STORMSHIELD V6.0

ADMINISTRATOR'S GUIDE

STORMSHIELD

https://mystormshield.eu/

TABLE OF CONTENTS

CHAPTER 2: STORMSHIELD INSTALLATION, UPDATES AND UNINSTALLATION

CHAPTER 3: UPDATING STORMSHIELD

CHAPTER 4: SKYRECON MANAGEMENT CONSOLE CONFIGURATION

CHAPTER 5: STORMSHIELD SERVER CONFIGURATION

CHAPTER 6: STORMSHIELD AGENT CONFIGURATION

CHAPTER 7: SIMPLIFIED MANAGEMENT MODE FOR EXTENDEDXP

CHAPTER 8: SYSTEM PROTECTION

CHAPTER 9: RULE-BASED PROTECTION

CHAPTER 15: ANTIVIRUS

CHAPTER 18: LOGS AND ALERTS

CHAPTER 19: TROUBLESHOOTING

LIST OF FIGURES

LIST OF TABLES

PREFACE

THANKS!

Dear Client,

Thank you for choosing the **StormShield** Security Suite from **SkyRecon Systems**.

Our proven, award-winning Security Suite provides consistent, powerful, 360-degree protection, via a single agent installed on user workstations and managed from a central console.

With just a single agent, StormShield allows companies to protect their entire population of desktop and mobile workstations from known or unknown attacks, and theft of critical data, without disrupting user activity.

WHAT IS THE TARGET AUDIENCE?

This documentation is intended for **System Administrators** who will deploy and manage the StormShield solution.

It contains all of the technical information necessary to install and operate the product on your system and network environment.

This technical documentation comes with Release Notes for the version of StormShield that you are using.

All images in this document are for representational purposes only, actual products may differ.

HOW THIS DOCUMENT IS ORGANIZED?

The document is organized as follows:

WRITING CONVENTIONS

FORMATS

Format conventions are described in the table below:

CONVENTION	MEANING
Update/License	Control labels, menu labels, etc.
Update/License	Control labels, menu labels, etc. in **Notes** or **Warnings**.
`notepad.exe`	File names, path names, etc.
`notepad.exe`	File names, path names, etc. in **Notes** or **Warnings**.
"Packs", page 39	Hypertext links.
"Packs", page 39	Hypertext links in **Notes** or **Warnings**.

Table 1.1: Writing conventions

ICONS

Icons are described in the table below:

Note — Valuable information or Tip

Warning — Critical information

CONTACT

Should you need further information on our products or professional services, do not hesitate to:

- call us at **+33 (0)9 69 32 96 29**.
- on our client area https://mystormshield.eu/.

Chapitre 1

STORMSHIELD OVERVIEW

ABOUT THIS CHAPTER

This chapter provides a general introduction to StormShield. It presents a summary of the product:

- Added value of StormShield :
  - Concept 1: Integrated security.
  - Concept 2: Proactive protection.
  - Concept 3: Adaptive control.
  - Concept 4: Flexible policy control.
  - Concept 5: Information feedback.
  - Concept 6: Data encryption.
  - Concept 7: ExtendedXP simplified management mode

- StormShield protection mechanisms :
  - Rule-based protection.
  - Automatic protections.
  - Profile-based protection.

- StormShield architecture :
  - Concepts :
    - Inter-component communication.
    - Workstation protection workstation.
    - Scalability and high availability.
  - StormShield components :
    - StormShield server.
    - SQL database.
    - SkyRecon management console..
    - StormShield agent.

- Packages, option and licenses :
  - Packages :
    - StormShield Professional Edition.
    - StormShield Secure Edition.
    - StormShield Server-Side Edition..
  - AVP option (AntiVirus Protection).
  - Licenses :
    - Updating your license.
    - Applying a license to an environment.
    - Information on licenses.

ADDED VALUE OF STORMSHIELD

In an ever more interconnected world, IT organizations have to introduce ever more complex security measures to face threats.

At present, there are few really satisfactory security solutions implemented on workstations. Security service providers mostly offer specialized solutions (hard disk encryption, antivirus, personal firewall).

Let us consider the examples of a firewall and an antivirus software which prove to be highly efficient against external threats. Their value, though, is limited when you install them on laptops located outside of your company's defense perimeter. Security flaws can also be exploited when network analysis and filtering fail to identify or counter threats.

SkyRecon Systems' approach encompasses seven basic concepts to make up for these deficencies.

CONCEPT 1: INTEGRATED SECURITY

This concept provides, all through a **single** agent, consistent security policies that encompass:

- Users.
- System-level security.
- Data protection.
- Network connectivity.

CONCEPT 2: PROACTIVE PROTECTION

This concept provides security policies relying on intelligent behavior-based (**unknown** threats) and signature-based (**known** threats) technologies. This eliminates the need for IT teams to periodically check and update PCs for compliance and remove unauthorized applications.

Unfortunately, new types of attacks are launched every day. Security measures based on signatures which must know what the threat is before its identification and prevention, no longer provide sufficient protection against new variants of viruses or against the spread of new malicious software.

Besides, antivirus software is unable to block an attack targeted at a specific organization. These programmed stealth attacks never lead to a signature being issued since antivirus solution vendors remain unaware of them.

Should a virus succeed in installing itself on a workstation, its operation will be neutralized by StormShield until the time when an antivirus signature becomes available to completely clean the workstation.

CONCEPT 3: ADAPTIVE CONTROL

This concept offers security and user control policies that change dynamically depending on the level of risk associated with the use of the endpoint (workstation, laptop, PDA, etc.) or the **environment** (WiFi).

For example, applications installed directly by users for personal use may present both a security threat and a source of lost productivity. StormShield provides the tools to apply different levels of control over how any individual or group may use their workstations.

CONCEPT 4: FLEXIBLE POLICY CONTROL

This concept gives IT the ability to secure endpoints through both quickly deployed **automatic protections** built into the security suite and fine-grained, customizable **configurations** that address your organization's specific security and policy requirements.

CONCEPT 5: INFORMATION FEEDBACK

StormShield provides a wide range of information on dangerous or suspect operations affecting the client workstation. This information forms an essential complement to the data from the network monitoring systems in the context of overall IT system protection.

CONCEPT 6: DATA ENCRYPTION

To help you protect your systems and data, StormShield provides a combination of **full-disk** encryption before booting and **file** encryption after booting.

Your data is protected at all time, regardless of the workstation user. The encryption policy which is managed from a centralized console, can be applied to:

- Any user.
- Any workstation.
- The whole hard disk.
- Removable devices.
- Specific files/folders.

CONCEPT 7: EXTENDEDXP SIMPLIFIED MANAGEMENT MODE

To specifically protect the Microsoft Windows XP operating system, StormShield provides a simplified management mode to users who have subscribed to the ExtendedXP Service. The administrator can assign an ExtendedXP role to a user of the SkyRecon console. It gives access to an optimized console providing a general and quick overview of the environment and enabling the import of configuration templates delivered with the security advisories from the ExtendedXP Service.

For more information about the ExtendedXP mode, refer to chapter "Simplified management mode for ExtendedXP", page 233.

STORMSHIELD PROTECTION MECHANISMS

OVERVIEW

StormShield includes three protection mechanisms to provide the highest possible level of workstation security:

- Rule-based protection.
- Automatic protections.
- Profile-based protection.

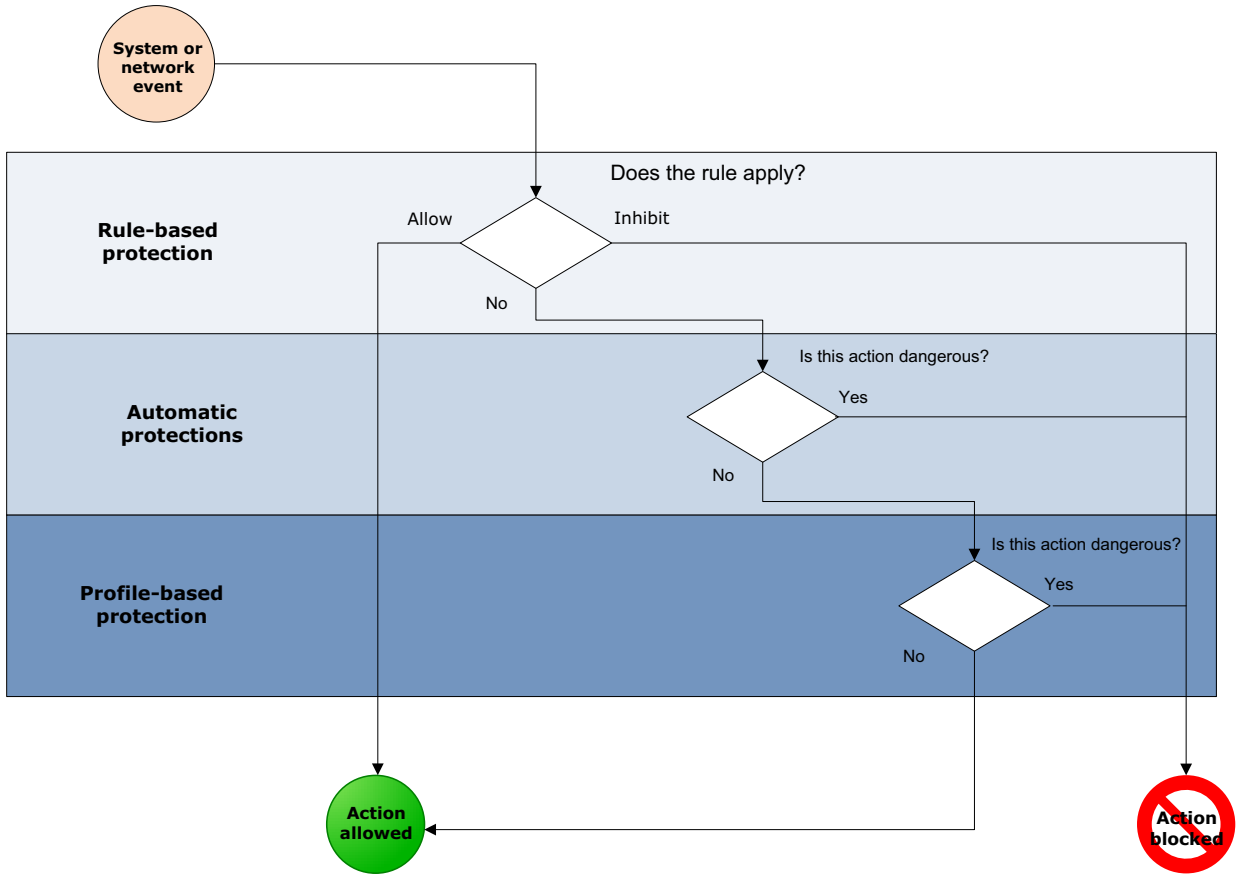


Fig. 1.1 : StormShield protection mechanisms

RULE-BASED PROTECTION

Rule-based protection is used to define and ensure the application of a security policy on points which are considered sensitive by the client. A security policy contains the formal rules set out to allow or ban access to the following:

- Application execution.
- Firewall network rules.
- Resource usage rules (network, files, register base) for each application.
- Usage rights on file types (depending on their extensions).
- Usage rights on mass storage devices.
- Trusted applications (which can override part or all of StormShield restrictions).

An explicit security policy can be applied to different workstation groups.

StormShield is supplied with predefined rules so that policies can be applied immediately by the administrator. These default rules may be modified at any time to adapt policies to company's requirements.

AUTOMATIC PROTECTIONS

Automatic protections are designed to detect and block **known** and **unknown** malicious codes using attack pattern identification instead of code identification.

Automatic protections do not require any configuring by the administrator. The administrator can, however, adjust these mechanisms to specify the level of how StormShield reacts to different events. For more information, see "Configuring automatic protections", page 260.

Two major categories of automatic protection mechanisms are built into StormShield:

- The first category covers application and system activities.

  This serves to protect the workstation against attempts to corrupt executable files and access sensitive system services or data.

- The second category comprises an Intrusion Detection System (IDS) so that the workstation can protect itself from attacks from the network.

  The mechanisms applied for detecting system or network attacks by the automatic protection system remain active on a permanent basis. StormShield's treatment of these events can be controlled by the administrator. Depending on the type of event that occurs, the system will send an alert or apply automatic counter measures as defined by the administrator.

PROFILE-BASED PROTECTION

Profile-based protection relies on an advanced capacity to monitor the system calls made by each application. During a learning phase, application behavior is monitored.

The learning phase is used to collect essential information on the actions performed while applications are running on your workstation. System calls are memorized to form a standard application profile. After this phase, the actions performed by the application while it is running are compared with its standard profile so as to detect any deviations that may occur. StormShield's exclusive technology means that these deviations can be handled intelligently by correlating and weighing them.

StormShield will detect any application behavior departing from its standard profile and will react according to the parameters set by the administrator.

Profile-based protection therefore constitutes a third line of defense that is especially suited to targeted attacks and to new high speed worms. Any attempted attacks based on corrupting applications or operating system services will be blocked, even if no signature or other mechanism is available for defending the system against them.

STORMSHIELD ARCHITECTURE

StormShield is a distributed protection system that covers all of the workstations belonging to an organization.
Its architecture is based on a multi-tier model and on deployment techniques that allow it to be quickly integrated into the organization's network.

CONCEPTS

Inter-component communication

Communications between all components are authenticated and encrypted using TLS and X509 v3 certificates. Mutual authentication is used between every component to reinforce solution security.

Workstation protection

Protection on each workstation is handled by a software module called **StormShield agent**.

The agent communicates with the deployment server, whose role is to distribute security policies to each agent and collect data concerning workstation security from them.

This data is stored by the server in a dedicated database which can also be accessed by the management console (*SkyRecon management console*).

Scalability and high availability

StormShield responds to the scalability and high availability requirements of the most demanding business environments.
High availability is based on load balancing and failover mechanisms, distributed over a number of deployment servers.

The StormShield agent requires at least one deployment server, called **master server**. Slave servers can be added to the master server.
The master server is the only server which communicates directly with the SkyRecon management console.
The master server shares the "Agent Groups" description and security policies with the slave servers.

StormShield components

StormShield is made up of the following components:

- StormShield server.
- SQL database.
- The SkyRecon management console.
- StormShield agents.

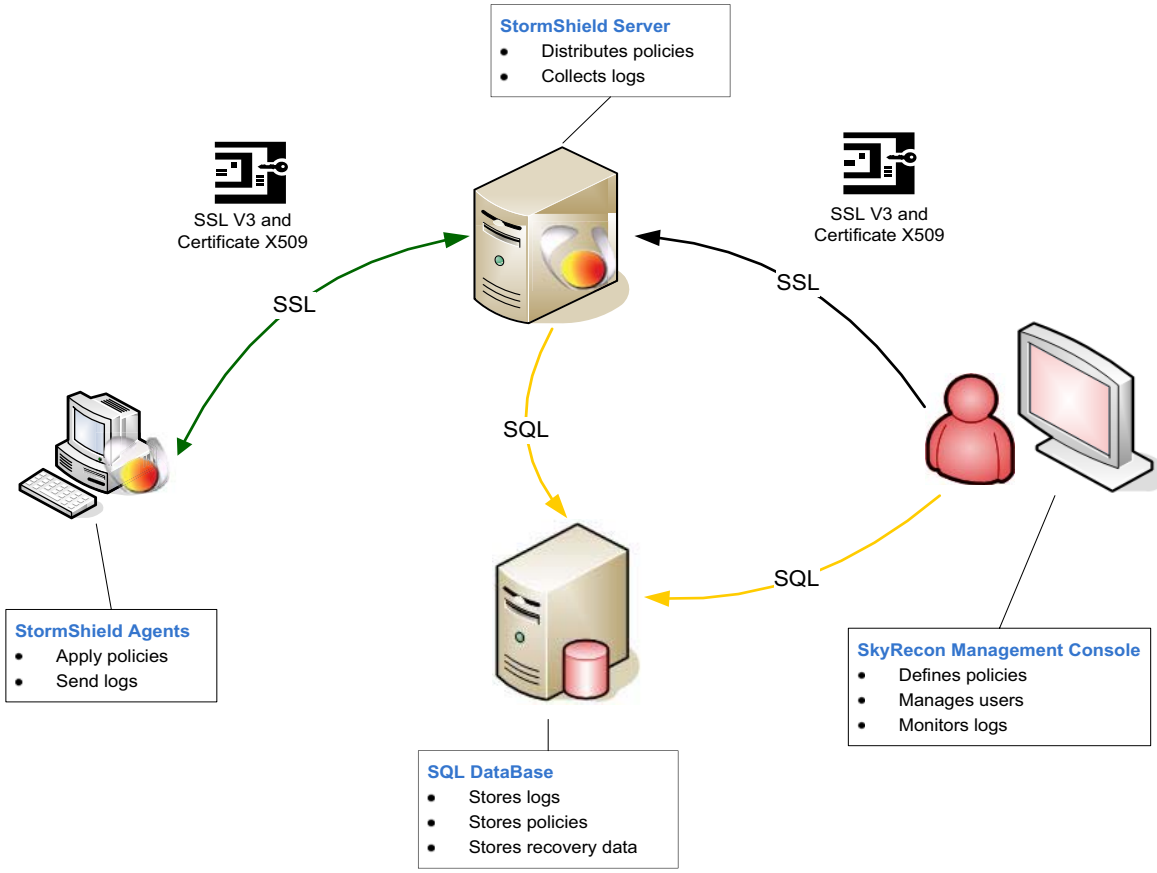


Fig. 1.2 : StormShield architecture

StormShield server

Master

The server is used to distribute security policies and collect logs.

The StormShield agent requires at least one deployment server, called master server.
There must be one master server at each geographical site.

Slave servers are optional. They can be used as failover backups and for load distribution.

Slave Servers

Slave servers can be added to the master server. The master server shares the "Agent Groups" description and security policies with the slave servers.

The SkyRecon management console communicates with all available servers. If a server is down when the console sends a configuration, the server will update its configuration from another server when it is back online.

Server load balancing

In the Configuration Editor, you can define a list of servers (master and slave) to share the load. You can also prioritize the servers.

Each time a configuration is deployed, the agents receive the addresses of the master server and slave servers that they are allowed to access, and the order in which to access them. When an agent attempts to connect to a server to determine whether a new configuration is available, it connects by default to the last server that it was connected to. If this server is overloaded, a message is sent to the agent requesting that it connects to another server.

The list of servers is used to define a priority based on agent geography.

Failover to slave server

If the master server is not available, the next available slave server in the prioritized list automatically takes over the role of the master server. The agents then communicate with the new master server and the administrator is notified of this change of roles.

When the original server is operational again, it automatically resumes its master function and the server that temporarily performed this function returns to its slave role.

SQL database

The SQL database is used to store the following data and information:

- Logs.
- Security policies.
- Recovery data.

A single SQL database can be assigned to several management consoles (if necessary).

SkyRecon management console.

The SkyRecon management console is used to:

- Define security policies.
- Manage users.
- Monitor logs.

The **features** of the SkyRecon management console depend on the StormShield package chosen by your company.

For more information, see "Packages", page 47.

StormShield agent

The agents installed on your workstations are used to apply security policies and send logs to the StormShield server.

PACKAGES, OPTION AND LICENSES

PACKAGES

StormShield is available in **three packages**, each offering features adapted to your needs:

- StormShield Professional Edition.
- StormShield Secure Edition.
- StormShield Server-Side Edition.

The StormShield packages exist in the following versions:

STORMSHIELD PACKAGES	32-bit version	64-bit version
Professional Edition	✓	✓
Secure Edition	✓	✓
Server-Side Edition	✓	✓
Antivirus option	✓	✓

Tableau 1.1 : StormShield versions

Each package requires a license. This license applies to a specific environment.

The Tableau 1.2, “StormShield packages and their features”, page 48 shows the features offered by each package.

STORMSHIELD FEATURES	Professional Edition (32 bits)	Professional Edition (64 bits)	Secure Edition (32 bits)	Secure Edition (64 bits)	Server-Side Edition
Security Policies					
• General Settings:					
◦ System Behavior Control	✓	✓	✓	✓	✓
◦ Process Behavior Control	✓	✓	✓	✓	✓
◦ Device Control	✓	✓	✓	✓	✓
◦ WiFi Encryption and Authentication	✓	✓	✓	✓	✓
◦ Network Activity Control	✓	✓	✓	✓	✓
• Network Firewall	✓	✓	✓	✓	✓
• Applicative rules	✓	✓	✓	✓	✓
• Extension rules	✓	✓	✓	✓	✓
• Kernel Components	✓	✗	✓	✗	✗
• Trusted rules	✓	✓	✓	✓	✓
• WiFi Access Points	✓	✓	✓	✓	✓
• Removable Devices	✓	✓	✓	✓	✓
Configurations					
• Agent Configuration	✓	✓	✓	✓	✓
• Temporary Web Access	✓	✓	✓	✓	✓
• Learning	✓	✓	✓	✓	✓
• Antivirus Configuration *(optional)*	✓	✓	✓	✓	✓

Tableau 1.2 : StormShield packages and their features (Page 1/2)

STORMSHIELD FEATURES	Professional Edition (32 bits)	Professional Edition (64 bits)	Secure Edition (32 bits)	Secure Edition (64 bits)	Server-Side Edition
Scripts					
• Tests	✓	✓	✓	✓	✓
• Actions	✓	✓	✓	✓	✓
• Batches	✓	✓	✓	✓	✓
Encryption Policies					
• General Settings	✗	✗	✓	✓	✗
• File Encryption Parameters	✗	✗	✓	✗	✗
• Full Disk Encryption Parameters	✗	✗	✓	✓	✗
The AVP option is available for all StormShield packages					

Tableau 1.2 : StormShield packages and their features (Page 2/2)

If you click on a hypertext link, use the key combination <**Alt+Left Arrow**> to go back to the start point.

StormShield Professional Edition

The Professional Edition package includes three features:

- Security policies.
- Configurations.
- Scripts.

"Security policies" feature

This feature enables the administrator to apply specific controls to the StormShield agents (via the server).

"Configurations" feature

This feature enables the administrator to apply policies and configurations that change dynamically.

"Scripts" feature

This feature enables the administrator to write customized scripts in order to define conditions under which policies and configurations are applied.

StormShield Secure Edition

The Secure Edition package includes the three Professional Edition features as well as the "Encryption Policies" feature.

"Encryption policies" feature

This additional feature enables the administrator to create encryption policies for hard disks and files.

StormShield Server-Side Edition.

The StormShield Server-Side Edition package is meant for servers running on these operation systems:

- Windows Server 2003 R2 32 bits
- Windows Server 2008 SP2 32 bits
- Windows Server 2008 R2 64 bits

The StormShield server and the StormShield agent cannot be installed on the same workstation.

The Server-Side Edition package includes the 64-bit Professional Edition'sfeatures.

The Server-Side Edition package is not compatible with the **Server Core** installation option in Windows Server 2008 R2.

For more information, see Tableau 1.2, “StormShield packages and their features”, page 48.

AVP OPTION

The AntiVirus Protection (AVP) option is available for each package.

The AVP option scans:

- Any driver on your workstation.
- Internet access to block unauthorized downloads.
- Incoming/outgoing emails.
- Modified files on your workstation or on the network.

Here is the detailed **Antivirus Policies** option on the SkyRecon management console:

- **General Settings**.
- **Real-Time Protection Parameters**:

  Checks any file modified on the workstation or network, when it is opened.
- **Web Protection Parameters**:

  Scans contents opened with a web browser (javascripts, ActiveX controls, downloads, etc.).
- **Mail Protection Parameters** scans incoming/outgoing emails and their attachments.
- **Scanner Parameters** scans files, boot sectors, etc.
- **Password Parameters**.

LICENSES

Updating your license

A license is dedicated to a specific environment. It can only be applied to this environment.

If you are using a version of StormShield lower than 6.0, you will need to update your license.
Should the updating process fail, a message will be displayed on your screen.

The new license file shows the total number of licenses and the number of licenses per option.

Examples:

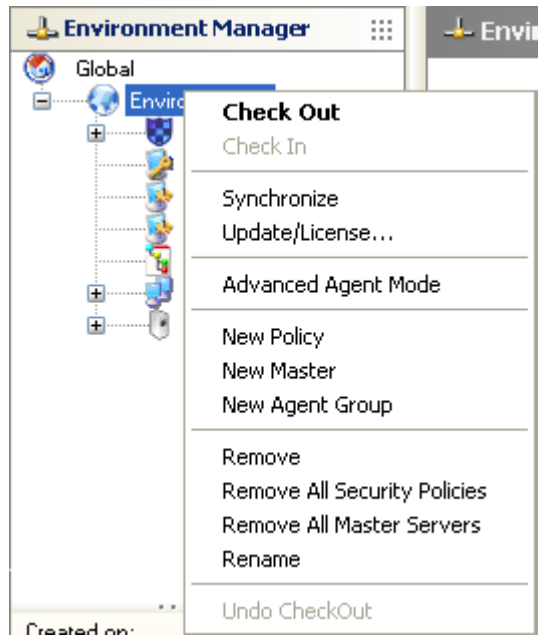
You have purchased a **StormShield Secure Edition** license for 20 workstations coming with the antivirus option.

You have purchased a **StormShield Server-Side Edition** license for 1000 workstations coming with the antivirus option

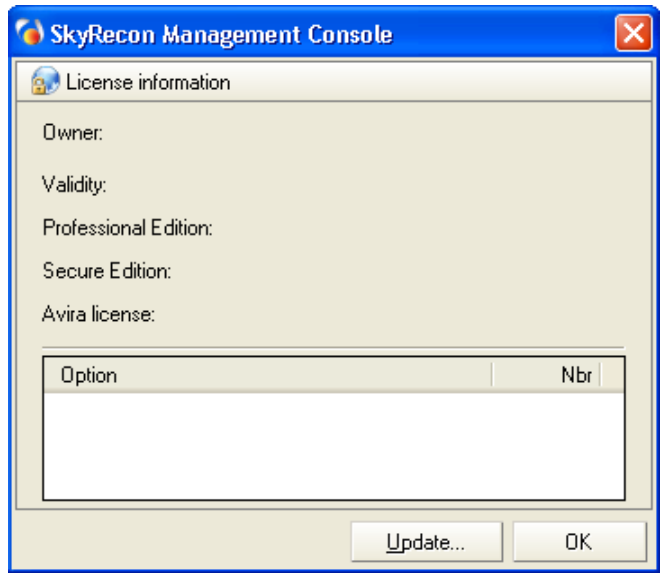
Applying a license to an environment

To update and apply a license to an environment, follow the steps below:

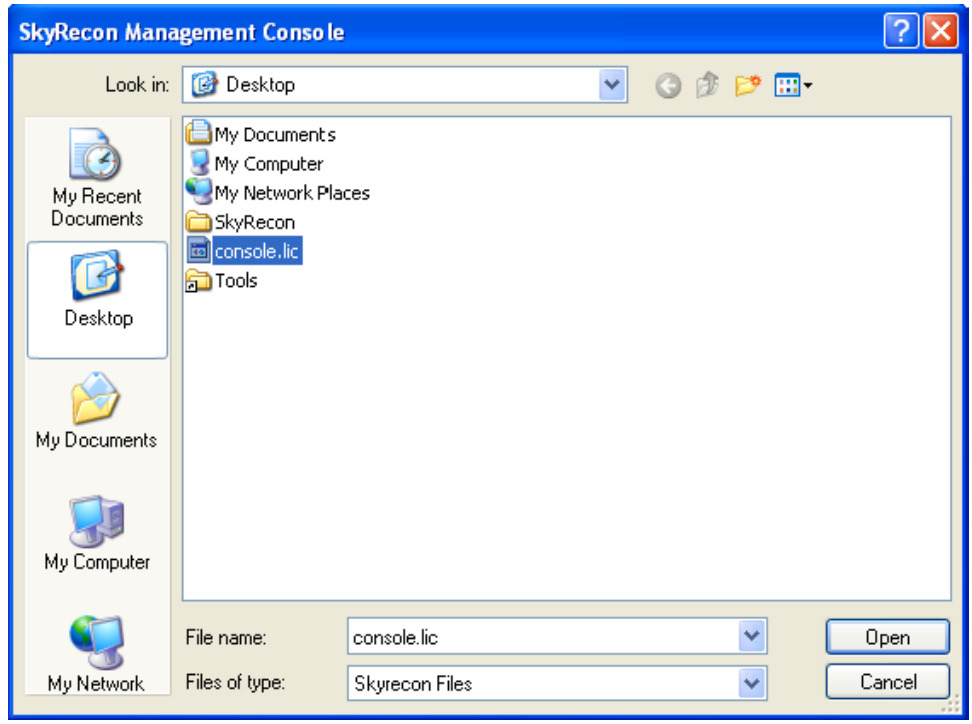
1. Right-click the environment and select **Update/License** from the menu.



2. To update the StormShield license, select **Update**.

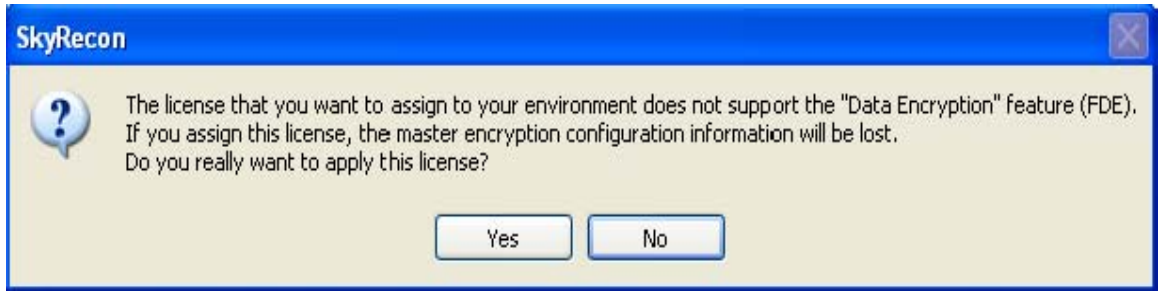


3. Select the StormShield license and click **Open**.
   If you have not purchased the antivirus option, go directly to Step 6.

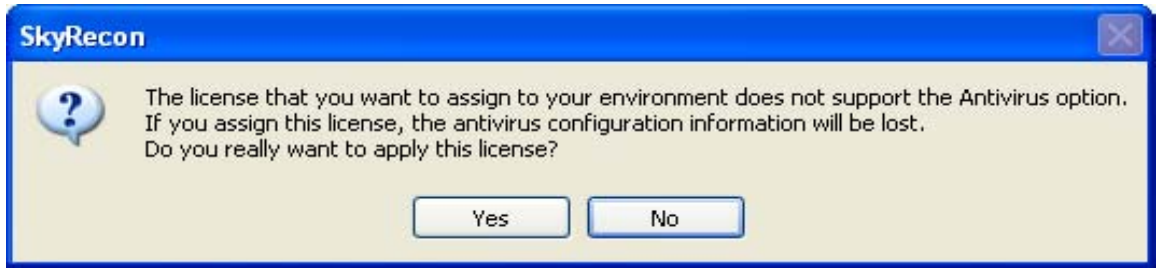


If the updated license **lacks features** supported by the old license, StormShield will warn you that you may lose information.
If you click **Yes**, information will indeed be lost.

Example 1: Applying a license that loses the encryption feature.

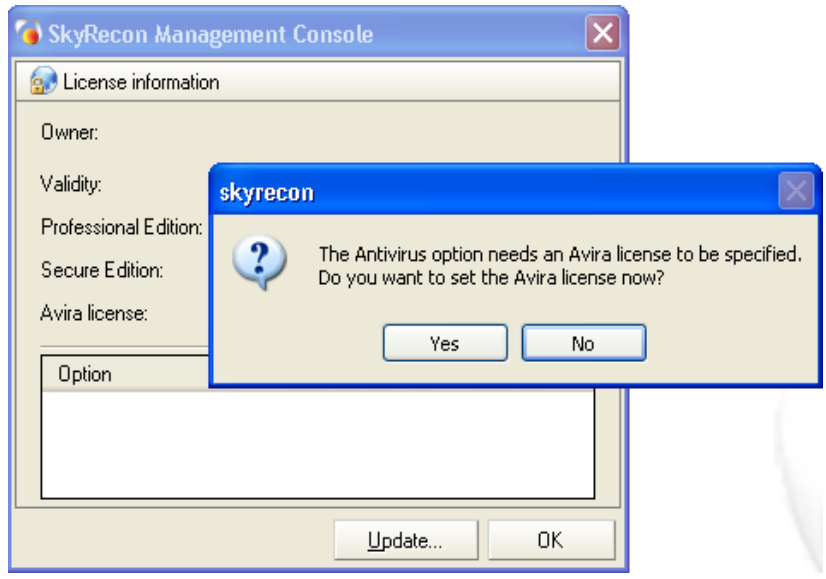


Example 2: Applying a license that loses the antivirus protection option.

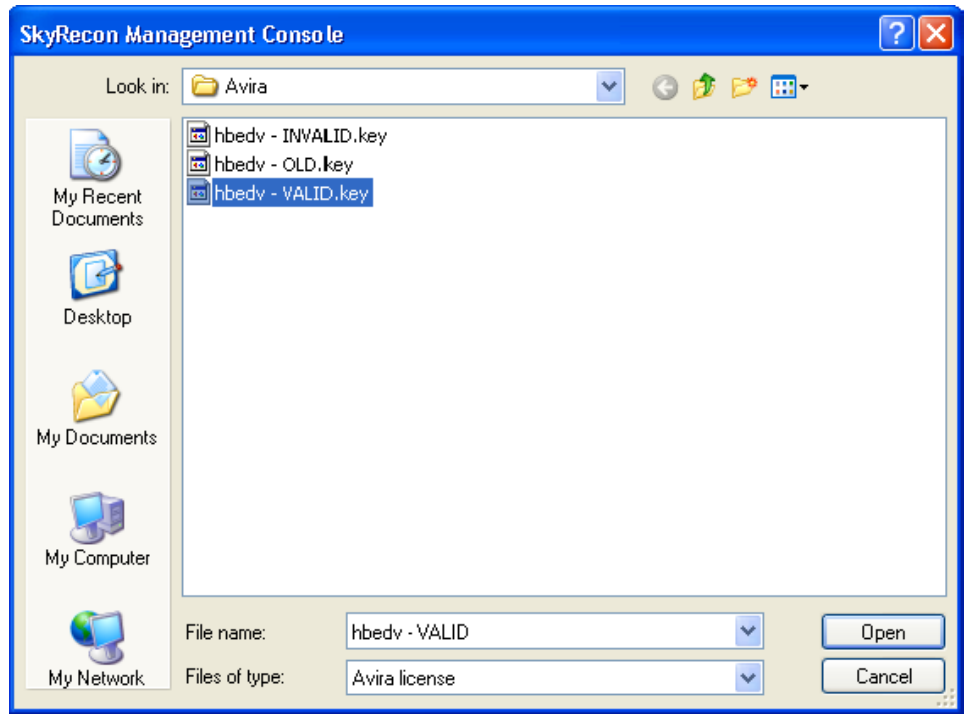


If you have a **limited license for evaluation purposes**, you will have a demo version of the SkyRecon management console. An expiry date is displayed on the lower panel if you click the environment you created previously.

4. To update the Avira license, click **Yes**.



5. Select the Avira license and click **Open**.

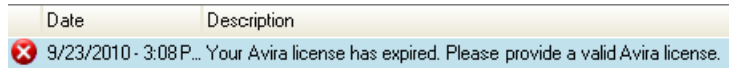


The following window is displayed.

6. Click **OK** to complete the update.

If the Avira license is no longer valid or has expired, a message is displayed at the bottom of the SkyRecon management console.

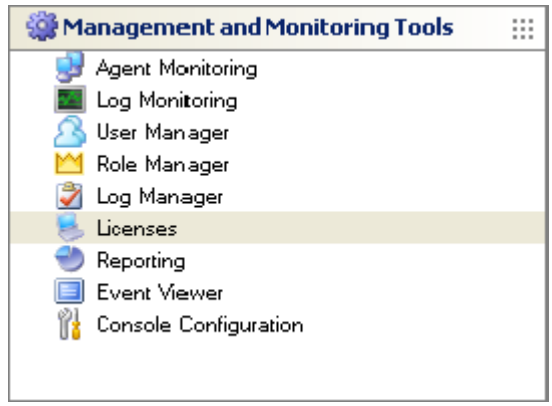
Example:



Information on licenses

To obtain information on your licenses, follow the steps below:

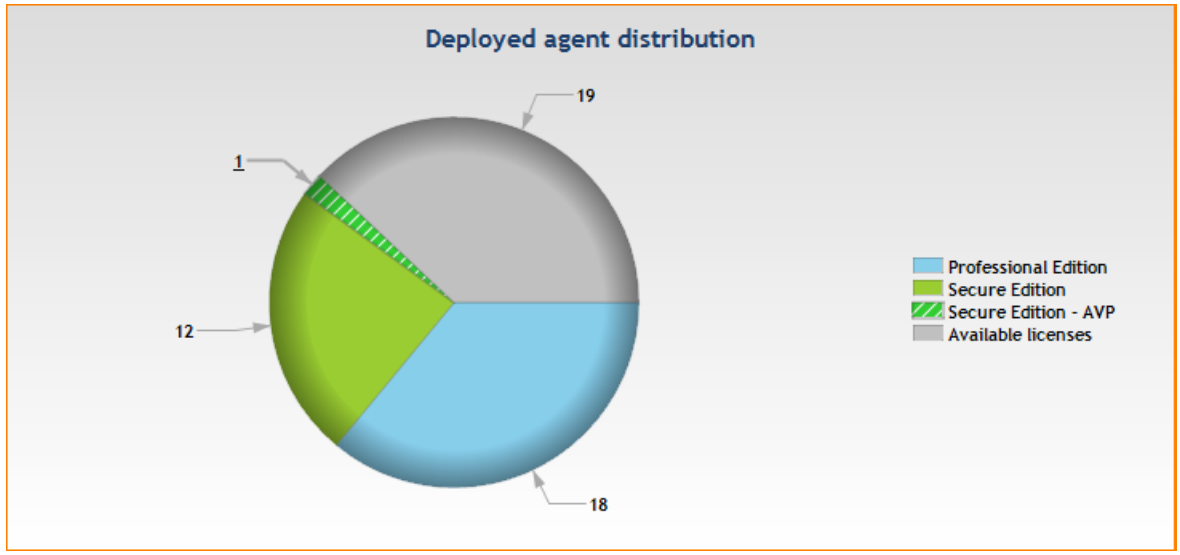
1. Click **Licenses** in the **Management and Monitoring Tools** panel.



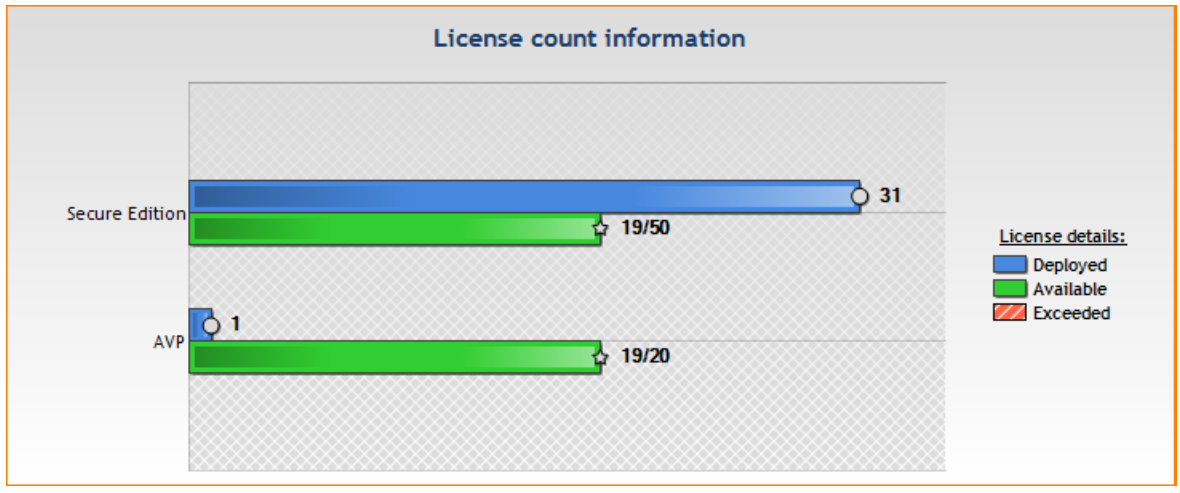
A report is displayed showing:

- The **Date** of the license report.

- The **Deployed agent distribution** and the number of licenses which are still available.



- **License count information** (including and not including the AVP option):
  - Deployed.
  - Available.
  - Exceeded.



2. Use the scroll down bar to display all information.
3. If you want to save the license report, click the icon .
   The report is saved to the location specified, in the `.png` format.

Chapitre 2

STORMSHIELD INSTALLATION, UPDATES AND UNINSTALLATION

ABOUT THIS CHAPTER

This chapter describes the following:

- System prerequisites for StormShield under Windows :
  - StormShield server prerequisites.
  - StormShield database prerequisites :
    - Using an existing database.
    - Using the embedded database.
  - Management console prerequisites.
  - StormShield agent prerequisites.

- StormShield installation :
  - Prerequisites.
  - Settings.
  - Procedure :
    - StormShield installation wizard.
    - Database setup wizard.
    - Environment configuration wizard.
    - Agent deployment wizard.

- Installing StormShield manually :
  - Prerequisites.
  - Procedure :
    - Installing the master server.
    - Installing slave servers.
    - Installing the SkyRecon management console.
    - Installing the StormShield database.
    - Configuring the environment.
    - Installing the agent.

- Downloading certificates :
  - Certificate validity period.
  - Login and password for downloading certificates.
  - Compatibility with system cloning tools.

- Post-installation tests.

- Updating components.

- Possible changes :
  - Changing the StormShield server IP address.
  - Changing the server TCP ports for HTTP and SSL services.

- Uninstalling components :
  - Uninstalling the server and the console.
  - Uninstalling the agent.
  - Removing the databases.

SYSTEM PREREQUISITES FOR STORMSHIELD UNDER WINDOWS

STORMSHIELD SERVER PREREQUISITES

To install and use StormShield Version 6.0 under Windows, you must satisfy the following **Server** environment prerequisites:

- Processor: 1 GHz minimum.
- Memory: 1 GB minimum.
- Hard disk space: 1 GB minimum.
- Hard disk space required for a server with antivirus: 1.5 GB minimum.
- Operating systems:
  - Windows Server 2003 R2 32 bits
  - Windows Server 2003 R2 64 bits
  - Windows Server 2003 SP2 32 bits
  - Windows Server 2003 SP2 64 bits
  - Windows Server 2008 SP2 32 bits
  - Windows Server 2008 R2 64 bits
- Static IP address of the machine where the server is installed.
- Incoming communication (StormShield server):
  - TCP port 16003.
  - TCP port 16005.
  - TCP port 16006.
  - TCP port 16007.
- Outgoing communication (StormShield server):
  - TCP port 16003.
  - TCP port 16006.
  - TCP port 16005.
- Incoming communication (Web server):
  - TCP port 80.
  - TCP port 443.

  You will have to choose other ports if they are already used by a Web server installed on the server machine.

  TCP ports 80 and 443 will be used by the Web server to deploy the agents installed with the server.
- Incoming communication (antivirus server):
  - TCP port 7080.

