

**Administration Guide**

# **GeSWall 2.3 Server 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GentleSecurity claims copyright in this program and documentation as an unpublished work, revisions of which were first licensed on the date indicated in the foregoing notice.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 2005-2006 © 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](mailto:gswsupport@gentlesecurity.com)

Web: [www.gentlesecurity.com](http://www.gentlesecurity.com)

Published on: June 2006

---

## Table of Contents

1. Introduction .....	4
1.1. Overview .....	4
1.2. Access Restriction Policy .....	7
2. Getting started with GeSWall .....	8
3. GeSWall Group Policy Extension.....	10
4. Configuring GeSWall Policy .....	13
4.1. Security Levels .....	13
4.2. Resources.....	14
4.3. Applications.....	16
4.4. Resource Name Syntax.....	20
4.5. Logs .....	23
5. Application Database Update.....	25

## 1. Introduction

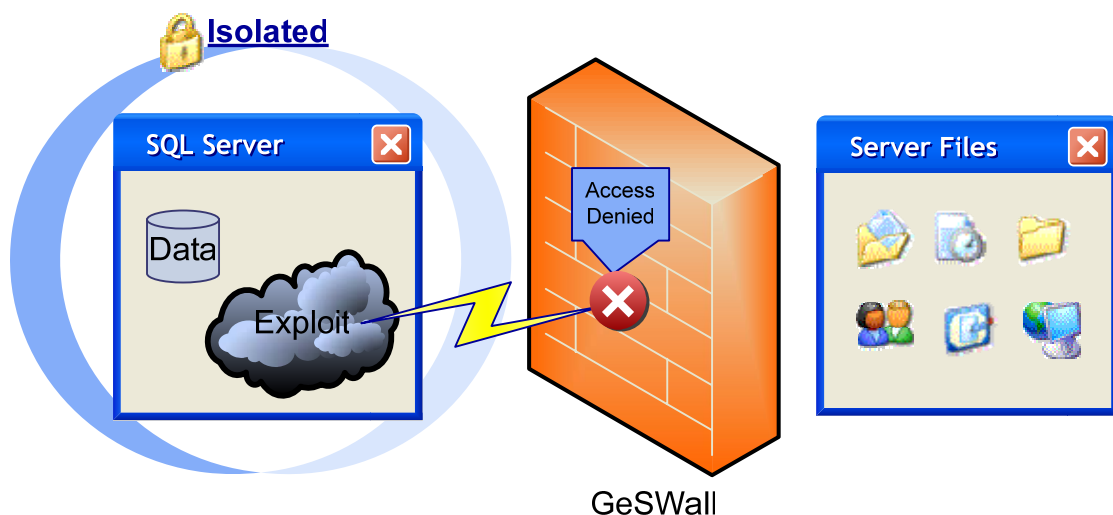
With GeSWall Server Edition, you can harden your Web, Mail and SQL Servers. Hardening implies an isolation security policy that prevents damage from targeted intrusions and effectively precludes various attacks, including:

- ✓ Targeted intrusions on your internal network
- ✓ Backdoors, rootkits, key loggers
- ✓ Malicious software infection

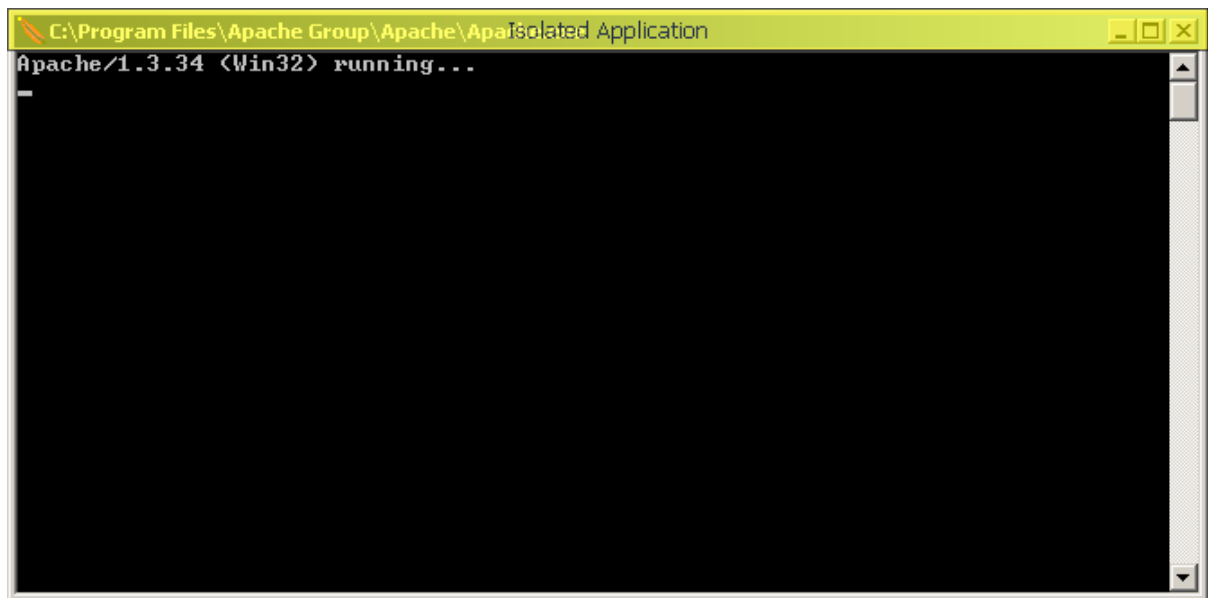
GeSWall provides powerful features to manage its security policy by means of Microsoft Windows Group Policy and Active Directory. This manual will guide you through them.

### 1.1. Overview

Once installed and enabled, GeSWall Server Edition dynamically isolates web, e-mail and sql server applications. Intrusions, exploits, viruses and trojans cannot pass through the isolation and so cannot cause damage.



