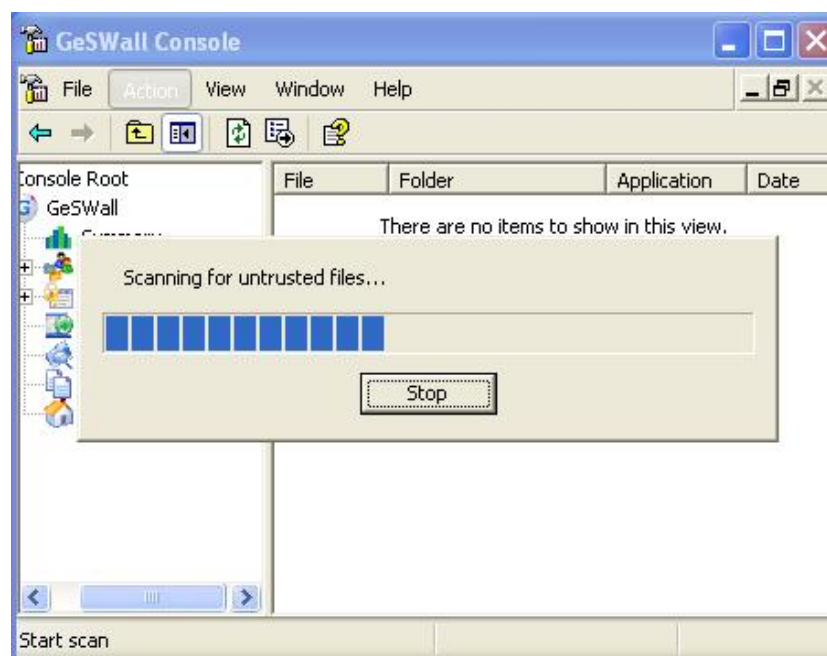
7.6 Untrusted Files

GeSWall tracks all files created or modified by isolated applications and labels them as untrusted. The files are marked by special overlay icon as described in “GeSWall Labels” section. “Isolated files” folder in the GeSWall Console allows managing those untrusted files.

By default, the list of untrusted files is empty.



A scanning is required to fill or refresh the list. The scanning process is started by “Action\Start scan...” menu item.



On scanning completion, a list of untrusted files appears in the right pane.

File	Folder	Application	Date
index.dat	C:\Documents and ...	Adobe Acrobat Rea...	2008/01/01
UserCache.bin	C:\Documents and ...	Adobe Acrobat Rea...	2007/12/29
index.dat	C:\Documents and ...	Adobe Acrobat Rea...	2008/01/01
AdobeCMapFnt08.lst	C:\Documents and ...	Adobe Acrobat Rea...	2007/12/29
index.dat	C:\Documents and ...	Adobe Acrobat Rea...	2008/01/01
hptg[2].js	C:\Documents and ...	Internet Explorer	2007/12/11
new[1].gif	C:\Documents and ...	Internet Explorer	2007/12/11
ovrW[2].css	C:\Documents and ...	Internet Explorer	2007/12/11
DA56D5D55CF669A22EAB...	C:\Documents and ...	Internet Explorer	2007/12/11
andr@rad.msn[2].txt	C:\Documents and ...	Internet Explorer	2007/07/26
86F1396496DFE1BAD68A...	C:\Documents and ...	Internet Explorer	2007/12/11
admin@questionmarket[1]...	C:\Documents and ...	Internet Explorer	2007/12/11
0000000001_0000000000...	C:\Documents and ...	Internet Explorer	2007/12/11
admin@www.msn[1].txt	C:\Documents and ...	Internet Explorer	2007/12/11
bookmarks.bak	C:\Documents and ...	Mozilla Firefox	2007/12/29
bookmarks.html	C:\Documents and ...	Mozilla Firefox	2007/12/29
localstore.rdf	C:\Documents and ...	Mozilla Firefox	2007/12/29
prefs.js	C:\Documents and ...	Mozilla Firefox	2007/12/29
_CACHE_001_	C:\Documents and ...	Mozilla Firefox	2007/12/29
_CACHE_002_	C:\Documents and ...	Mozilla Firefox	2007/12/04
_CACHE_003	C:\Documents and ...	Mozilla Firefox	2007/12/04

The list has four columns:

- File – file name.
- Folder – file directory name.
- Application – name of isolated application that created or modified the file last time. Note application name is available only for known applications that are defined in the Application Database.
- Date – date and time of file modification. The format: Year/Month/Day Hour:Minute:Second

The list view could be sorted by file name, folder name, application or date via clicking on corresponding column name. For example previous figure has the list sorted by application name.