STORMSHIELD DATABASE PREREQUISITES

To install and use StormShield Version 6.0 under Windows, you must satisfy the following **Database environment** prerequisites:

- Any Windows release compatible with **MS SQL Server 2005**, **MS SQL Server 2008, MS SQL Server 2008 R2** or **MS SQL Server 2012**.
- Communication with the StormShield server and the console:
  - **TCP dynamic port** defined in:

    `SQL Server 2005 Network Configuration > Protocols for [database instance] > TCP/IP > Properties > IP Addresses > IPAll > TCP Dynamic Port.`

    For more information, see "Changing the TCP port for MS SQL Server 2005", page 65.
  - **UDP port** 1434.
- **Hard disk space**: ~ 10 MB for the initialized StormShield database (excluding the SQL engine), and an additional space to be determined depending on the security policies.

  Additional hard disk space is required for the following:
  - Log database: 30 MB per agent for one year.
  - Identification database: 1 MB per agent.
  - Encryption key database: 1 MB per agent.

Use information only as an estimate for disk space requirements. Disk space requirements depend on the security policies implemented and log settings.

MS SQL Server 2005 Express Edition is supplied with StormShield and can be installed directly using the StormShield installation tools.

When installing the database, use the **Mixed Mode** authentication mode.

You must use **Case-Insensitive** collations in MS SQL Server 2005 otherwise the scripts necessary to install the StormShield database will not be supported.

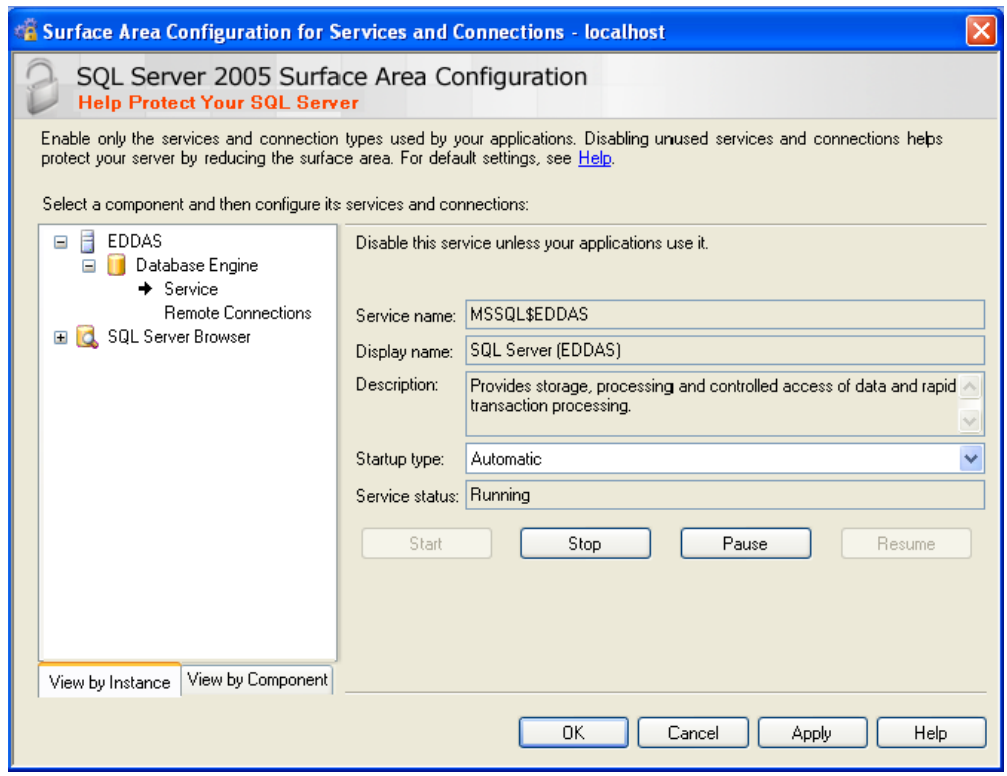
Using an existing database

A mixed (NT and SQL) authentication mode and TCP connectivity are required.

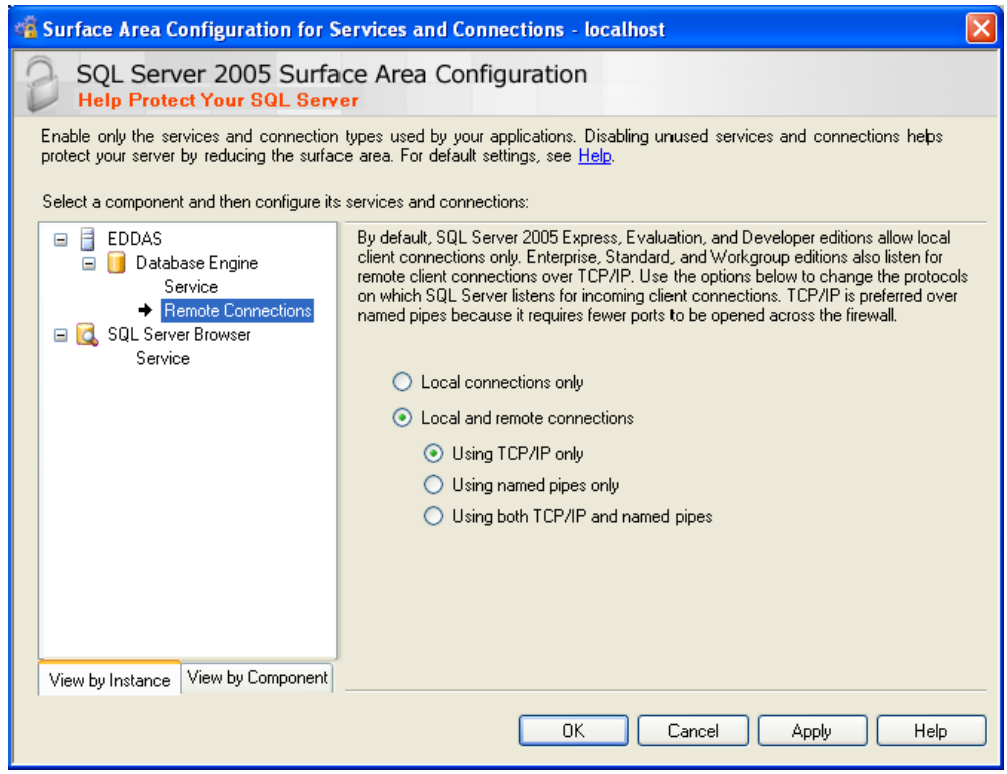
How to change connection parameters to MS SQL Server 2005

To change connection parameters (local or remote access) to MS SQL Server 2005, use **Surface Area Configuration for Services and Connections**. This tool displays information on:

- The SQL Server service (EDDAS):



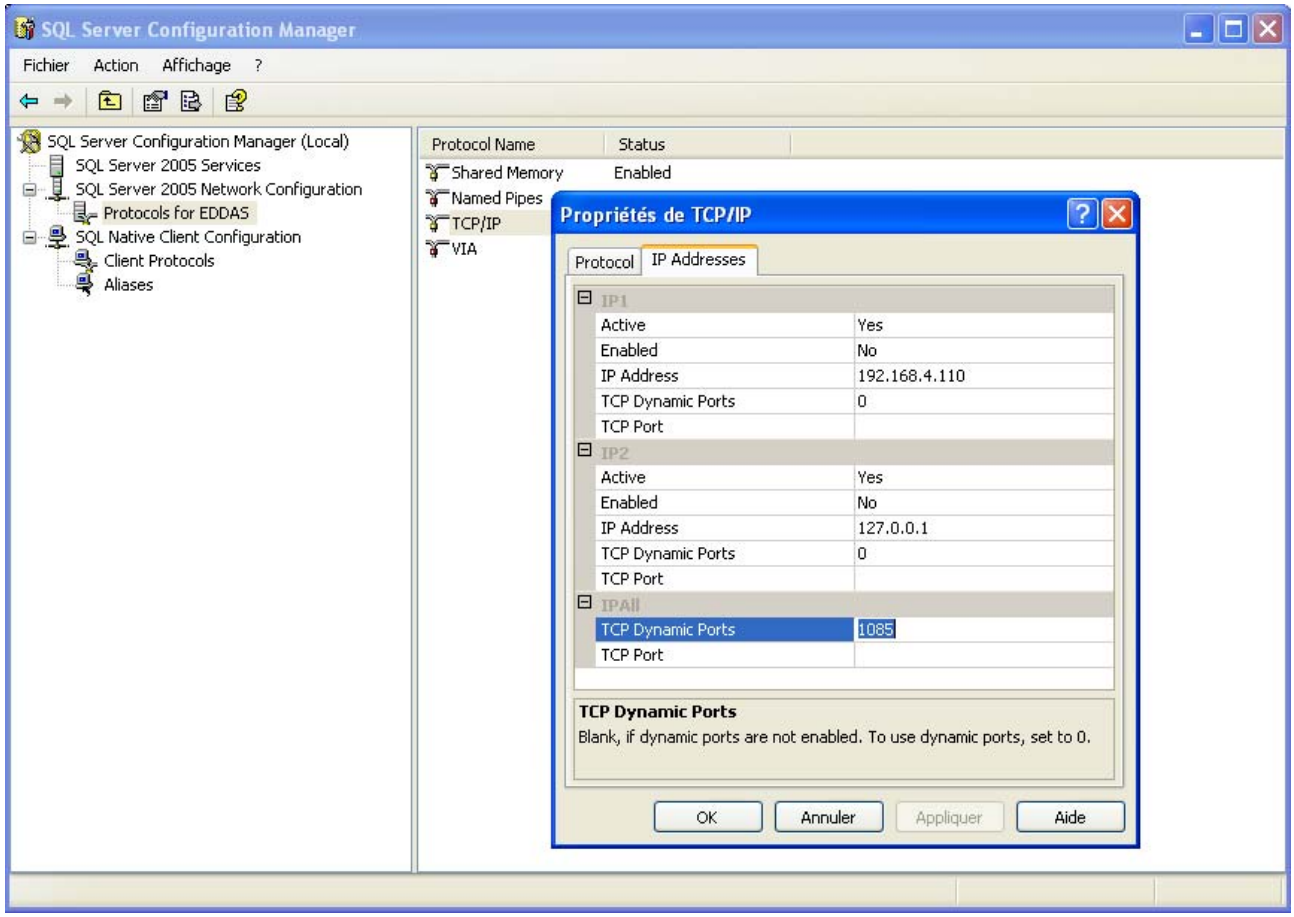
- Local and remote connections:



Changing the TCP port for MS SQL Server 2005

To change the TCP port number assigned to the database instance, use **SQL Server Configuration Manager** in:

```
SQL Server 2005 Network Configuration > Protocols for [database instance] > TCP/IP > Properties > IP Addresses > IPAll > TCP Dynamic Ports
```



Using the embedded database

Check on the target machine that there is no database instance having the same name than the database to be installed (EDDAS). For this purpose, make sure that the list of services in the control panel does not include the **SQL SERVER (EDDAS)** service.

MANAGEMENT CONSOLE PREREQUISITES

To use the management console, you must satisfy the following prerequisites:

- Pentium III: ~800 MHz recommended.
- RAM: 512 MB recommended.
- Hard disk space: 50 MB.
- Operating system:

Operating system	32-bit version	64-bit version
Windows Server 2003 SP1	✓	✓
Windows Server 2003 SP2	✓	✓
Windows Server 2008 SP1	✓	✓
Windows Server 2008 SP2	✓	✓
Windows Vista SP1	✓	✓
Windows Vista SP2	✓	✓
Windows 7	✓	✓

- Framework .Net 2.0.
- Microsoft Visual C++ 2008 Redistributable.
- Static IP address of the machine where the first server is installed.
- IP address or name of the machine where the database is installed.
- Outgoing communication:
  - TCP port 16007.
  - UDP port 1434.
- Password of the database system administrator account.

STORMSHIELD AGENT PREREQUISITES

To use the StormShield agent, you must satisfy the following prerequisites:

- Pentium IV: 3 GHz.
- RAM: 512 MB (minimum), 1 GB (recommended).
- Hard disk space: 25 MB (90 MB with agent logs).
- Hard disk space required for a server with antivirus: 350 MB.

- Operating system:

Operating system	32-bit version	64-bit version
Windows XP SP3	✓	-
Windows Vista SP2	✓	✗
Windows 7	✓	✓
Windows Server 2008 R2	-	✓

- GINA (*Graphical Identification and Authentication*) :

  If your company uses a strong authentication system based on a DLL `gina`, you must install the authentication product before installing StormShield.

  When you need to uninstall the authentication product, first uninstall StormShield. StormShield saves the existing `gina.dll` location upon installation, and will restore it upon uninstallation.

  The remark on the `gina` DLL only applies to **Windows XP** environments.

- Incoming communication:
  - TCP port 16006.
- Outgoing communication:
  - TCP port 16005.
  - TCP port 16006.
  - TCP port 443 (customizable).
  - TCP port 80 (customizable).
  - TCP port 7080.
- Local loop:
  - TCP port 16010.
  - TCP port 16011.
  - TCP port 16012.

STORMSHIELD INSTALLATION

PREREQUISITES

Before installing StormShield, check that the following files/folders are present:

- The **bin** folder including the following files:
  - `server.exe`
  - `console.exe`
- The **resources_x86** (32 bits) or **resources_x64** (64 bits) folder including the following files:
  - `dotnetfx.exe` (Microsoft .Net Framework).
  - `MSXML6.msi` (Microsoft MSXML 6.0 Parser).
  - `SQLEXPR.exe` (Microsoft SQL Server 2005 Express Edition).
  - `SSMSEE.msi` (Advanced Services for Microsoft SQL Server 2005 Express Edition).
  - `vcredist.exe` (Microsoft Visual C++ 2008 Redistributable).
  - `WindowsInstaller.exe` (Microsoft Windows Installer 4.5).
- The `setup.exe` file (StormShield).

SETTINGS

When starting the installation process, you must define the followingsettings:

- Installation Type:
  - Full Install.
  - Simple Install (without wizard).
  - Server Only (additional servers).
  - Console Only (remote console).
  - Custom Install.
- Components:
  - Server.
    - Generate certificates.
  - SQL Server 2005 Express Edition.
    - SQL Server Management Studio Express.
  - Console.

- Administration Tools.
  - Database installation.
  - Console Configuration.
  - Agent deployment.
- Installation Folder.

PROCEDURE

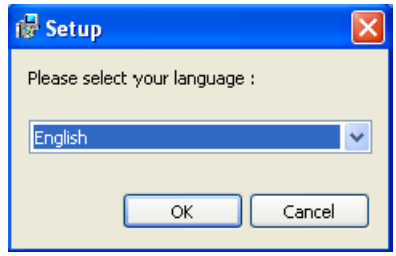
StormShield is installed in **four** stages using the features displayed in the installation tools window:

1. StormShield installation wizard.
2. StormShield database setup wizard.
3. Environment configuration wizard.
4. Agent deployment wizard.

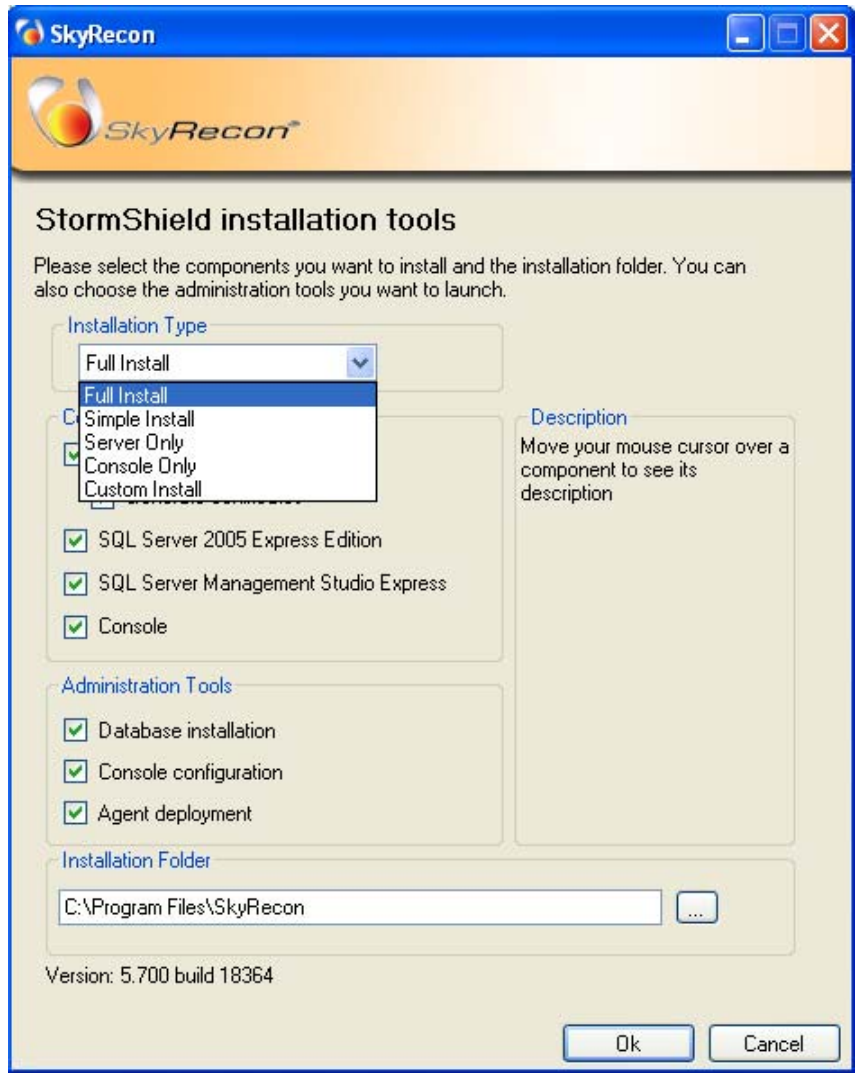
StormShield installation wizard

To install StormShield, follow the steps below:

1. Double-click `setup.exe`.
2. Select a language.



3. Define your settings.

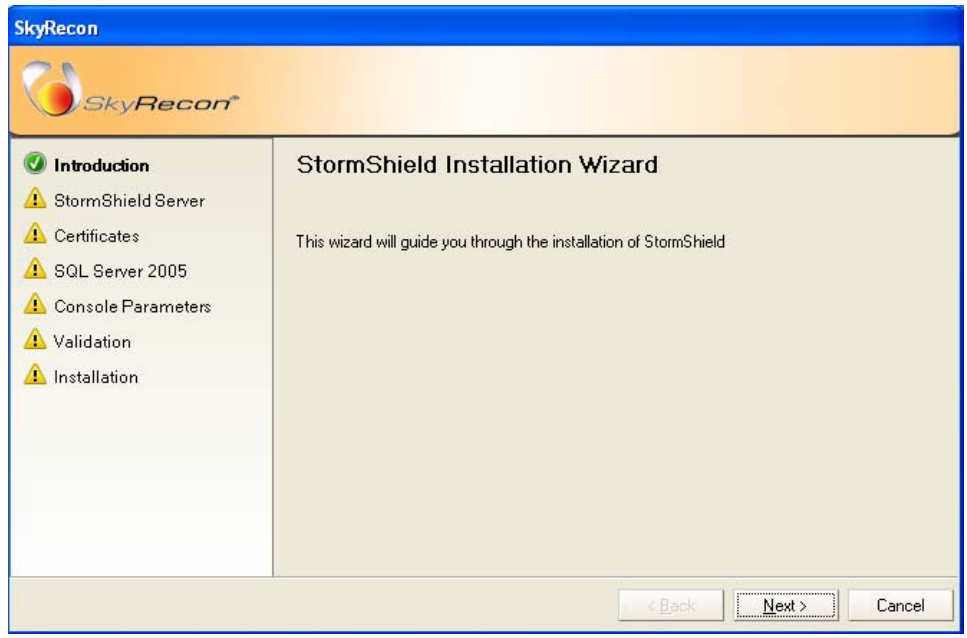


- The **Installation Type** that you wish to launch:
  - Full Install.
  - Simple Install (without wizard).
  - Server Only (slave server).
  - Console Only (remote console).
  - Custom Install.
- The StormShield **Components** that you wish to install (if you choose an installation type other than **Full Install**):
  - The StormShield Server (and its certificate).
  - The SQL server database.
  - The SkyRecon management console.

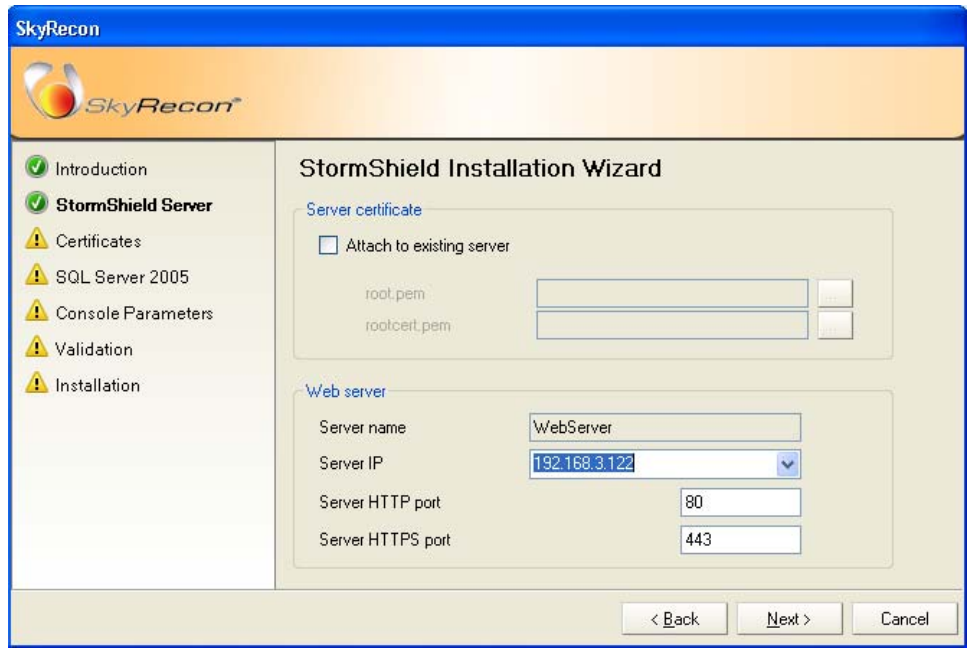
- The **Administration Tools** that you wish to use to install StormShield:
  - Database installation (StormShield database setup wizard).
  - Console configuration (Environment configuration wizard).
  - Agent deployment (Agent deployment wizard).
- The **Installation folder** for StormShield.

Click **OK** to validate your settings.

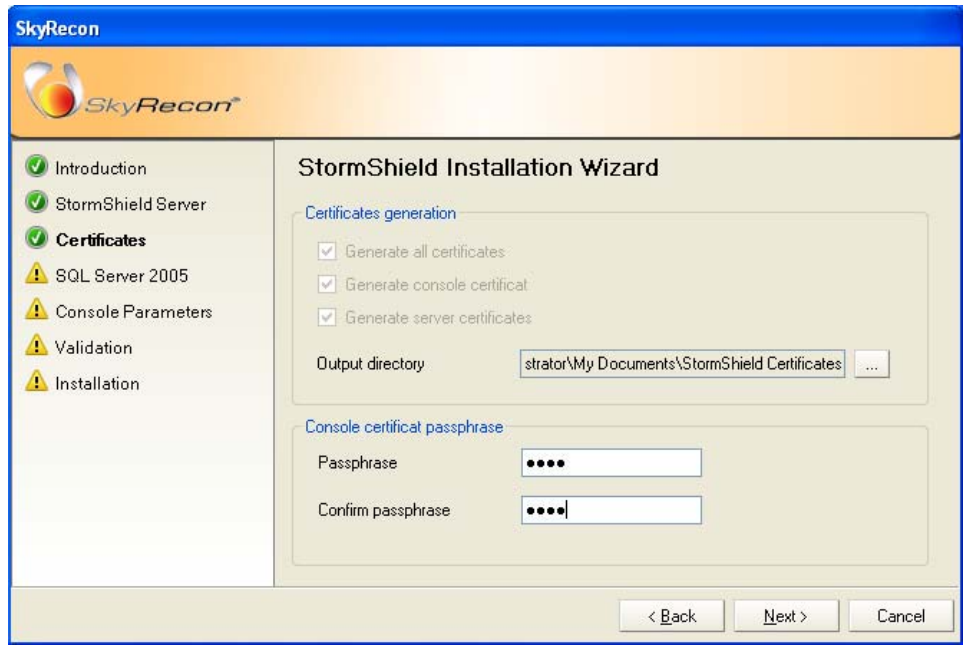
4. To start the StormShield installation procedure, click **Next**.



5. Enter the server IP address and click **Next**.



6. Enter and confirm the new console certificate password.
Click **Next**.

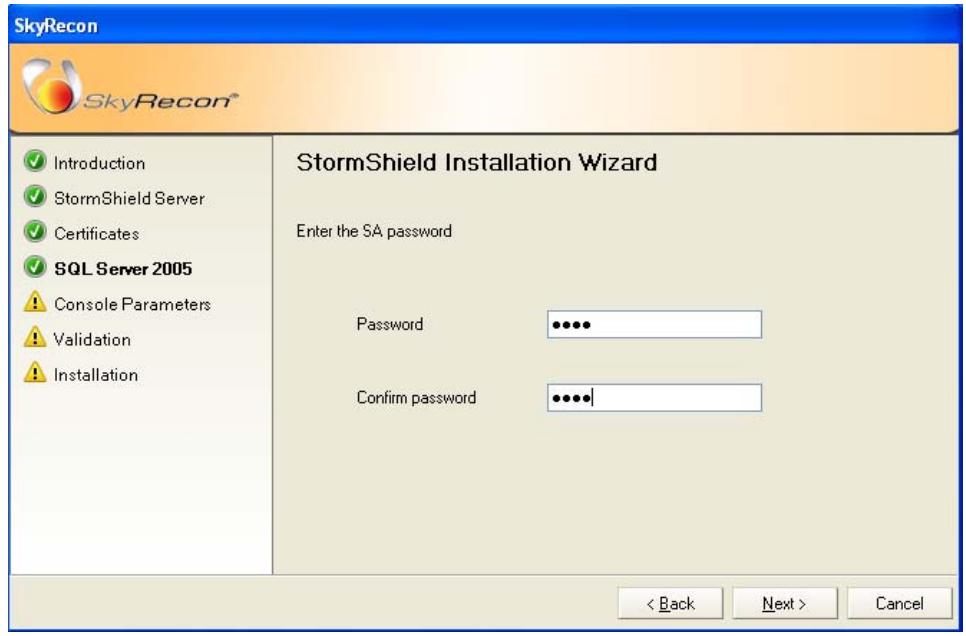


If you have ticked **Server** and **Generate certificates** boxes in the **Components** section (See "Define your settings.", page 70), the

Generate certificates settings in the window above are greyed out and cannot be used.

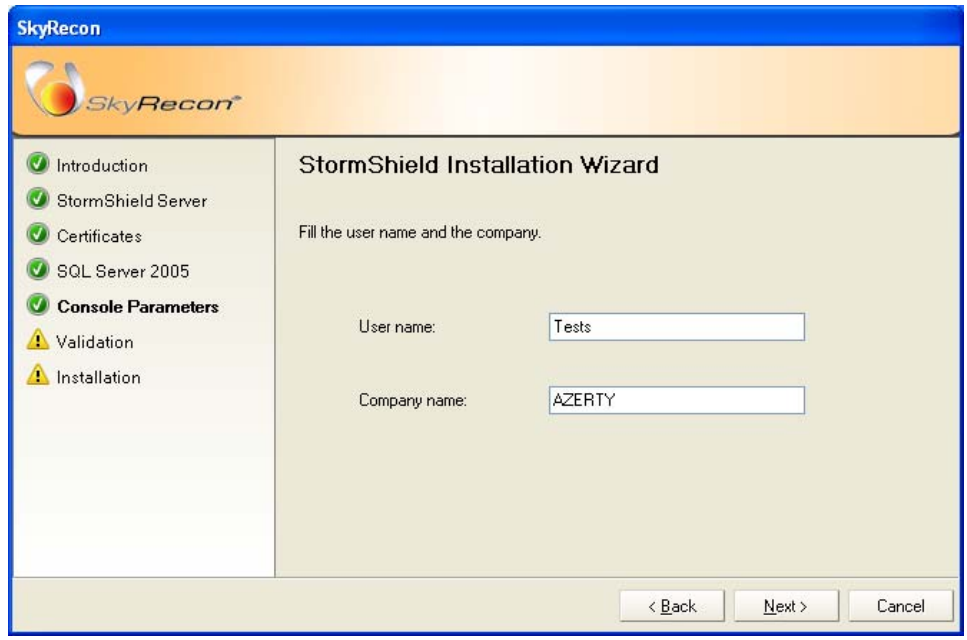
7. Enter and confirm the new SuperAdmin (**sa**) account password for the database server.

   Click **Next**.



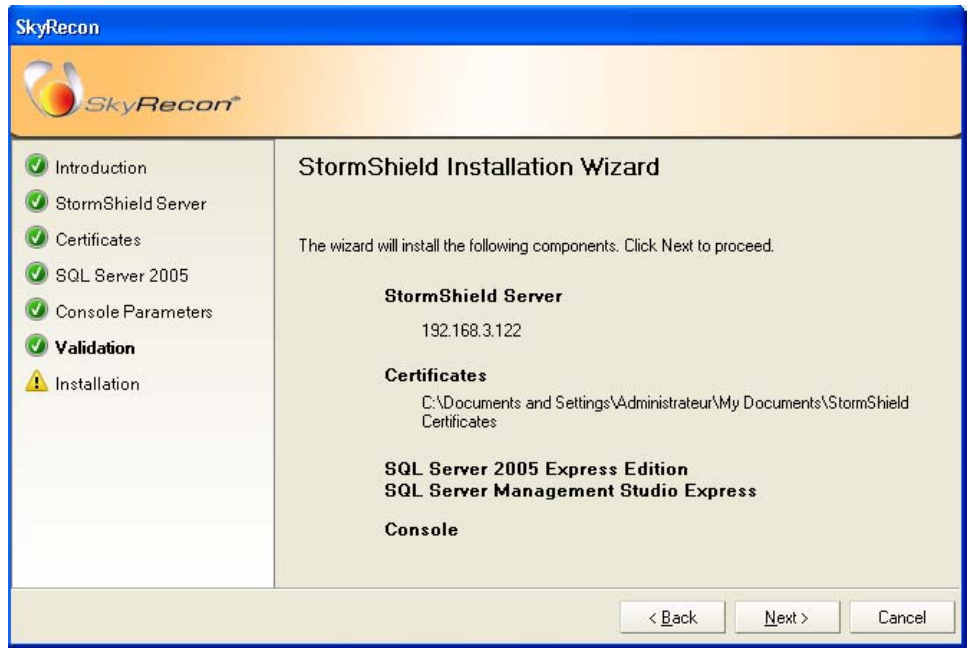
8. Enter your user name and company name.

Click **Next**.

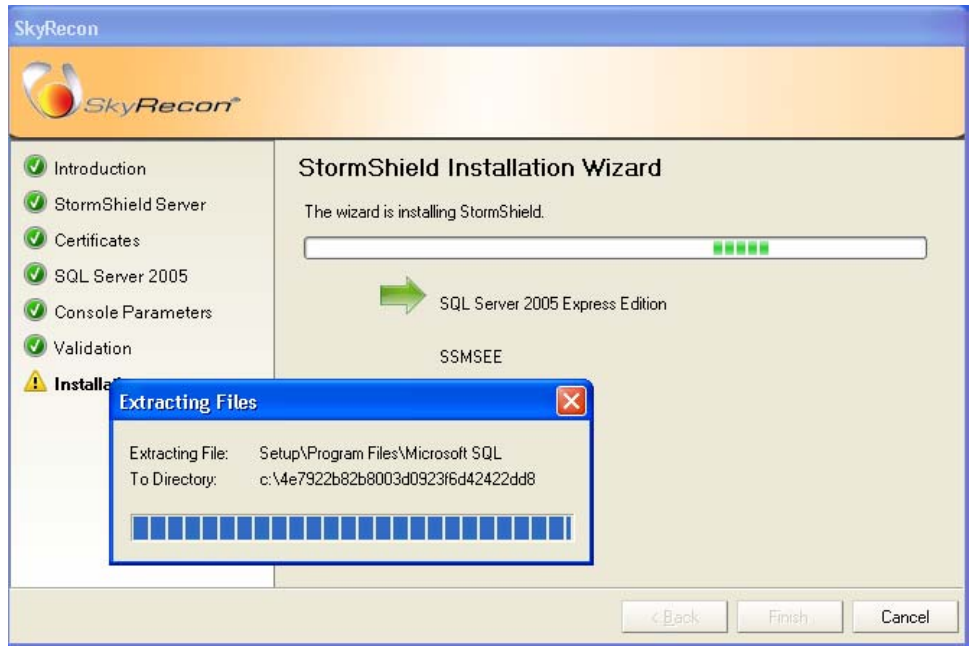


9. The following window is displayed. It summarizes the settings that you have just defined.

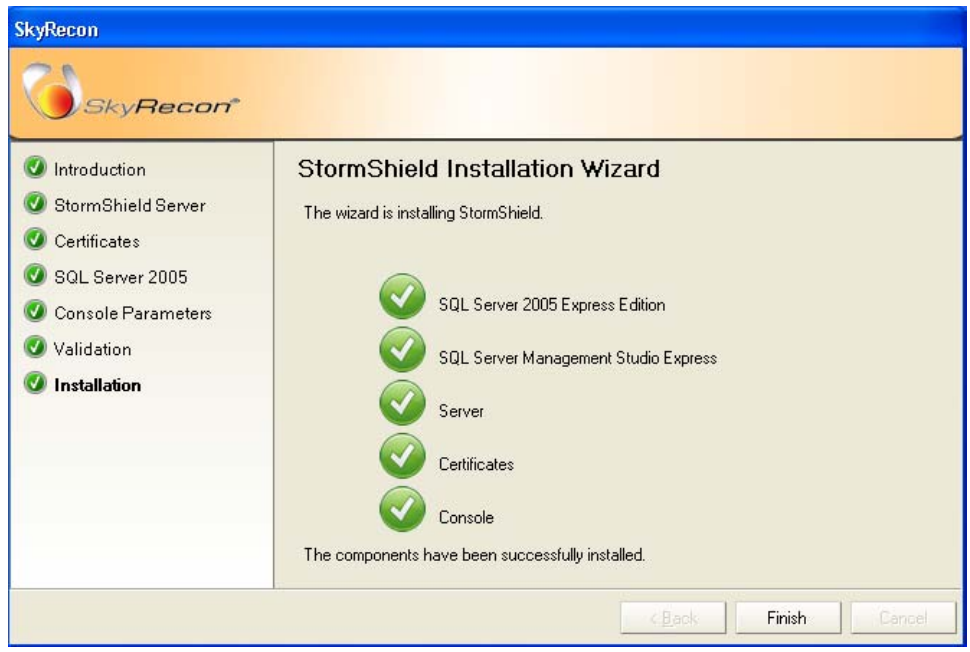
   Click **Next**.



10. Wait until the installation procedure is completed.



11. The window below shows that the components have been properly installed. Click **Finish**.

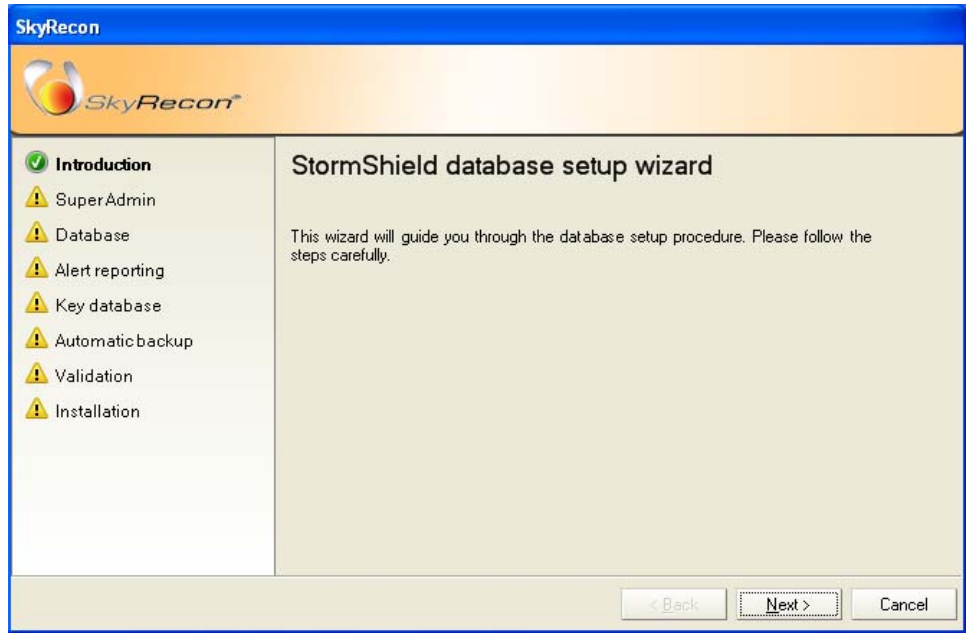


Database setup wizard

To install the StormShield database, follow the steps below:

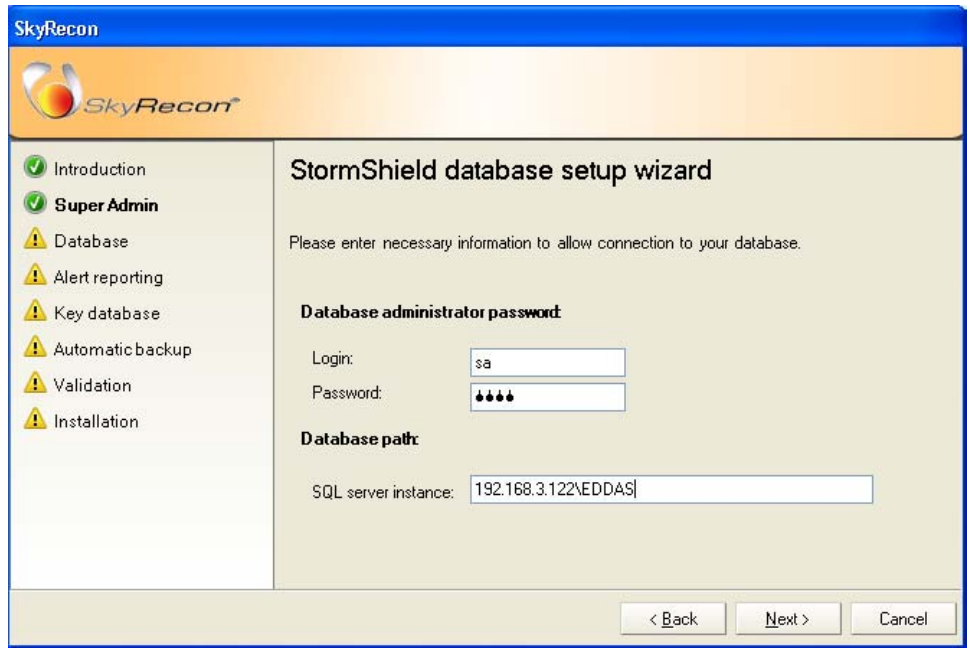
1. After installing StormShield, the StormShield database setup wizard window is displayed.

   Click **Next**.



2. To connect to the database, enter:
   - The database administrator login.
   - The database administrator password.
   - The database instance.

Click **Next**.



To declare the SQL server instance, two methods are available:

- **Method 1**:

If the SQL server uses a fixed port (example: 1433), declare the SQL port in the instance field in either way:

- SqlServeur,1433
- 192.168.1.1,1433

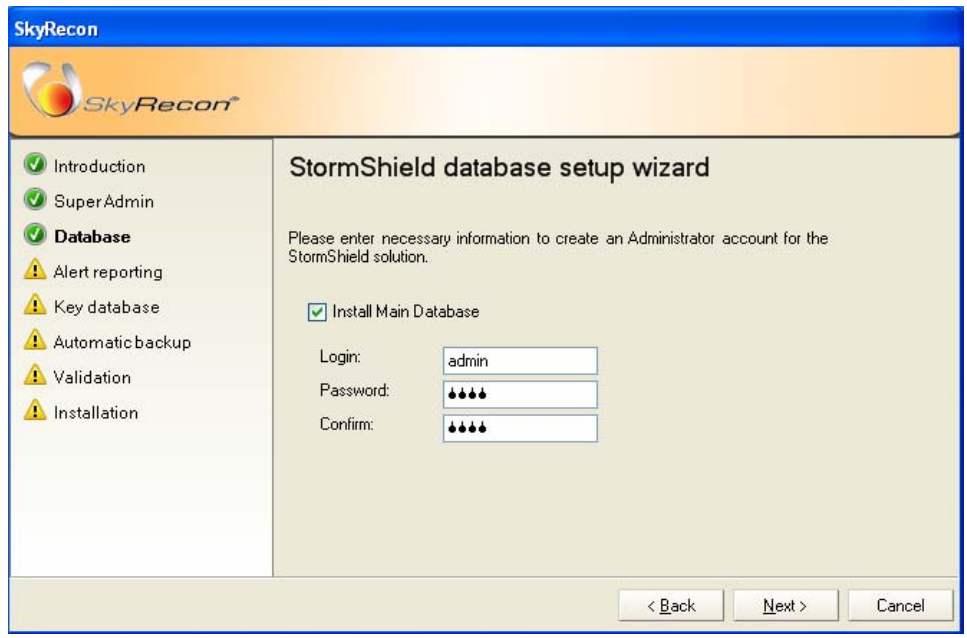
- **Method 2**:

If the SQL server uses a dynamic port, declare the SQL instance in either of the following ways:

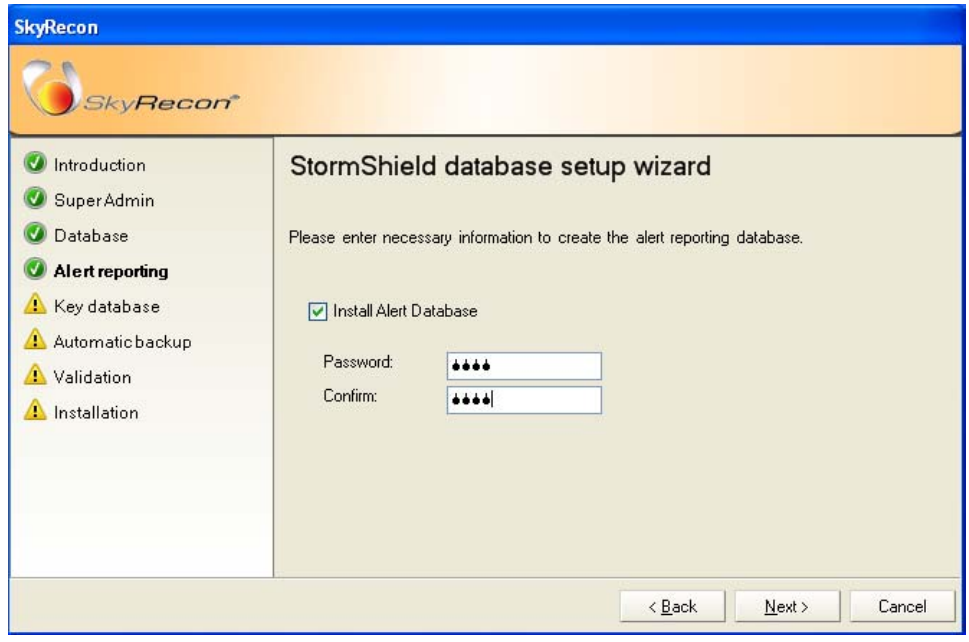
- SqlServeur\EDDAS
- 192.168.1.1\EDDAS

Method 2 also applies when the SQL server uses a fixed port. But, declaring a named instance requires the installation of the SQL Browser Service.