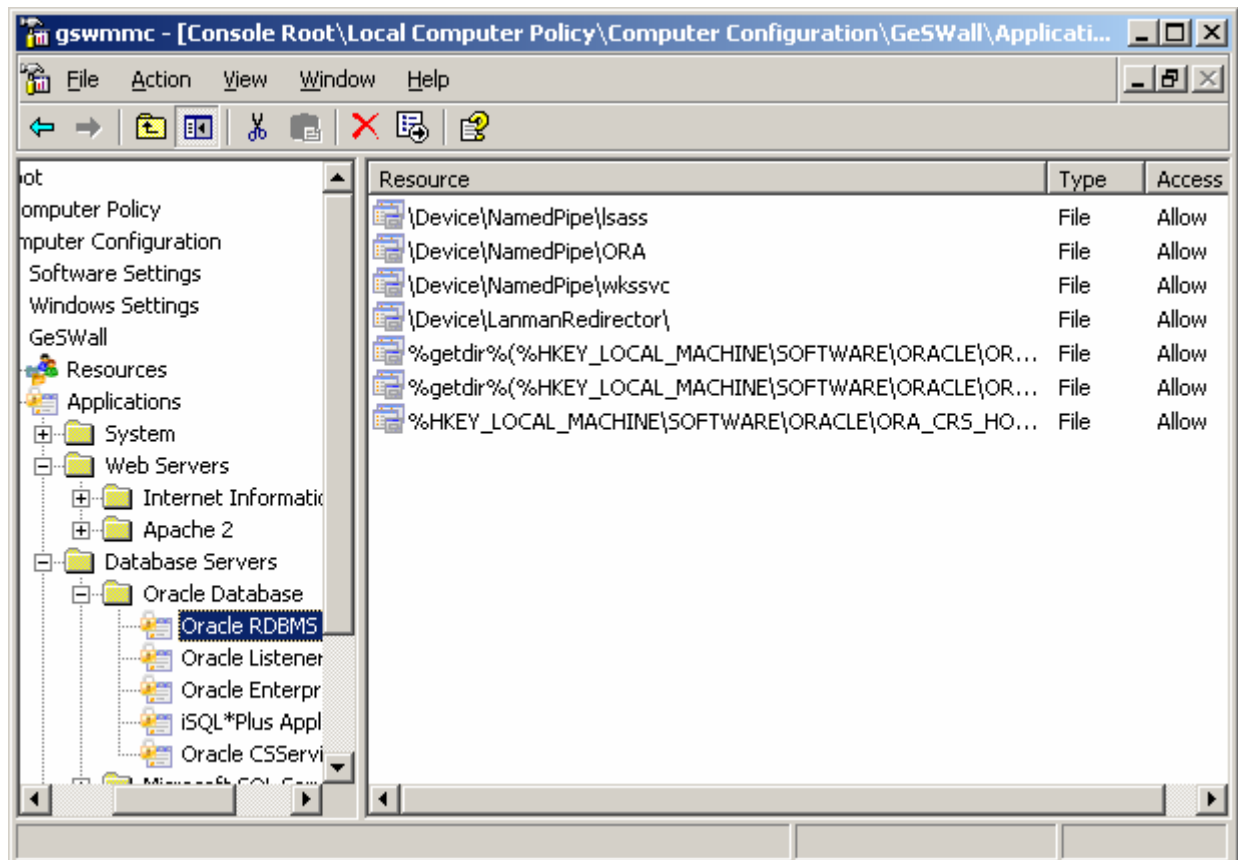
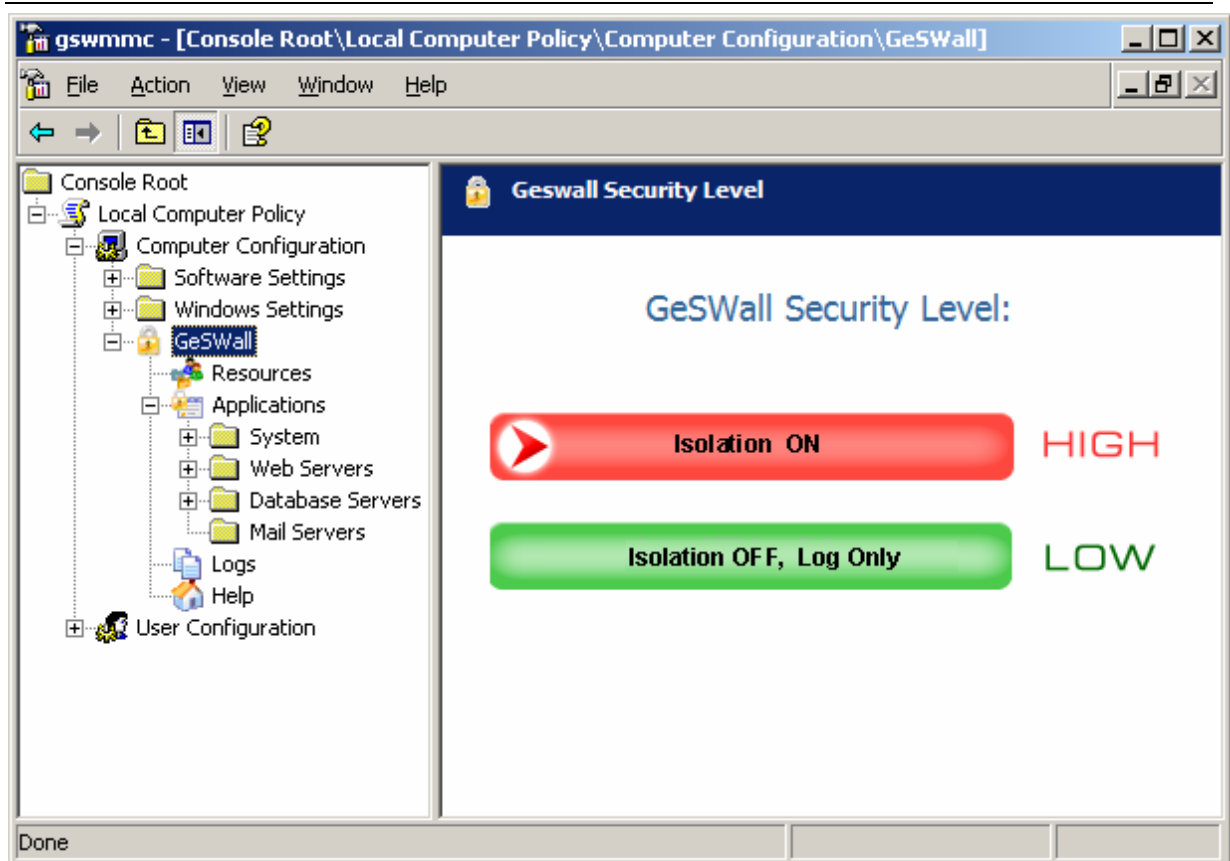
An access restriction policy prevents leaks of confidential files and unauthorized modification of files, registry, etc., coming through an isolated server application.



Besides general restrictions, GeSWall adjusts its policy according to specific application rules. The rules describe specific resources required for server's functionality. In case of intrusion, an attack scope and damage are limited only by these resources.

GeSWall Server Edition has pre-configured hardening rules for most popular Web, SQL and Mail servers. Pre-configured rules come in an open Application Database. GentleSecurity keeps the database up to date by adding information about new versions and additional server applications. Administrator's task is just supplementing rules for a particular environment.

GeSWall Server Edition integrates into Windows Group Policy as an extension, which allows centrally manage GeSWall policy settings as a part of Group Policy: for particular Active Directory site, domain, organizational unit or particular machine.



---

## 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. May create new untrusted resources, e.g. files.
4. 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. You can specify untrusted and confidential resources explicitly by their name or ownership.