Two context menu operations are available for selected items in untrusted files list:

- Delete file – permanent erasing of untrusted file.
- Label as trusted – labeling file as trusted, so it does not appear in the list anymore. The operation is similar to “Label as Trusted” command in Windows Explorer context menu (see “GeSWall’s Labels” section).

The operations could be performed on a single file or on selected subset of files.

File	Folder	Application	Date
index.dat	C:\Documents and ...	Adobe Acrobat Rea...	2008/01/01
UserCache.bin	C:\Documents and ...	Adobe Acrobat Rea...	2007/12/29
index.dat	C:\Documents and ...	Adobe Acrobat Rea...	2008/01/01
AdobeCMapFnt08.lst	C:\Documents and ...	Adobe Acrobat Rea...	2007/12/29
index.dat	C:\Documents and ...	Adobe Acrobat Rea...	2008/01/01
hptg[2].js	C:\Documents and ...	Internet Explorer	2007/12/11
new[1].gif	C:\Documents and ...	Internet Explorer	2007/12/11
ovrW[2].css	C:\Documents and ...	Internet Explorer	2007/12/11
DA56D5D55CF669A...	C:\Documents and ...	Internet Explorer	2007/12/11
andr@rad.msn[2].txt	C:\Documents and ...	Internet Explorer	2007/07/26
86F1396496DFE1BAD68A...	C:\Documents and ...	Internet Explorer	2007/12/11
admin@questionmarket[1]...	C:\Documents and ...	Internet Explorer	2007/12/11
0000000001_0000000000...	C:\Documents and ...	Internet Explorer	2007/12/11
admin@www.msn[1].txt	C:\Documents and ...	Internet Explorer	2007/12/11
bookmarks.bak	C:\Documents and ...	Mozilla Firefox	2007/12/29
bookmarks.html	C:\Documents and ...	Mozilla Firefox	2007/12/29
localstore.rdf	C:\Documents and ...	Mozilla Firefox	2007/12/29
prefs.js	C:\Documents and ...	Mozilla Firefox	2007/12/29
_CACHE_001_	C:\Documents and ...	Mozilla Firefox	2007/12/29
_CACHE_002_	C:\Documents and ...	Mozilla Firefox	2007/12/04
_CACHE_003	C:\Documents and ...	Mozilla Firefox	2007/12/04

The result of scanning is cached and displayed on subsequent launches of GeSWall Console. Start a new scanning for getting updated list.