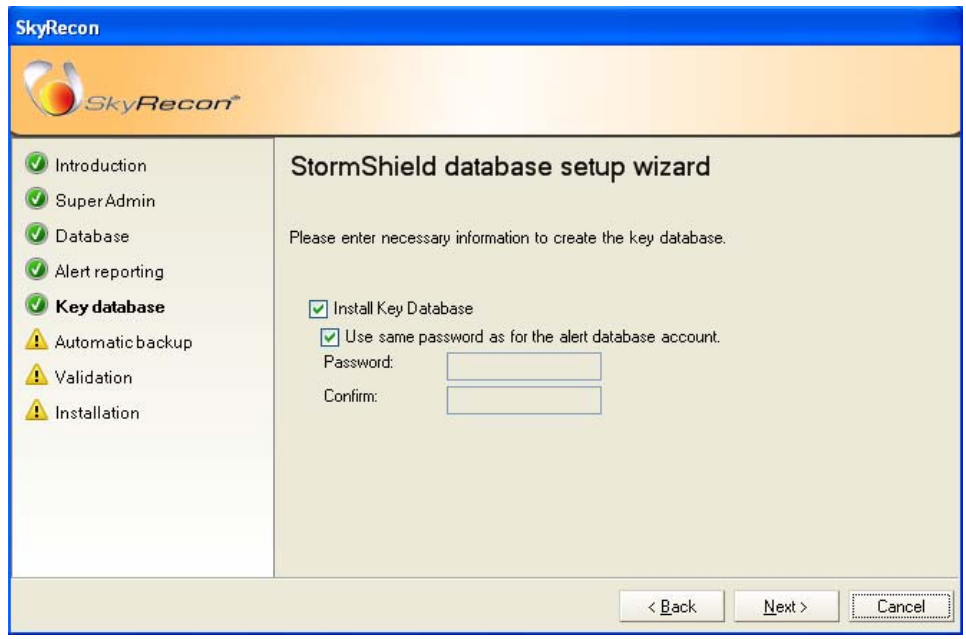
3. To create an Administrator account dedicated to the StormShield main database:
   - Check **Install Main Database**.
   - Enter the password.
   - Confirm the password.
   - Click **Next**.



4. To enable alert reporting to the StormShield server:
   - Check **Install Alert Database**.
   - Enter the password.
   - Confirm the password.
   - Click **Next**.

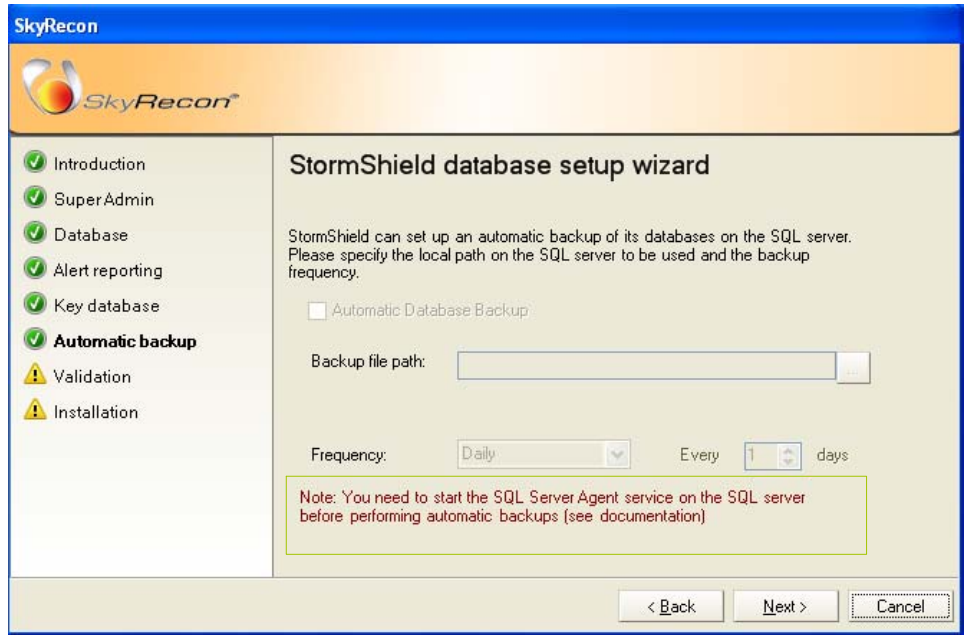


5. To enable the database account:
   - Check **Install Key Database**.
   - Check **Use same password as for the alert database account**.
   - Click **Next**.



If needed, you can select a different password for the key database. If so, uncheck **Use same password as for the alert database account**.

6. To save automatically the main database on the server, follow the steps below:
   - Check **Automatic Database Backup**.
   - Enter the backup file path.
   - Select the backup frequency.
   - Click **Next**.



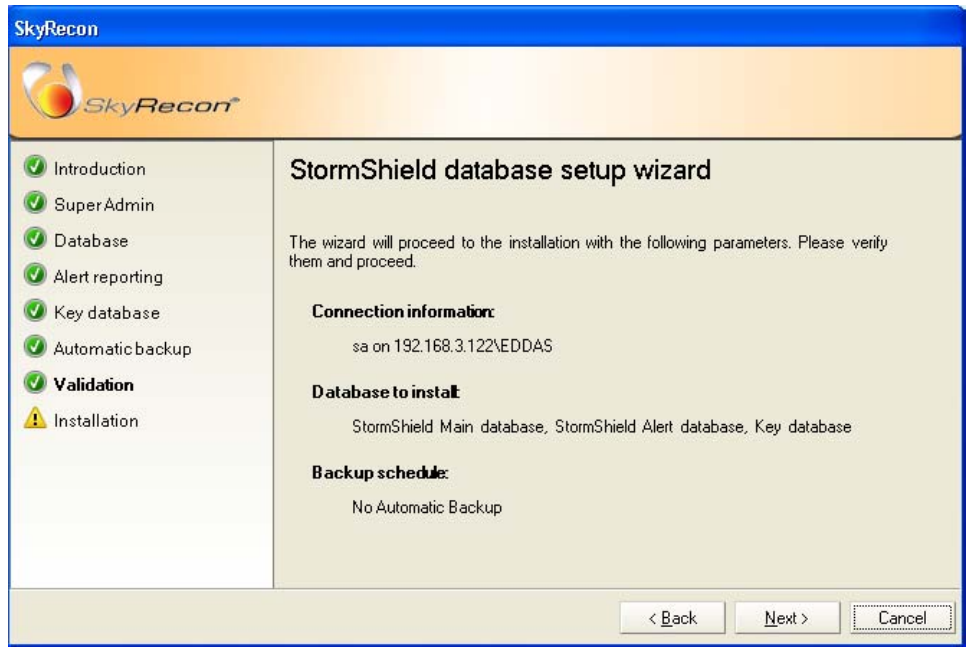
This feature is available only if you have access to the **SQL SERVER AGENT [EDDAS]** service.

To enable automatic backup, it is necessary to start the **SQL SERVER AGENT** service before finishing this step.

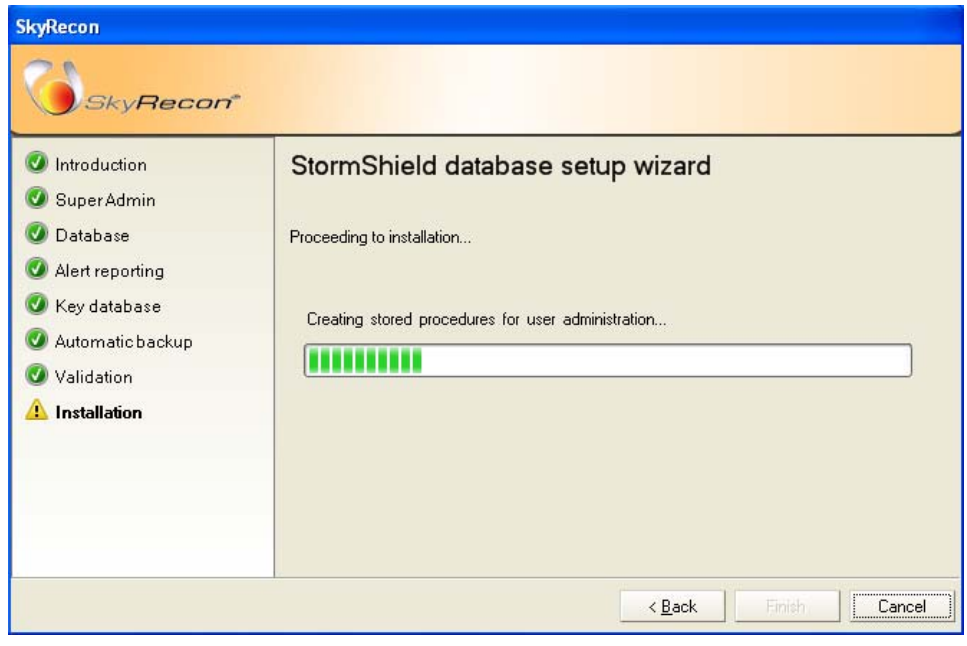
To back up your database in a directory other than the default directory (example: `.\Mssql\Backup`), assign Read/Write rights to the security group `SQLServer2005MSSQLUser$ServerName$SQLInstance`.

7. The following window is displayed. It summarizes the settings that you have just defined.

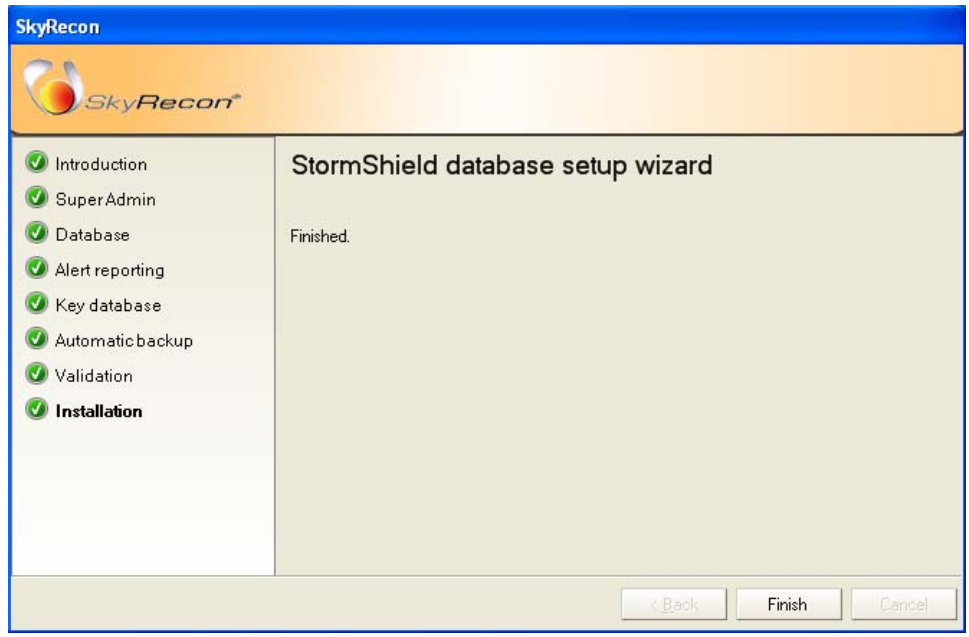
   Click **Next** to validate your settings.



8. Wait until the installation procedure is completed.



9. Complete the configuration by clicking **Finish**.



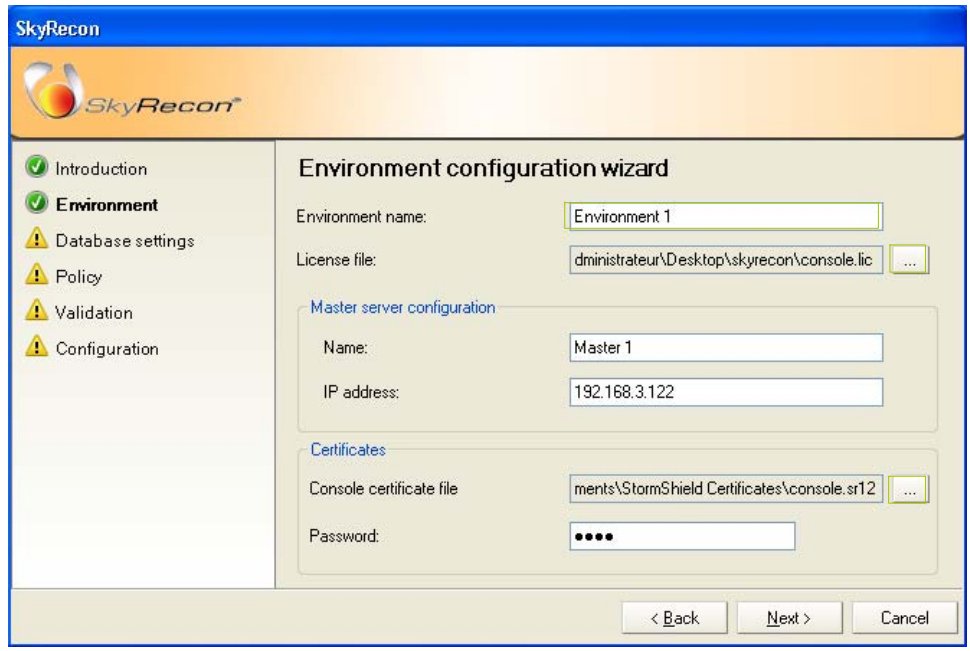
Environment configuration wizard

To configure the SkyRecon management console and create an operational environment, follow the steps below:

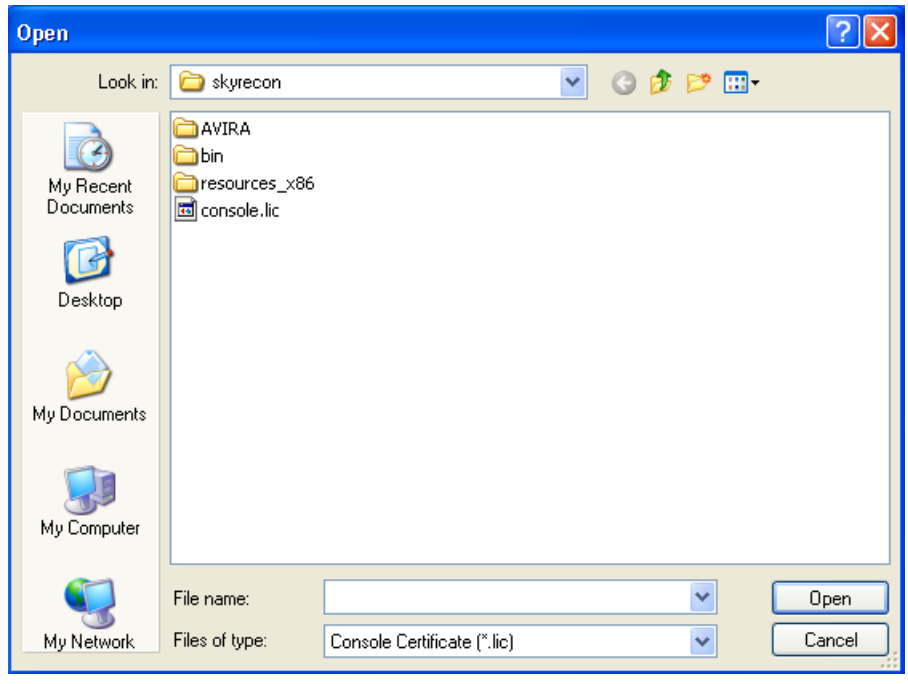
1. After installing the StormShield database, the Environment configuration wizard window is displayed.

   Click **Next**.

2. To define the console environment, enter the following information and click **Next**:
   - Enter the environment name.

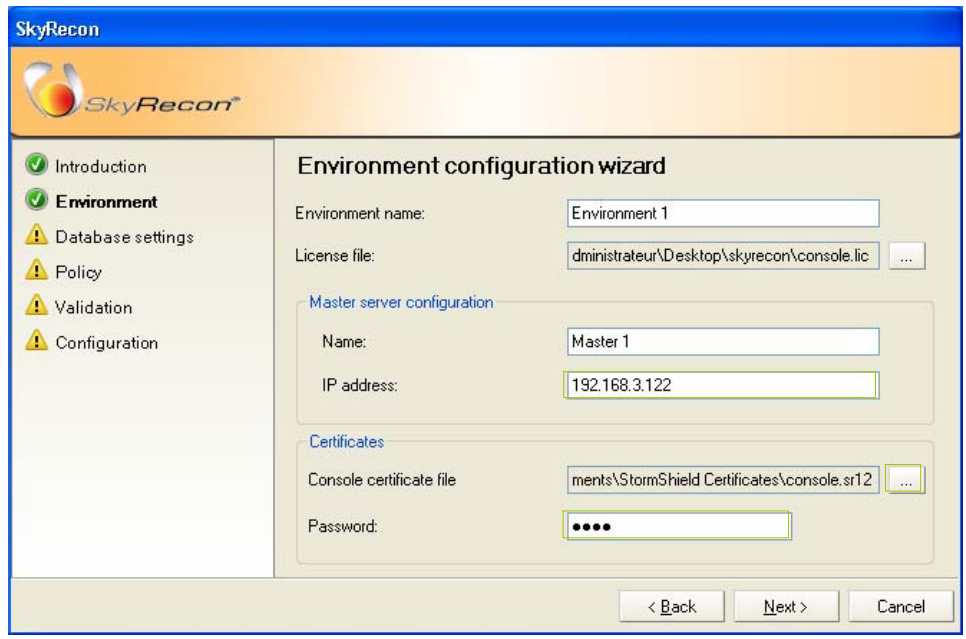


   - Select the license file using ... .

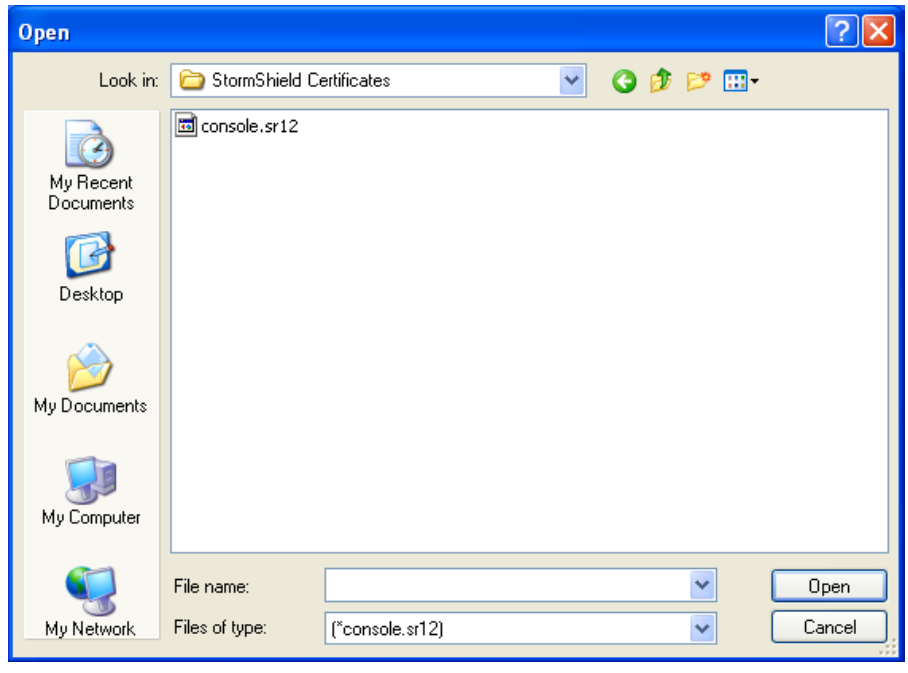


   - Enter the master server configuration name.

- Enter the IP address of the master server.



- Select the output directory for console certificates using ... .

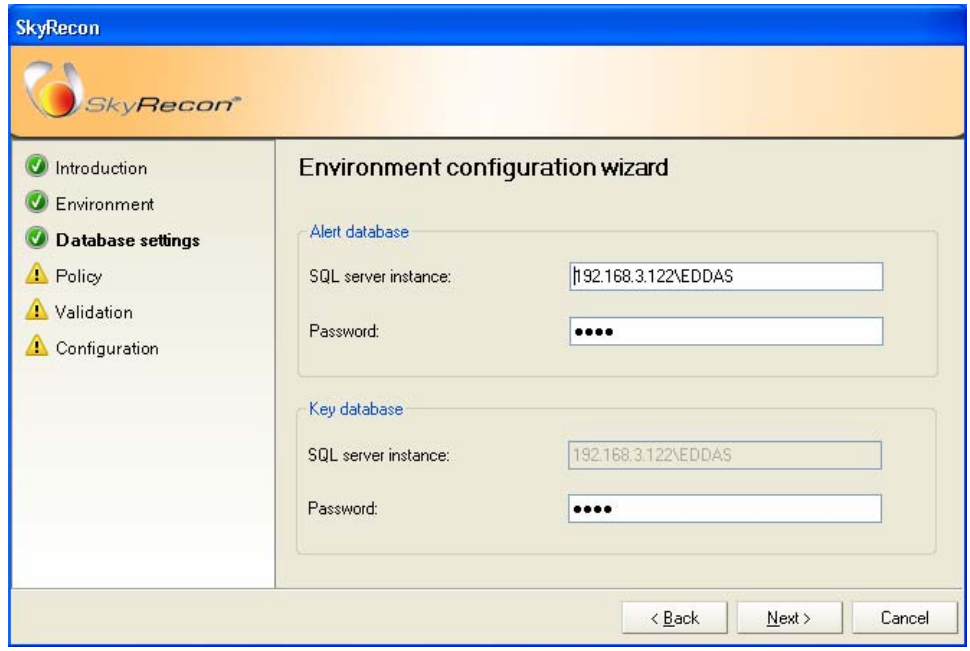


- Enter the passphrase associated with the console certificates generated when installing StormShield.

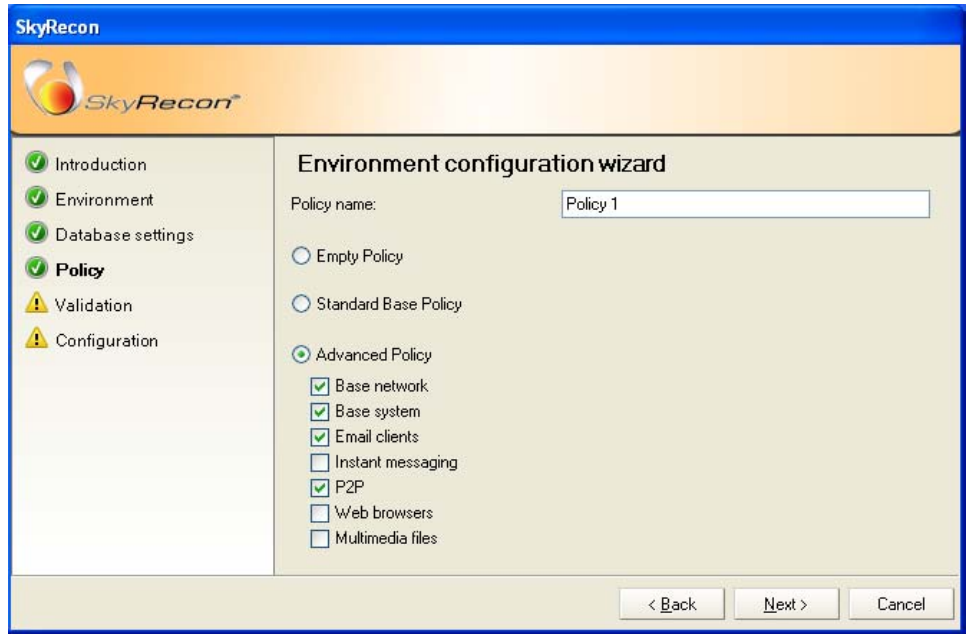
3. To configure the connection between the database and the console, enter the database passwords defined when installing StormShield:

- Alert database.
- Key database.

Click **Next**.

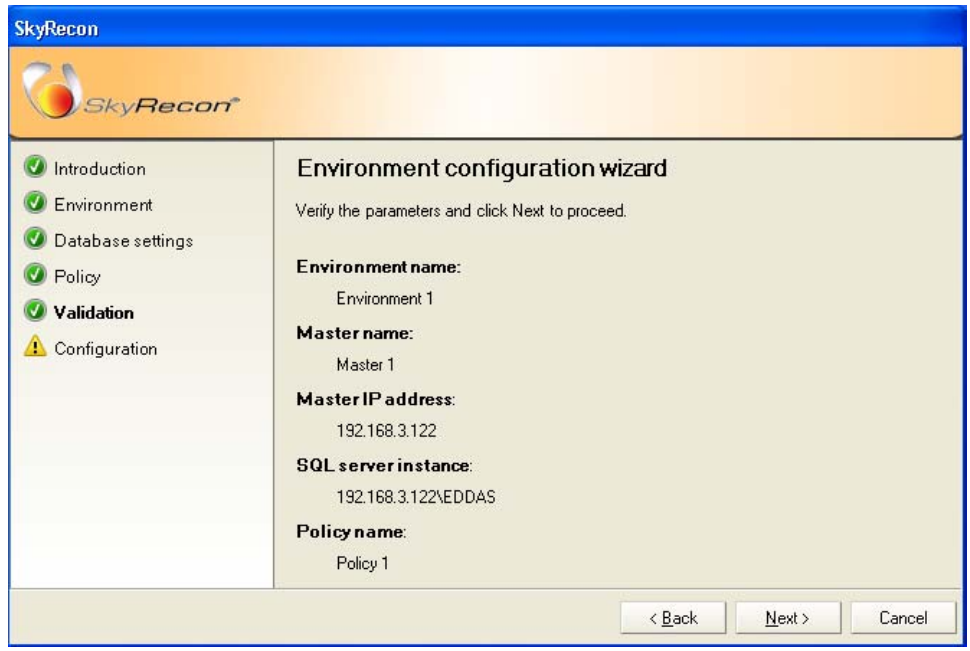


4. To define the security policy to be applied, check required items.
   Click **Next**.

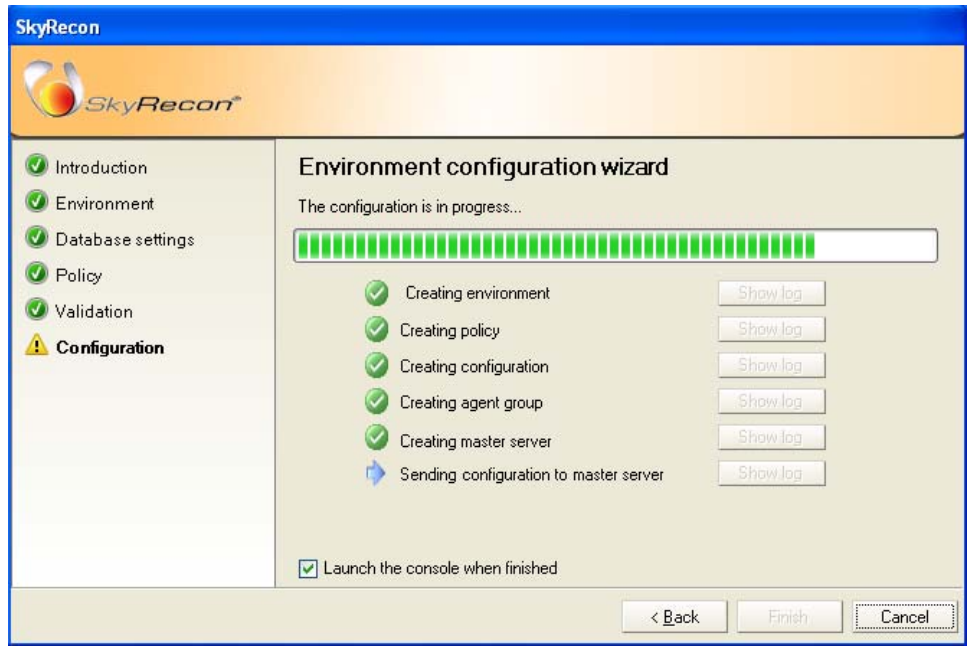


5. The following window is displayed. It summarizes the settings that you have just defined.

   Click **Next** to validate your settings.



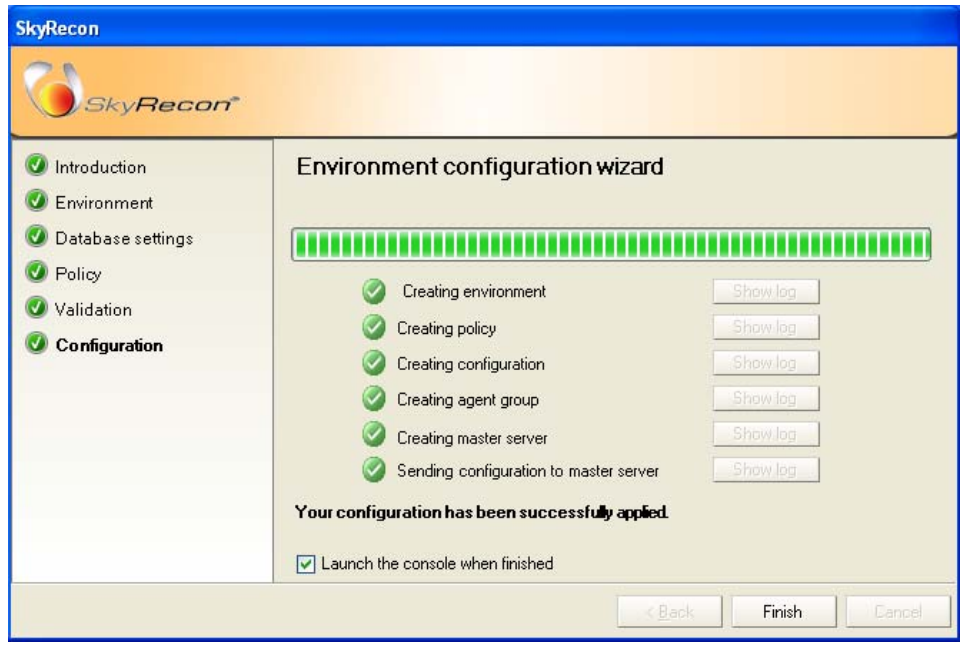
6. The window below shows that the configuration is in progress.



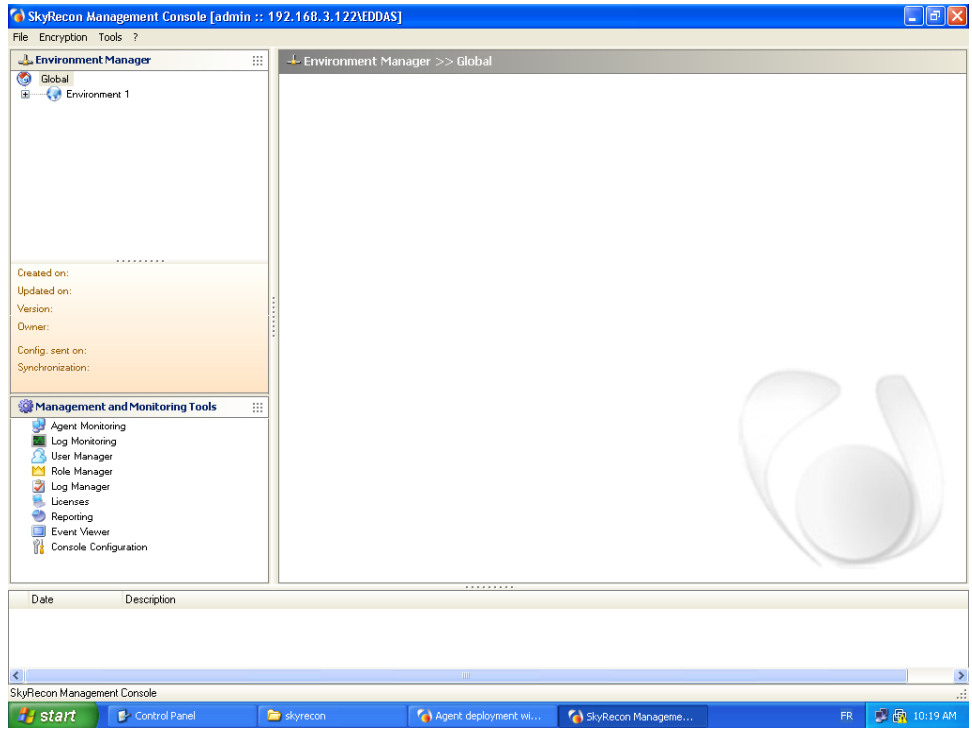
The **Launch the console when finished** box is checked by default. You can uncheck it if needed.

7. Click **Yes** if you want to install the certificate.

8. The window below shows that your environment has been properly configured.



9. The window below is displayed if you have ticked off the **Launch the console when finished** box.
   For more information, see "The window below shows that the configuration is in progress.", page 86.

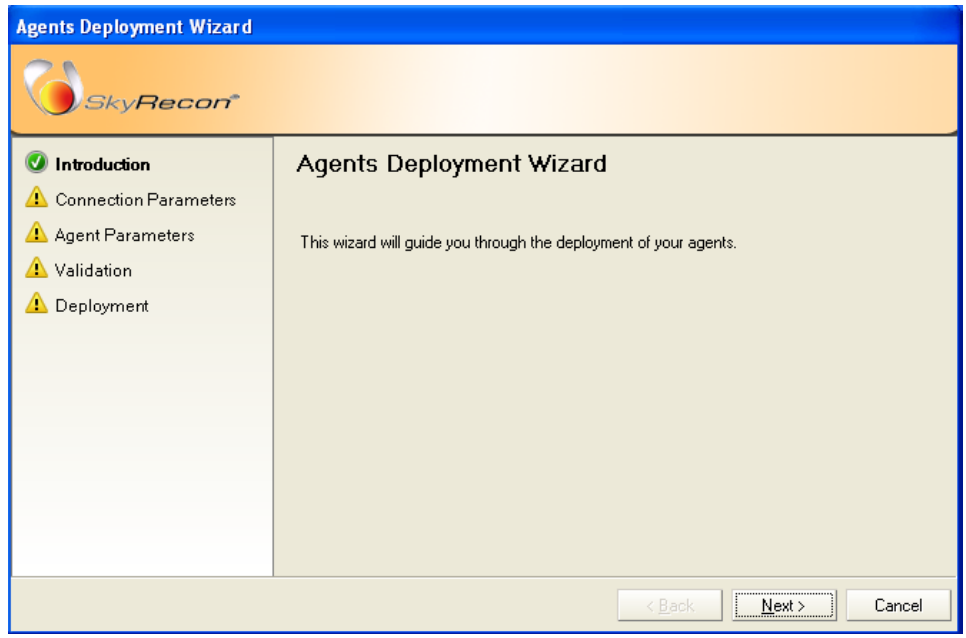


The agent deployment wizard launches behind the management console window. Minimize the window to proceed with the installation.

Agent deployment wizard

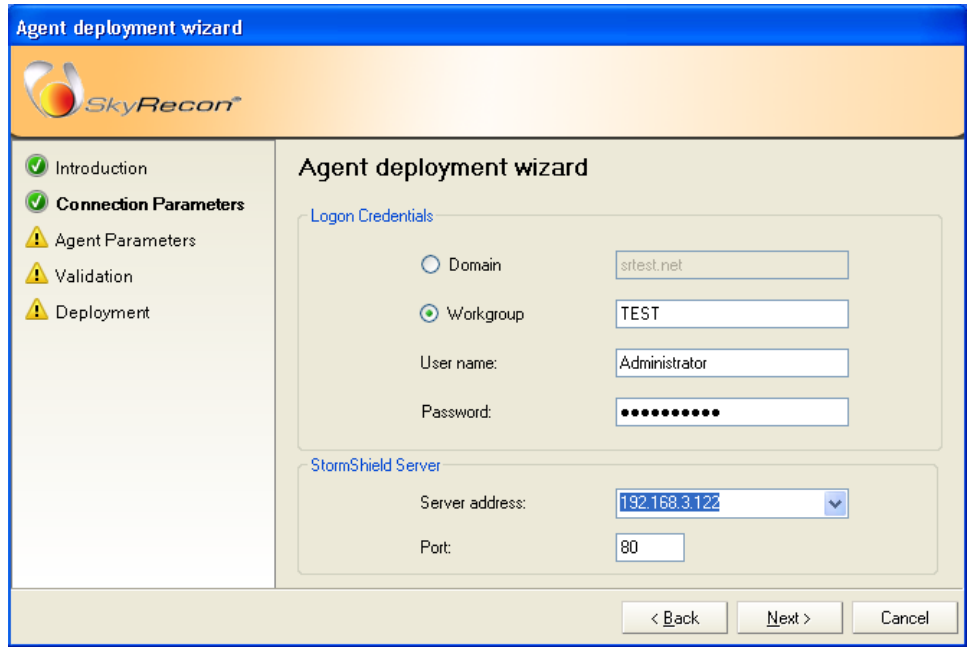
To deploy agents, follow the steps below:

1. After configuring your environment, the following window is displayed. Click **Next**.



2. Enter the following connection parameters:
   - The domain name (or workgroup).
   - The user name.
   - The user password.
   - The StormShield server IP address.
   - The port number of the web server installed with the StormShield server.

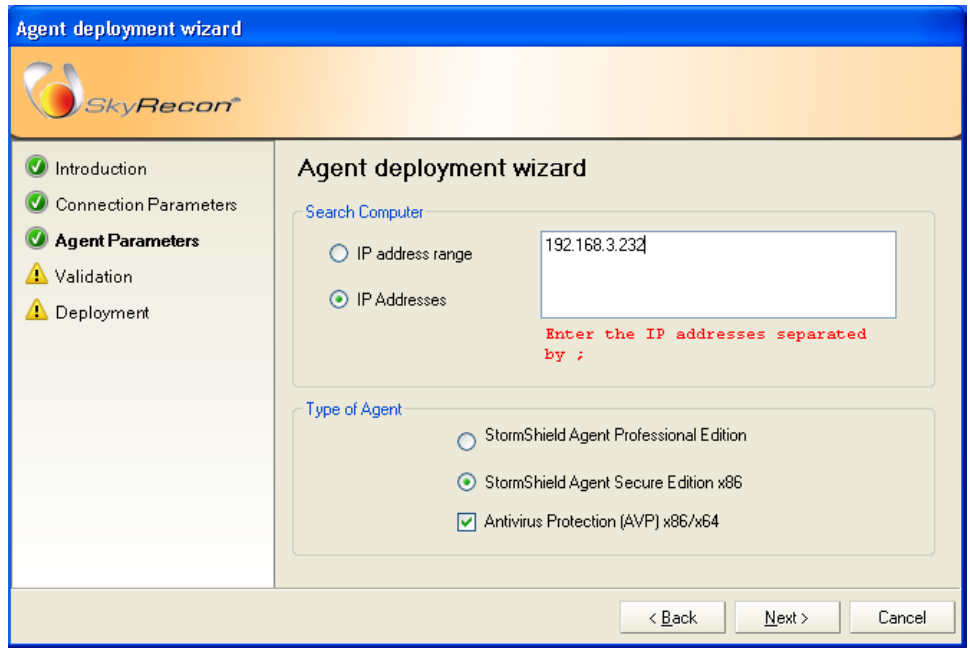
   Click **Next**.



The account used must have Administrator rights on the workstation.

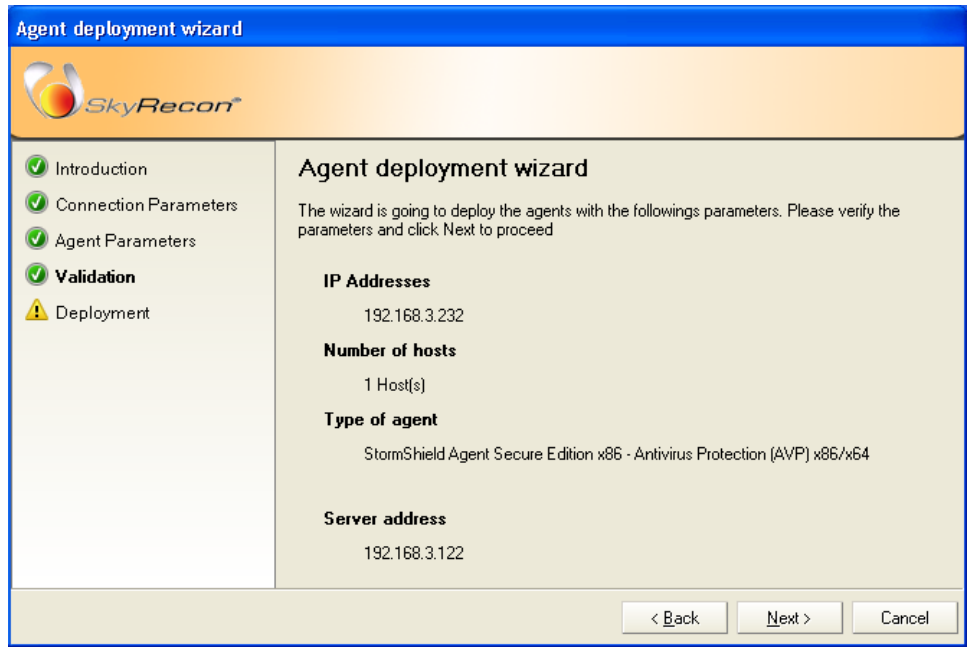
3. Customize the agent parameters:
   - Define the list of machines on which to install the agent by:
     - IP address range.
     - IP address.
   - Select the StormShield package to be installed:
     - StormShield Agent Professional Edition.
     - StormShield Agent Secure Edition.
   - Tick the **Antivirus Protection (AVP)** box if your license includes this option.

- Click **Next**.



4. The following window is displayed. It summarizes the settings that you have just defined.

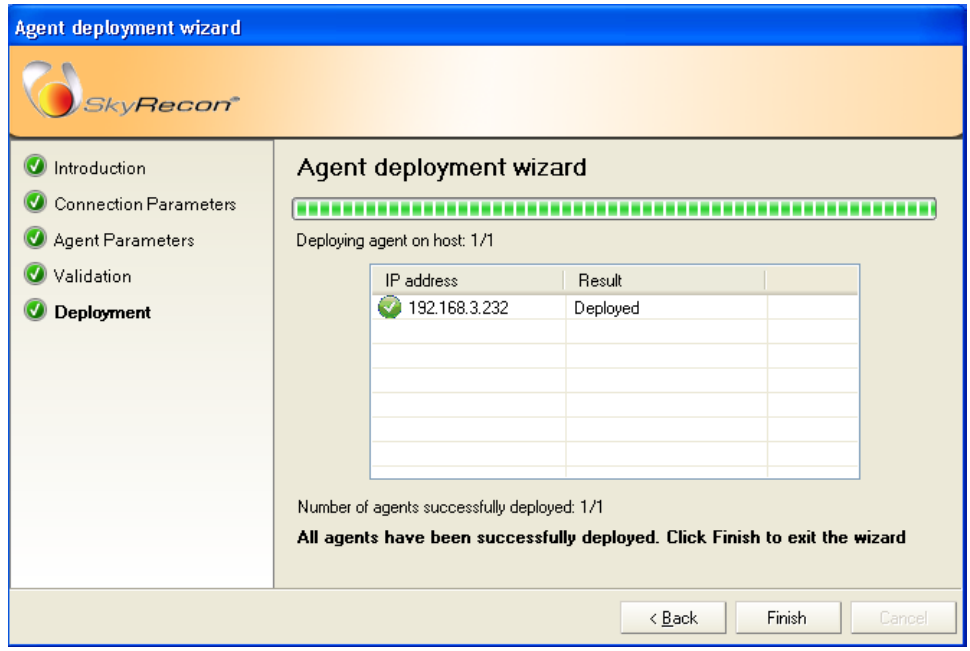
   Click **Next** to validate your settings.