## 2. Getting started with GeSWall

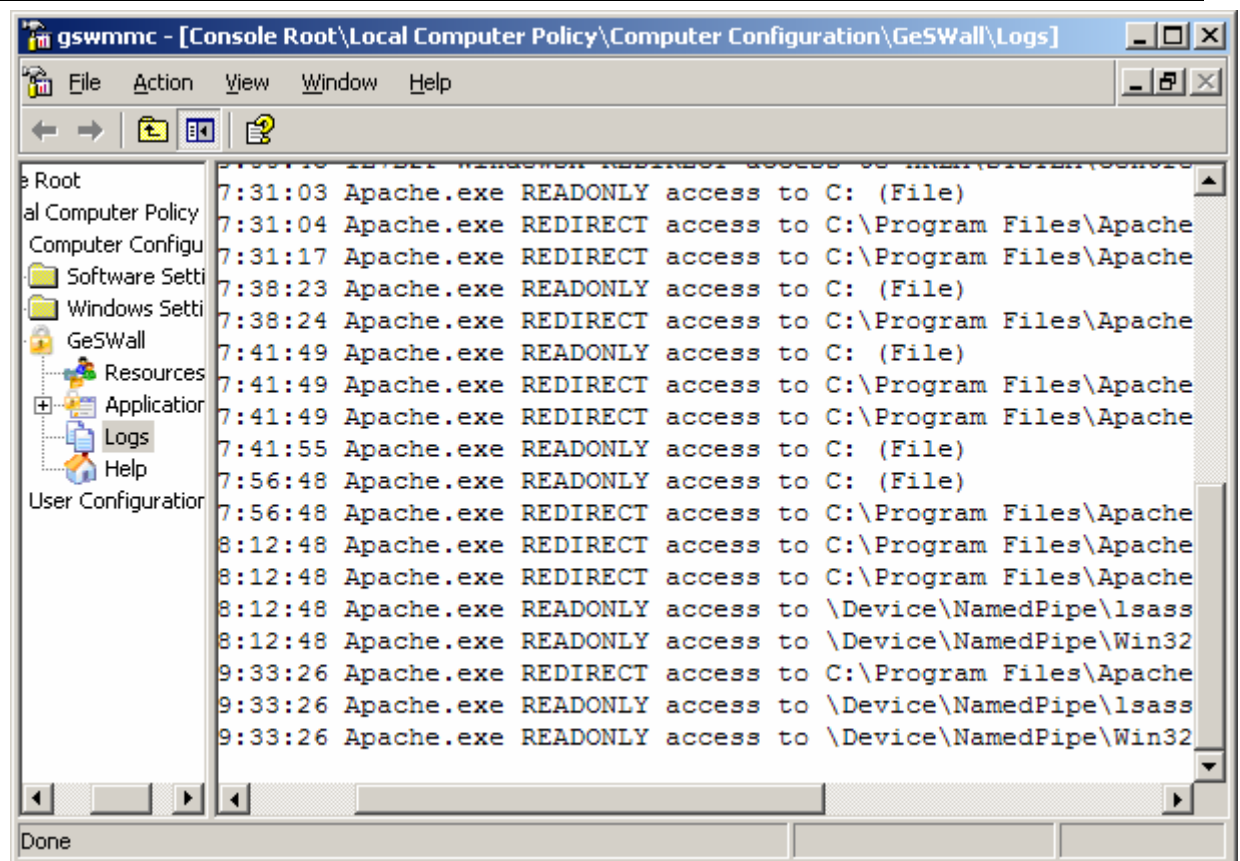
For installation, click on the downloaded *geswall\_s.msi* and follow the instructions. After reboot, GeSWall starts in “Log Only” mode. This means GeSWall does not enforce its isolation policy yet to let you setup additional policy rules.

Start GeSWall Console by shortcut in GeSWall menu: Start/Programs/GeSWall Server Edition/GeSWall Console. Check a list of default server applications – applications that have default isolation rules.



If required, setup additional rules for particular server applications you want to isolate and which are not present in the list. Note, that GeSWall loads rules on application start. Thus, you would need to restart a server process in order to apply a new configuration.

Close the Console, leave services running for some time in order to activate its functionality. Then open the Console again and read the log entries.



Whenever you see entry with restricted access to a resource such as file or registry, create an additional rule allowing access to this resource. (See section 4.3) Then restart the server process and read the log entries again.

Repeat the procedure until you are convinced that a server application has unrestricted access to all required resources. Please note, that read access is not restricted unless resources are files declared as confidential (see Resources section). This means you need only setup rules for resources, which must be modified by an application.

Once rules are set, switch Security Level to “Isolation ON” and restart server applications. From this moment, the applications are isolated from the rest of system. A successful intrusion attack based on vulnerability or mis-configuration will not cause damage as it will not be able go through the isolation layer to other system resources and applications.

Resource names follow Resource Name Syntax that provides universal resource names that are valid in any environment (see Resource Name Syntax section). This allows you to compose generic rules, which can be applied to a wide set of servers. Therefore, you can apply and centrally manage your isolation policy on the scope of Active Directory domain, organizational unit or site (see GeSWall Group Policy Extension section).

### 3. GeSWall Group Policy Extension

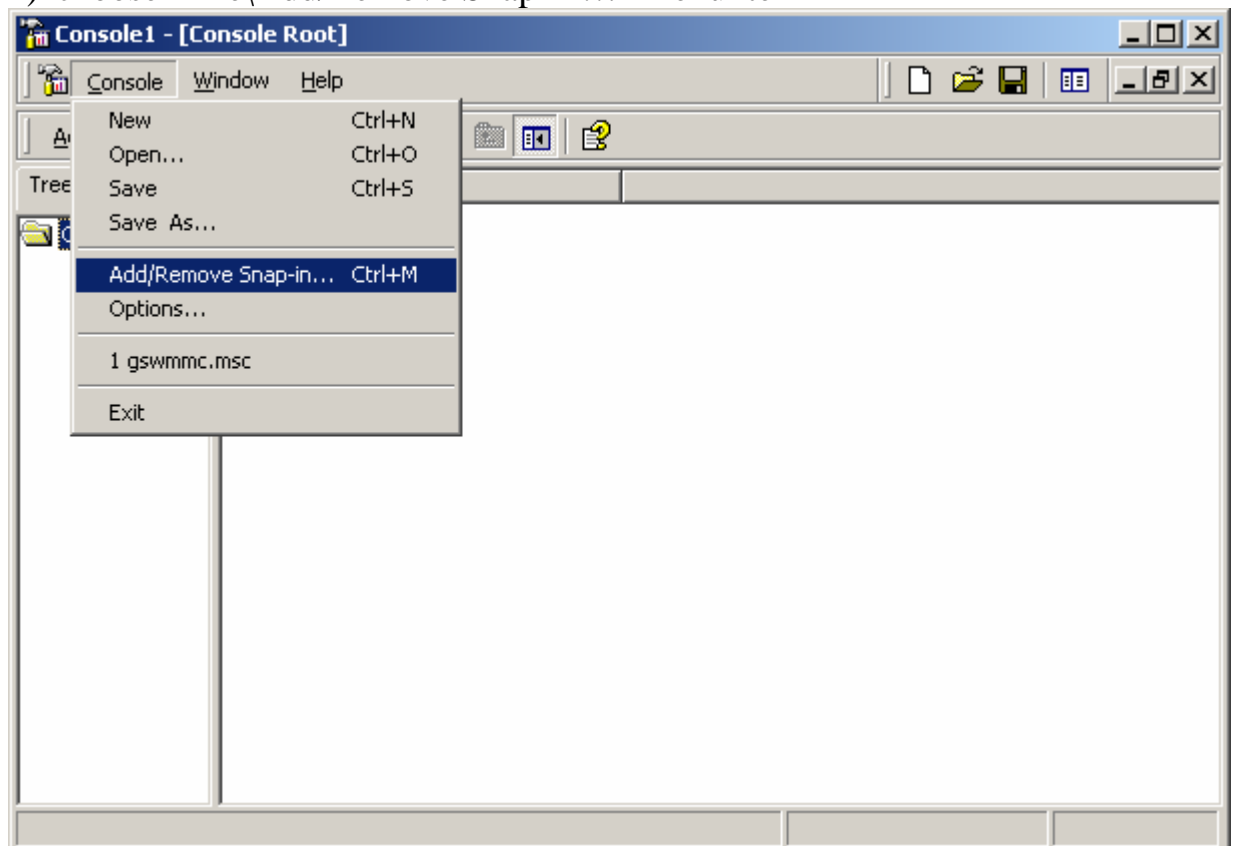
GeSWall Server Edition integrates into Windows Group Policy as an extension, which allows you to centrally manage GeSWall policy settings as a part of Group Policy. The extension provides the ability to set GeSWall policy on any Active Directory level:

- Machine – policy applied for particular machine
- Site – policy applied for entire Active Directory Site
- Domain – policy applied for whole Active Directory domain
- Organizational Unit – policy applied for particular Active Directory organizational unit.

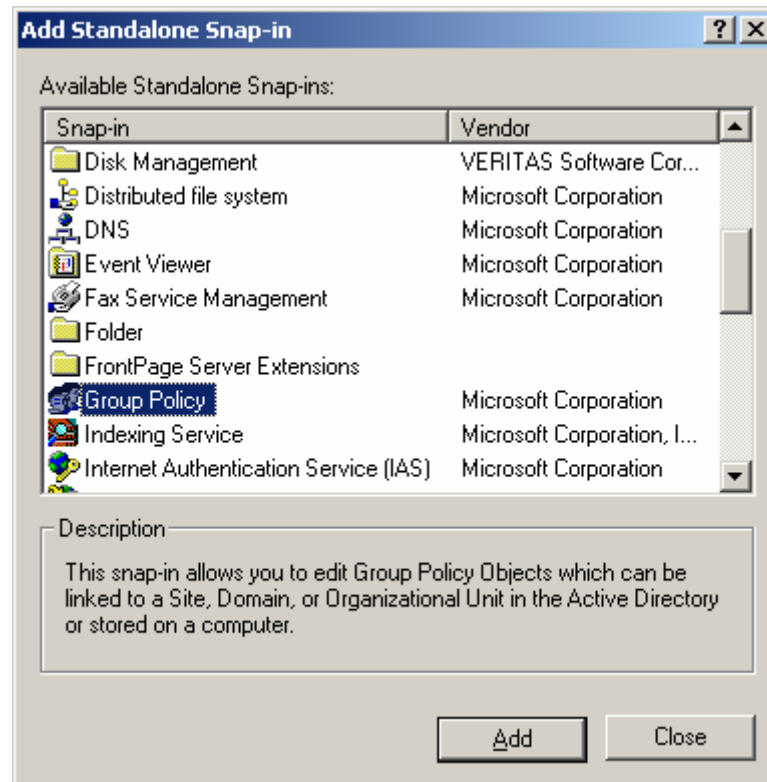
The GeSWall's Management Console is an MMC (Microsoft Management Console) snap-in. When installed, GeSWall appears as a new node of Group Policy. For the local machine, policy can be set through a shortcut in the GeSWall menu: Start/Programs/GeSWall Server Edition/GeSWall Console.

Setting policy on other targets, such as the domain would requires these steps:

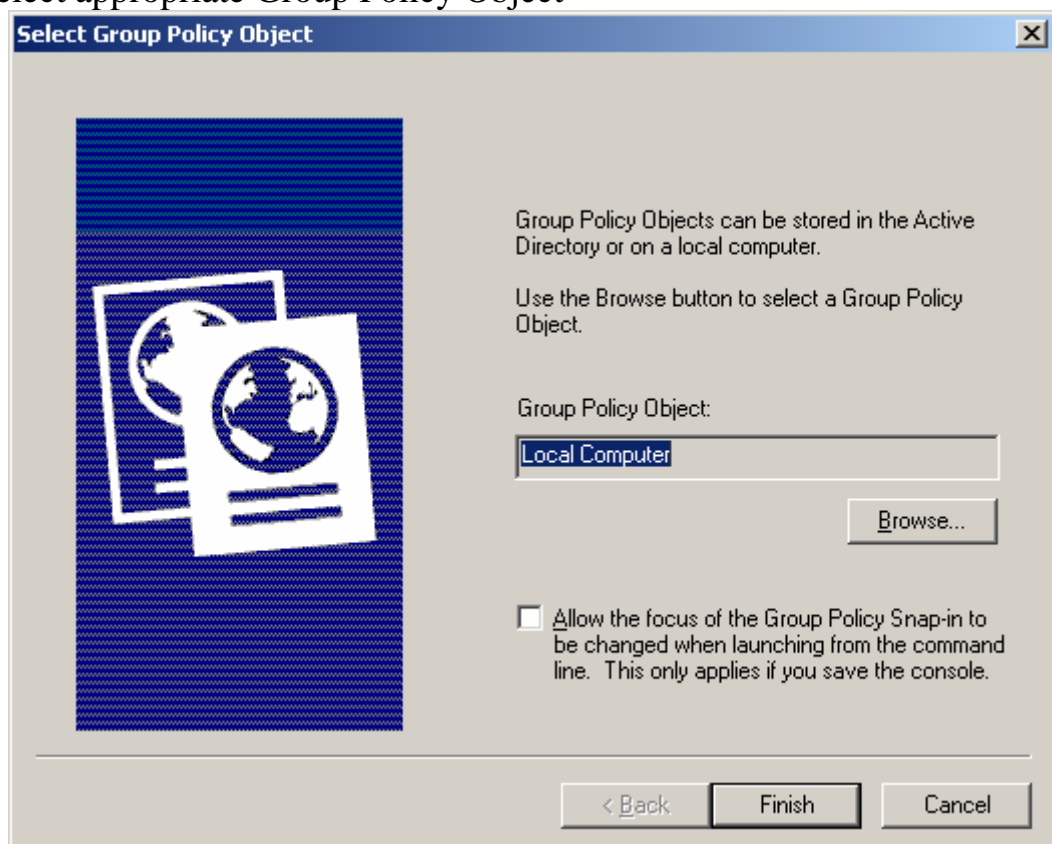
- 1) start mmc.exe
- 2) choose “File\Add/Remove Snap-In...” menu item