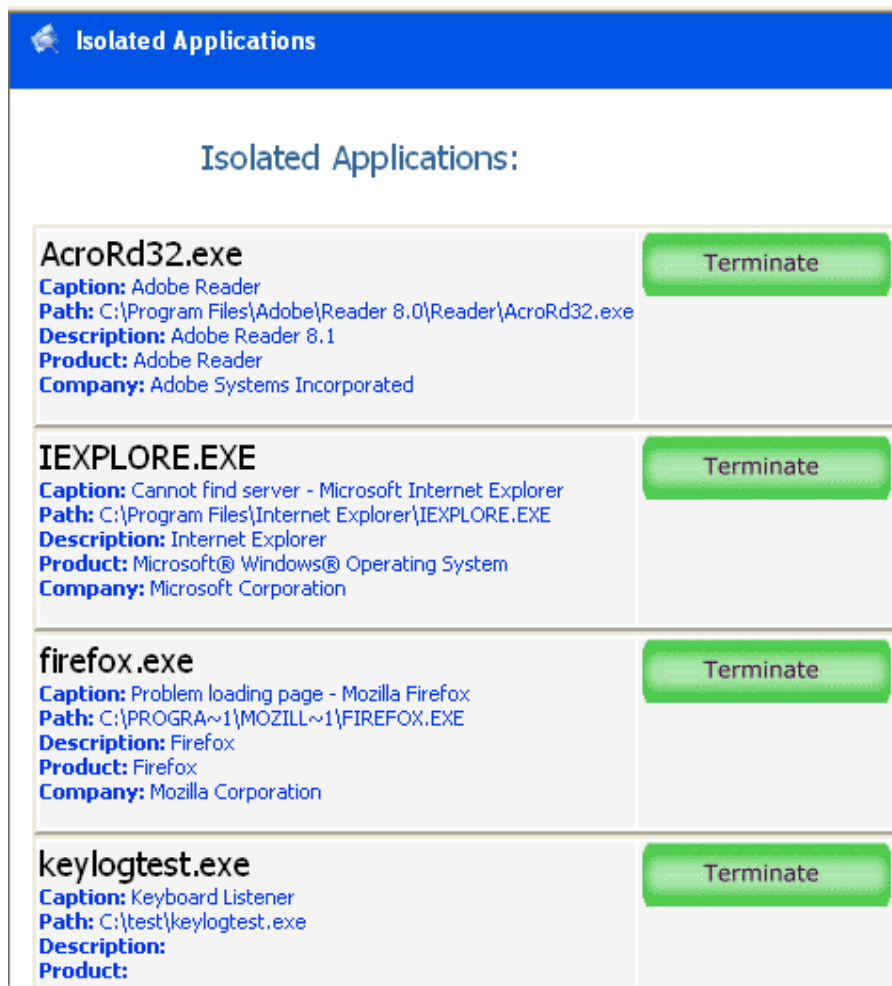
7.7 Isolated Applications

“Isolated Applications” folder enumerates isolated application instances or processes. The feature is useful for advanced analysis of isolated applications.

On selection of “Isolated Applications” folder, right pane lists all currently running isolated processes with relevant information, such as:

- Caption – main window caption name;
- Path – full path to the application executable;
- Description – application description provided by software vendor;
- Product – product name;
- Company – software vendor name.

You have an option to terminate selected process by clicking on green “Terminate” button. Additionally, all isolated processes might be terminated at once via “Action\Terminate all” menu item.



Isolated Applications

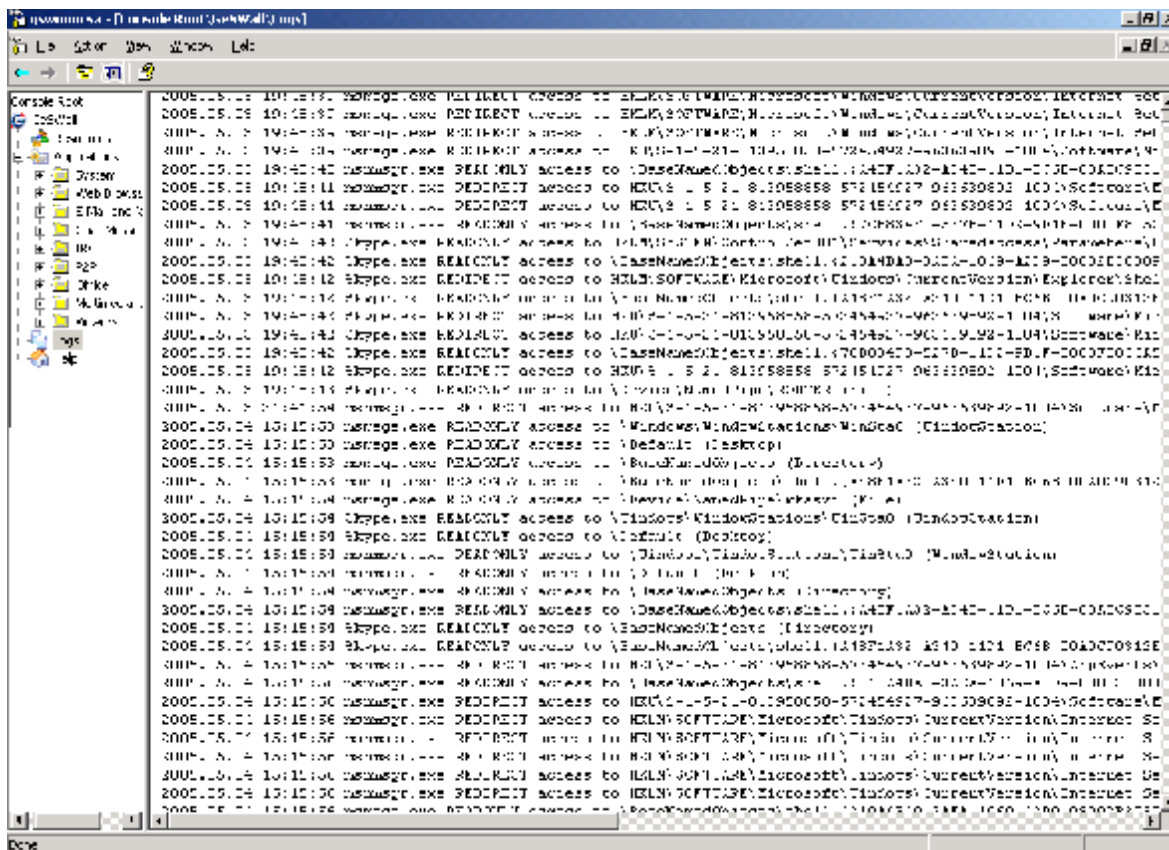
Isolated Applications:

AcroRd32.exe Caption: Adobe Reader Path: C:\Program Files\Adobe\Reader 8.0\Reader\AcroRd32.exe Description: Adobe Reader 8.1 Product: Adobe Reader Company: Adobe Systems Incorporated	Terminate
IEXPLORE.EXE Caption: Cannot find server - Microsoft Internet Explorer Path: C:\Program Files\Internet Explorer\IEXPLORE.EXE Description: Internet Explorer Product: Microsoft® Windows® Operating System Company: Microsoft Corporation	Terminate
firefox.exe Caption: Problem loading page - Mozilla Firefox Path: C:\PROGRA~1\MOZILL~1\FIREFOX.EXE Description: Firefox Product: Firefox Company: Mozilla Corporation	Terminate
keylogtest.exe Caption: Keyboard Listener Path: C:\test\keylogtest.exe Description: Product:	Terminate

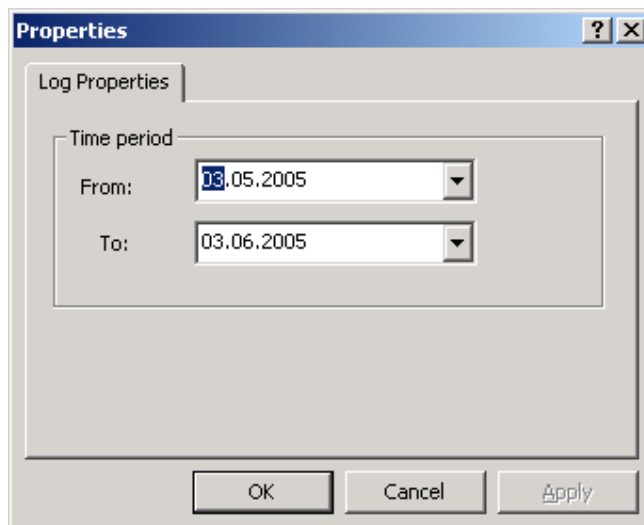
The list of processes is updated on each switching to “Isolated Applications” folder or on demand: selecting “Action\Refresh” menu item or pressing “F5” key.

7.8 Logs

Whenever GeSWall restricts an access, it records the event to the log. The log can be viewed in the 'Logs' folder of the GeSWall Console as shown in the picture below.



By default, it shows the records for the current day. You may adjust the view by 'Action\Log Properties...' context menu to choose the required time period.



An event record has the following fields:

Date	Local zone date in format YYYY.MM.DD
Time	Local zone time in format HH:MM:SS
Application file name	The name of application executable (not a full path)
Access restriction type	<ul style="list-style-type: none"> • REDONLY access – access was restricted to read only • REDIRECT access – access was redirected to a local copy • DENY access – access was denied • DENY message – window message sending was denied
Resource name	Full name of resource, e.g. file name, registry name.
Resource type	Native name of resource in terms of operation system: <ul style="list-style-type: none"> • Debug • Desktop • Device • Directory • Event • File • IO completion port • Job • Registry • Keyed event • Mutant • Network • LPC port • Process • Profile • Section • Semaphore • Symbolic link • System object • Thread • Token • Timer • Waitable port • Windows station

Usually you will find dozens of event records for running isolated applications because those applications are restricted in access according to the Access Restriction Policy. The event records do not necessarily indicate intrusion attempts but in most cases are restrictions of optional application functionality, which could be mal-ware or intrusion damage activity. This is similar to firewall logs which frequently show large numbers of blocked connection attempts.