5. The following window is displayed.

   Wait until the agent deployment is completed.

   Click **Finish**.



In order to use the agent deployment wizard, make sure that:

- The Web service of the StormShield server can be accessed by any machine on which the agent is going to be deployed.
- Administrative Tools can be accessed by workstations.
  If another application or a user already accesses Administrative Tools on the machine on which the agent is going to be deployed, deployment fails.

If problems arise, check that access is not blocked by a firewall and that simple file sharing is disabled.

INSTALLING STORMSHIELD MANUALLY

PREREQUISITES

It should be noted that:

- Either the Microsoft XP embedded firewall must be disabled before installing the agent.
- Or TCP port 16006 must be opened to allow StormShield server connections.

PROCEDURE

The manual installation procedure of StormShield includes **six** steps:

1. Install the master server.
2. Install a slave server.

> **Slave servers** can be installed at any time after the relevant master server has been installed.

3. Install the SkyRecon console.
4. Install the database.
5. Configure an environment (console).
6. Install the agents.

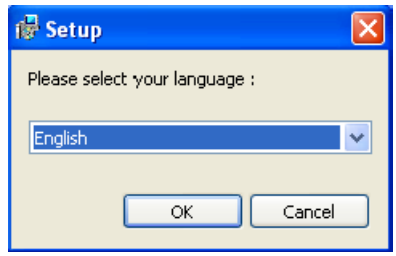
Installing the master server

> If you have the **Antivirus Protection (AVP)** option, you must use the server installer `server.exe` which includes the antivirus option.

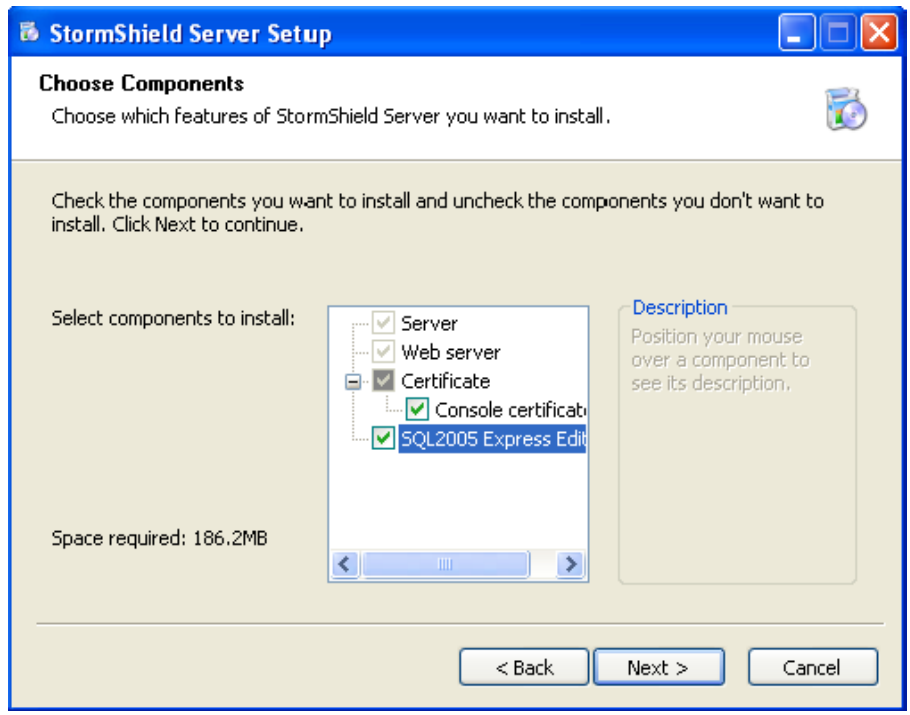
To install the master server with the installer, follow the steps below:

1. Go to the `bin` folder and double-click `server.exe`.
   The StormShield master server installer is starting up.

2. Select the setup language.



3. Select the components to be installed:



You can choose among:

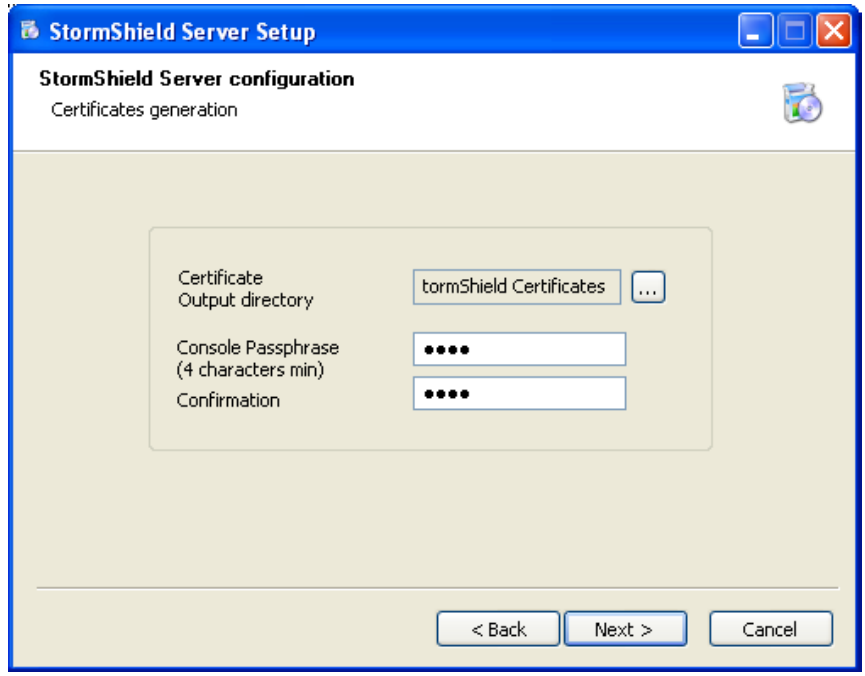
- The StormShield server and Apache Web server boxes are ticked and grayed out by default.
- The console certificate.
- The MS SQL Server 2005 database (Express Edition).

The MS SQL Server 2005 database can be deselected if you prefer to install it on a different machine or if an MS-SQL server is already installed for using the StormShield database.

4. Click **Next** to request the server certificate generation.

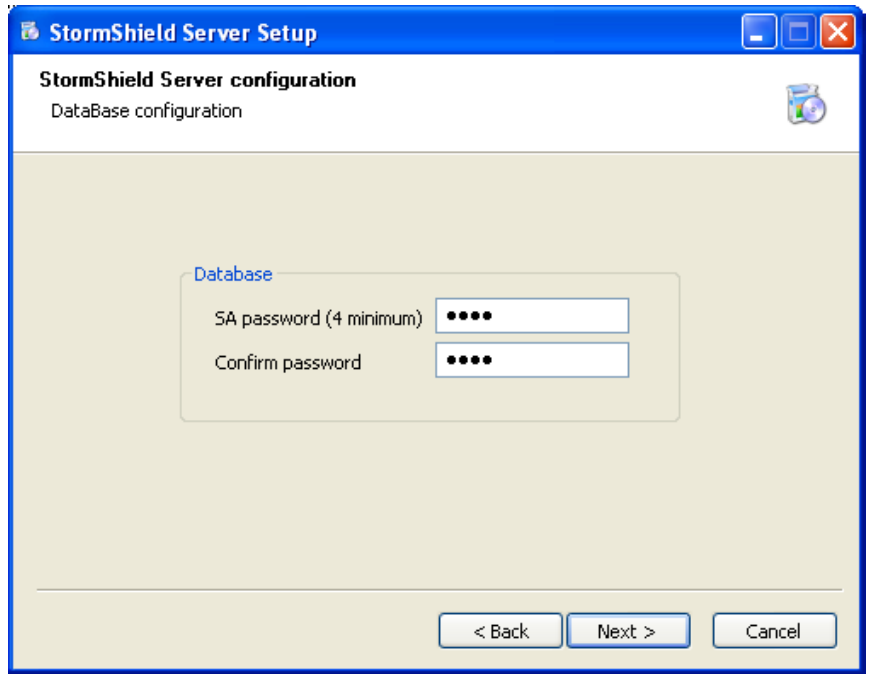
5. Enter the IP address of the server and the ports used by the embedded web server.

   The installer prompts you for this information if the web server box has been ticked.



By default, ports 80 and 443 are used. These values must be changed if a web server already uses these ports on the target machine.

6. Enter the parameters to generate the console certificate.



his step appears only if the Console certificates box was ticked.

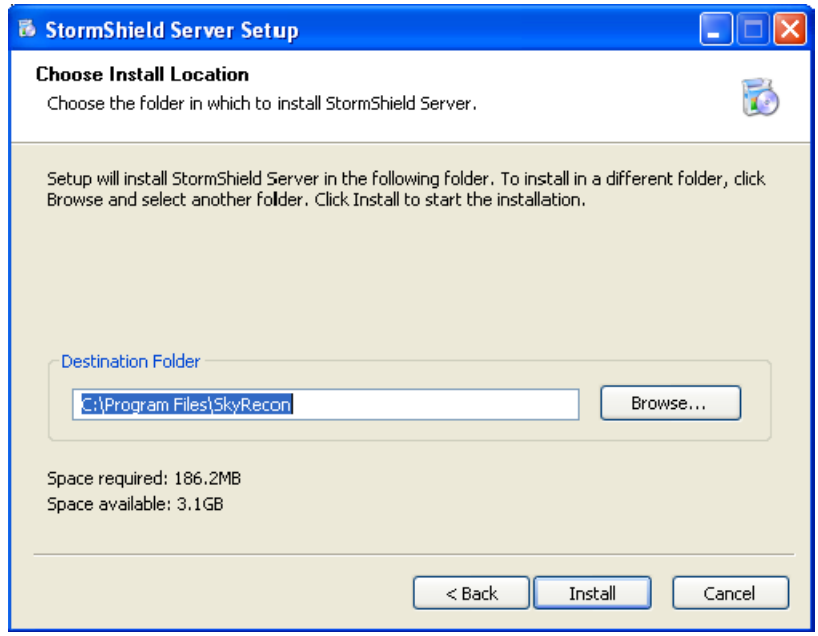
If so, you will have to specify the target directory where certificates will be created, and the password used to protect them.

Ensure that the target directory is always accessible from the machine on which the console is to be installed, unless you wish to copy the certificates and transfer them to a location that is accessible to the console.

The password is case sensitive. It must contain at least four alphanumeric characters. This password is also required to access the SkyRecon management console.

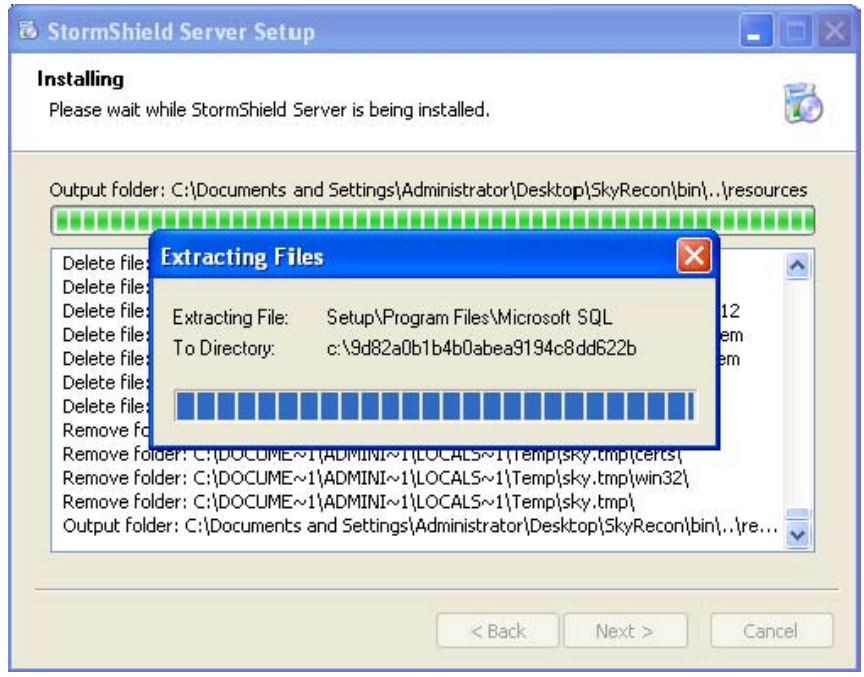
7. Enter the administrator password for the database.

   This step appears only if the database box was ticked.



8. Define the StormShield server installation path on the target machine.

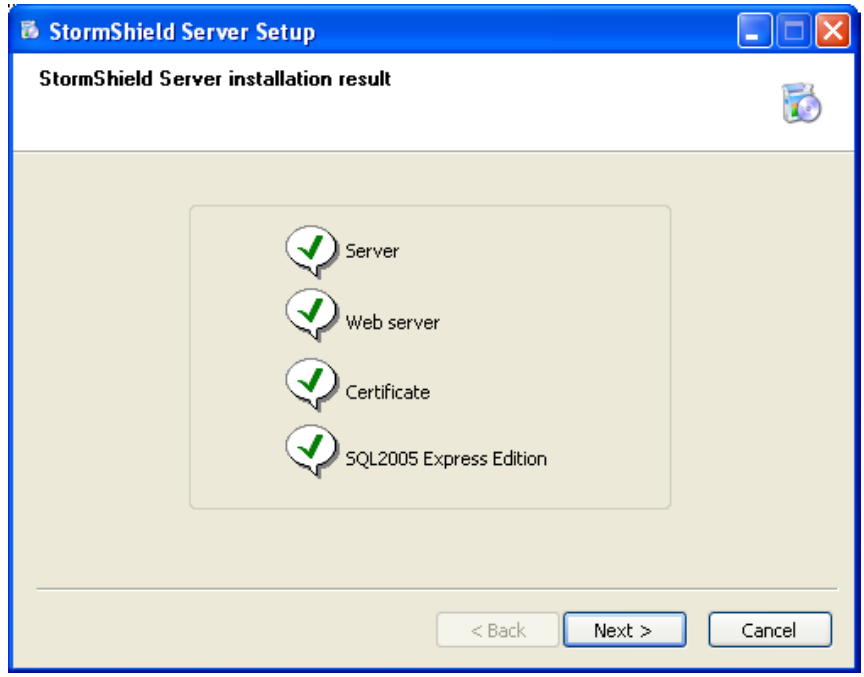
   Click **Install**.



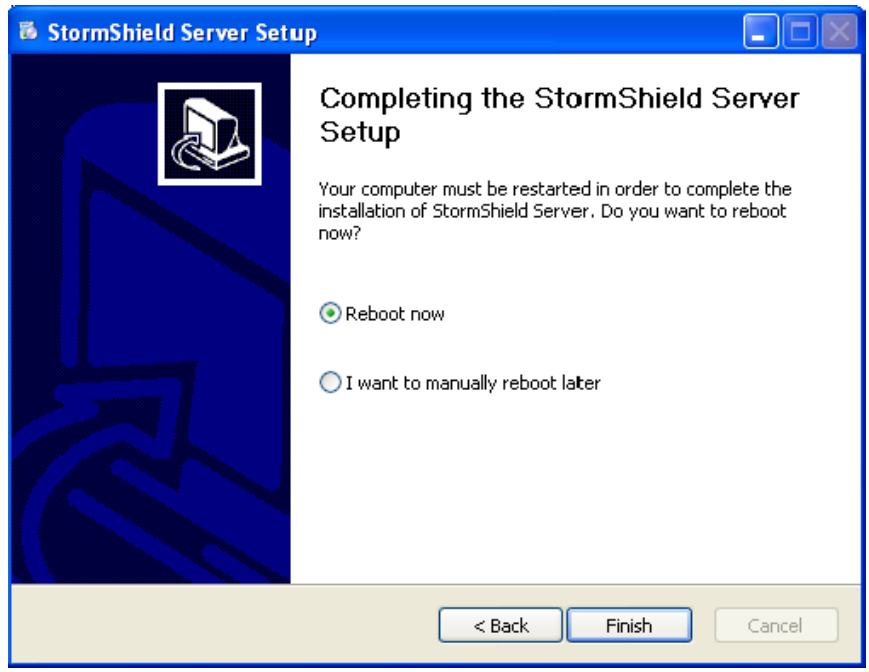
9. Wait until the installation is completed.

10. Check the installation report.

    This report shows the installation status of the selected components.



11. Reboot the machine to start the server.



Installing slave servers

Slave servers are optional. They are used to distribute the load of requests between agents and servers and ensure high availability at deployment server level.
Indeed, a slave server automatically takes over for the master server in the event the master server accidentally stops working.

Number of slave servers

The number of slave servers depends on:

- The number of agents deployed.
- The network speed.
- The configuration size.
- The number of alerts and logs returned.

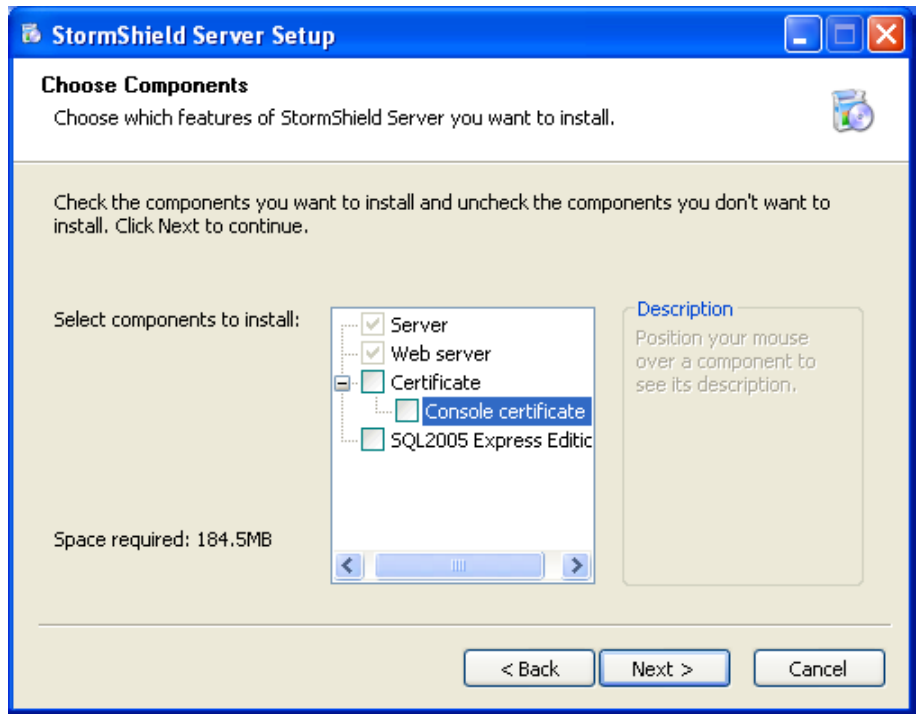
Procedure

A slave server is installed using the same installer as for the server.

To install an additional server, follow the steps below:

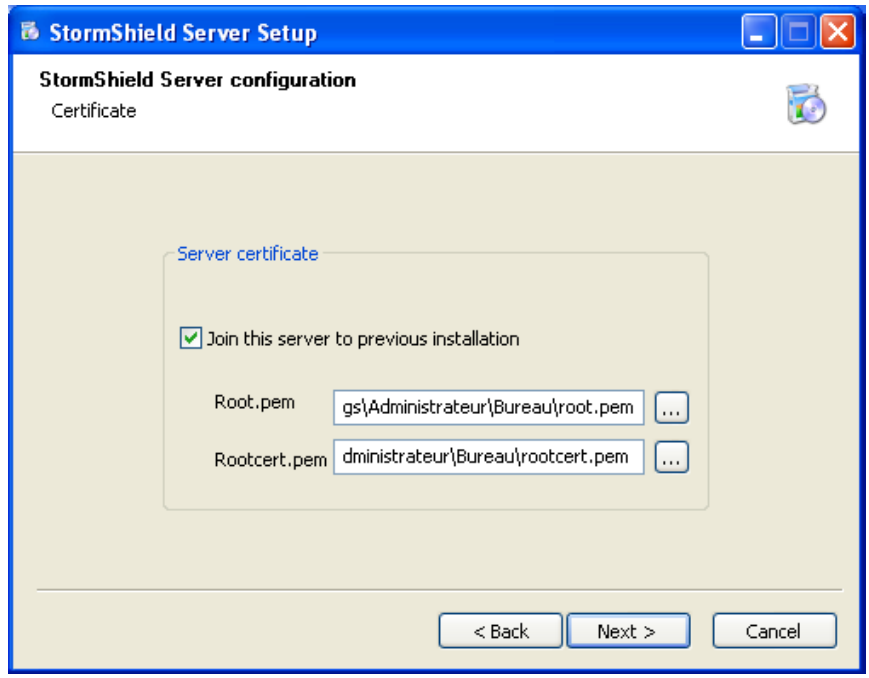
1. Go to the `bin` folder and double-click `server.exe`.
2. Select the installer language.
   Click **OK**.
3. A window is displayed in which the following components are grayed out by default:
   - The StormShield server.
   - The Web server (Apache) used to deploy agents in download mode.
4. Deselect certificates as the latter are the console certificates that were generated when the master server was installed.

5. Deselect the MS SQL Server 2005 database to consolidate all the data returned from the agents in the same database which is already installed with the master server.

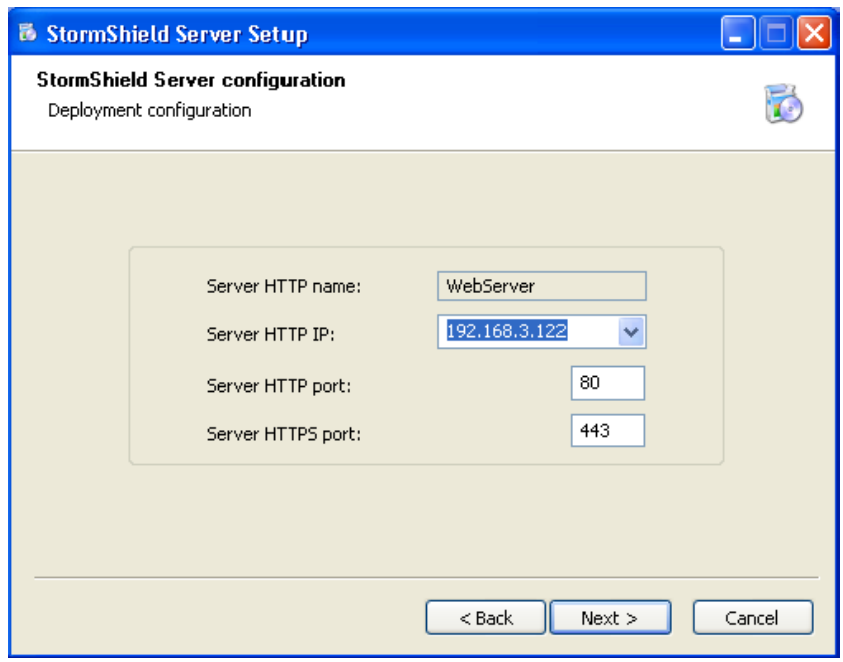


6. Specify the path to access the two files containing the master server certificate. The following files were generated when installing the master server:
   - `root.pem` (Certificate Authority).
   - `rootcert.pem` (certificate).

These files were placed in the master server installation directory.



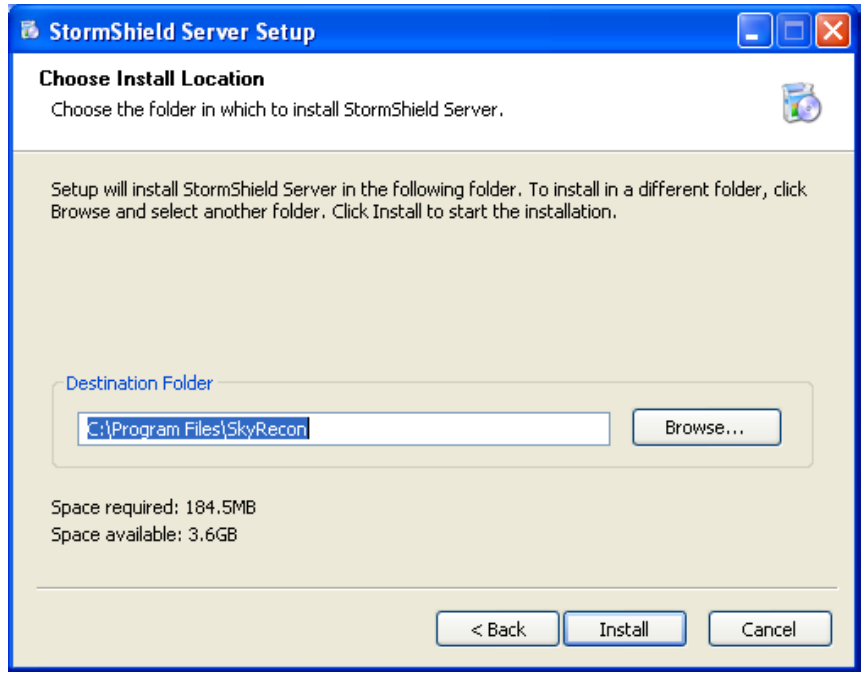
7. Enter the IP address of the master server and the ports used by the embedded web server.



By default, ports 80 and 443 are used. These values must be changed if a web server already uses these ports on the target machine.

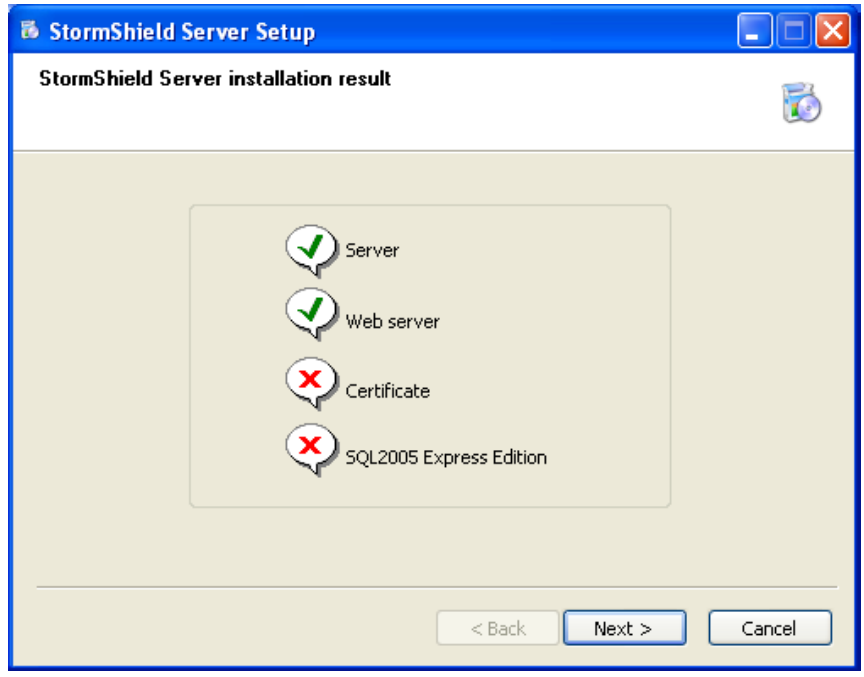
8. Define the server installation path on the target machine.

   Click **Install**.



9. Check the installation report.

   This report shows the installation status of the selected components.



10. Reboot the machine to start the server.

Installing the SkyRecon management console

The console software is installed on the target machine using the installer provided for this purpose.

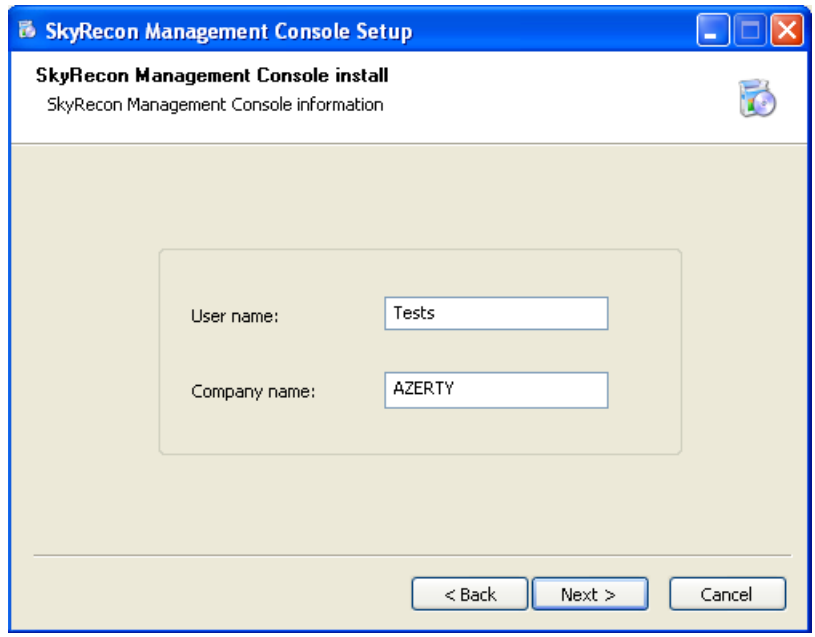
When installing the console with the installer, follow the steps below:

1. Go to the `bin` folder and double-click `console.exe`.

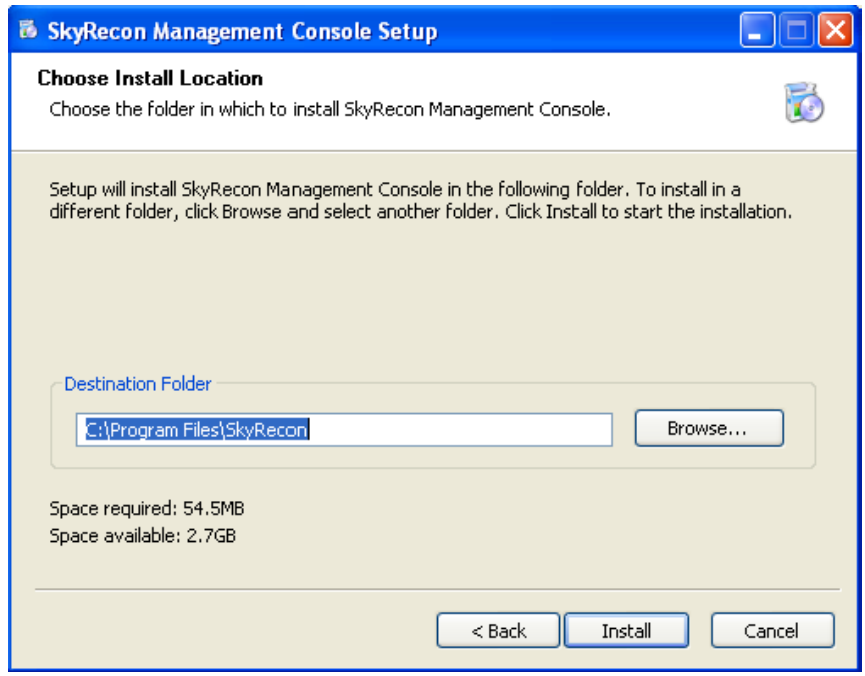
   This operation runs the installation of Microsoft.NET Framework (if not already installed on the computer).

2. Select the installer language.

3. Identify the user and the company.



4. Click **Install**.



5. Click **Finish** to complete the console installation.

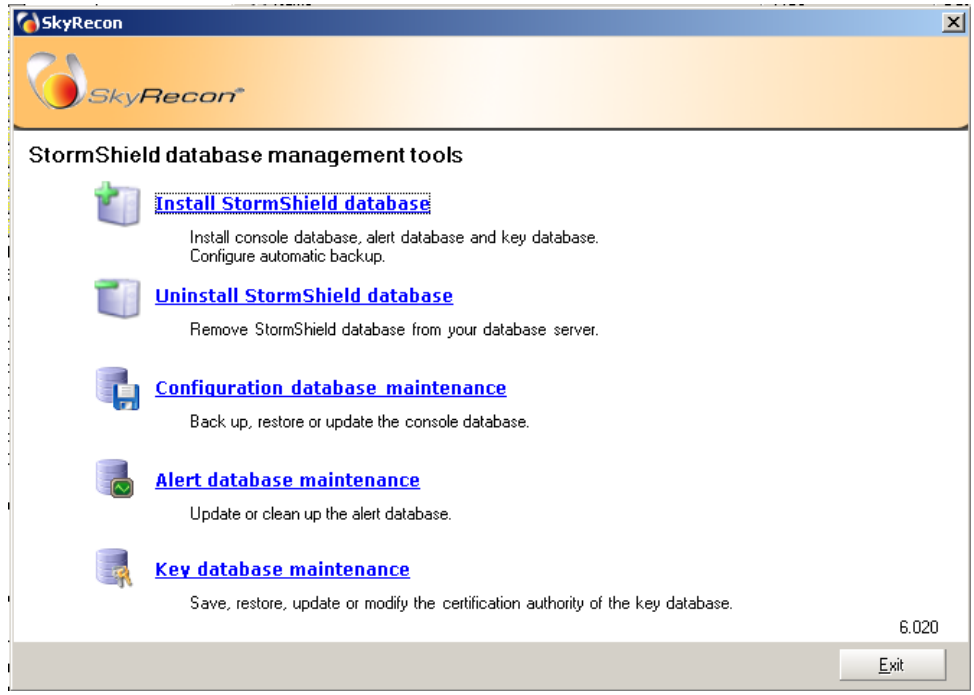
Installing the StormShield database

To install the StormShield database with the installer provided for this purpose, follow the steps below:

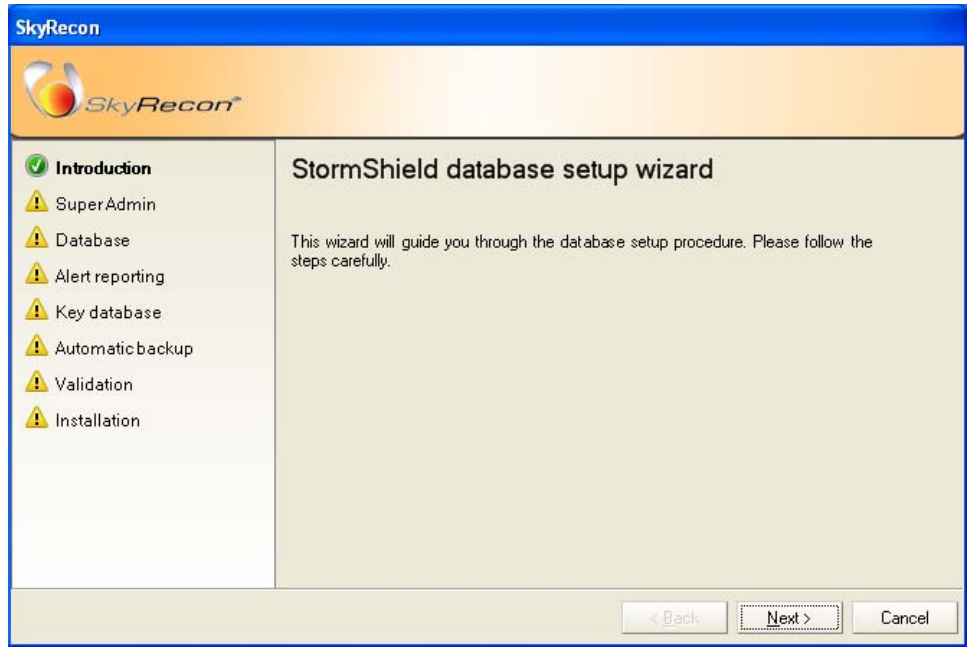
1. Start the database installation program which is called `DBInstaller` and represented by the icon :

   `Start\Programs\SkyRecon\DBInstaller`

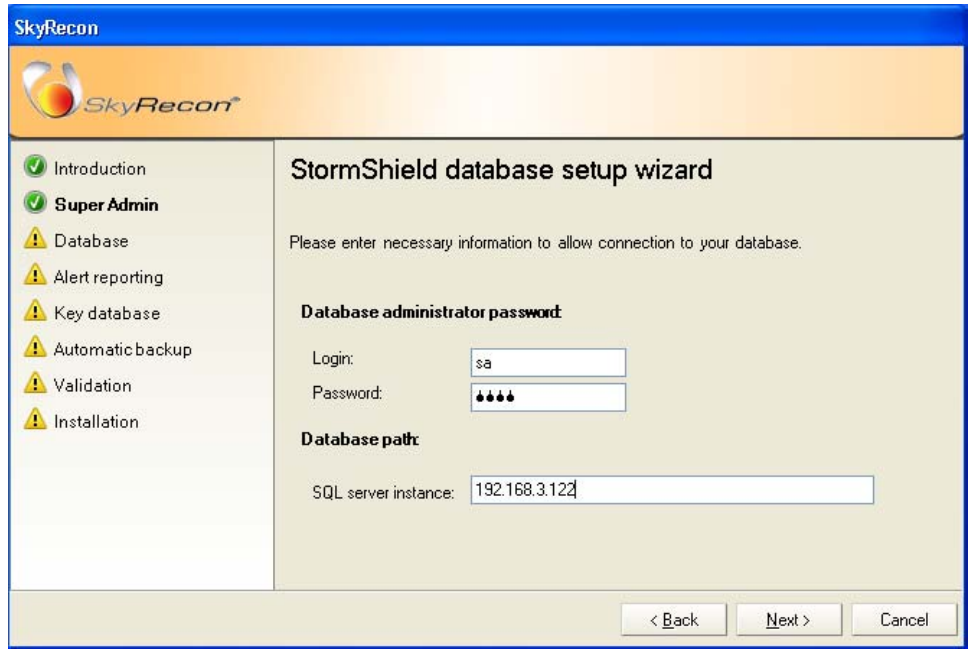
The following window is displayed. Select **Install StormShield database**.



2. Install the database using the StormShield database setup wizard.



3. Define the parameters required to create the database:
   - The name and password of the database system administrator (**sa**) account.
   - The IP address of the MS SQL Server 2005 database server machine.
   - Optionally, the port used to access the database.

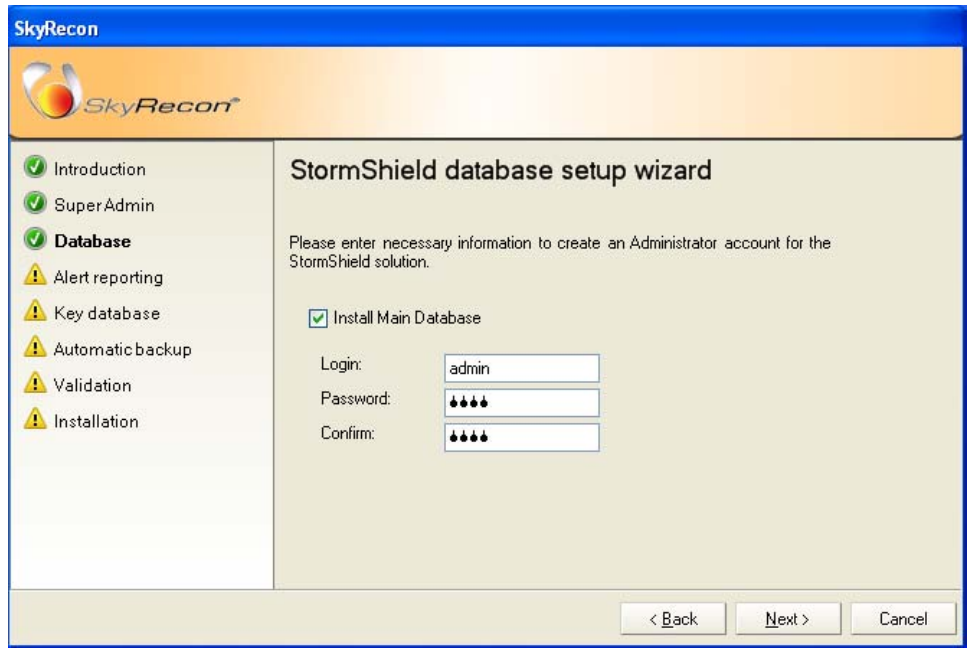


The **sa** account is only used to create the database and the server and console user accounts.

The Server and Console user accounts are used respectively by the StormShield server and the SkyRecon management console to connect to the database.

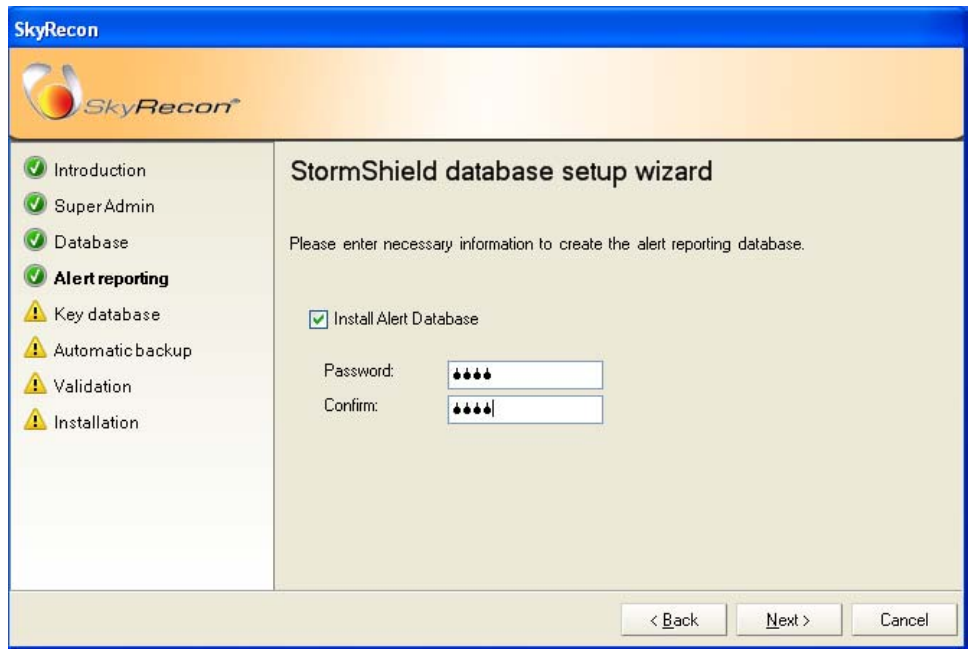
4. Install the main database.

   You must define a password that will be used by the StormShield administrator account (admin).