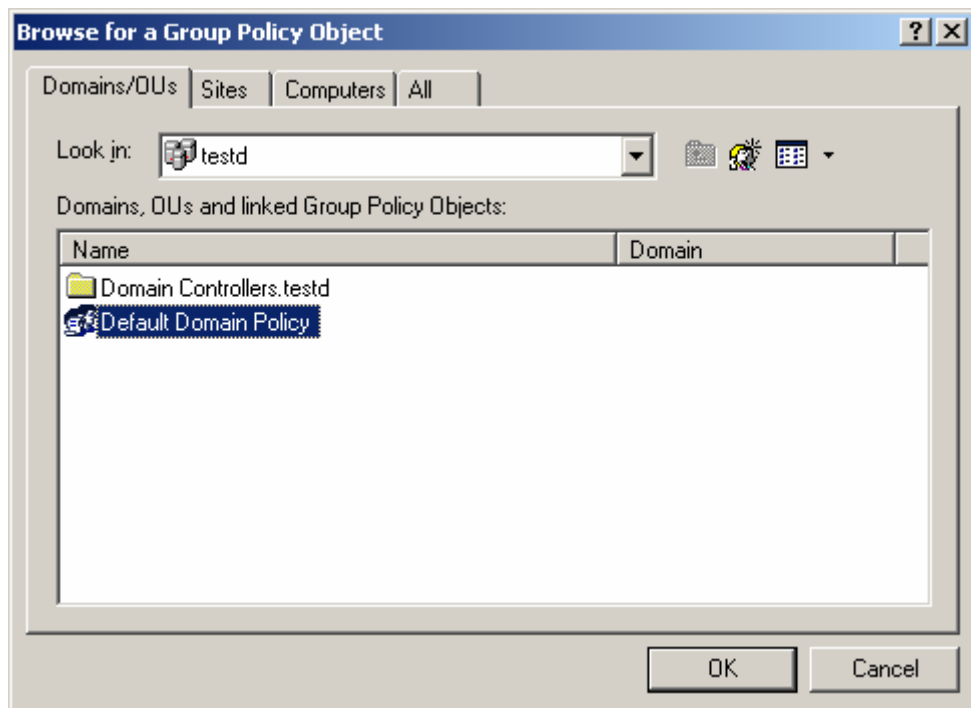
- 3) press Add button
- 4) select “Group Policy Object Editor”



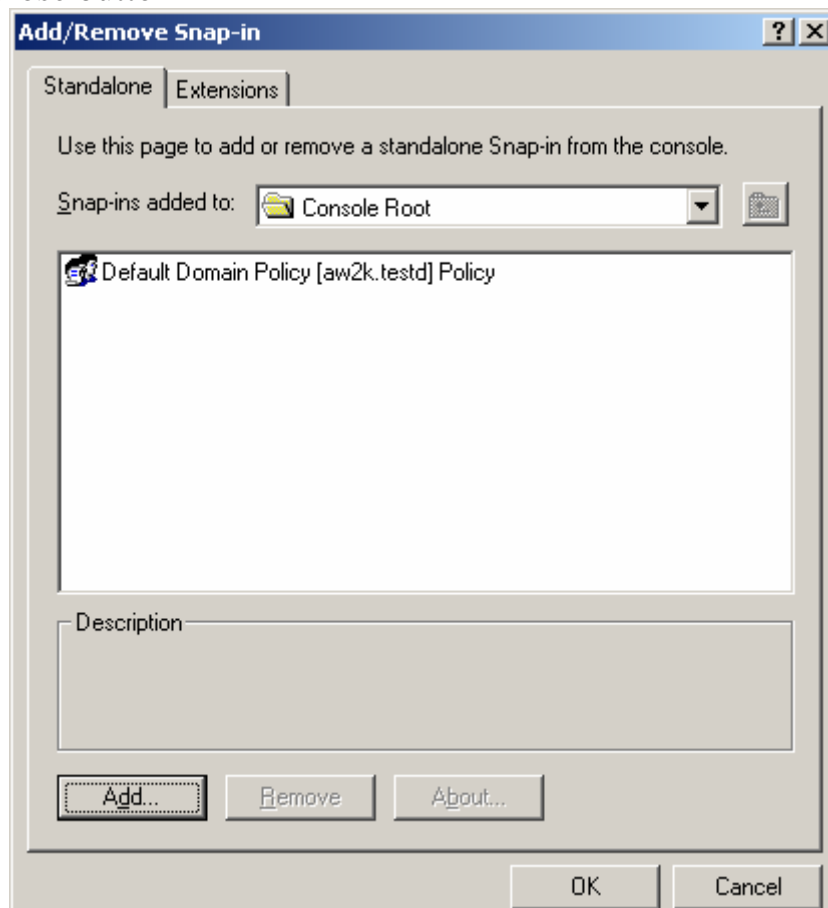
- 5) press "Add" button
- 6) select appropriate Group Policy Object



You can choose the scope of GeSWall policy among Active Directory domains, OUs, sites and machines.



- 7) press "Finish" button
- 8) press Close button



- 9) press OK button

Note: to run the Console you must have rights to the Group Policy link you choose; for local machine policy, you must be a member of the local administrators group.

## 4. Configuring GeSWall Policy

### 4.1. Security Levels

GeSWall supports two 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.



A red tick marks the current Security Level. 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.

#### Isolation OFF, Log Only

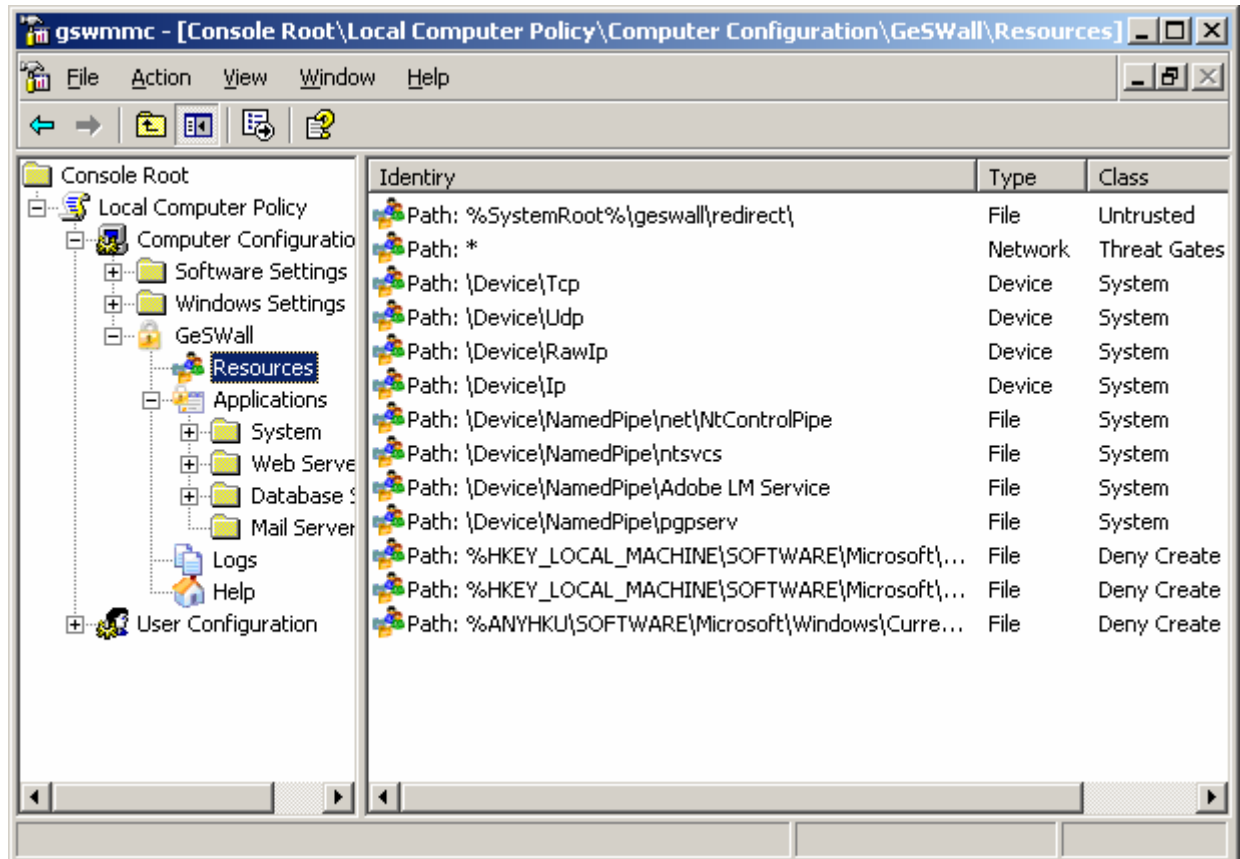
GeSWall applies its isolation policy but instead of restricting an access, only logs events. The level is particularly useful for authoring specific rules for your server applications. It reveals objects an application requires access to. This is the default security level.