Analyzing logged events for attack traces requires specialized expertise in computer security and GeSWall is not intended to be an intrusion detection product.

The log is particularly useful for debugging application problems while authoring specific rules for new applications.

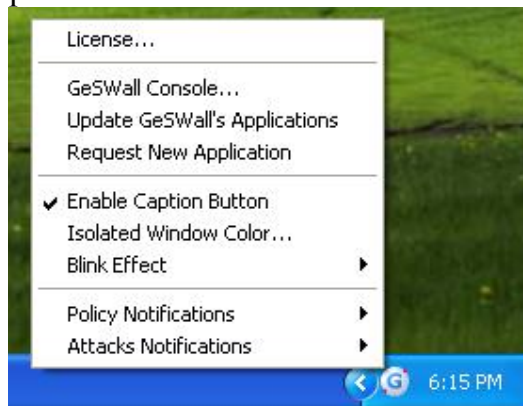
8 Application Database Update

GeSWall comes with a default application database, which contains specific rules for most popular internet applications including web browsers, e-mail clients, messengers, etc. Moreover, GentleSecurity maintains that database on a regular basis and lets you get automatic periodic updates for corrected rules and additional applications. The purpose is to have more safe applications and to protect you from more internet threats. Ideally, all internet applications should run isolated.

When GeSWall detects an application database update is available it automatically update the database and notifies you about the status with a tray balloon message, as shown on the picture below.



Click on the GeSWall tray icon and choose the 'Update GeSWall's Applications' menu item to start an update.



GeSWall downloads an update package from www.gentlesecurity.com and applies it to application database. During processing, it notifies you about update progress



...and completion status.



Automatic update does not prevent you creating your own rules for present or new applications. GeSWall merges update changes with your changes by following these rules:

- Add non-present application definitions from update package.
- Set an application identification method (Version information, Name or Digest) as specified in the update package.
- Add non-present specific rules and resources from the update package.
- Modify and delete specific rules and resources created by GentleSecurity during installation (default database) or previous updates.

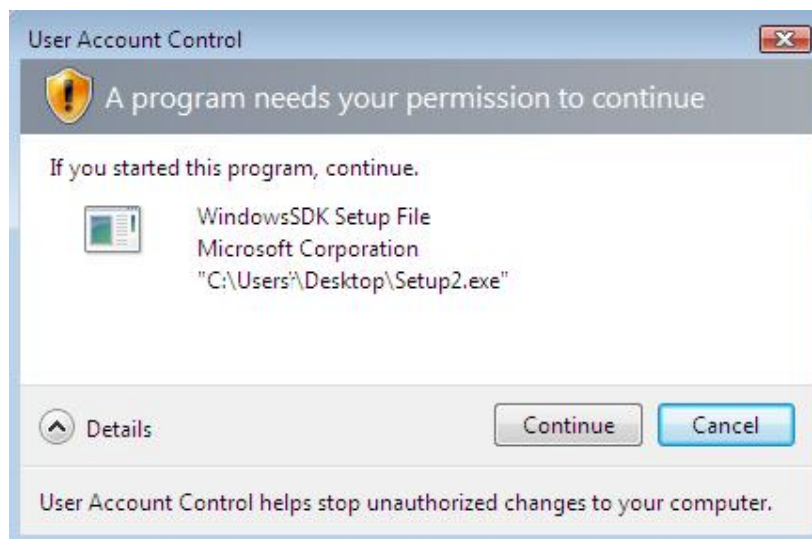
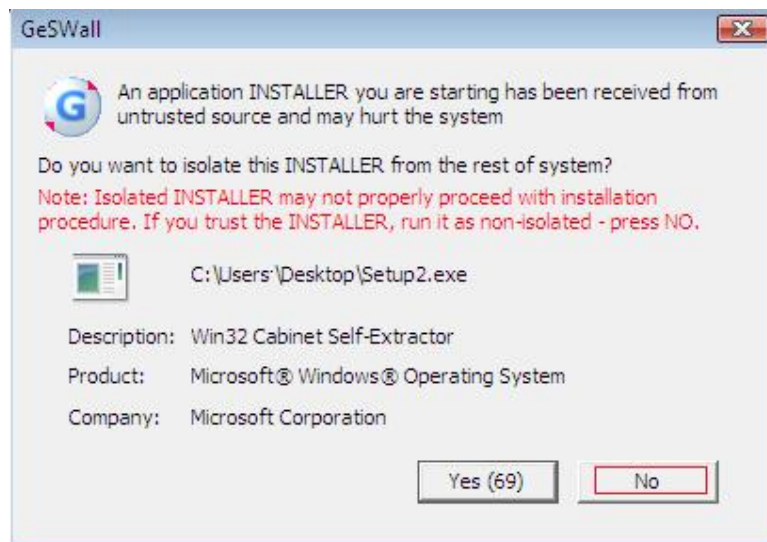
All your changes including group and application display names, group's hierarchy, security levels, additional rules and resources definitions are kept untouched.