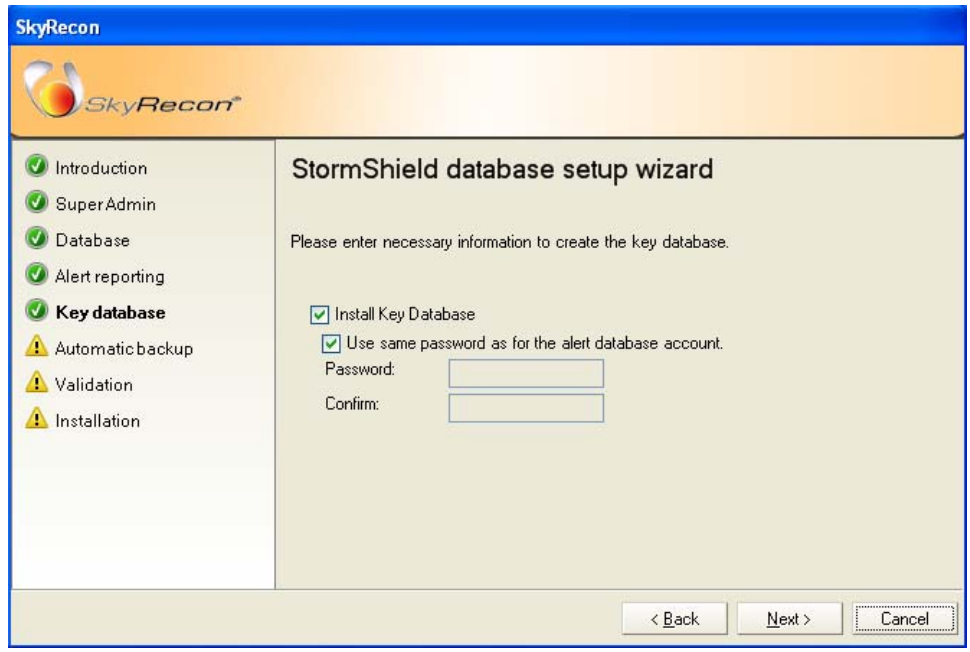
5. Install the alert database.

   You must define a password that will be used by the StormShield server to write in the database.



6. Install the key database.

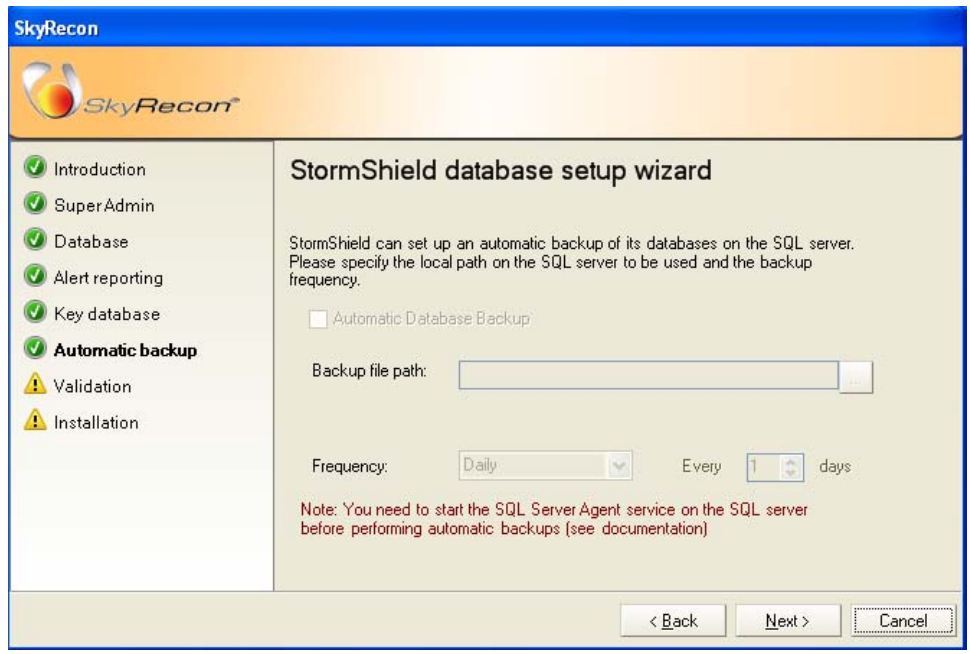
   You must define a password for the StormShield server to manage the encryption keys in the database.



7. Optional: create a backup job.

   To do so, start the **SQL SERVER AGENT** service.

   Click **Next**.

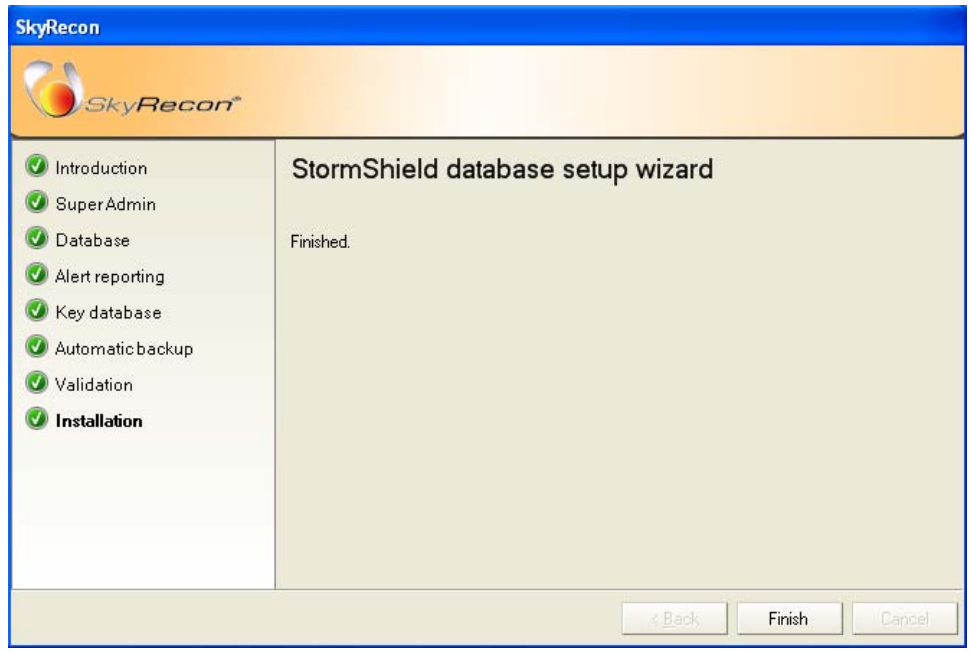


To back up your database in a directory other than the default directory (example: `.\Mssql\Backup`), assign Read/Write rights to the security group `SQLServer2005MSSQLUser$ServerName$SQLInstance`.

8. The following window is displayed. It summarizes the settings that you have just defined.

   Click **Next**.

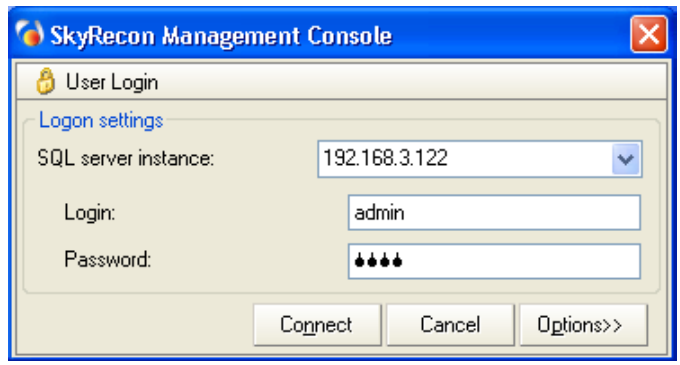
9. The following window is displayed. Click **Finish**.



Configuring the environment

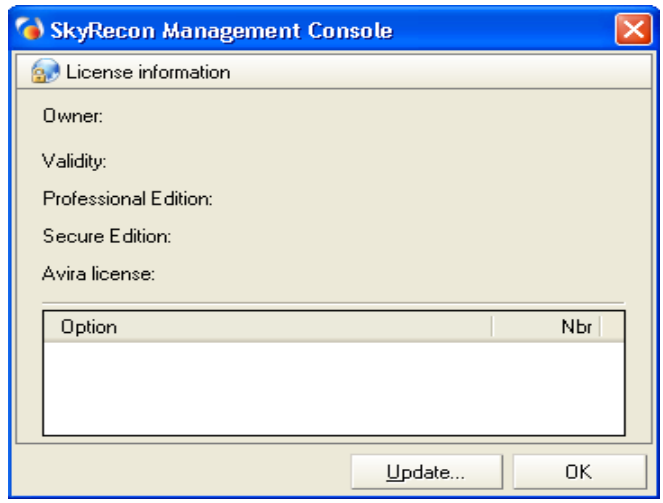
To configure the environment on the SkyRecon management console, follow the steps below:

1. Click the icon to open the console.
2. Enter the console user identifier and the password defined during database installation.

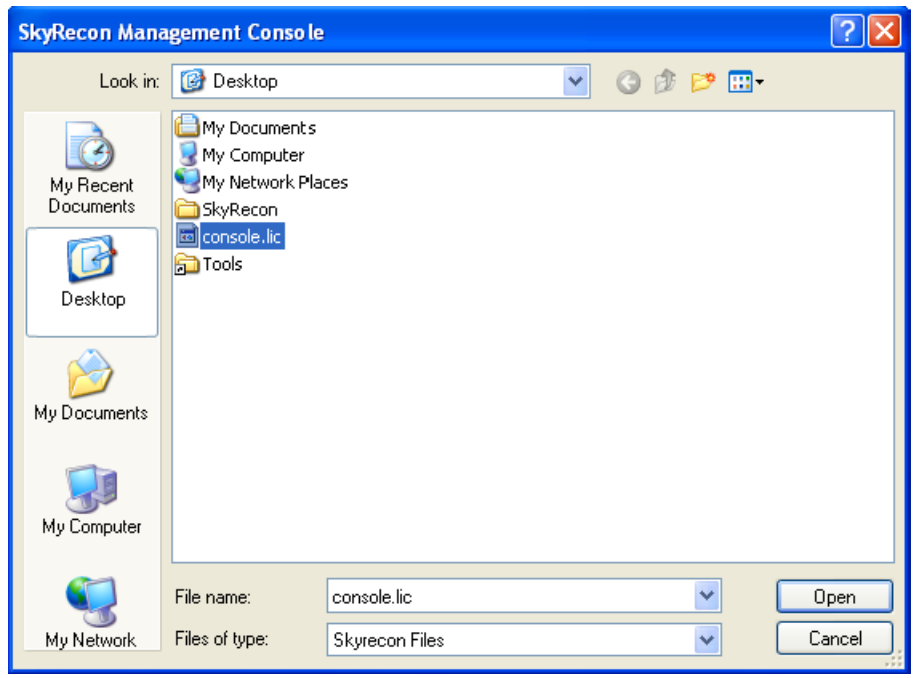


3. To configure a new environment, follow the steps below:
   - Right-click **Global** to display the right-click menu.
   - Click **New Environment**

4. Click **Update** and select your StormShield license file.

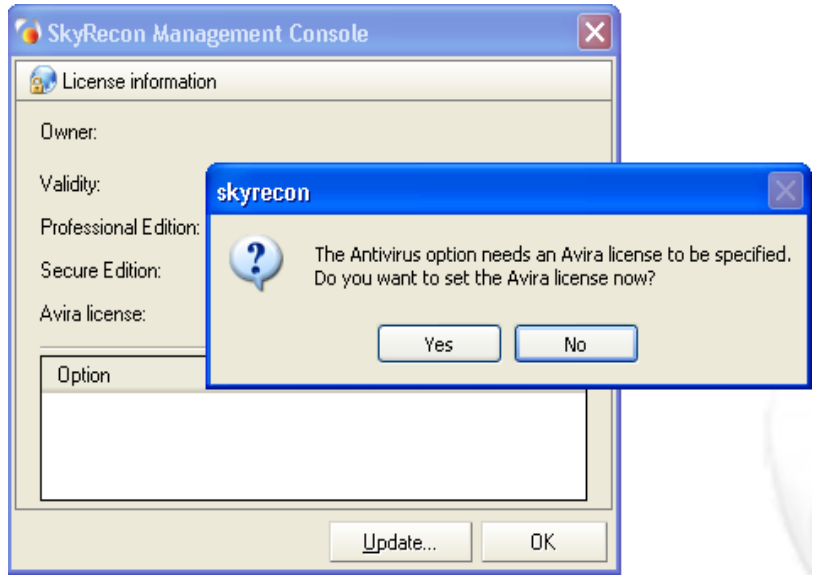


5. To enable your StormShield license, click **Open**.

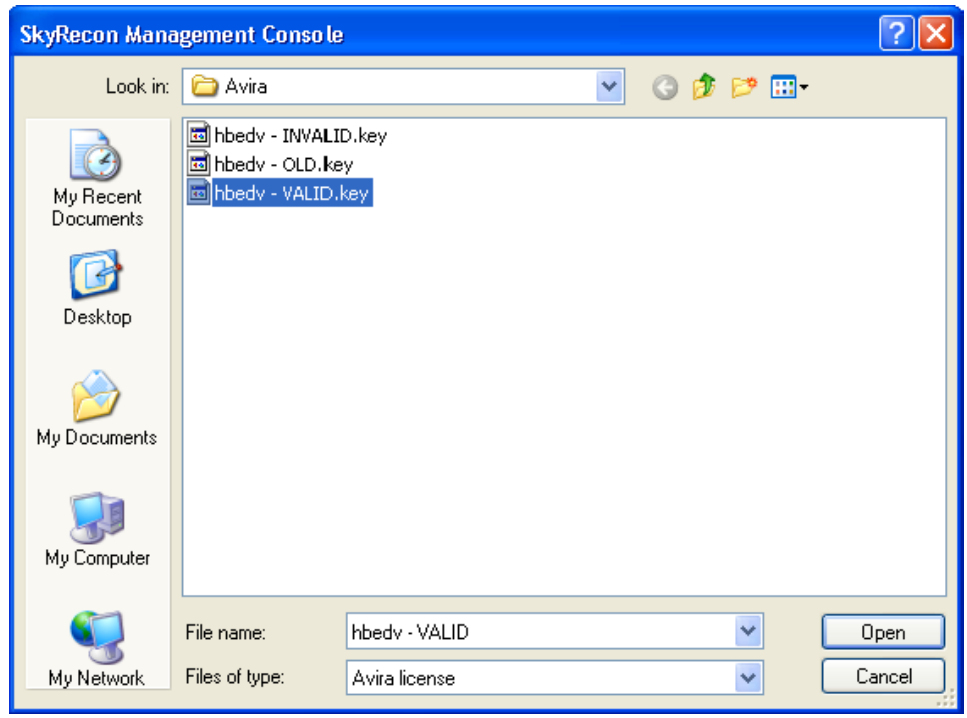


6. If you have not purchased the **Antivirus** option (blank field), click OK and go directly to step 9.

7. If your StormShield license includes the **Antivirus** option, a window is displayed to select the Avira license file.
Select **Yes** to proceed.

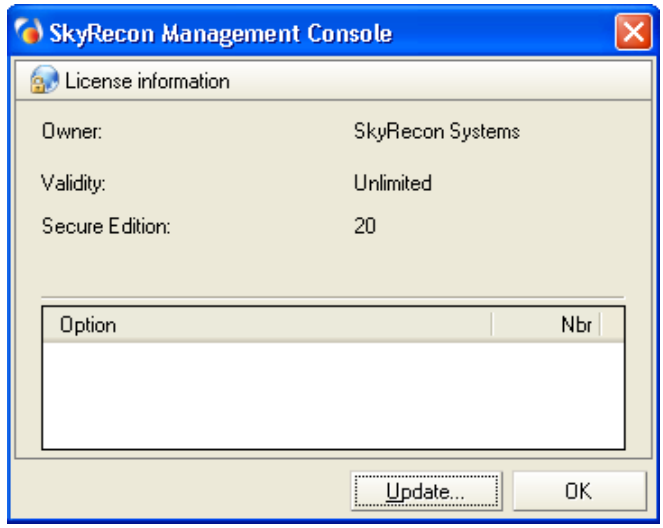


8. Select the Avira license and click **Open**.

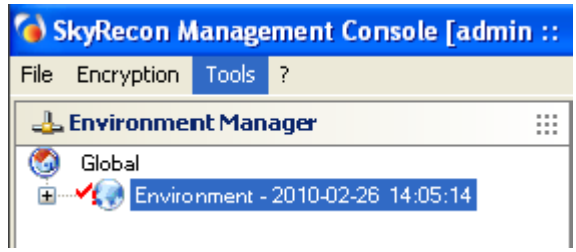


9. To complete the update:
   - **With** the Antivirus option, click **OK**:

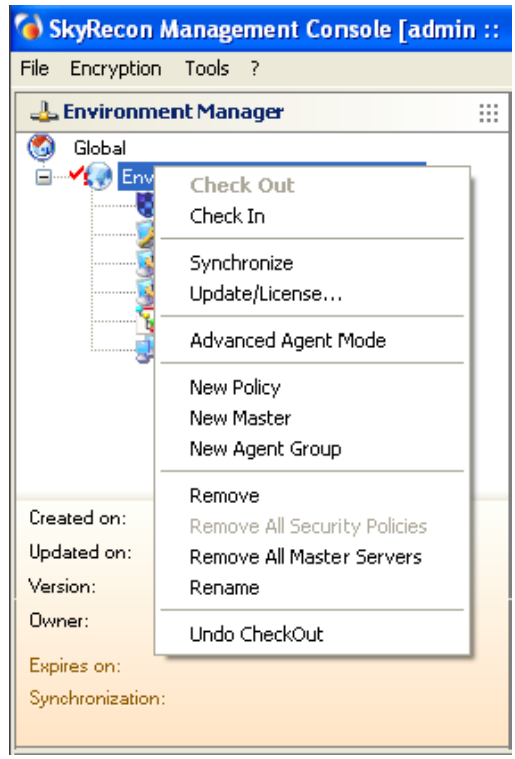
   - **Without** the Antivirus option, click **OK**:



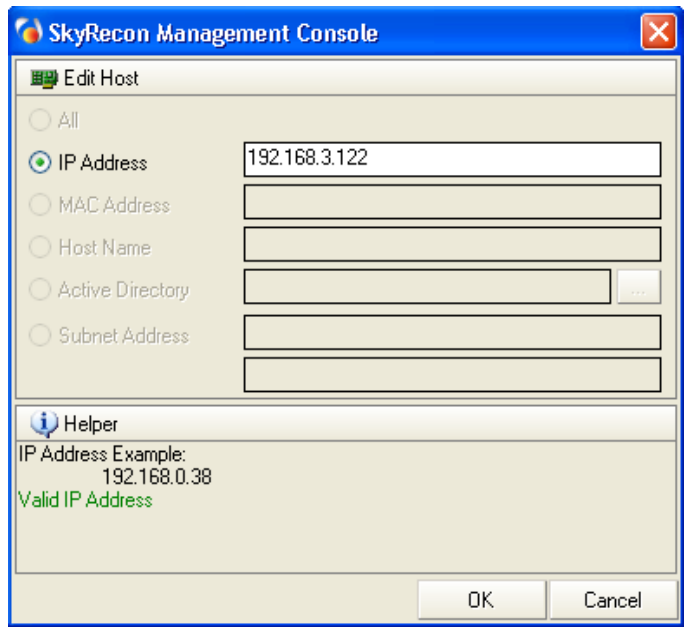
The environment that you have just created is displayed as follows:



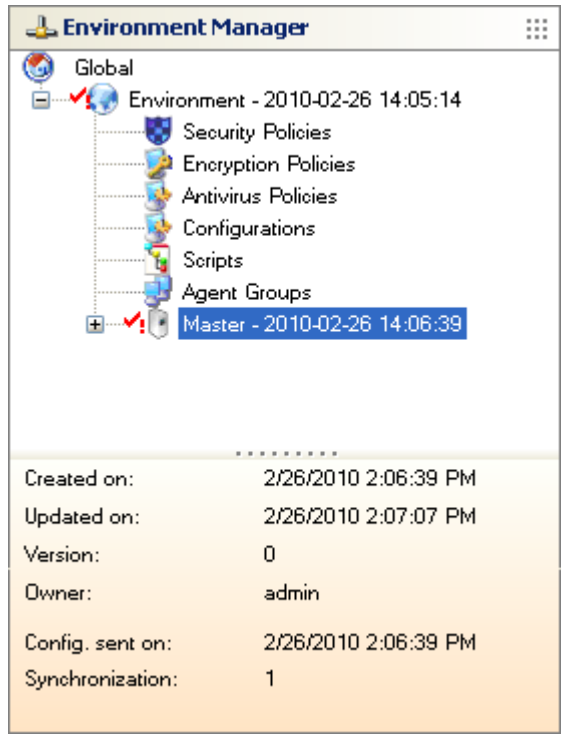
10. Now add a new StormShield master server: To do so, he must follow the steps below:
    - Click **New Master**.



    - Enter the master server IP address and click **OK**.



The master server that you have just created is displayed as follows:



Installing the agent

Downloading the agent from the Web server

Downloading the StormShield agent from a Web server is the default deployment mode when no other remote deployment tool is available.

In this mode, the agent installer is downloaded and run manually from each client workstation.

The access address for this page is the Web server IP address as entered when the server was installed. If port 80 by default has been changed, you need to specify the port assigned as a suffix to the IP address in the web browser address field.

Installation

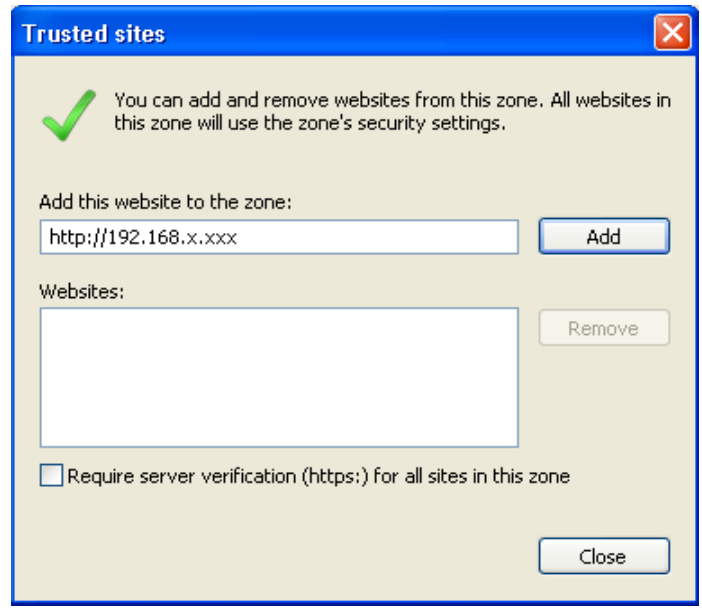
Before installing an agent, the administrator must have:

- Created at least one agent group.
- Applied a configuration and a security policy to the agent group.
- Associated the agent group with the master server.
- Performed a synchronization.

The agent installer can be run directly from the Web page or stored locally for a later installation.

This is a silent procedure, therefore no particular information is requested during agent installation.

If you wish to download the installation `.msi` file of the **StormShield Server-Side Edition** agent with Internet Explorer, you must add the StormShield server IP address to your **Trusted sites**.



A message is displayed in a pop up window above the system tray when the installation is completed. The computer must be rebooted to activate the agent.

Since this installation mode must be repeated on each client workstation, it is mostly used for testing and pilot environments.

You must use the **Administrator** account to install the StormShield agent. If you install the agent with any other account, the installation will start but will not finish properly.

StormShield agent installation directory

The agent can be installed in a directory other than the directory used by default, that is:

```
c:\Program Files\SkyRecon\StormShield Agent\
```

Changing the StormShield agent installation path

To change the agent installation path, follow the steps below:

1. On the server side, open the following file:

   ```
   [program files]\SkyRecon\StormShield Server\Apache\cgi-bin\msi.nsi
   ```

   Locate the following line:

```
;;WriteINIStr '$TEMP\sky.tmp\sky.cnf' Agent Install_path 'C:\Program
Files\company'
```

2. Remove the comments (`;;`).

   Replace `C:\Program Files\company` with the target installation path `[custom path]`.

   If the line is commented, the default value `%program files%\SkyRecon` will be used.

3. Save the file.
4. Run `[program files]\SkyRecon\StormShield Server\generate_msi.exe`.

   The StormShield agent will be installed in the custom path. The path will resemble: `[custom path]\StormShield agent\`.

Using GPO to deploy StormShield agents

Active Directory® Group Policy Objects (GPO) are used to deploy applications using the Microsoft Windows Installer service. This is a silent procedure as no particular information is requested from the user during installation.

Remote deployment using GPO requires a specific file format called `MSI`. This type of file can be used to perform remote installations without user intervention.

The `MSI` file is located in the `files` subfolder of the server installation directory that is by default:

```
c:\Program Files\SkyRecon\StormShield Server\Apache\cgi-bin\files
```

System cloning tools are not compatible with the **Secure Edition** agents.

Before creating the system image, check that there is no certificate file (`agent.srn`) in the StormShield agent installation directory.

DOWNLOADING CERTIFICATES

To secure communication between StormShield components (console, server and agent), each component uses its own certificate.

Each agent must have a unique certificate to securely communicate with the server.

When an agent has just been installed on a workstation, no certificate is provided for the StormShield agent instances. They need to obtain a certificate for communicating with the StormShield server.

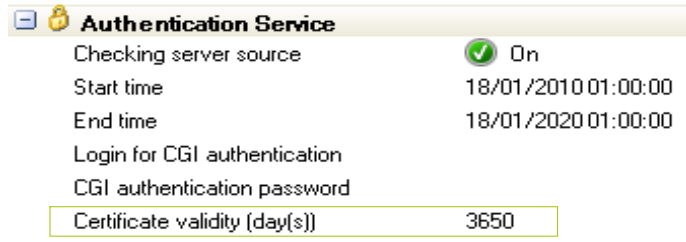
For this purpose, a certificate server is installed on the StormShield server which is accessible by default through TCP port 443.

For more information on how to configure, uninstall the agent or deactivate protections, see "StormShield Agent Configuration", page 205.

CERTIFICATE VALIDITY PERIOD

For security reasons, downloading certificates should be restricted to a limited time period, usually the time necessary to deploy the StormShield agent instances on the network.

The certificate time period can be configured on the SkyRecon management console by selecting a master server in the Environment Manager tree.
The configuration options are displayed in the interactive panel on the right. The parameter Certificate validity day(s) is under **Environment Manager > Master server > Authentication service**.



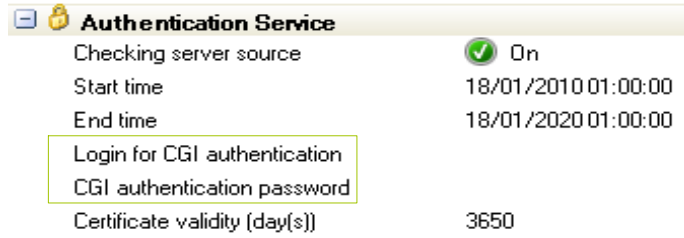
By default, the certificate time period is limited to **10 years** from the console installation date.

Change the value of the certificate availability **End Time** if you prefer a shorter period.

LOGIN AND PASSWORD FOR DOWNLOADING CERTIFICATES

It is possible to define a login and a password to allow an administrator to download certificates from a web page.

To do so, use the fields **Login for CGI authentication** and **CGI authentication password**.



To download a certificate, point your web browser to:

```
https://<Server IP address>/ssl/cgi
```

On the certificate server authentication page, enter the user login and password.

If authentication is successful, a dialog box opens to download the file named `agent.srn`. This file must be copied into the agent installation folder.

COMPATIBILITY WITH SYSTEM CLONING TOOLS

The StormShield agent is compatible with system cloning tools.

System cloning tools are **not** compatible with the StormShield Secure Edition agents.

To create a disk image of a system containing the agent, install the agent on the principal system as shown in "Installing the agent", page 116.

Each agent requires a unique certificate. The installation of an agent on the master workstation must not include its certificate.

To prevent this, in the **Authentication Service** parameter of the SkyRecon management console, we recommend that you define an invalid date before the creation date of the master.

Before creating the master image, you must check that the StormShield agent installation directory contains no:

- `agent.srn file`
- `host_guid.sro file`
- file in the `vfs` directory.

If this is not the case, you must delete these files.

The **Authentication service** parameters are available under Environment Manager > [Master server] in the StormShield server configuration parameters.

When clone systems are deployed, reset the period of availability of the Authentication Service to allow each StormShield agent to retrieve its own certificate.

POST-INSTALLATION TESTS

COMPONENT TESTS

It is recommended to test all StormShield components after product installation.

Follow the steps below to test the whole StormShield operating sequence:

1. Identify a target machine through the network description.
2. Define a simple and easily testable configuration.
3. A simple configuration example consists in preventing the NotePad application from opening any text file with a `.txt` extension.
   For more information, see "Rule-Based Protection", page 281.
4. Send the configuration (and deploy the agent on the target machine if this has not already been done).
5. Check that the rule set out is applied on the target machine.
6. Check access to the events stored in the database.

Should a problem arise, see "Troubleshooting", page 675.

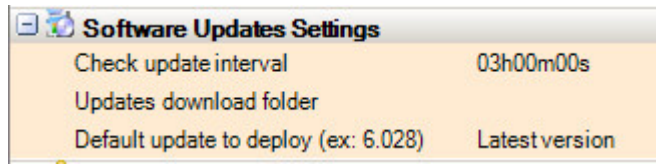
UPDATING COMPONENTS

GRAPHICAL INTERFACE

StormShield offers several ways to retrieve and apply software updates to its components.

The update mode can be configured from the SkyRecon management console and the master server via **Environment Manager > [Master server name] > Software Updates Settings**.

The parameters for updating StormShield components are the following:



- **Check update interval**:

  This is a period of time (example: 03h00m00s) to check if there are any new updates to the StormShield server or console.

- **Updates download folder**:

  This is the path where the updates are located. You need to create in this folder a file named version.sro which only contains the version number of updates to download, under the format “6.028”.

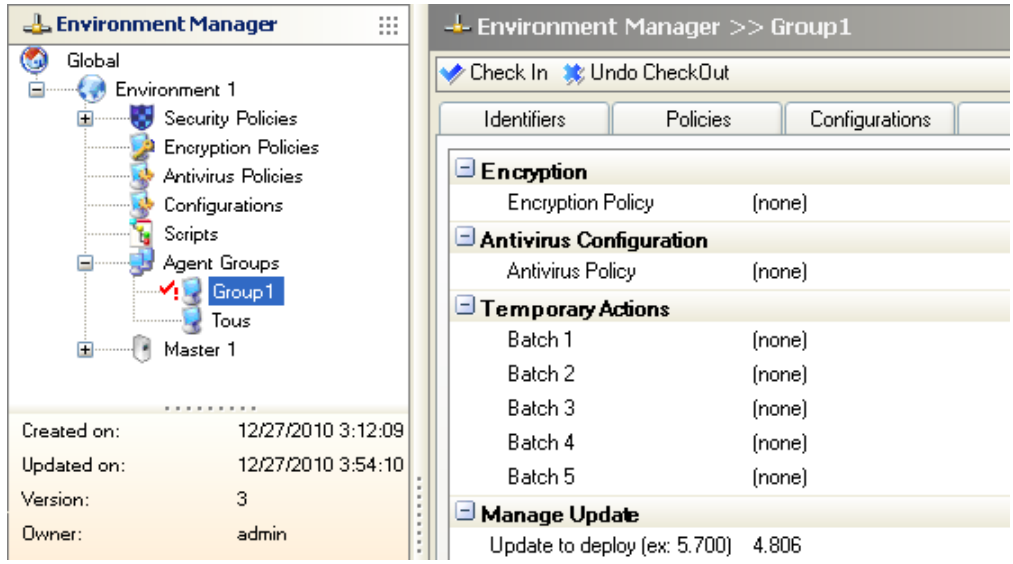
- **Default update to deploy (e.g.: 6.000)** :

  This is the maximum number of the StormShield version applied to the agents.

  If you do not wish to use this parameter, select **Latest version**. Agent groups will automatically be updated to the latest StormShield version.

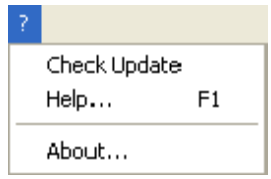
  If you wish to use a specific version, the agent group which has been assigned a specific version will not be updated above the version defined in Default update to deploy (ex.: 4.806).

Example: The limited version assigned to agent group **Group 1** is version 4.806.



On-demand updates

The console can be updated on demand using the menu option ? > **Check Update**.



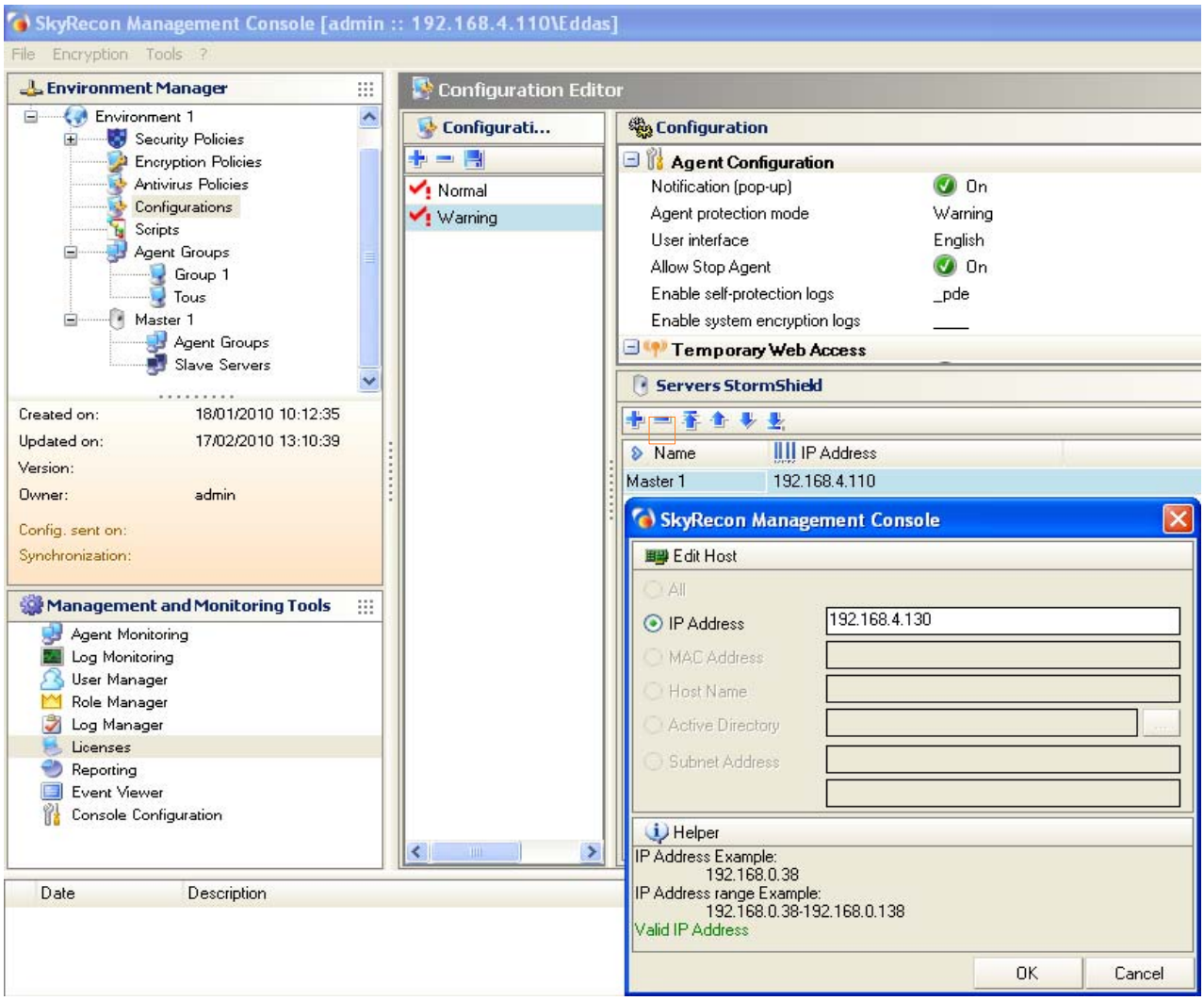
POSSIBLE CHANGES

CHANGING THE STORMSHIELD SERVER IP ADDRESS

After installing and configuring StormShield, you may at some point need to change the IP address of your master server and update the StormShield agents accordingly.

To do so, he must follow the steps below:

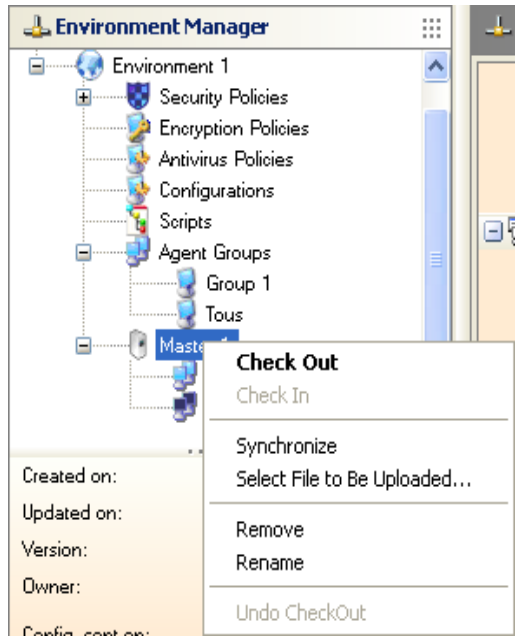
1. Edit all StormShield agent configurations in the Configuration Editor:
   - Click **Configurations** in the Environment Manager.
   - Click ✚ in the **StormShield Servers** panel.



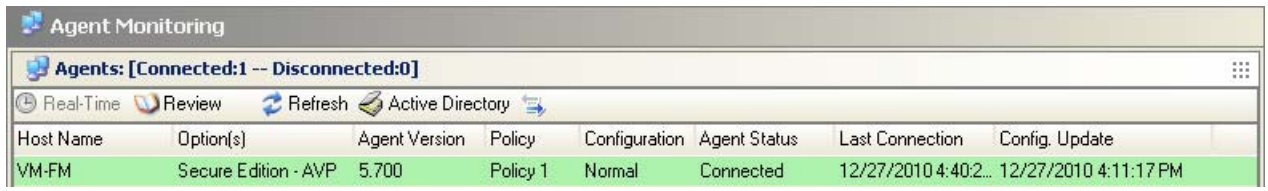
   - Add the new IP address.

2. Send the new configuration to update the agents with the new IP address of the master server.

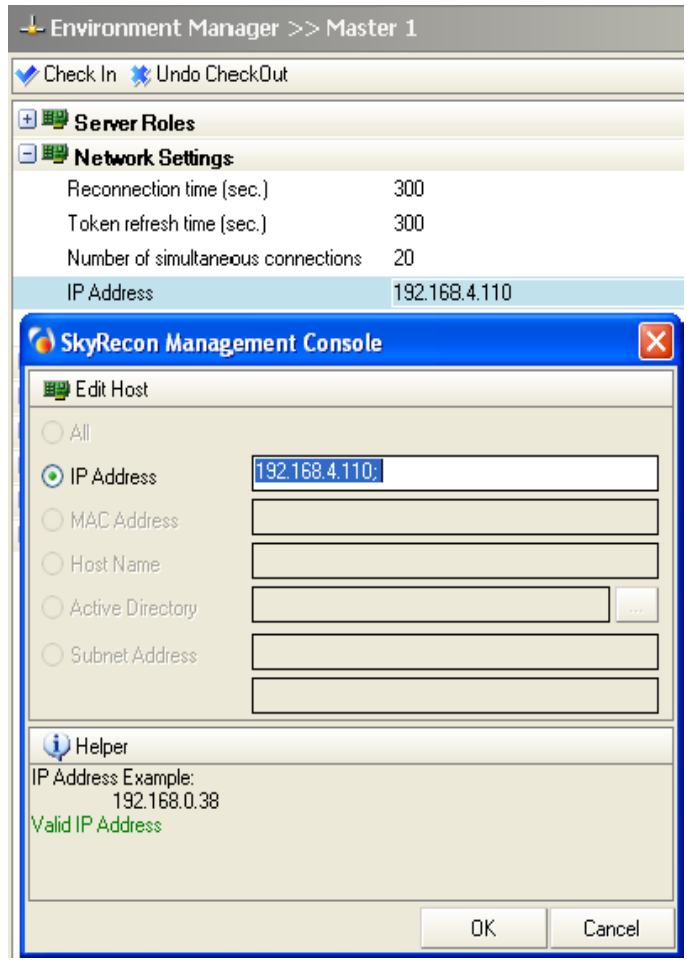
   To send a new configuration, right-click **Synchronize**.



3. heck under **Agent Monitoring** that the new configuration has been properly applied to the agents (Example: Config. Update).



4. Once the agents have been updated:
   - Delete the old IP address for each configuration in the **Configuration Editor**.
   - Replace the old IP address with the new one in **Environment Manager > Master server > Network Settings**.



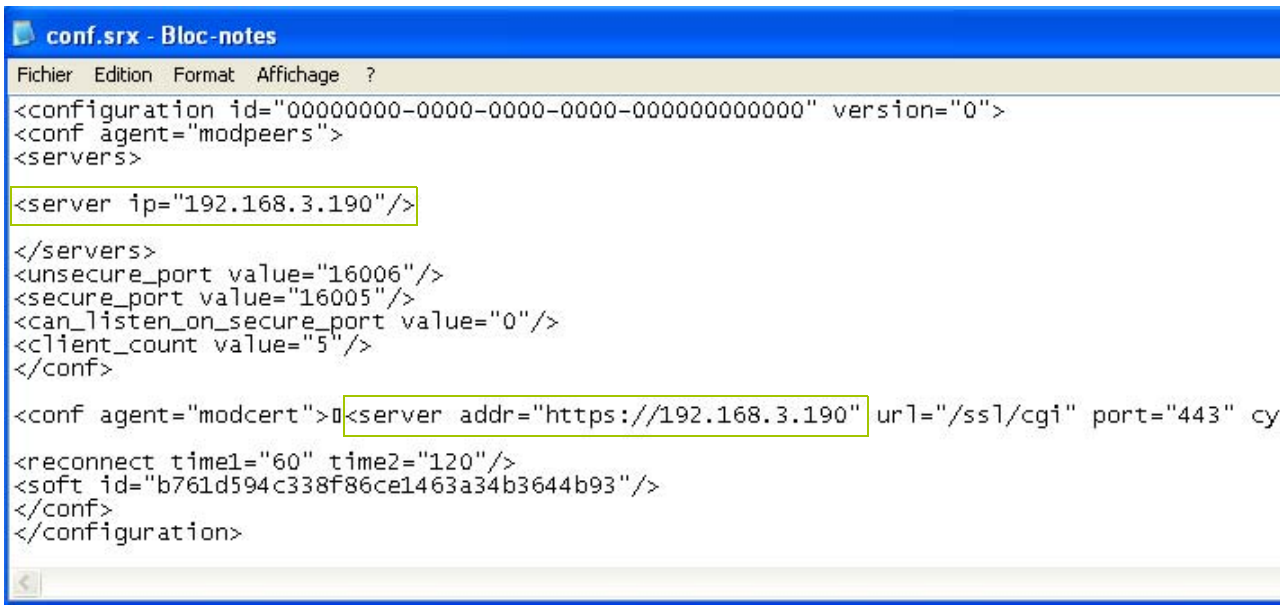
5. Change the server IP address on the network card.
6. Send this configuration from the master server to update the agents with the new IP address of the master server and remove the old IP address.
7. If an MS SQL server is installed on the StormShield server, you must restart the server immediately.

After updating the master server and the agent IP addresses, you will need to update the **agent installer** so that new agents can use the new IP address.