#### Isolation ON

GeSWall effectively isolates server applications defined in the Application Database. Switch to this level when log entries expose no restricted access to files or registry.

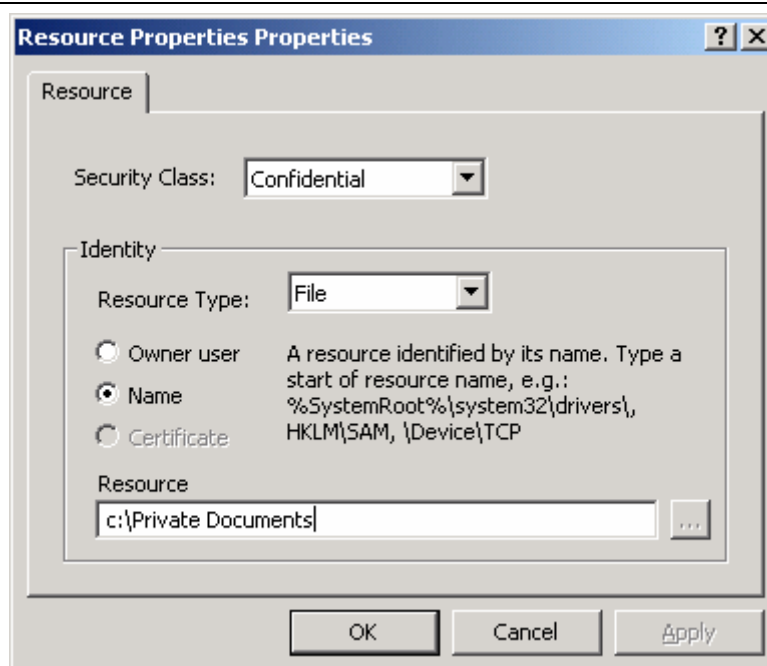
## 4.2. Resources

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 files, 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.

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

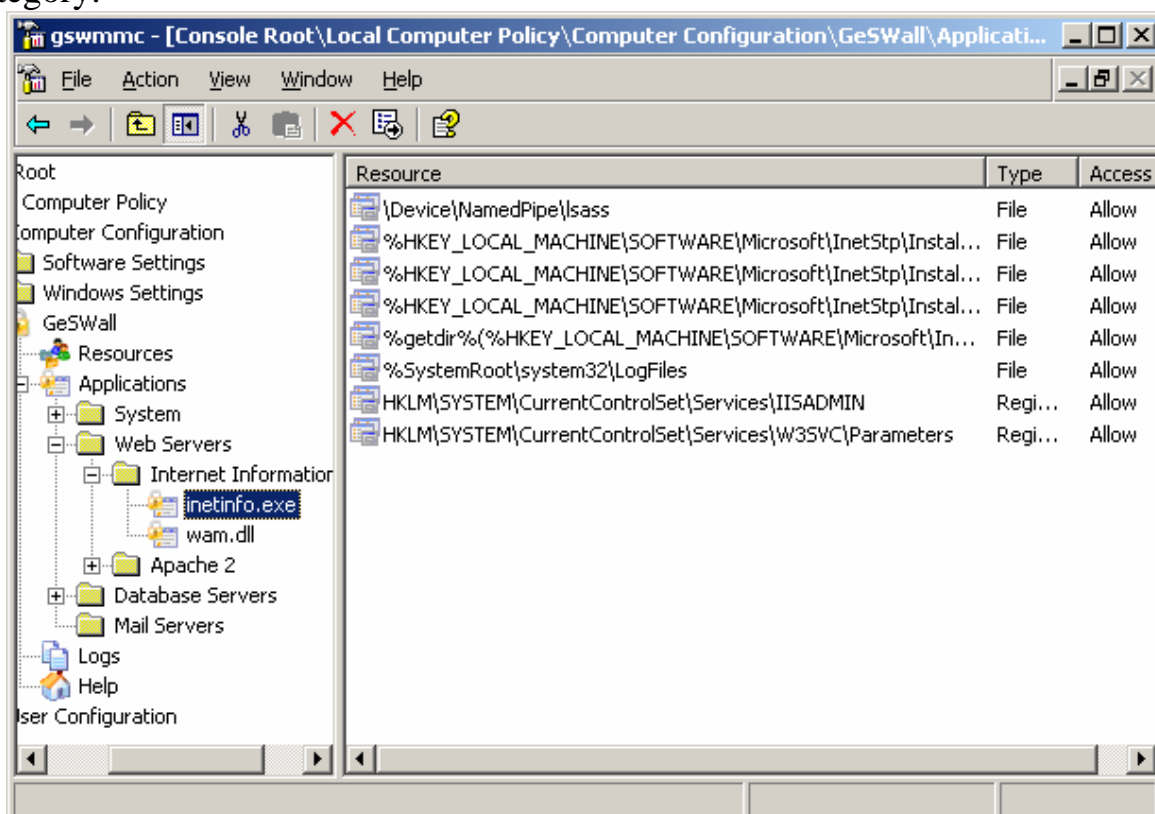
- device – device object exposed by Windows kernel, e.g. \Device\Tcp (exposed by tcpip.sys driver to implement tcp networking), \Device\Cdrom (usual name of cdrom drives)
- network – network interfaces
- system object – an object representing particular windows service, e.g.: SAM\_DOMAIN\%MACHINENAME% - represent SAM database interface for given machine
- 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.