So, whenever you get an application, which is not currently in the GeSWall application database, you can safely create the application definitions and specific rules yourself. Future updates will only amplify your specific rules.

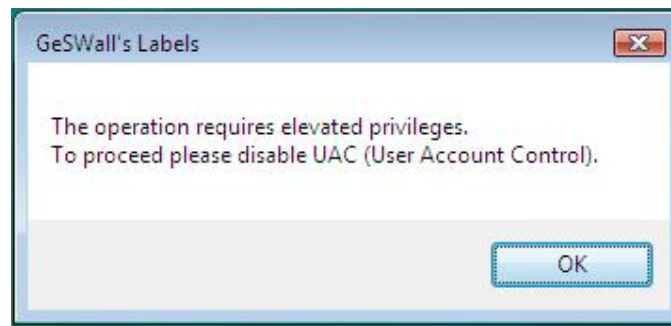
Instead of adding application definition on your own, you can submit a request on www.gentlesecurity.com, by clicking the 'Request New Application' menu item of the GeSWall tray icon. If there is sufficient demand, GentleSecurity will handle your request and you will get the application supported with a future automatic update.

9 Windows Vista UAC (User Account Control)

GeSWall supports working together with Windows Vista's UAC (User Account Control). GeSWall ensures that you do not get UAC dialogs for isolated application. UAC pop-up dialog appears as usual if you refuse to isolate an application at GeSWall's notice as illustrated on the figures:



However, GeSWall doesn't support label operations as described in section "4. GeSWall's Labels" when run as administrator with enabled UAC. In that case it displays a notice as on the figure below.

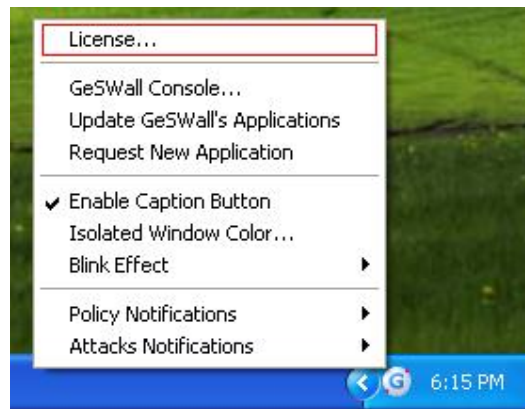


So you should use Untrusted Files browser as described in “7.6 Untrusted Files”.

10 Licensing

GeSWall Professional Edition is delivered as a trial version. The trial is fully functional for 15 days. After 15 days the product switches to the functionality available in Freeware version.

Using of GeSWall Professional Edition for more than 15 days requires an appropriate license. You may check your current license by License menu item in the GeSWall's tray icon, as shown on the figures below.



The license is a file you receive on purchase. For applying new license, open “GeSWall License” dialog, select a license file location and press “Authorize” button.



Once the new license is applied, the dialog displays relevant information including License Number which is required for the support inquiries.