To do so, follow the steps below:

1. Go to the installation directory of the primary server.
2. Update all references to the IP address in the following file:

   `[install directory]\Apache\cgi-bin\conf.srx`



3. Double-click the following file:

   `[install directory]\Generate_msi.exe`

   The installer has been updated, you can now download new agents from the Web server.

CHANGING THE SERVER TCP PORTS FOR HTTP AND SSL SERVICES

To modify the server TCP ports for HTTP and SSL services (after installation), follow the steps below:

1. After installing the server, you can change the two TCP ports used for the HTTP/SSL server by editing the following server files:

   `C:\Program Files\SkyRecon\StormShieldServer\Apache\conf\httpd.conf`

   `C:\Program Files\SkyRecon\StormShield Server\Apache\conf\ssl.conf`

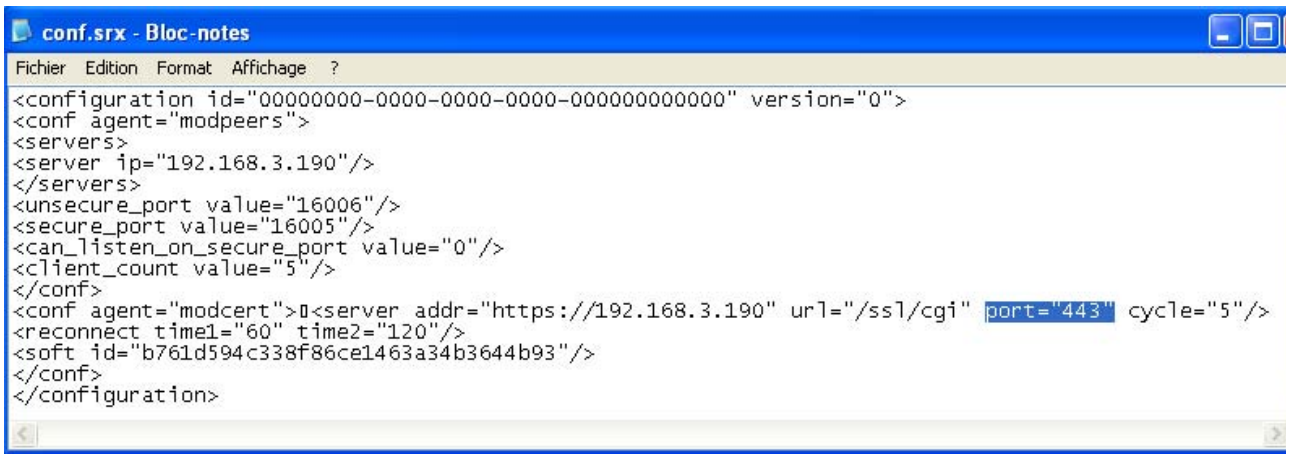
2. In the `httpd.conf` file, change the port values assigned to **Listen** and **ServerName WebServer** (default port is 80).
3. In the `ssl.conf` file, change the port values assigned to **Listen**, **ServerName WebServer** and **VirtualHost** (default port is 443).
4. Restart the server.

Now, you must update the agent installer for it to take into account the new TCP ports of the server.

1. Go to the installation directory of the primary server.

   `C:\Program Files\SkyRecon\StormShieldServer\Apache\cgi-bin\`

2. In the `conf.srx` file, change the TCP port value (default port is 443).



3. Double-click the following file:

   `[install directory]\Generate_msi.exe`

   The installer has been updated, you can now download new agents from the Web server.

UNINSTALLING COMPONENTS

UNINSTALLING THE SERVER AND THE CONSOLE

The SkyRecon console and the StormShield servers can be uninstalled using the uninstall tools accessible from:

- The **Start** menu on the systems that host these components.
- The Windows **Add/Remove Programs** service accessible via the Control Panel.

UNINSTALLING THE AGENT

The StormShield agent can be uninstalled using the program file `SRend.exe` located in the installation directory.

The default path for the uninstaller is:

```
C:\Program Files\Skyrecon\StormShield Agent\Srend.exe
```

This is a silent procedure, without any user intervention. Each workstation must be rebooted after file removal.

If the agent was installed by remote deployment using GPO, you can also use this same tool to uninstall the agent silently.

You need to be an Administrator of the computer to uninstall the agent.
The **Stop Agent** parameter must be set to Allowed in the **Agent Configuration** to proceed with the uninstallation.

To uninstall the agent from a workstation, first disable the protection against executable file creation.

If you have purchased the **StormShield Secure Edition**, the user must restart the system twice in order to:

- Decrypt files.

  Decrypt data at uninstallation and End/Start date of allow uninstall must be configured in the master server configuration parameters.

- Uninstall StormShield after all files are decrypted.

REMOVING THE DATABASES

The MS SQL Server 2005 database is uninstalled using the Windows **Add/Remove Programs** service or the database installer.

The database must be removed before uninstalling the console.

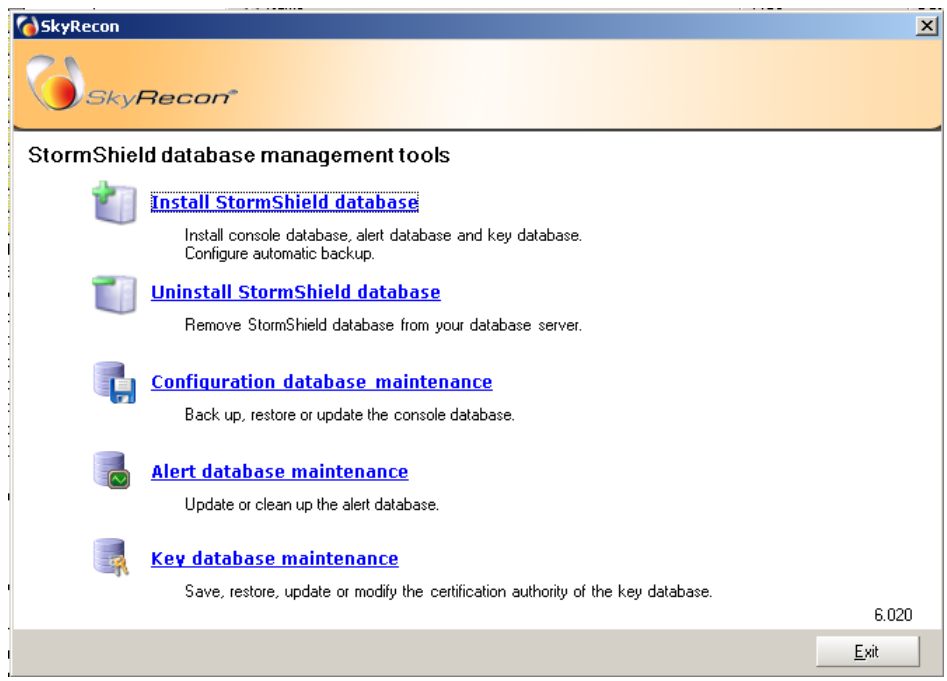
If you uninstall the console before removing the database, DBInstaller will be uninstalled and you will no longer be able to remove the database.

To remove the database, follow the steps below:

1. Go to `Start>All programs>SkyRecon>DBInstaller`.

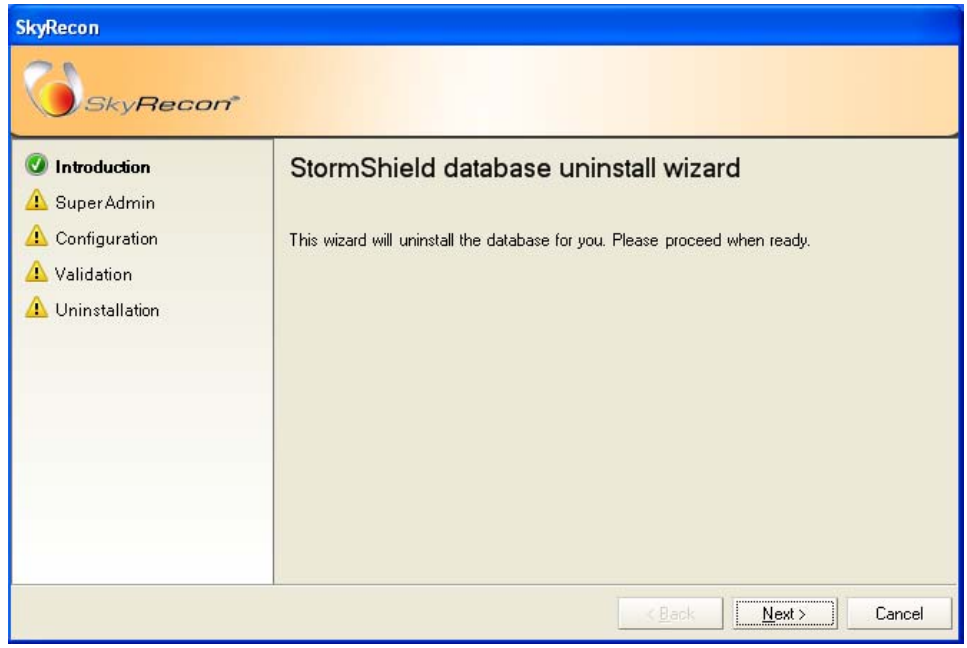
   The database management tools window opens.

2. Click **Uninstall StormShield database**.



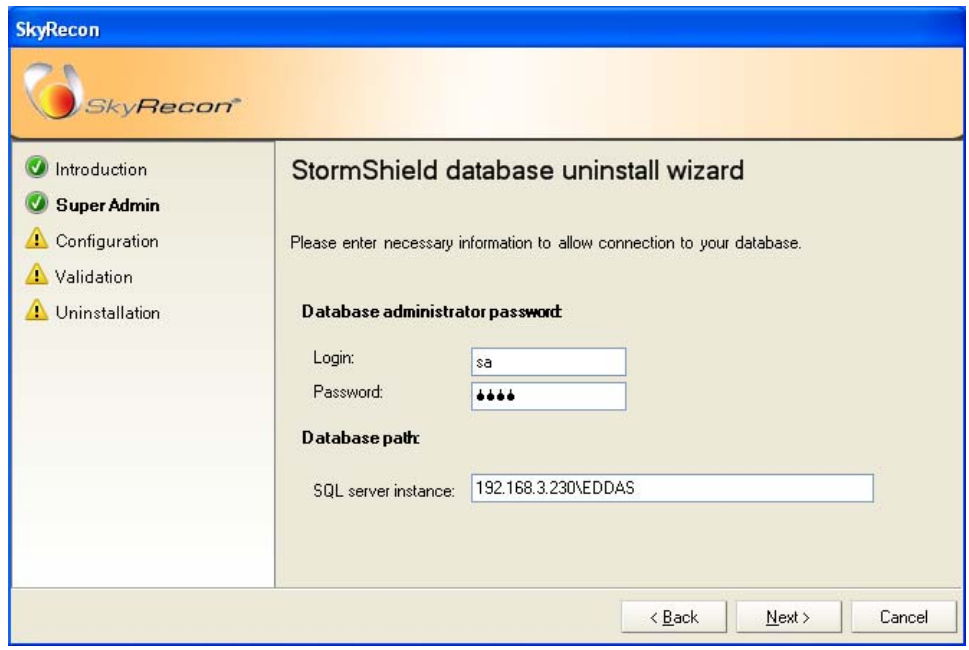
3. The following window is displayed.

   Click **Next**.



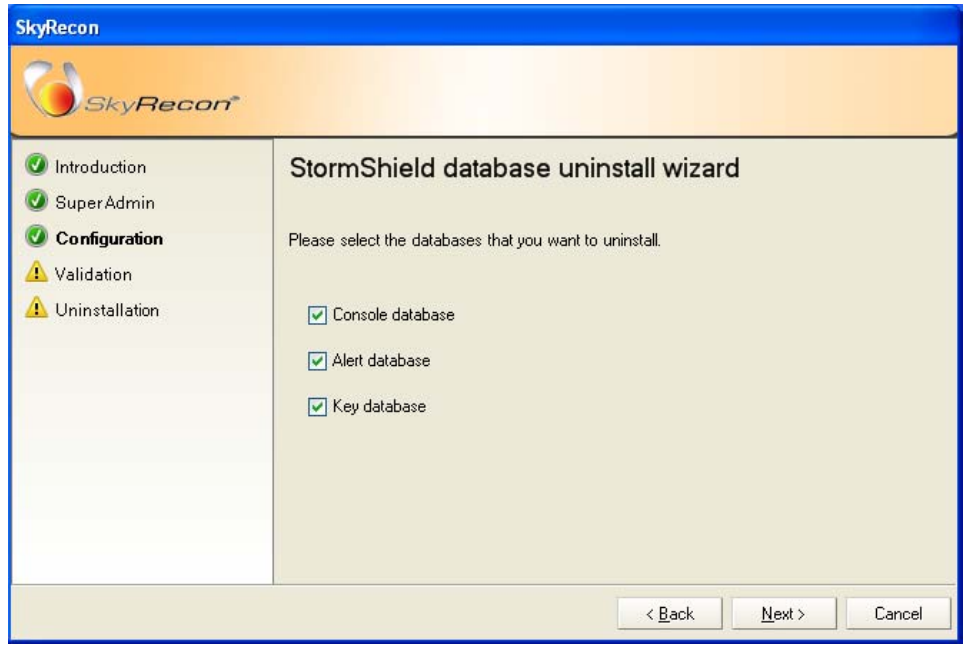
4. Enter the SuperAdmin information to connect to the database:
   - The SuperAdmin login.
   - The SuperAdmin password (by default `sa`).
   - The database path.

   Click **Next**.



5. Select the databases to be uninstalled.

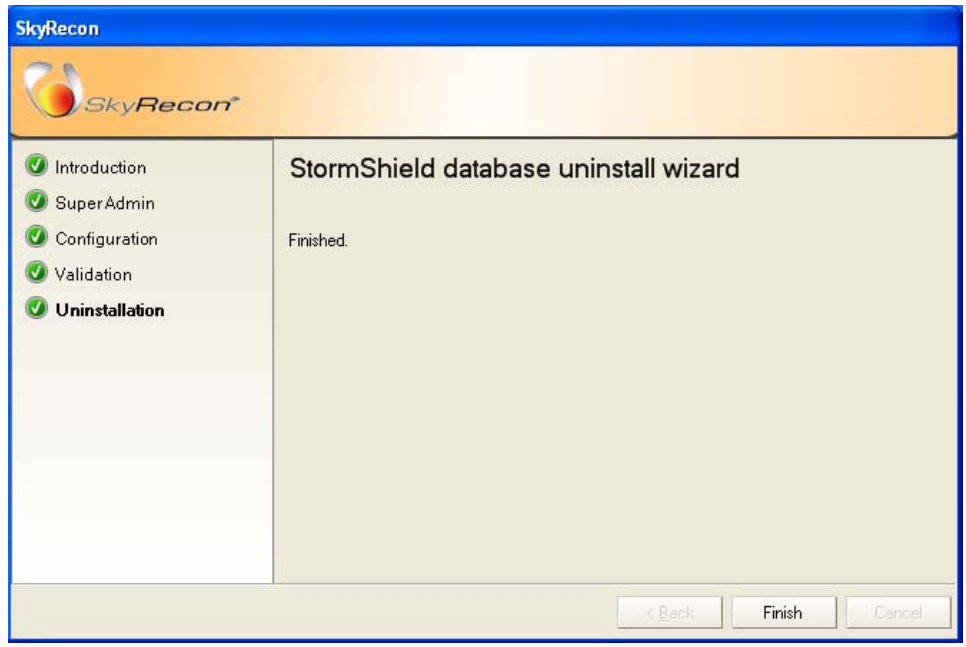
   Click **Next**.



6. Before starting the uninstallation process, check the information displayed.

   Click **Next**.

7. The uninstallation process is finished.



Chapter 3

UPDATING STORMSHIELD

ABOUT THIS CHAPTER

This chapter describes the StormShield updating procedures:

- With MS SQL Server 2000 on your workstation:
  - Recommendations.
  - Procedure.

- With MS SQL Server 2005 on your workstation:
  - Prerequisites.
  - Procedure.

WITH MS SQL SERVER 2000

RECOMMENDATIONS

If your database server belongs to the MS SQL Server 2005 or MS SQL Server 2005 Express Edition type, go directly to "With MS SQL Server 2005", page 152.

It is highly recommended to save your database before updating StormShield.

If your database server belongs to the **MSDE** or **SQL Server 2000** type, you must first save your database. To start the procedure, go to "Procedure", page 141.
Afterwards, you will be able to uninstall the database server and finally migrate your database to MS SQL Server 2005 or MS SQL Server 2005 Express Edition.

In version 5.2, the StormShield database includes:

- The Console database.
- The Alerts database.
- The Keys database.

Direct updating to version 6.0 is only possible from a version 5.2.x.

In order to update StormShield from an earlier version, you must first update to version V4.8.

To update StormShield from a version earlier than version 6.0, you have to save your database.
Then, you will be able to uninstall your database server.

PROCEDURE

When using a version lower than 4.5.10, see Updating procedure (version 5.2) on our extranet site.

Saving the StormShield database

Saving the Console database

To save your Console database, follow the steps below:

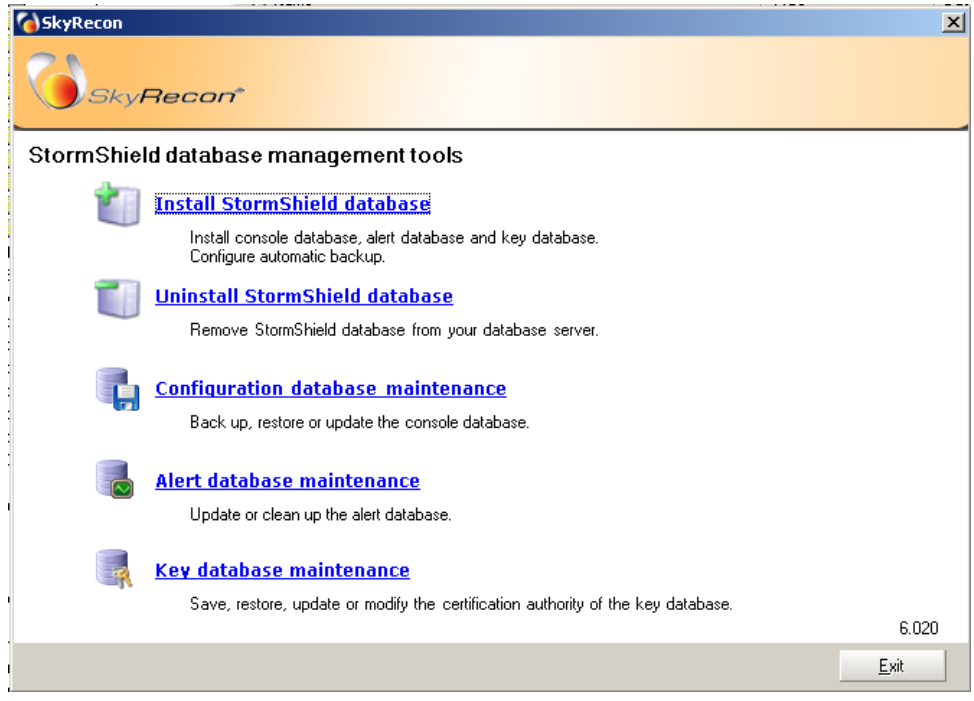
1. Close the SkyRecon management console.
2. Launch `DbInstaller.exe` located by default in:

   `C:\Program Files\Skyrecon\SkyRecon Management Console\DBInstall`

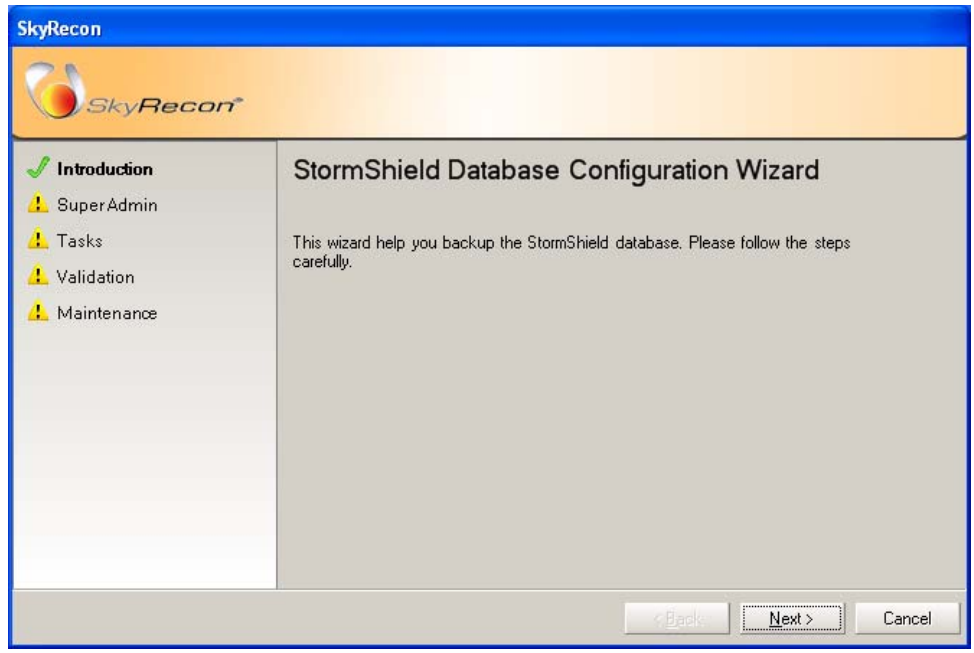
   `DbInstaller.exe` is directly accessible from the **Start** menu.

   `DbInstaller.exe` is represented by the icon .

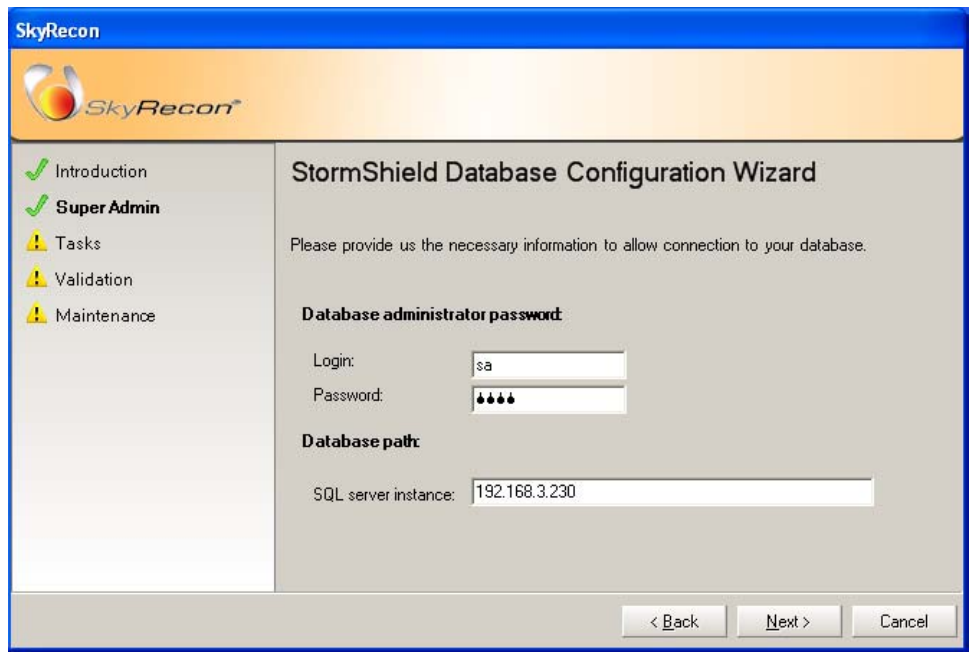
   This will start the StormShield database management tool.
3. Select **Configuration database maintenance**.



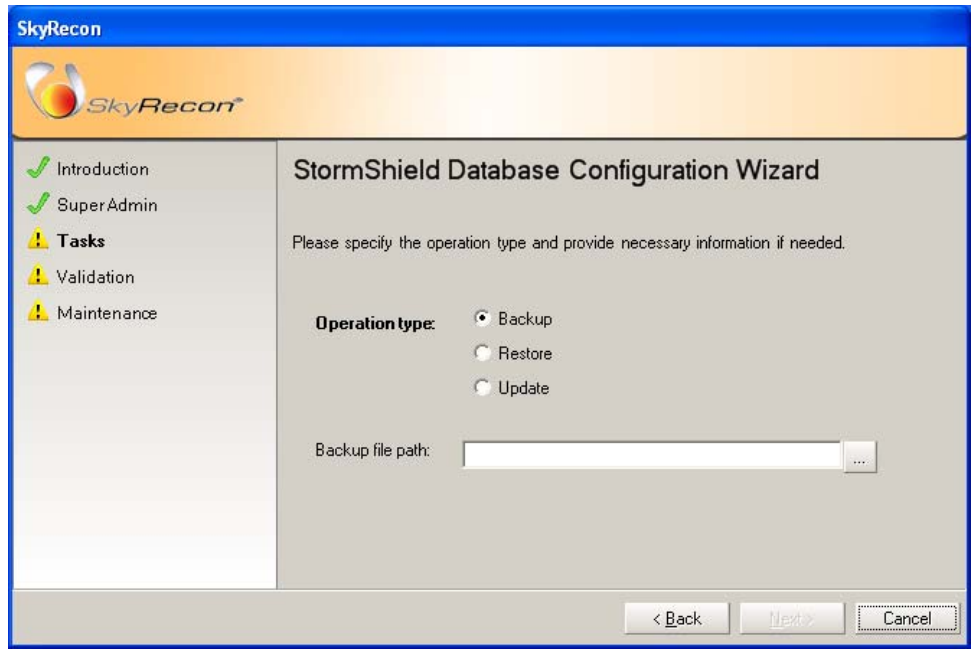
4. Click **Next** to open the window that establishes connection to the StormShield database.



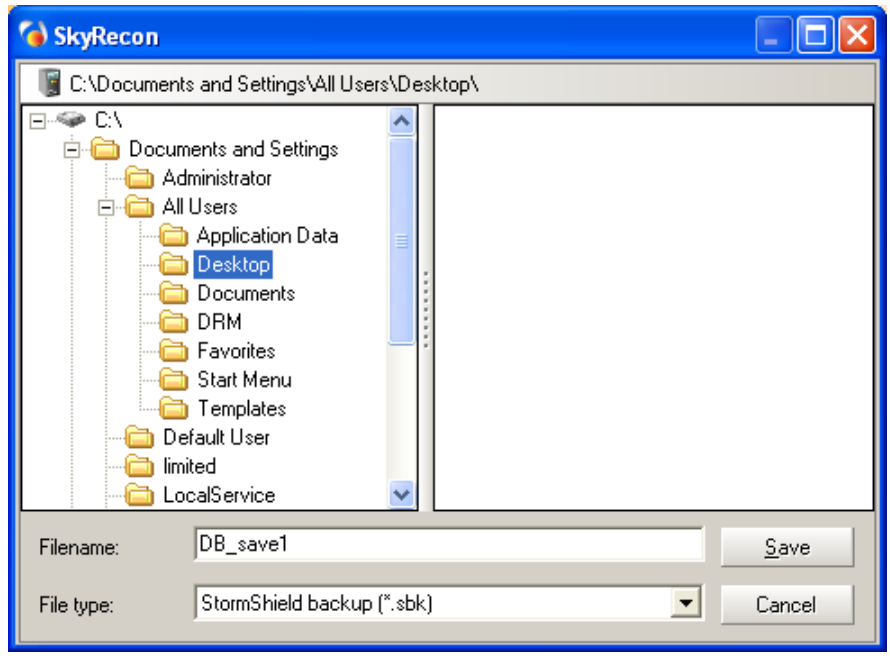
5. Enter:
   - The system administrator login and password used to establish a connection to the database server (**sa** account).
   - The database instance.
   - Click **Next**.



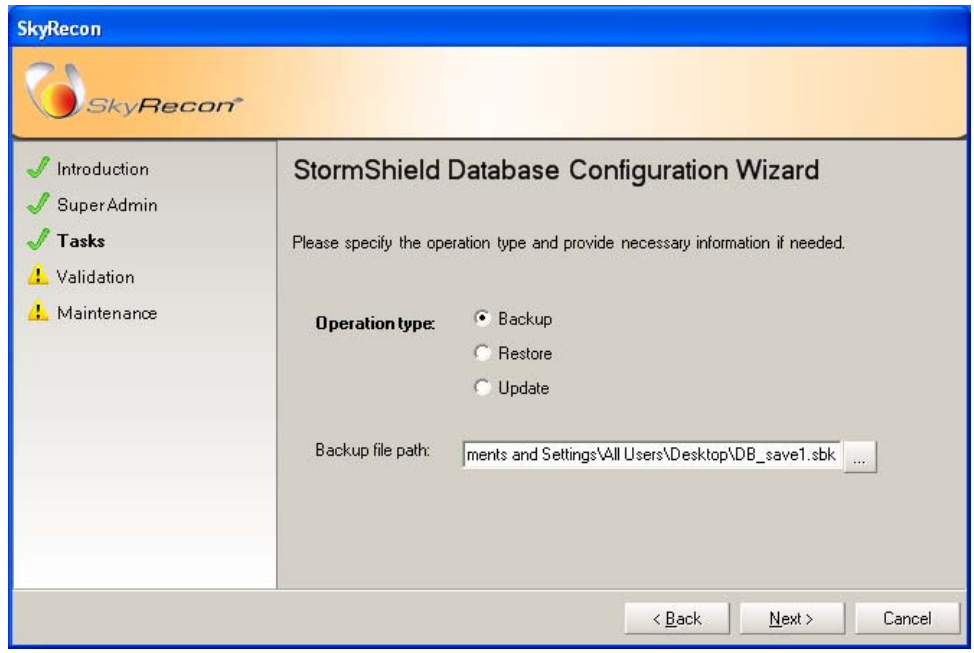
6. Below Operation type, click on the **Backup** radio button.



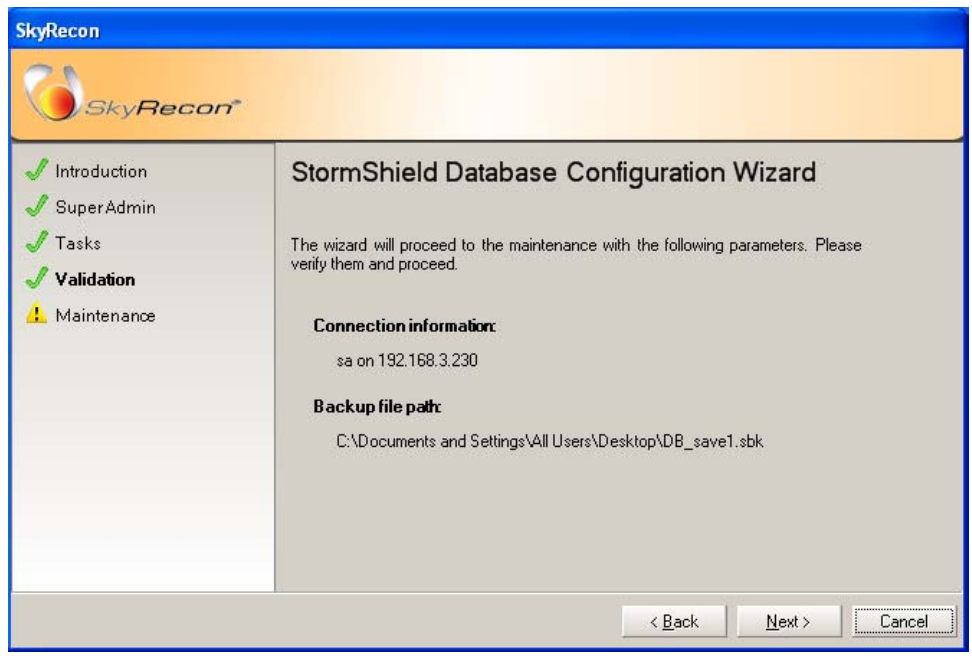
7. Click ... to select the backup filepath and enter a backup filename.
Click **Save**.
The backup will be saved on the machine that hosts the database.



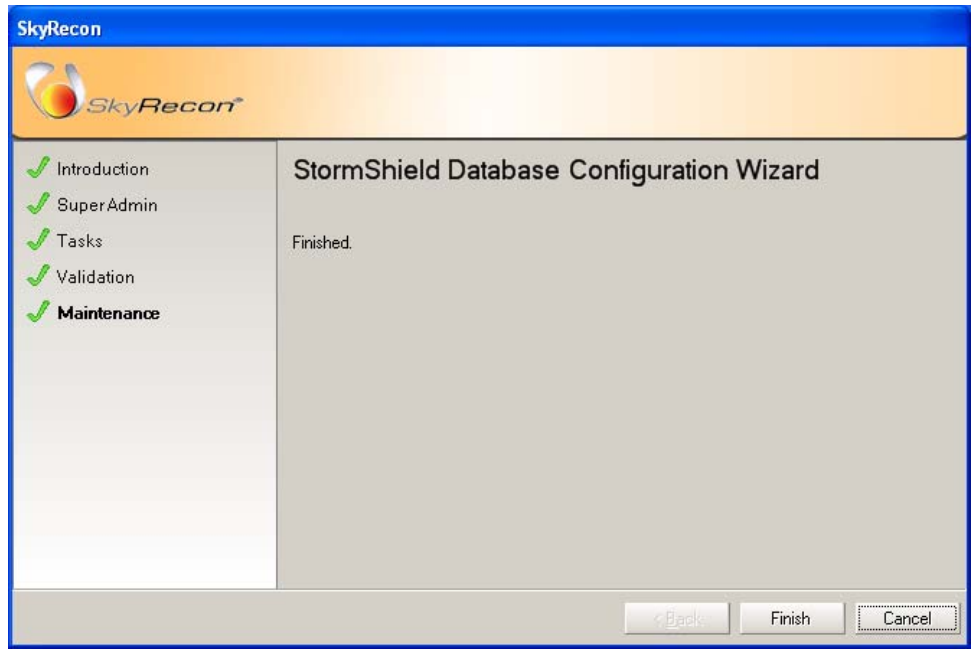
8. Click **Next**.



9. A summary is displayed.
Click **Next**.



10. Click **Finish** to complete the backup.



Saving the Keys database

To save your Keys database, follow the steps below:

1. Launch **DbInstaller**.
2. Click **Keys database maintenance**.
3. Repeat Steps 1 to 9 in "Saving the Console database", page 141 and rename the backup file.

Saving the Alerts database (logs)

This operation is optional. It requires the SQL Server management tools.

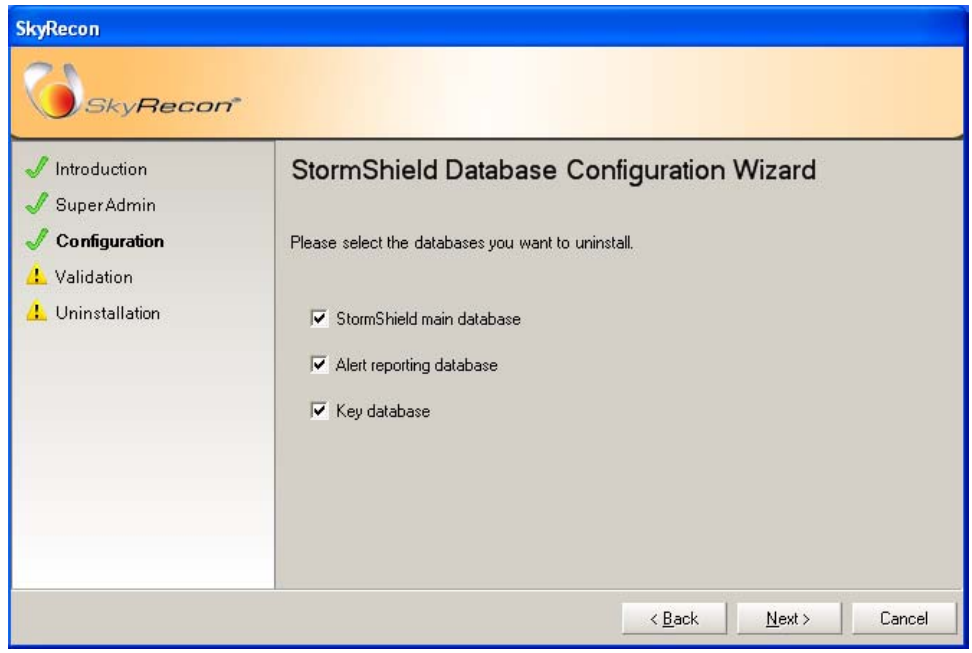
For more information, contact your DataBase Administrator or our Professional Services at `support@skyrecon.com`.

Uninstalling the StormShield database

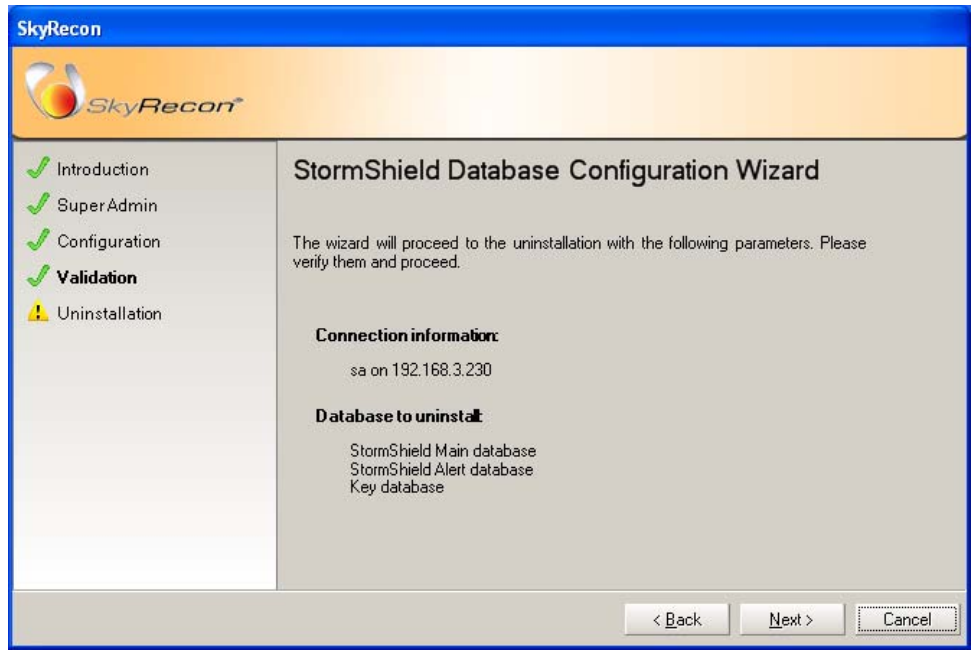
To uninstall your StormShield database, follow the steps below:

1. Launch **DbInstaller**.
2. Click **Uninstall StormShield database**.

3. Select the databases that you wish to uninstall.
Click **Next**.



4. A summary is displayed.
Click **Next**.



5. Click **Finish** to complete the uninstallation process.

Uninstalling the StormShield database server

To uninstall the database server (MSDE or SQL Server 2000), use the uninstalling tools accessible from:

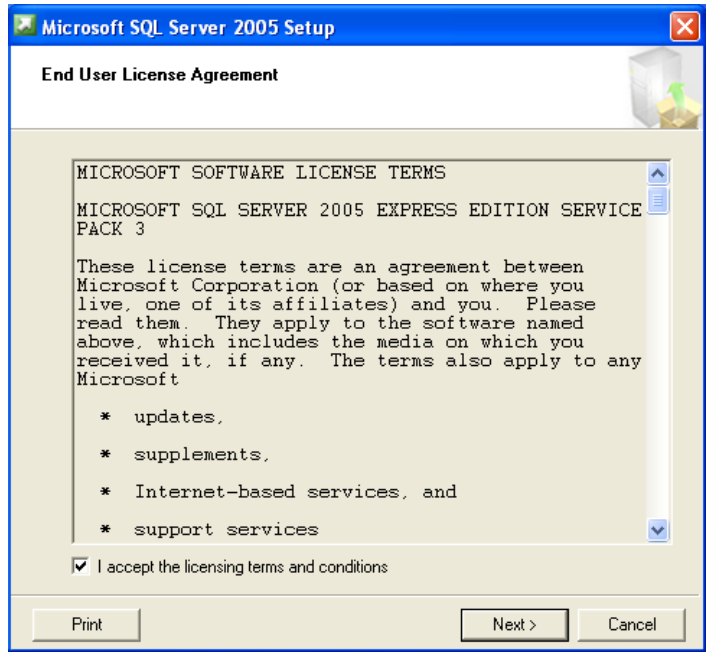
- The **Start** menu in the server software.
- The **Add or Remove programs** service in Windows accessible from the Control Panel.

Installing the new StormShield database server

First of all, check that the `SQLEXPR.exe` (MS SQL Server 2005 Express Edition) file and if required, the `SSMSEE.msi` file (Advanced Services for MS SQL Server 2005 Express Edition) are on your workstation.

To install MS SQL Server 2005, follow the steps below:

1. Click `SQLEXPR.exe`.
2. The window below is displayed.



3. Define the settings for the new database server.

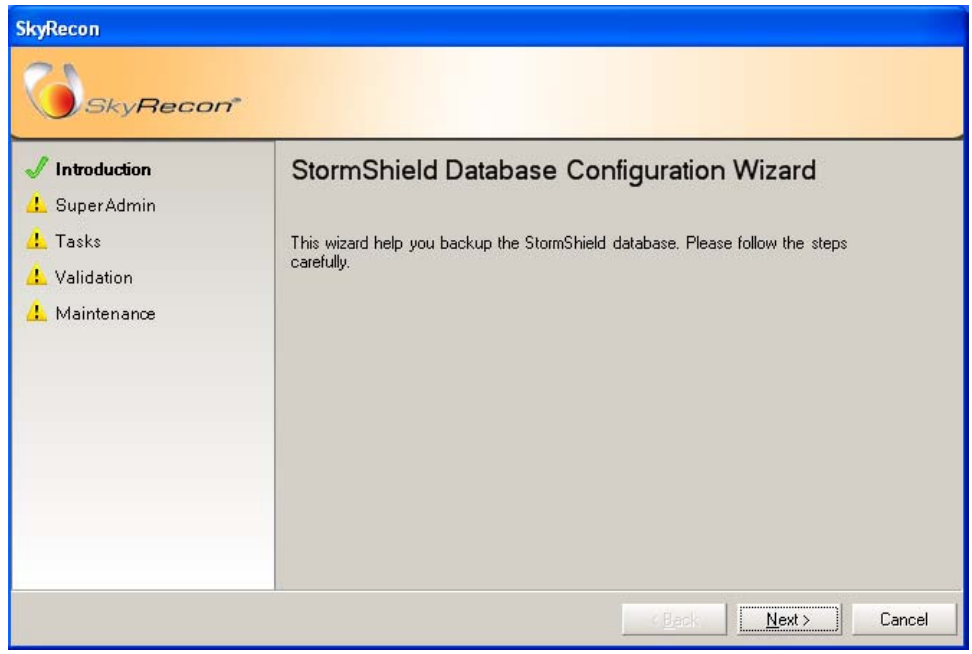
When installing the database, use the **Mixed Mode** authentication mode.