### 4.3. Applications

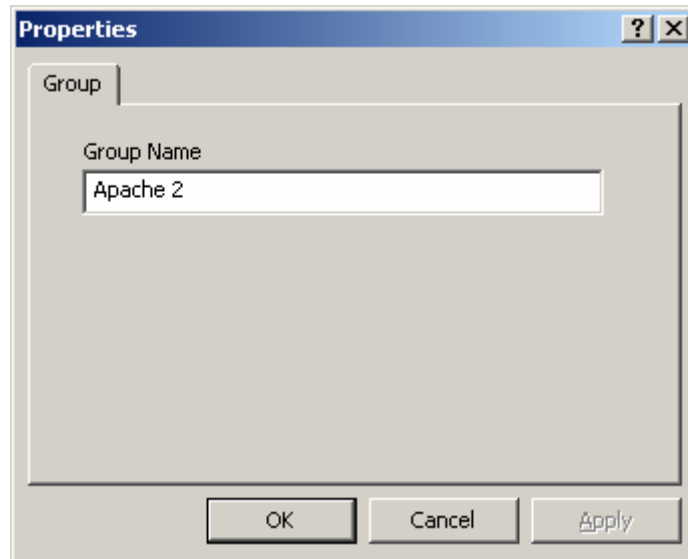
The ‘Applications’ folder contains known application definitions together with specific rules, which comprise the application database. For easy browsing applications are organized into logical groups, according to the application category.



The default application database has the following groups:

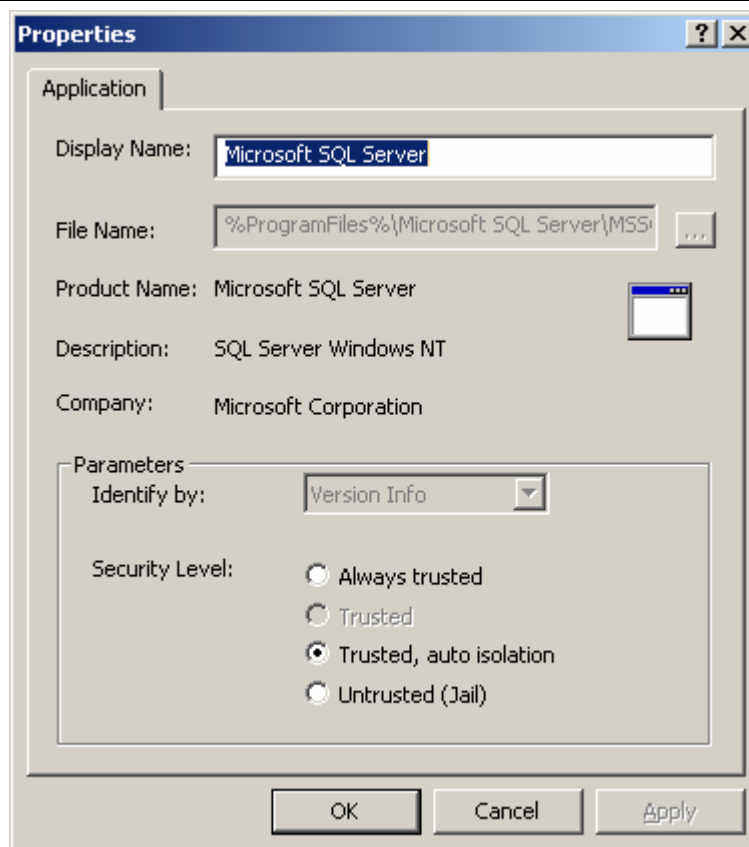
- System – Windows system and GeSWall components
- Web Servers
- Database Servers
- Mail Servers

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, Name or Digest.

**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.

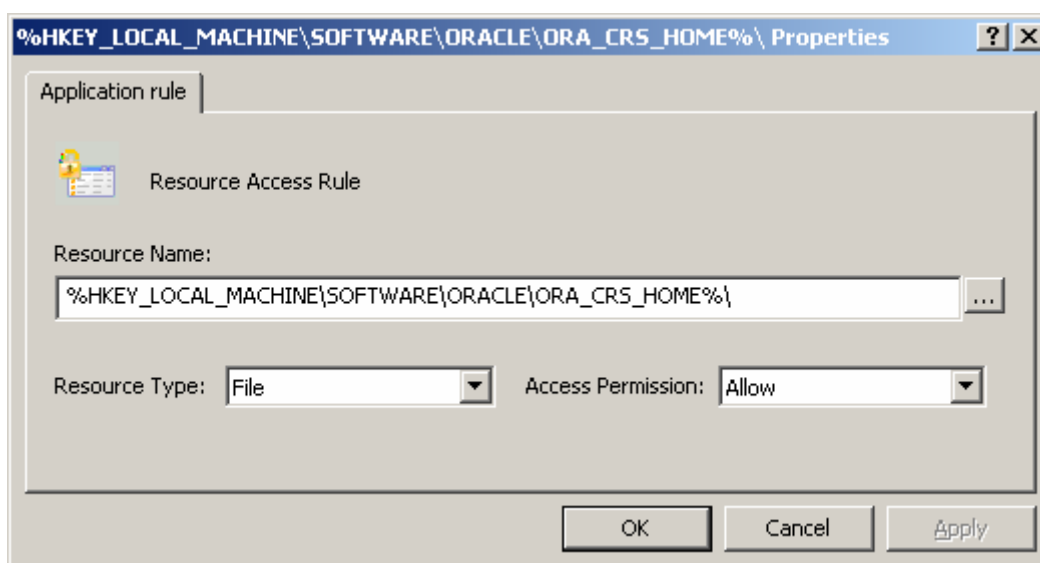
**Digest** is the sha1 hash of an application executable file. Digest might be used to correctly identify a particular application version or certain untrusted applications. Hash is a strongest identification method. Even a single byte change leads to a new digest. However, you may need more effort to support it, as any update of the application requires a new application definition.

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

- Always trusted – 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
- Trusted, auto isolation – the same as Trusted but once it tries to establish a network connection or access untrusted resources it is isolated automatically without a pop-up dialog
- 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.

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.

#### 4.4. 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 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

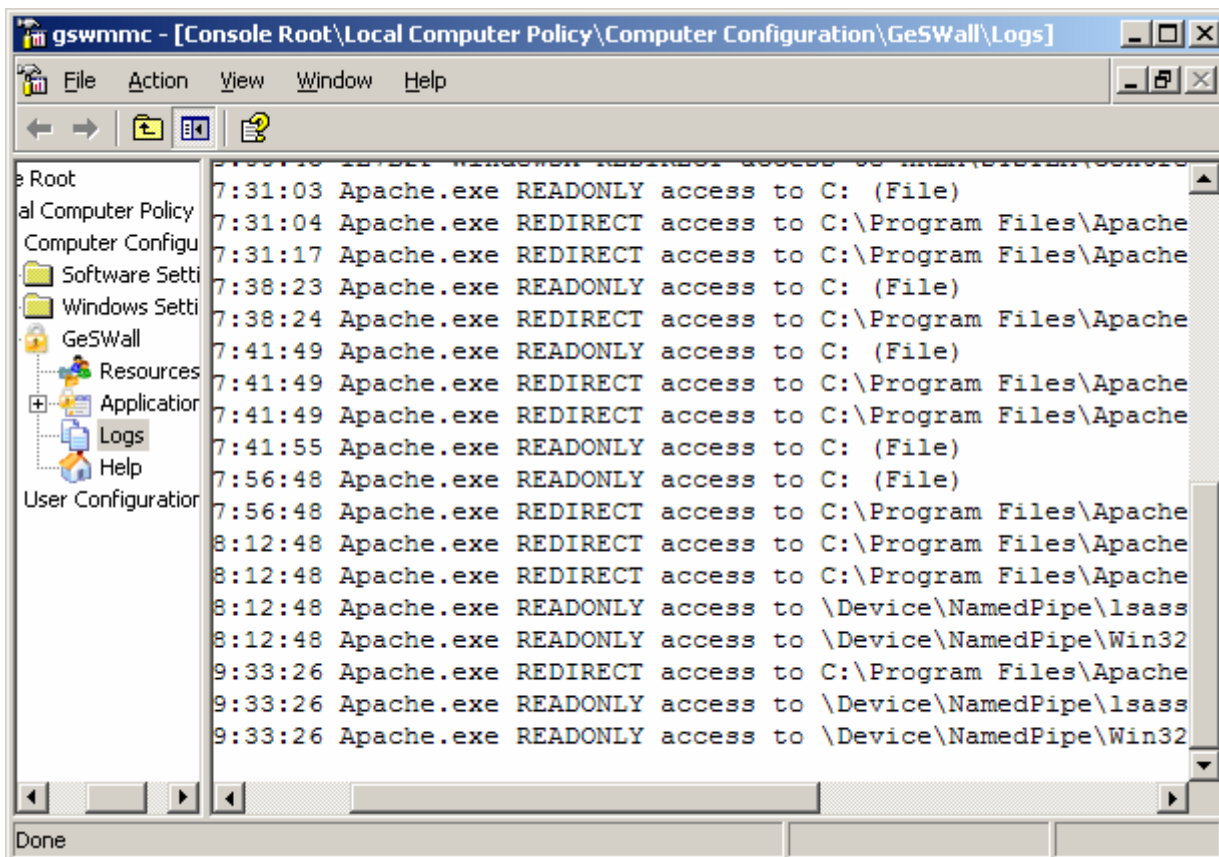
Function to get a long name from parameter's file name, e.g.

`%longname%(c:\PROGRA~1\INTERN~1\ IEXPLORE.EXE)`  
expands to `c:\Program Files\Internet Explorer\IEXPLORE.EXE`

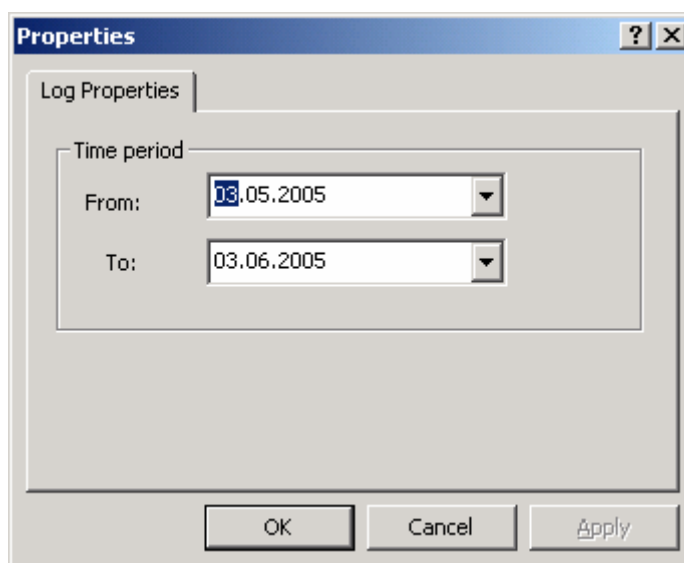
Note, macro-recursion is not supported, so you cannot use one macro-substitution within another one. However, macro-substitution is allowed as a parameter for a macro-substitution function.

## 4.5. 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"> <li>• REDONLY access – access was restricted to read only</li> <li>• REDIRECT access – access was redirected to a local copy</li> <li>• DENY access – access was denied</li> <li>• DENY message – window message sending was denied</li> </ul>
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"> <li>• Debug</li> <li>• Desktop</li> <li>• Device</li> <li>• Directory</li> <li>• Event</li> <li>• File</li> <li>• IO completion port</li> <li>• Job</li> <li>• Registry</li> <li>• Keyed event</li> <li>• LPC port</li> <li>• Mutant</li> <li>• Network</li> <li>• Process</li> <li>• Profile</li> <li>• Section</li> <li>• Semaphore</li> <li>• Symbolic link</li> <li>• System object</li> <li>• Thread</li> <li>• Token</li> <li>• Timer</li> <li>• Waitable port</li> <li>• Windows station</li> </ul>

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.

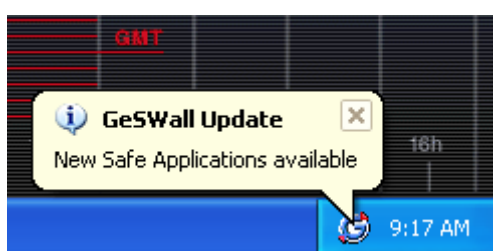
Analyzing logged events for attack traces requires specialized expertise in computer security and GeSWall is not intended to be an intrusion detection product.

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

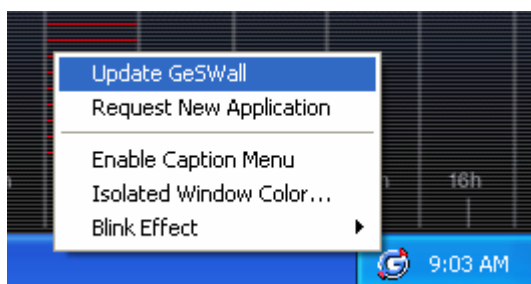
## 5. Application Database Update

GeSWall Server Edition 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 notifies you about it with a tray balloon message, as shown on the picture below.



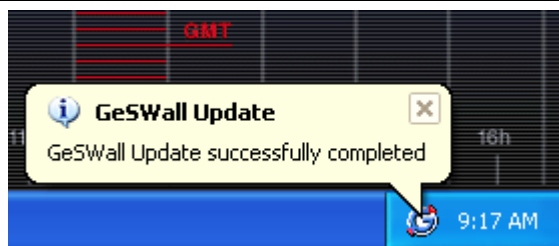
Click on the GeSWall tray icon and choose the 'Update GeSWall' menu item to start an update.



GeSWall downloads an update package from [www.gentlesecurity.com](http://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](http://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.