Restoring the StormShield database

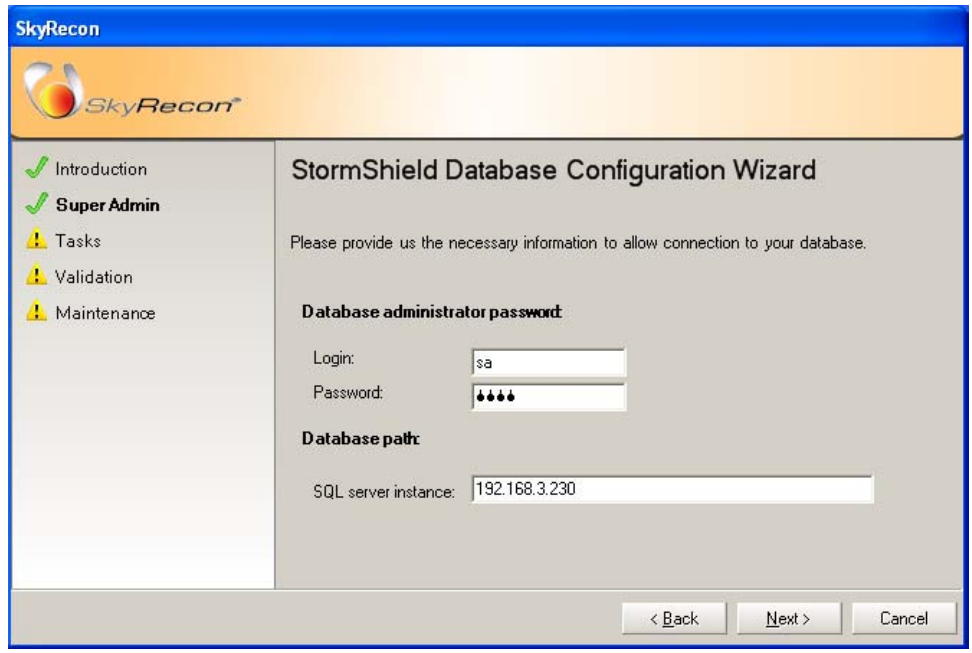
Restoring the Console database

To restore the Console database, follow the steps below:

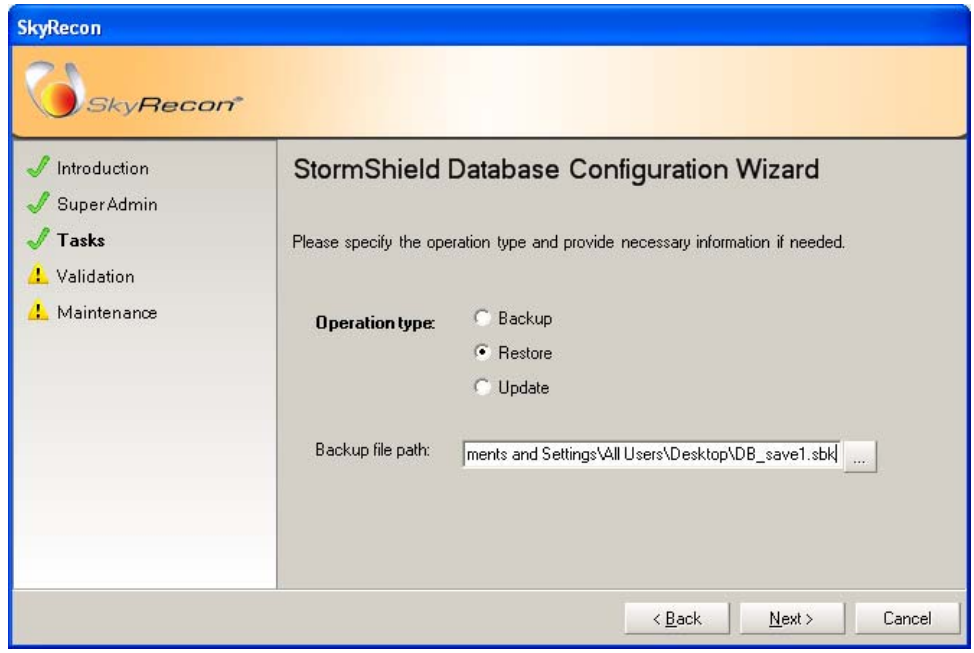
1. Launch **DbInstaller**.
2. Click **Console database maintenance**.
3. Click **Next**.



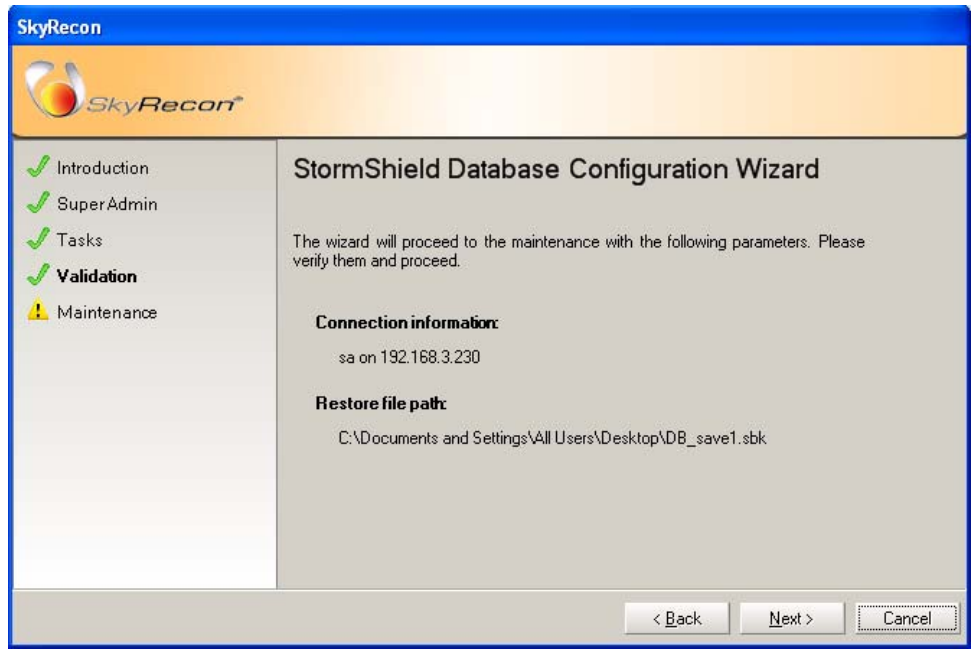
4. Enter the required information and click **Next**.



5. Below Operation type, click on the **Restoration** radio button.
   Click ... to select the path and the name of the file to be restored.



6. Check information displayed.
   Click **Next**.



7. Click **Finish** to complete the restoration process.

Restoring the Keys database

To restore the Keys database, follow the steps below:

1. Launch **DbInstaller**.
2. Click **Keys database maintenance**.
3. Click **Next**.
4. Enter the required information and click **Next**.
5. Below Operation type, click on the **Restoration** radio button.
   Click ... to select the path and the name of the file to be restored.
6. Check information.
   Click **Next**.
7. Click **Finish** to complete the restoration process.

Restoring the Alerts database

This operation is optional.

Checking your modifications

To check that the StormShield database has been effectively restored and that the MS SQL Server 2005 operates properly, connect to the SkyRecon console management (version 5.2).

Downloading the new version patches

Before updating StormShield, you must first download its patches using the link provided by SkyRecon Systems.

If you wish to only update the StormShield server, just download the server patch.

Before updating StormShield to a new version, there are six **patch** files to be downloaded:

- **Server**:
  - `stormshieldserver_win32_5.2xx.srh`
  - `stormshieldserver_win32_5.2xx.sru`
- **Console**:
  - `skyreconconsole_win32_5.2xx.srh`
  - `skyreconconsole_win32_5.2xx.sru`

- **Agent**:
  - `stormshieldagent_win32_5.2xx.srh`
  - `stormshieldagent_win32_5.2xx.sru`

Explanations:

- The symbol **xx** corresponds to the update version number.
- Files with a **.srh** extension are patch headers.
- Files with a **.sru** extension are patch files.
- Patch headers are used to authenticate patch files.

Restarting the StormShield server service

Restart the StormShield server service (`srservice.exe`) to force the server updating process.

For more information, see "Updating the StormShield server", page 159.

Updating your license file

After updating the SkyRecon management console to version 6.0, update your license file.

For more information, see:

- "Updating the SkyRecon management console", page 160.
- "Packages, option and licenses", page 47.

One license is required per environment. For more information, see "Packages, option and licenses", page 47.

WITH MS SQL SERVER 2005

PREREQUISITES

Saving the StormShield database

In version 6.0, the StormShield database includes:

- The Console database.
- The Alert database.
- The Key database.

To backup your database in a directory other than the default directory
(example: `.\Mssql\Backup`), assign Read/Write rights to the security group `SQLServer2005MSSQLUser$ServerName$SQLInstance`.

Saving the Console database

To save your Console database, follow the steps below:

1. Close the SkyRecon management console.
2. Launch `DbInstaller.exe` located by default in:

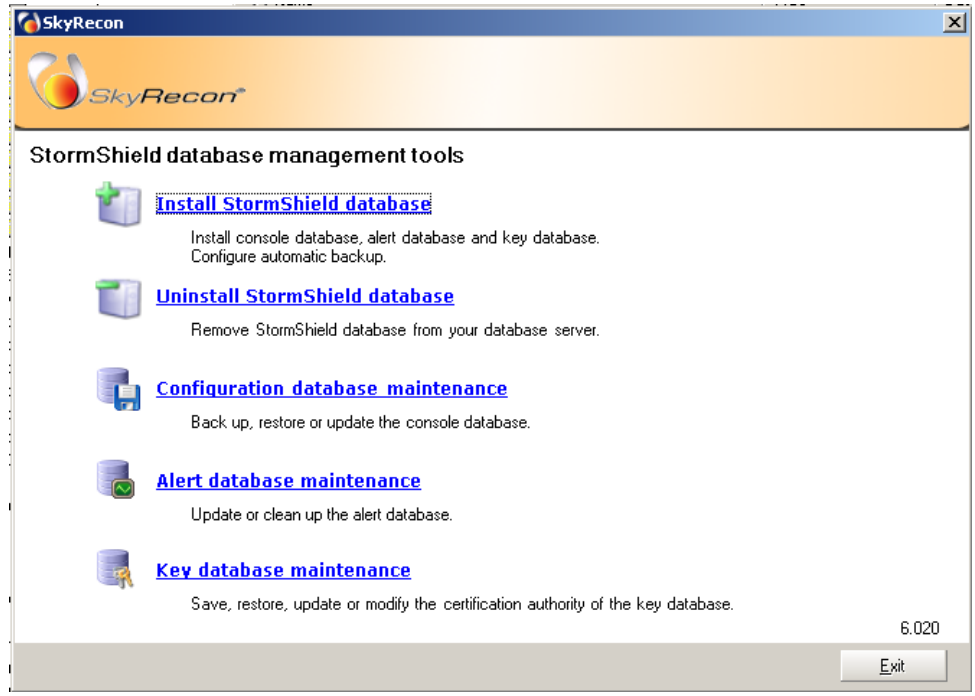
   `C:\Program Files\Skyrecon\SkyRecon Management Console\DBInstall`

   `DbInstaller.exe` is directly accessible from the **Start** menu.

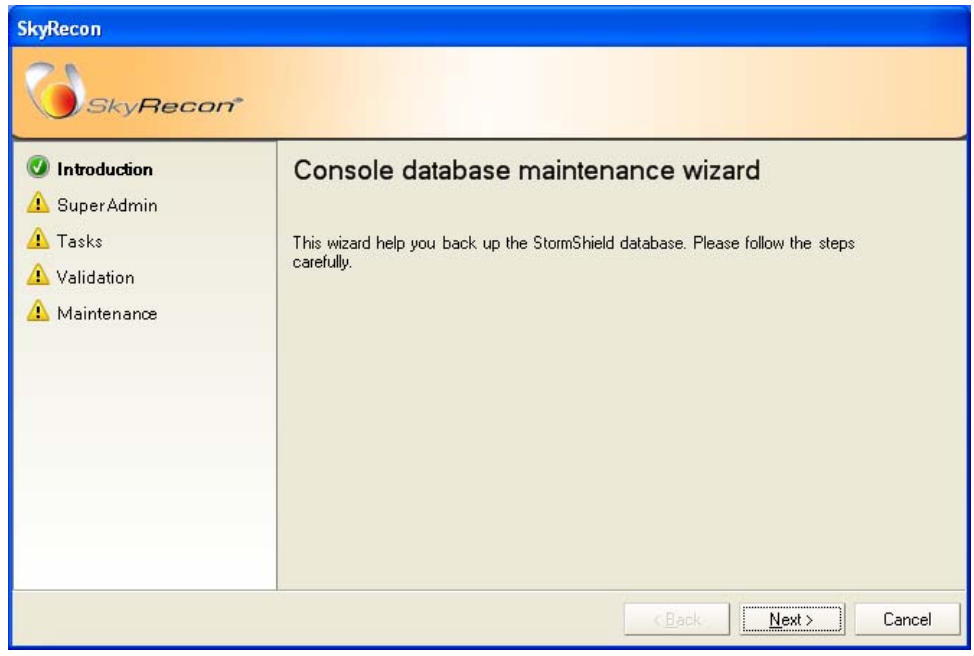
   `DbInstaller.exe` is represented by the icon  .

   This will start the StormShield database management tools.

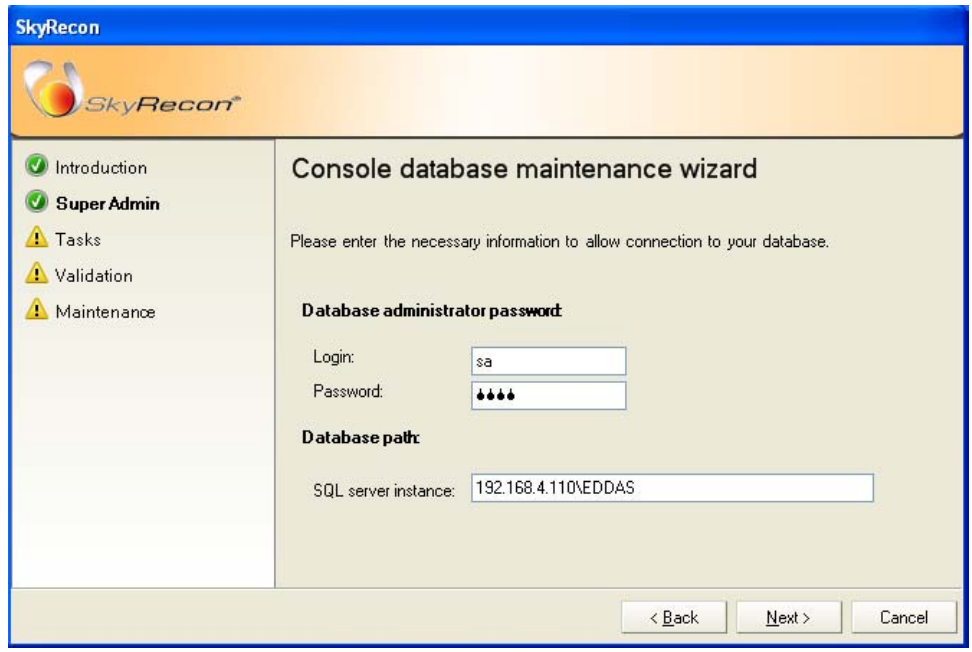
3. Select **Configuration database maintenance**.



4. Click **Next** to open the window that establishes connection to the StormShield database.

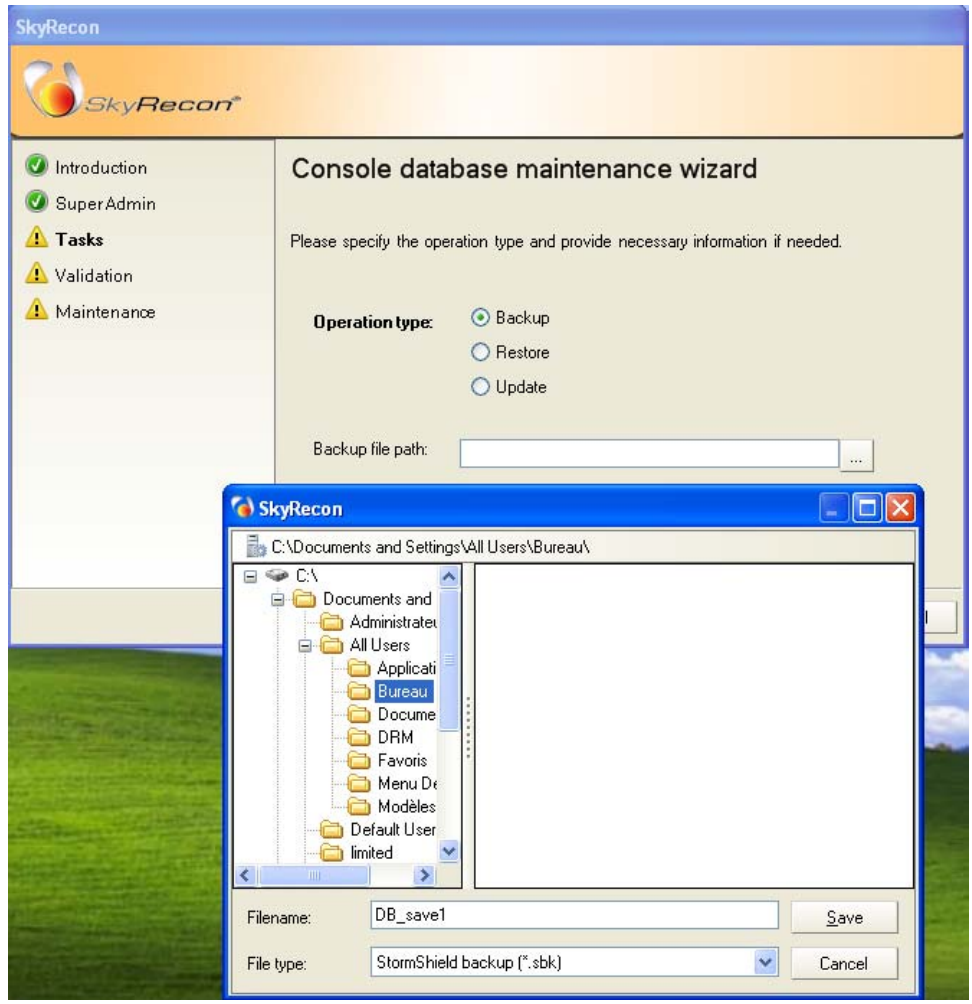


5. Enter:
   - The system administrator login and password used for the database server (**sa** account).
   - The IP address or the netbios name of the database server. If several instances are installed, you can specify it.
     Example: `[database IP instance]\EDDAS`.
   - Click **Next**.

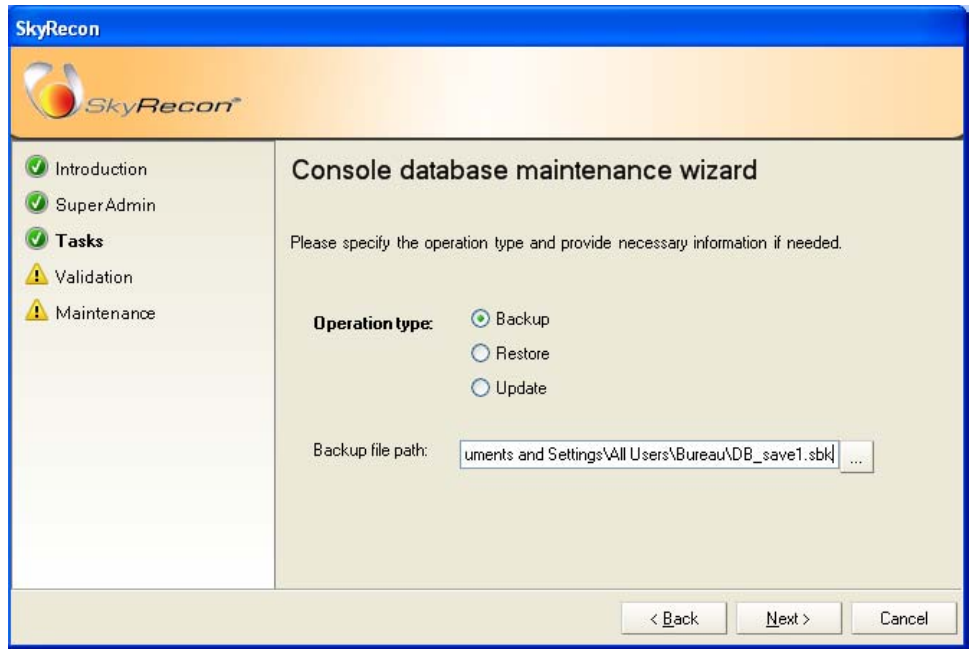


6. Below Operation type, click on the **Save** radio button.

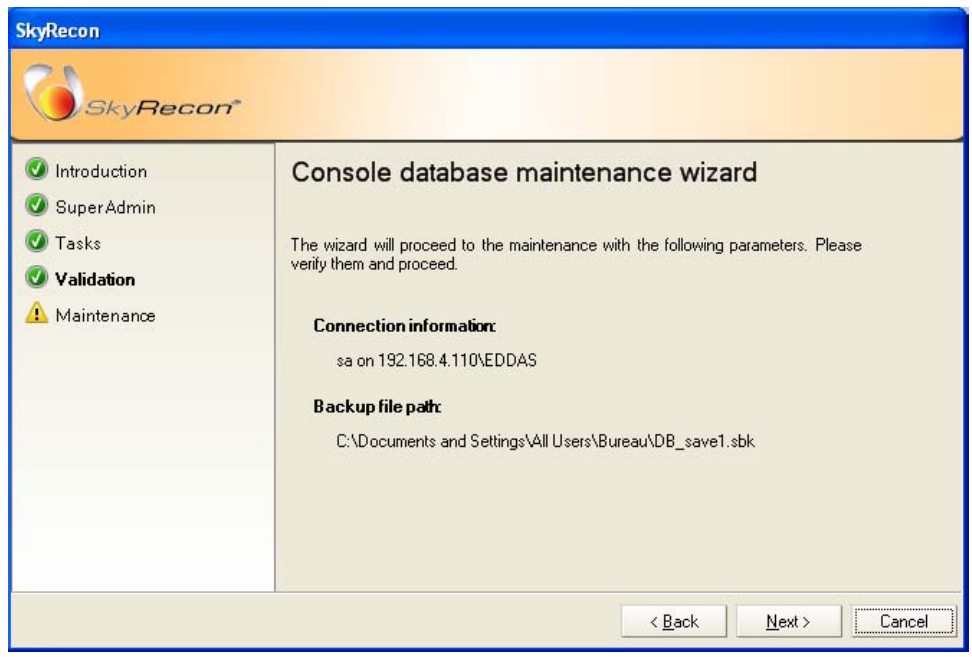
7. Click ... to select the backup filepath and enter a backup filename.
Click **Save**.
The backup will be saved on the machine that hosts the database.



8. Click **Next**.



9. A summary is displayed.
Click **Next**.



10. Click **Finish** to complete the backup.

Saving the Key database

Repeat the procedure "Saving the Console database", page 152.

Saving the Alert database

Repeat the procedure "Saving the Console database", page 152.

Downloading your patches

Before updating StormShield, you must first download its **patches** using the link provided by SkyRecon Systems.

If you wish to only update the StormShield server, just download the server patch.

If you want to define separately the update settings applicable to the StormShield server and agents, use **Default update to deploy (ex.: 5.700)** under [Master server] > Software Updates Settings.

For more information, see "Default update to deploy (e.g.: 6.000) :", page 124.

Before updating StormShield to a new version, there are six **patch** files to be downloaded:

- **Server**:
  - `stormshieldserver_win32_6.0xx.srh`
  - `stormshieldserver_win32_6.0xx.sru`
- **Console**:
  - `skyreconconsole_win32_6.0xx.srh`
  - `skyreconconsole_win32_6.0xx.sru`
- **Agent**:
  - `stormshieldagent_win32_6.0xx.srh`
  - `stormshieldagent_win32_6.0xx.sru`

Explanations:

- The symbol **xx** corresponds to the update version number.
- Files with a **.srh** extension are patch headers.
- Files with a **.sru** extension are patch files.
- Patch headers are used to authenticate patch files.

PROCEDURE

Updating the StormShield agent

There are two ways to update the StormShield agent:

- Automatic update.
- Manual update.

Automatic update

Copy the agent update files in the `patchs` folder located by default in the StormShield server installation directory in:

```
C:\Program Files\Skyrecon\StormShield Server
```

If an agent connects to a slave server, the slave server will download the patches from the master server in order to distribute them to the connected agents.

The agents will download the update and install it automatically (without user intervention).

The update is applied only after the agent has been rebooted. However, StormShield continues to protect the computer until it reboots.

Manual update

The agent should be able to connect to the StormShield server to be updated manually.

To update the agent manually, follow the steps below:

1. Check the StormShield agent version by opening the `version.sro` file which is located in:

   ```
   C:\Program Files\Skyrecon\StormShield Agent\conf
   ```

2. Rename the patch file by replacing its version number to match the agent version currently installed.

   For example, if you are updating from version 5.2 to version 6.0, rename the patch:

   - `stormshieldagent_win32_5.7.srh` in `stormshieldagent_win32_5.2.srh`
   - `stormshieldagent_win32_5.7.sru` in `stormshieldagent_win32_5.2.sru`

3. Install the update by copying the agent patch in the `patchs` folder located in the StormShield agent installation directory which is by default:

   `C:\Program Files\Skyrecon\StormShield Agent\`

4. To update immediately, force the agent to connect to the server:

   - Right-click on the StormShield Monitor icon in the system tray.
   - Go to **Other operations > Reconnect to server**.

   A pop-up window and a message in the user interface of the StormShield agent will be displayed when the update is finished.

   The changes you have made to the agent will be applied after reboot.

5. Reboot the computer when receiving the reboot notification issued when the update is completed.

Updating the StormShield server

To update the StormShield server, follow the steps below:

1. Copy the server update files in the `patchs` folder which is located by default in the StormShield server installation directory in:

   `C:\Program Files\Skyrecon\StormShield Server`

2. The server will update itself according to the settings defined in **Software Updates Settings** in the master server configuration.

3. When the StormShield server begins the automatic update, the `updater.sro` file appears in the `patchs` folder.

   The update runs in background mode and takes about five minutes.

   When the update is completed:

   - The `updater.sro` file is removed.
   - The `log.txt` is created in the `Log` folder which is located at the root of the StormShield server.
   - The master server also sends updates to the slave servers.
     The slave servers share the same update process as the master server.

4. Reboot the server on which are installed the server patches. The reboot can be postponed but it is required to update the StormShield server service (`srservice.exe`).

Updating the StormShield server does not apply the possible configuration updates of the Apache server. You can manually apply updates by executing «`skyapache.exe --update`» located in `Program Files\SkyRecon\StormShield Server\Apache\conf` from an administrator command line. Former configuration files are renamed `httpd.conf.old` and `ssl.conf.old`. Reboot the StormShield server to take into account these modifications.

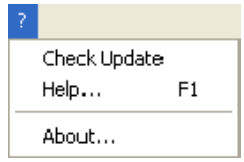
Updating the SkyRecon management console

To update the SkyRecon management console, follow the steps below:

1. Copy the console update files in the `patchs` folder located by default in the StormShield server installation directory in:

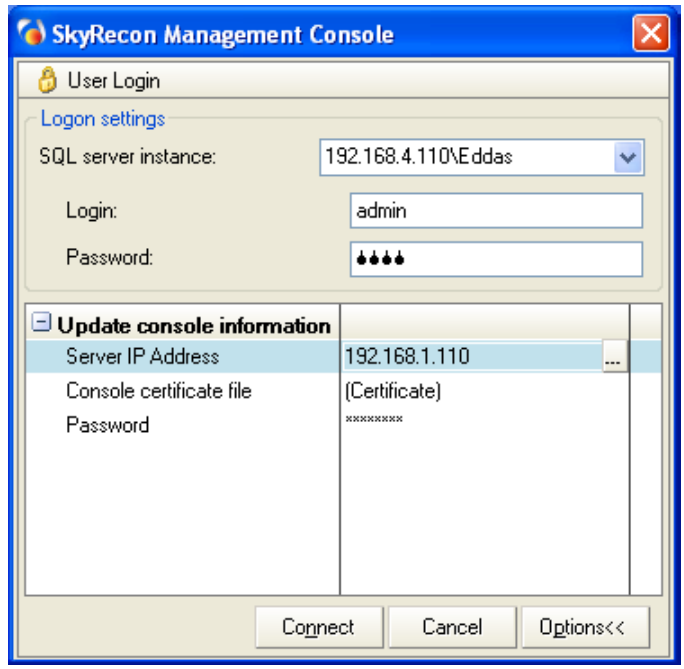
   `C:\Program Files\Skyrecon\StormShield Server`

2. On the console, click ? and select **Check Update**.



3. A dialog box opens to inform you that an update is available. Click **Yes**.

4. To update other consoles, enter the required information to establish the connection between the console(s) and the server:
   - Click **Options**.



   - Update the following console information using ... :
     - Server IP address.
     - Console certificate file:
       Specify the path to the console certificate file. This file protects communications between the master server and the console.
     - Password:
       Enter the password set when installing the server to prevent any illegal use of certificates.

5. Click **Connect**.
   The SkyRecon management console opens.

> Now, you have to update the StormShield database (Console database, Alert database and Key database) for the console and database versions to match.

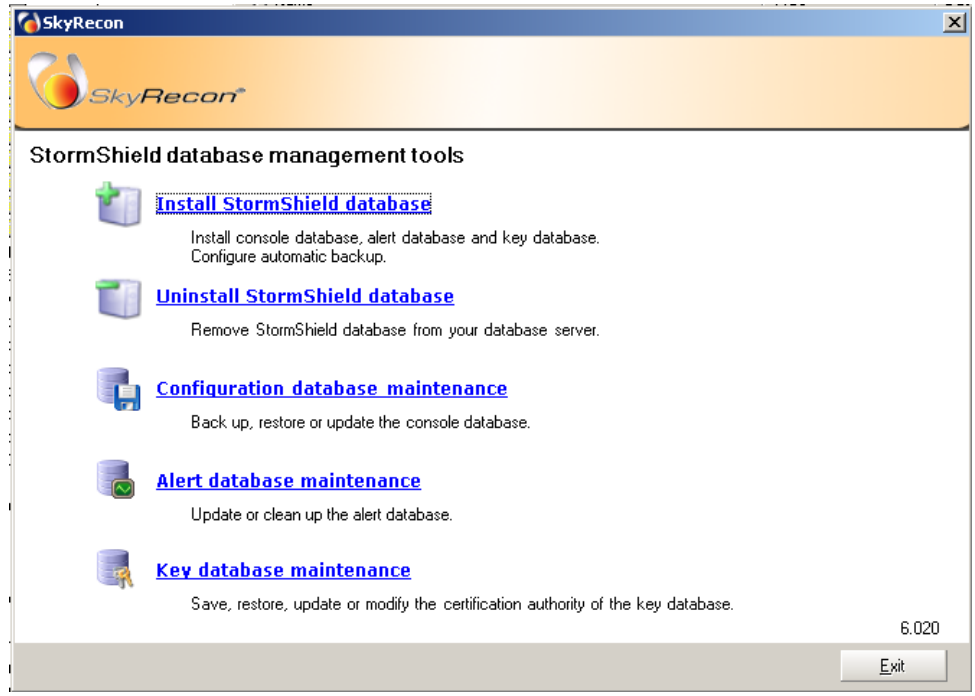
Updating the StormShield database

Updating the Console database

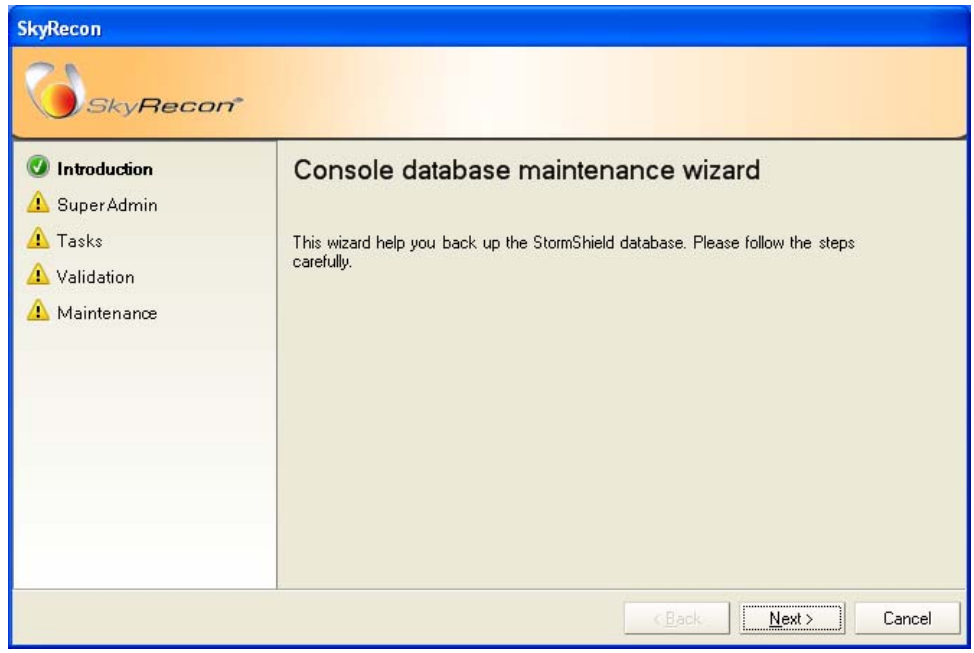
To update the Console database, use the **DBInstaller** utility which is accessible from the **Start** menu.

1. Launch `DBinstaller.exe`.

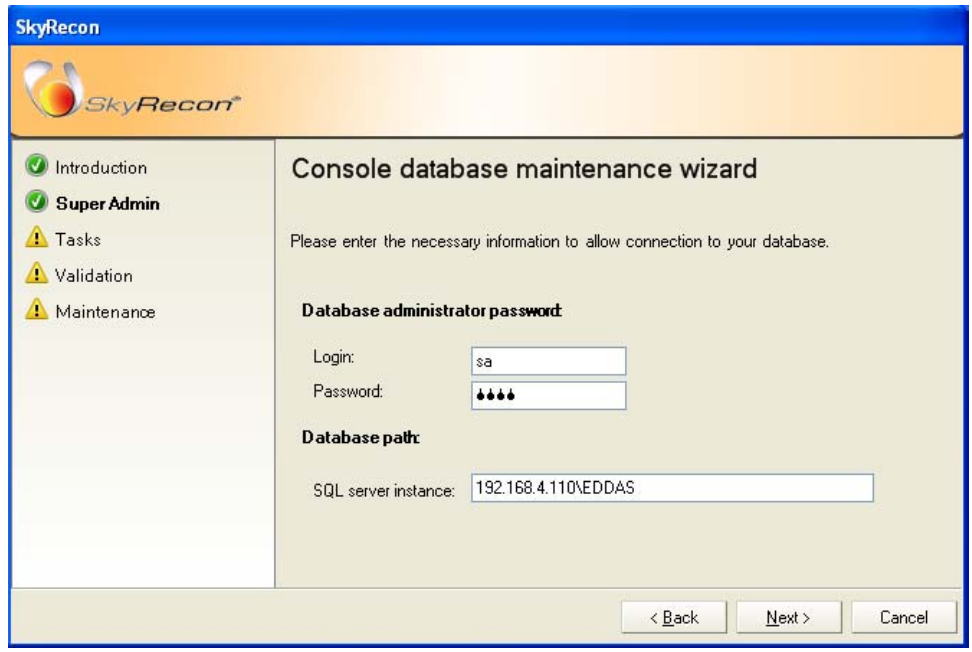
2. Select **Configuration database maintenance**.
The window below is displayed.



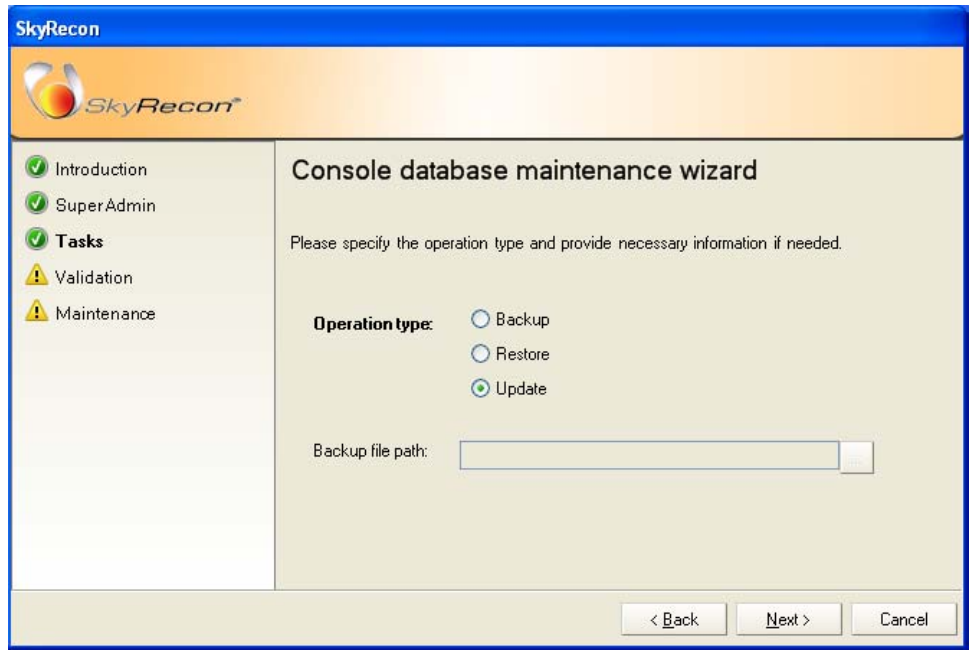
3. Click **Next**.



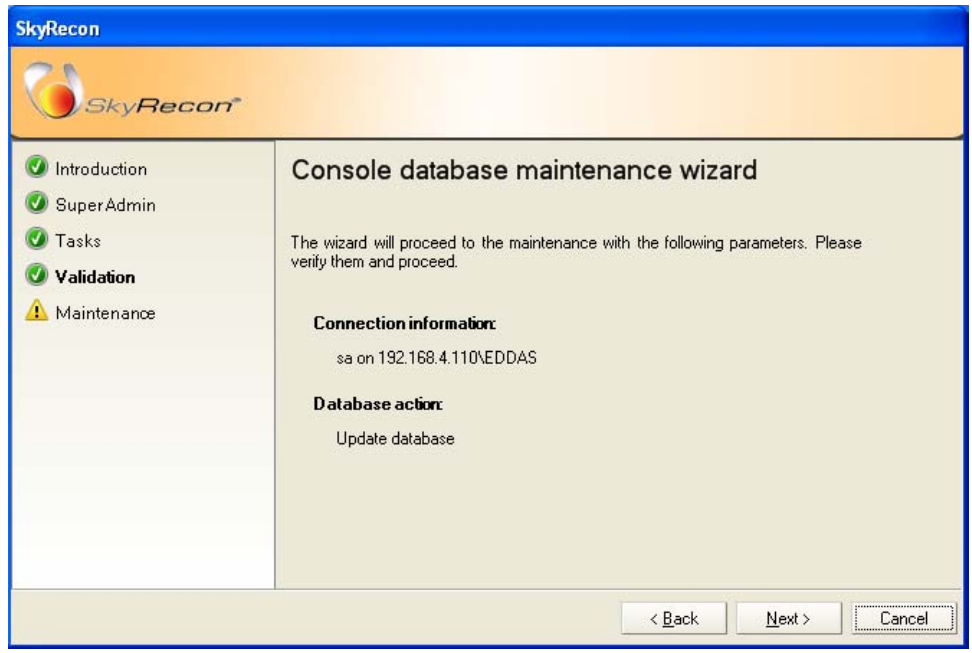
4. Enter the required information.



5. Select **Update**.
Click **Next**.



6. Check information.
   Click **Next**.



7. Wait until the update process is completed.
   Click **Finish**.

Updating the Alert database

1. Launch `DBInstaller.exe`.
2. Select **Alert database maintenance**.
3. Repeat the same steps as in "Updating the Console database", page 161.

If you use the **Professional Edition** package, the update process is over.

If you use the **Secure Edition** package, go to "Updating the Key database", page 164.

Updating the Key database

If you use the **Secure Edition** package, follow the steps below:

1. Launch `DBInstaller.exe`.
2. Select **Key database maintenance**.
3. Repeat the same steps as in "Updating the Console database", page 161.

The update process is over. Now, you can use the SkyRecon management console.

Proceed with the updating procedure of the StormShield server and agents.

Chapter 4

SKYRECON MANAGEMENT CONSOLE CONFIGURATION

ABOUT THIS CHAPTER

This chapter presents the SkyRecon management console and its configuration by the Administrator.

It includes the following:

- Getting started with the console.

- Console overview:
  - Environment Manager.
  - Management and Monitoring Tools.
  - Console Configuration panel.

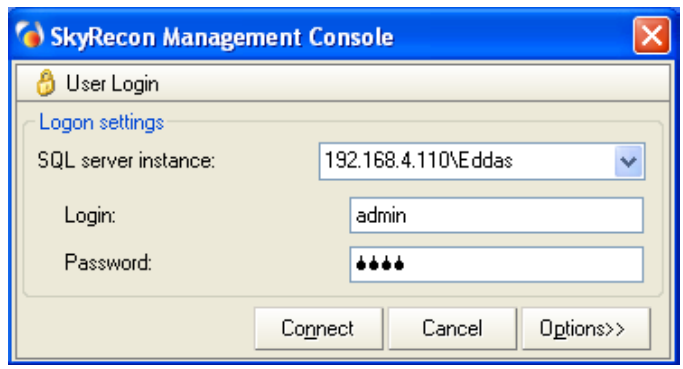
GETTING STARTED

The SkyRecon management console can be started in two ways:

- To start the console from the **Start** menu, select:

  `Programs > SkyRecon > SkyRecon Management Console`

- To start the console from the desktop:
  - Double-click the SkyRecon management console icon .
  - Enter the login and password.
  - Click **Connect** (or press Enter on your keyboard) to access the SkyRecon management console.



If this is the first time that you use the console, see "Configuring the environment", page 110.

CONSOLE OVERVIEW

The working screen of the SkyRecon management console is displayed as follows:

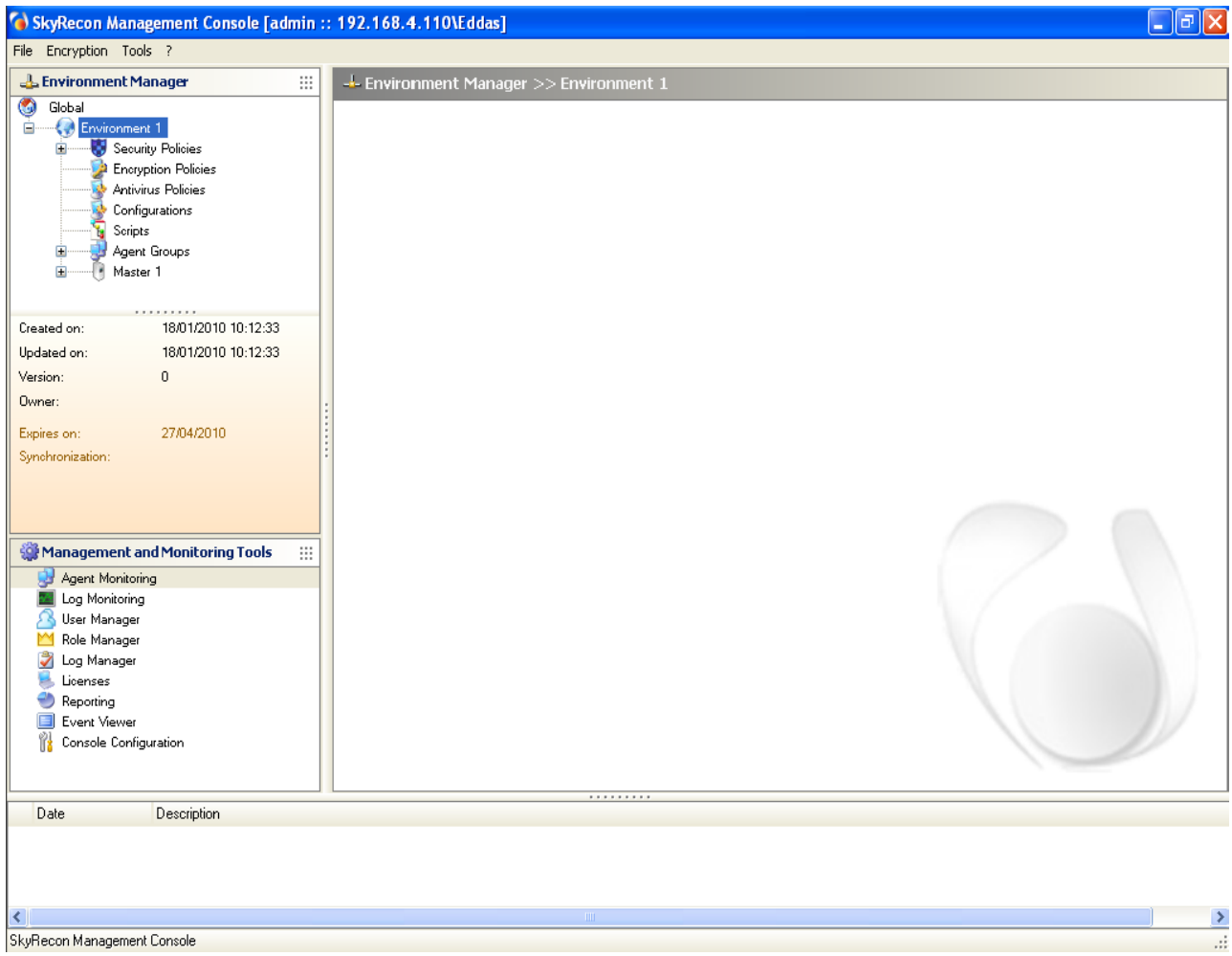
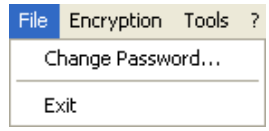


Fig. 4.1: Working screen of the SkyRecon management console

- **Menu bar**:

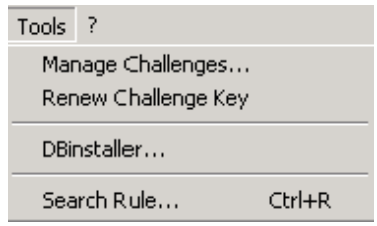
  This is a standard Windows menu bar which provides access to the various console features:

  - File:

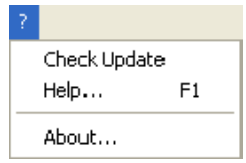


- Encryption:

- Tools:



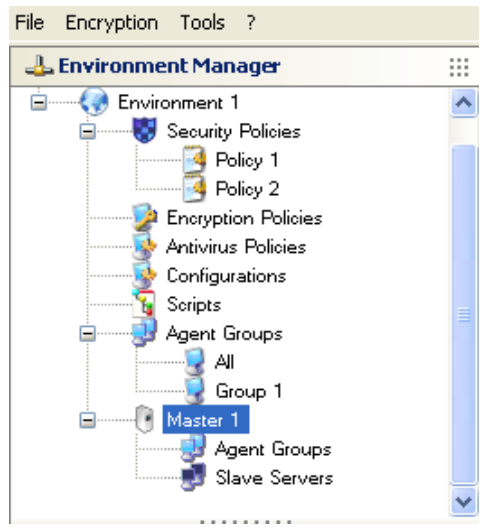
- ? :



- **Environment Manager**:

  This area is used to manage:

  - Policies (security, encryption, antivirus).
  - Configurations.
  - Scripts.
  - Agent groups (assigned to different master servers).
  - Servers (master and slave).

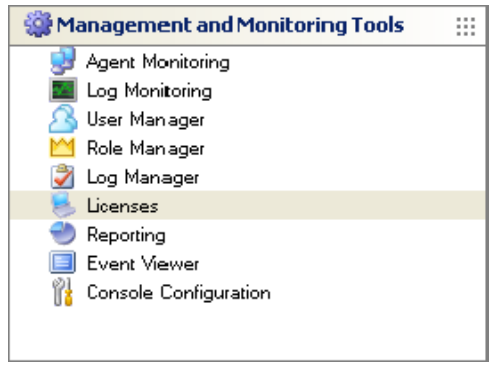


- **Version details**:

These details include:

- The console creation date.
- The console update date.
- The console version (Example: Policy 1, version 2).
- Owner (admin).
- The console expiry date (if any).
- The date when the latest configuration was sent.
- Number of synchronizations.

- **Management and Monitoring Tools**:

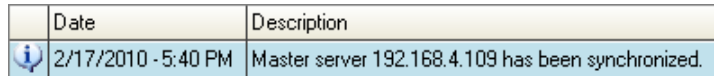


This area is used to display and modify:

- Agents.
- Logs.
- Users.
- Roles.
- Licenses.
- Reports.
- Events.
- Console.

- **Status bar:**

  This bar displays the **Date** and **Description** of the status messages related to the operations performed by the console.



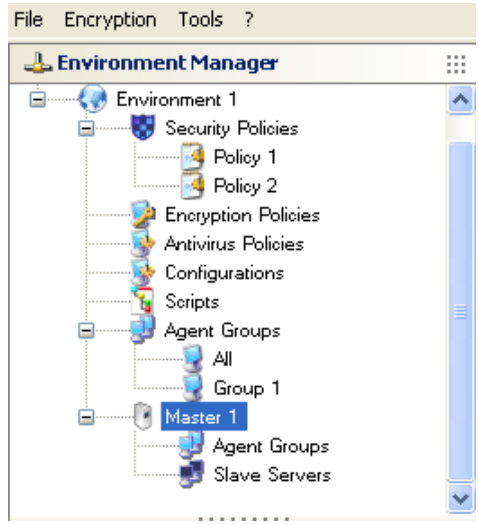
ENVIRONMENT MANAGER

The Environment Manager is where you create environments.

In order to apply a security policy to an agent group, check that the **Draft Version** in the right-click menu in the Environment Manager area is unticked.
The draft version feature prevents an administrator from applying a security policy to an agent group as long as the policy has not been validated.
The security policy names are edited in red when Draft Version is enabled.
When a security policy is being edited by an administrator, a lock is displayed for the other administrators using the console. These administrators will not be able to display the draft version of the security policy.

Environment

The first level corresponds to the environment.



It is used to manage:

- Policies (security, encryption, antivirus).
- Configurations.
- Scripts.
- Agent groups.
- Servers.

Each environment is associated with any number of master servers and an unlimited number of slave servers.

The workstations to be protected are assigned to a single environment. They can be gathered into agent groups that are homogeneous from a security policy viewpoint.

Forming agent groups can be based on:

- IP addressing.
- Machine names.
- Active Directory.

When IP addressing is used, a single IP address, a list of IP addresses or a subnetwork address can be specified.

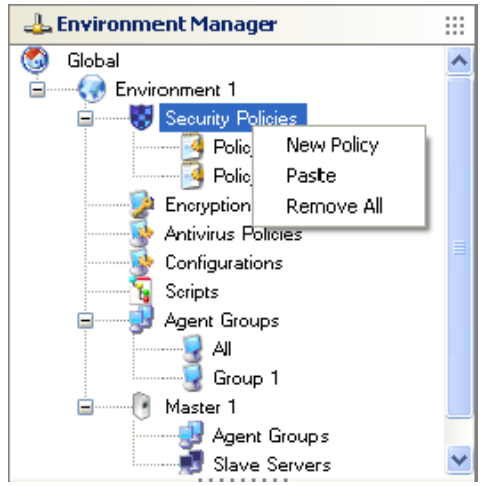
When Active Directory is used, it is possible to target the name of a machine or a group of machines declared in the directory (example: in the form of an organizational unit (OU)).

Policies

Policies are handled in **three** stages:

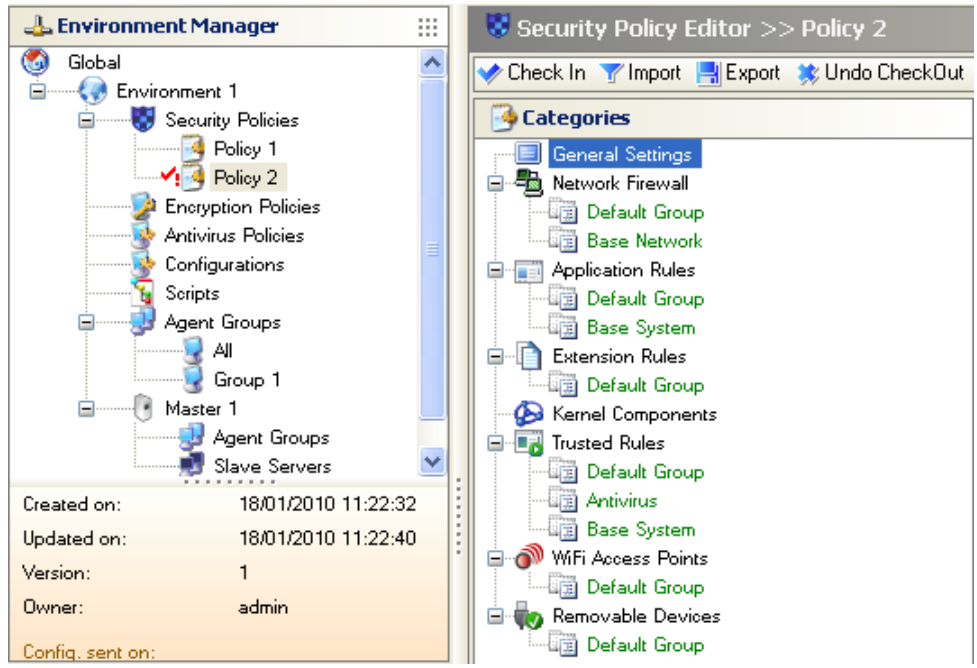
1. Policy creation:

   Policies are created on the console in the **Environment Manager**.



2. Policy configuration:

   Policies are configured in the **Security Policy Editor**.

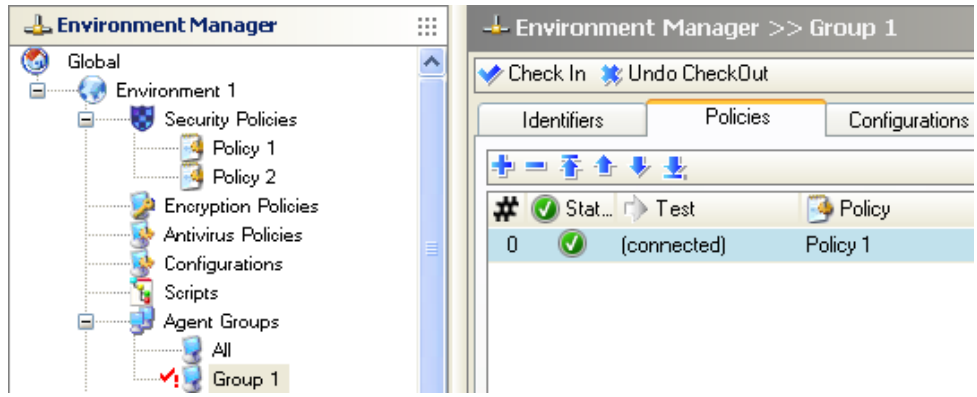


The Security Policy Editor is used to create and name the security policies which can contain a combination of:

- Automatic protection rules.
- Firewall network rules.
- Application access rights.
- Kernel component protection.
- Application behaviors.
- Device access rights.

3. Policy assignment:

   Policies are assigned to agent groups via the **Environment Manager** from the **Policies** tab:



Agent Groups

Agent groups are managed either in standard or in advance mode.

Standard mode

Standard mode is handled as follows:

- Agent group overview.
- Assigning agent groups to master servers.
- Deploying policies for agent groups and collecting logs.

Overview

Agent groups are to be found at environment level in the **Environment Manager**.

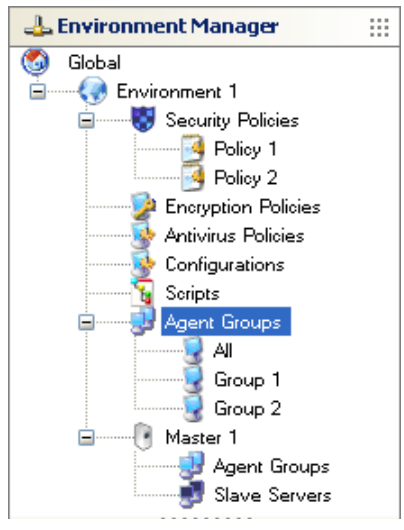


Fig. 4.2: Agent groups in a tree structure

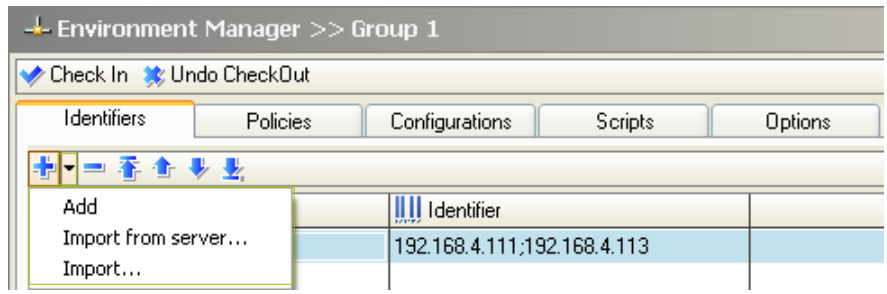
The deployment of agents and security policies requires a preliminary operation. Agents must be described to access the client workstations to be protected.

By default, when creating an environment, **Agent Groups** is empty but available.

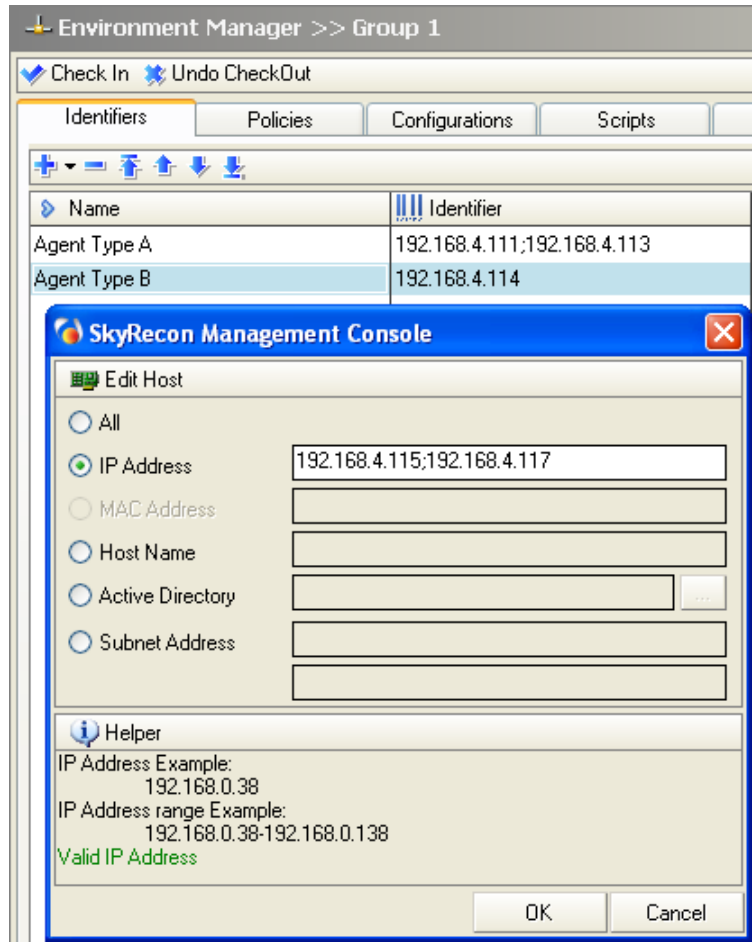
To describe each agent group, follow the steps below:

1. Go to **Agent Groups** level in the Environment Manager.
2. Edit the agent group to be described.
3. Add and define the agent identifiers via the toolbar and ... .

   To add an identifier, three options are available:



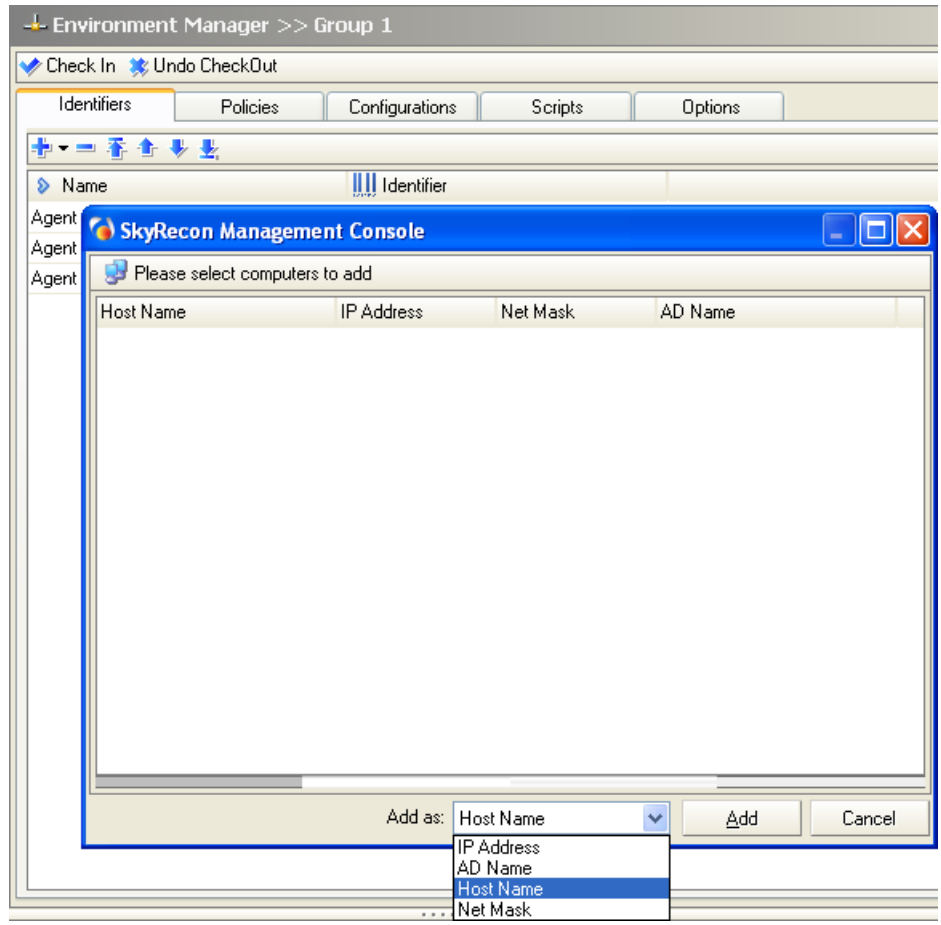
- **Add**



This option is used to add an identifier via the following radio buttons:

- **All**:
  All agents will be added to the agent group.
- **IP Address**:
  The agents with matching IP address will be added to the agent group.
- **Host Name**:
  The agents with matching hostname will be added to the agent group. You can use the wildcard star (*).
  Example: Workstation*.
- **Active Directory**:
  The agents with matching AD name or OU will be added to the agent group.
- **Subnet Address**:
  The agents which belong to the IP subnet address specified will be added to the agent group.

- **Import from server**

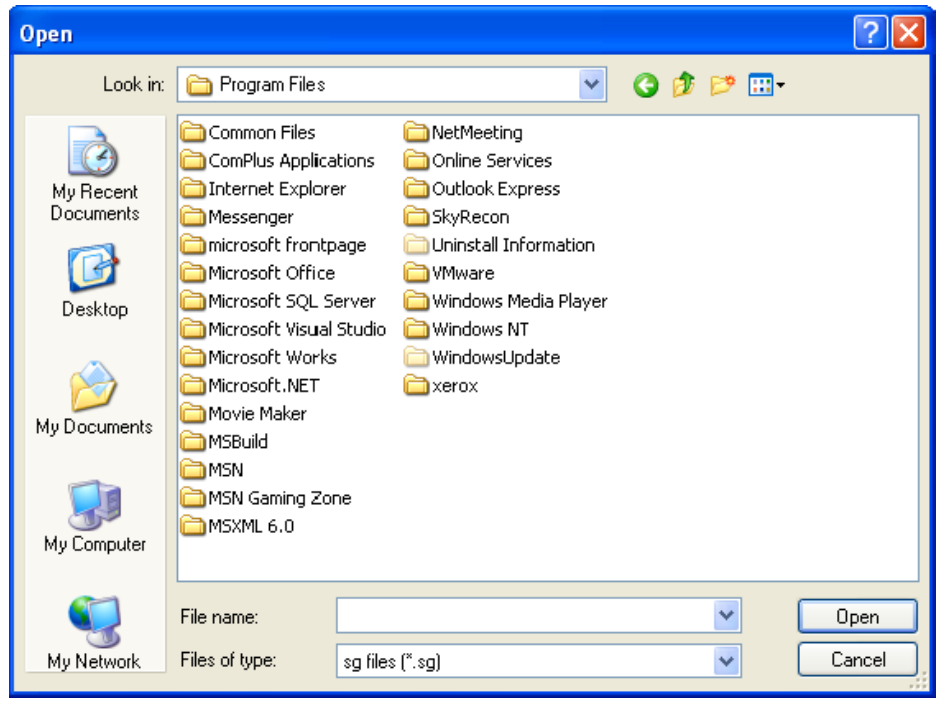


This option is used to add an identifier via the following radio buttons:

- Host Name.
- IP Address.
- AD Name.
- Host Name.
- Net Mask.

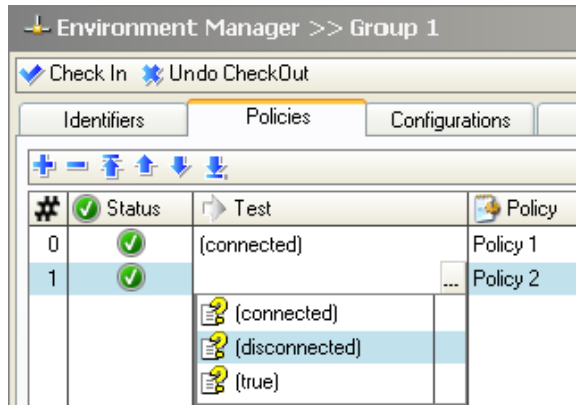
- **Import**

  This option is used to add an identifier via the following window:

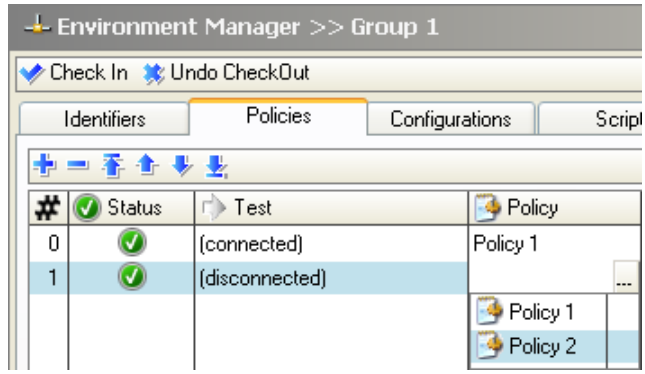


4. Add and define the policies via the toolbar and ....
   - Check the status.

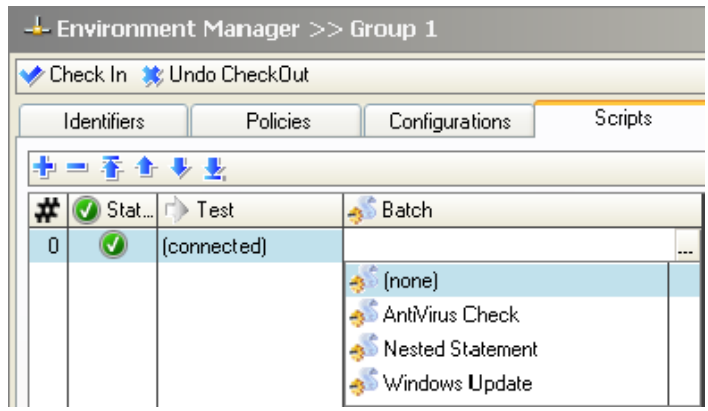
- Select the test to be applied.



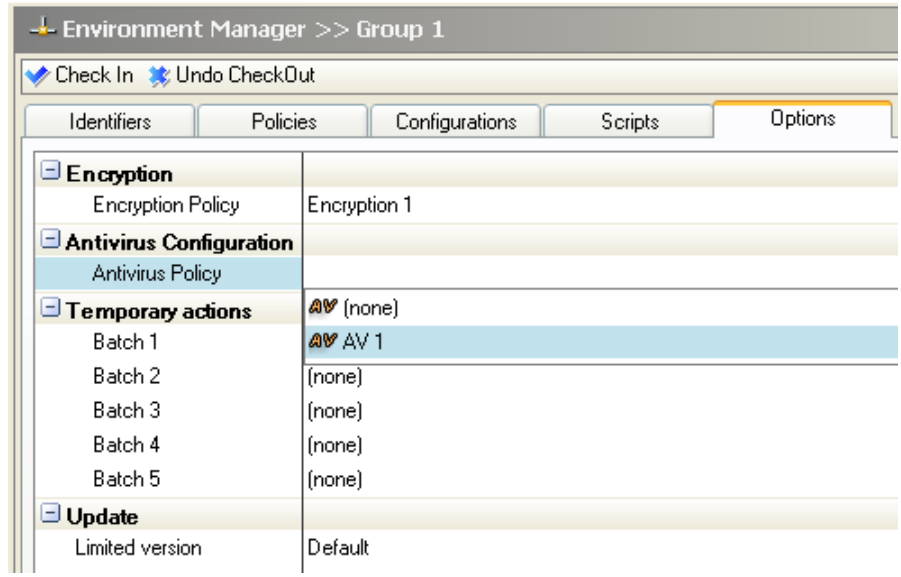
- Select the security policy.



5. Add and define the configurations via the toolbar and ... .
6. Add and define the scripts via the toolbar and ... .



7. Add and define the options via the toolbar and ...



8. Click to validate your parameters.

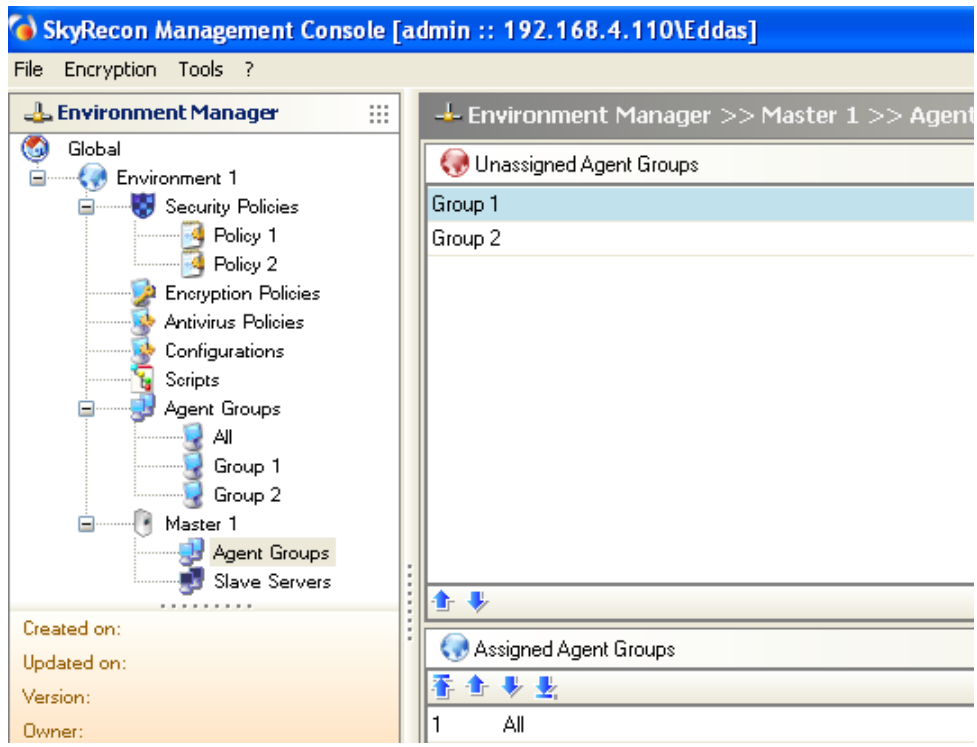
Assigning agent groups to master servers

After creating an agent group, it is not assigned to any master server. This operation must be done manually for every server.

An agent group can be assigned to several master servers.

To assign agent groups, follow the steps below:

1. Click **Agent Groups** under a master server.



2. Move the unassigned agent groups to the **Assigned Agent Groups** panel using the arrows.

The order of the agent groups is important as the first found rule for the configuration is used when a StormShield agent connects to the server.

Deploying policies and collecting logs

Security policies are deployed and data on agent activities are collected using **tokens**.

At regular intervals defined by the administrator, the server notifies the agents through the circulation of tokens. These tokens are sent from one machine to another and back to the server.

This communication model protects the network from a distributed denial of service caused by a large number of agents trying to connect simultaneously the server.

On receiving the token, each agent performs actions such as security policy update or log transmission to the server.

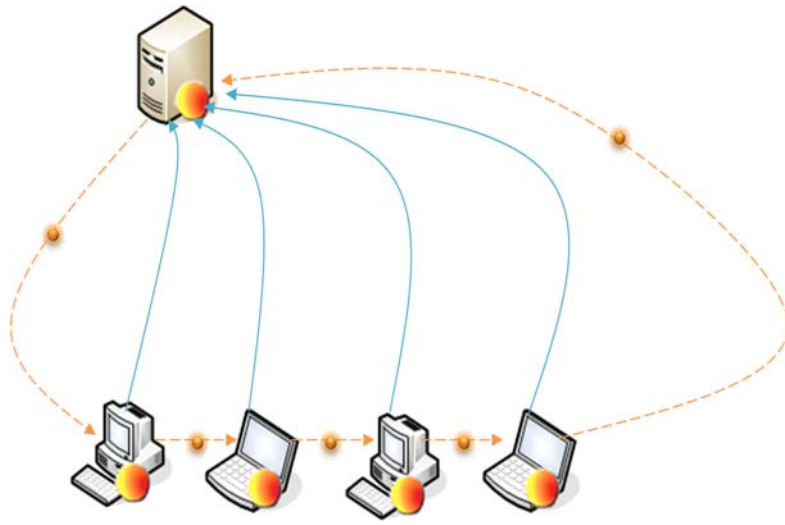


Fig. 4.3: Deployment of policies by token

The token rotation period (also called refresh time) is configurable by the administrator to optimize the allocation of bandwidth for StormShield.

Number of agents per server	Number of simultaneous connections (LAN)	Token refresh time (in seconds)	Reconnection time in disconnected mode to the master server (in seconds)
1 to 500	100 to 50	60 to 600	60 to 300
500 to 2000	70 to 20	600 to 1800	300 to 600
2000 to 4000	50 to 10	1800 to 3600	600 to 1200
4000 to 8000	100 to 10	3600 to 7200	600 to 1200
+ 8000	250 to 50	3600 to 7200	600 to 1200

The maximum number of agents is: 10000 to 20000.

The console enables to configure up to 1000 simultaneous connections but the StormShield server automatically limits to 500 if it is installed on a 32-bit machine (on a 64-bit machine, the maximum number of simultaneous connections managed by the server is 1000).

If agents are connected via a wide area network (WAN), the number of necessary simultaneous connections significantly increases because the time during which each agent remains connected is longer. The definition of this number strongly depends on the characteristics of the network (throughput, round trip delay, etc.) and on the number of agents concerned.

If more than 200 simultaneous connections must be configured, make sure you have enough RAM (4 Gb on 32-bit machines, 8 to 16 Gb on 64-bit machines) and enough processors.

These details are based on our observations in different configurations.

The less often the token is sent, the fewer the agent connections. This implies that the load distributed across the network and the occupation rate of the servers will decrease significantly.

On the other hand, the log refresh and policy deployment time intervals are significantly affected by the small number of tokens in circulation.

Advanced mode

Advanced mode is handled as follows:

- Purpose.
- Enabling the advanced mode.
- Defining agent collections.

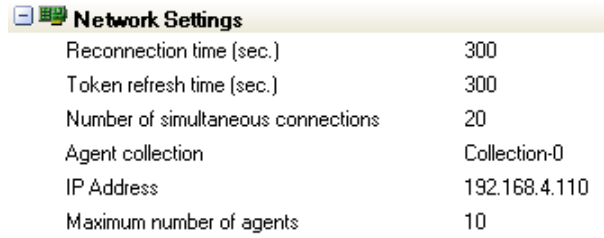
Purpose

The advanced mode is used to create agent collections.

Agent collections consist of agent groups which have been previously created by administrator. The administrator can add to a collection one or several agent groups.

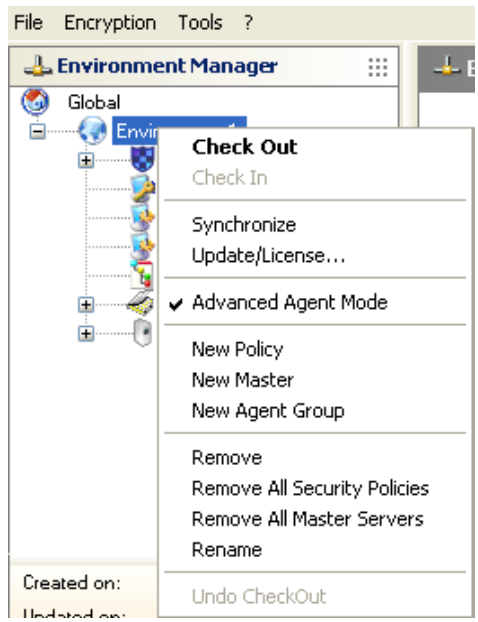
This feature makes it easier to manage a large number of agents.

The agent collection must be assigned to the master server in **Environment Manager > [Server Name] > Network Settings**.

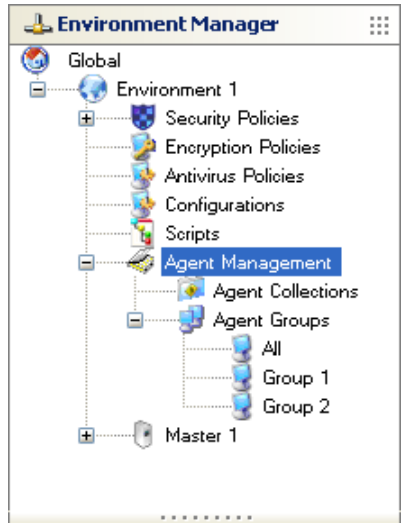


Enabling the advanced mode

To enable the advanced mode, right-click on the name of your environment and select **Advanced Agent Mode**.



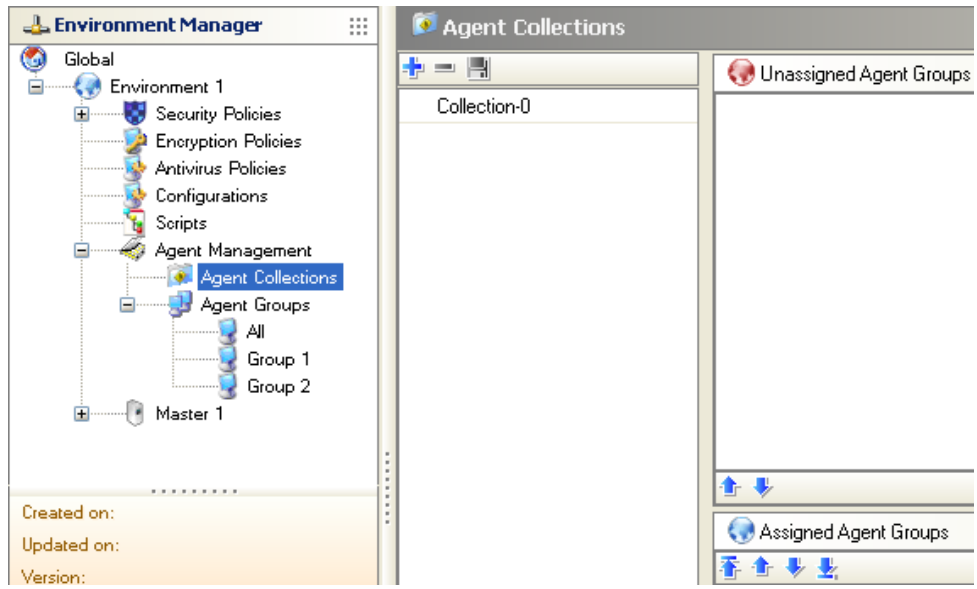
The graphical interface at agent level has changed.



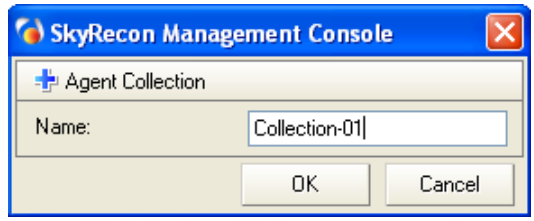
Defining agent collections

To create an agent collection, follow the steps below:

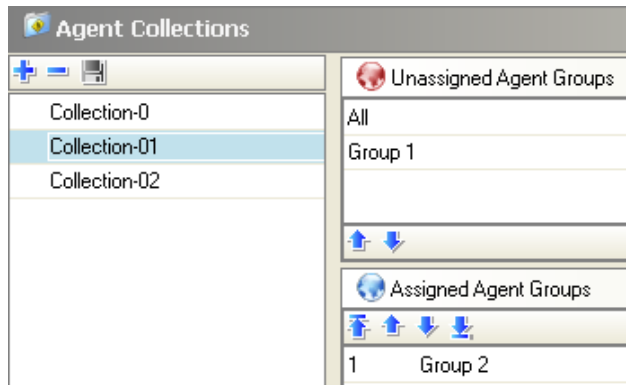
1. Click ✚.



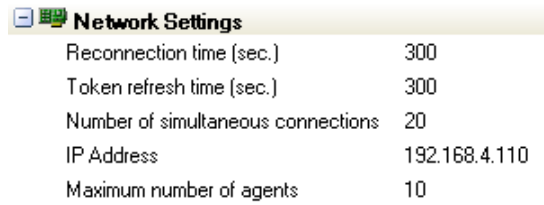
2. Rename the agent collection.



3. Move the agent groups to configure your agent collection using the arrows.



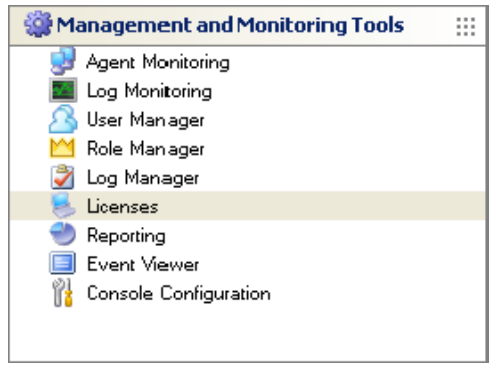
4. Assign the agent collection to the master server in **Environment Manager > [Server Name] > Network Settings**.



5. Validate your environment and the master server parameters.
6. Synchronize to update your agents.

MANAGEMENT AND MONITORING TOOLS

The Management and Monitoring Tools panel is located in the bottom part of the SkyRecon management console:



The Management and Monitoring Tools panel is used to manage and monitor the elements below.

Agent Monitoring

This area provides the administrator with a clear and global view of the agent status to check the versions of the configurations and agents.

For more information, see "Agent Monitoring", page 596.

Log Monitoring

This area records any suspicious activity on the workstations and the corresponding reaction of the StormShield agent.

For more information, see "Log Monitoring", page 603.

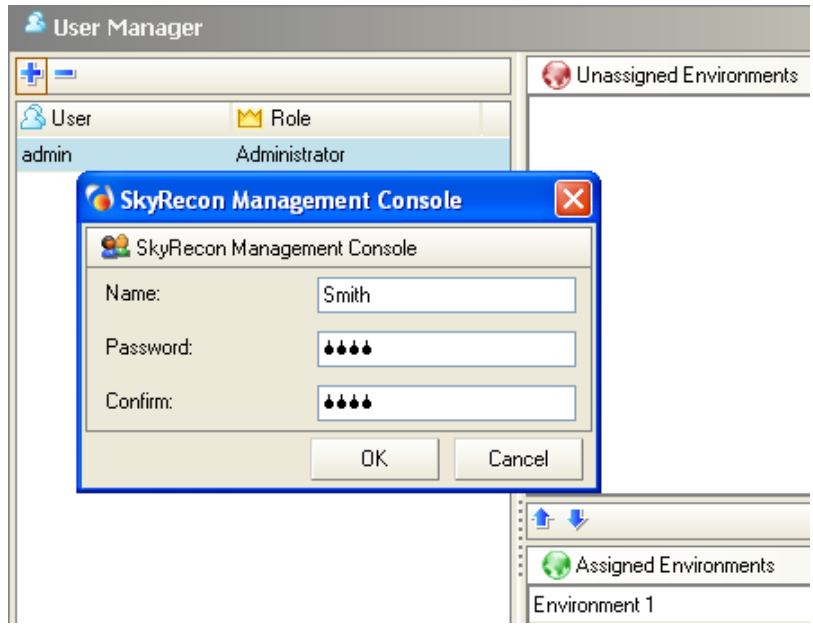
User Manager

This area is used to define the users who can access the SkyRecon management console, and select the roles assigned to these users.

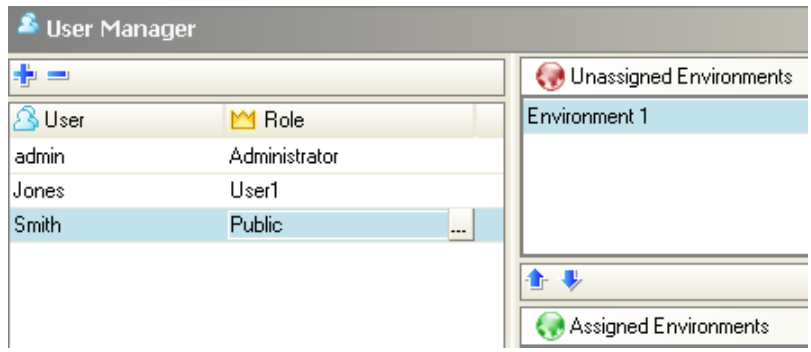
To add a user, follow the steps below:

1. Click **User Manager**.
2. Click .

3. Fill in the three fields and validate.

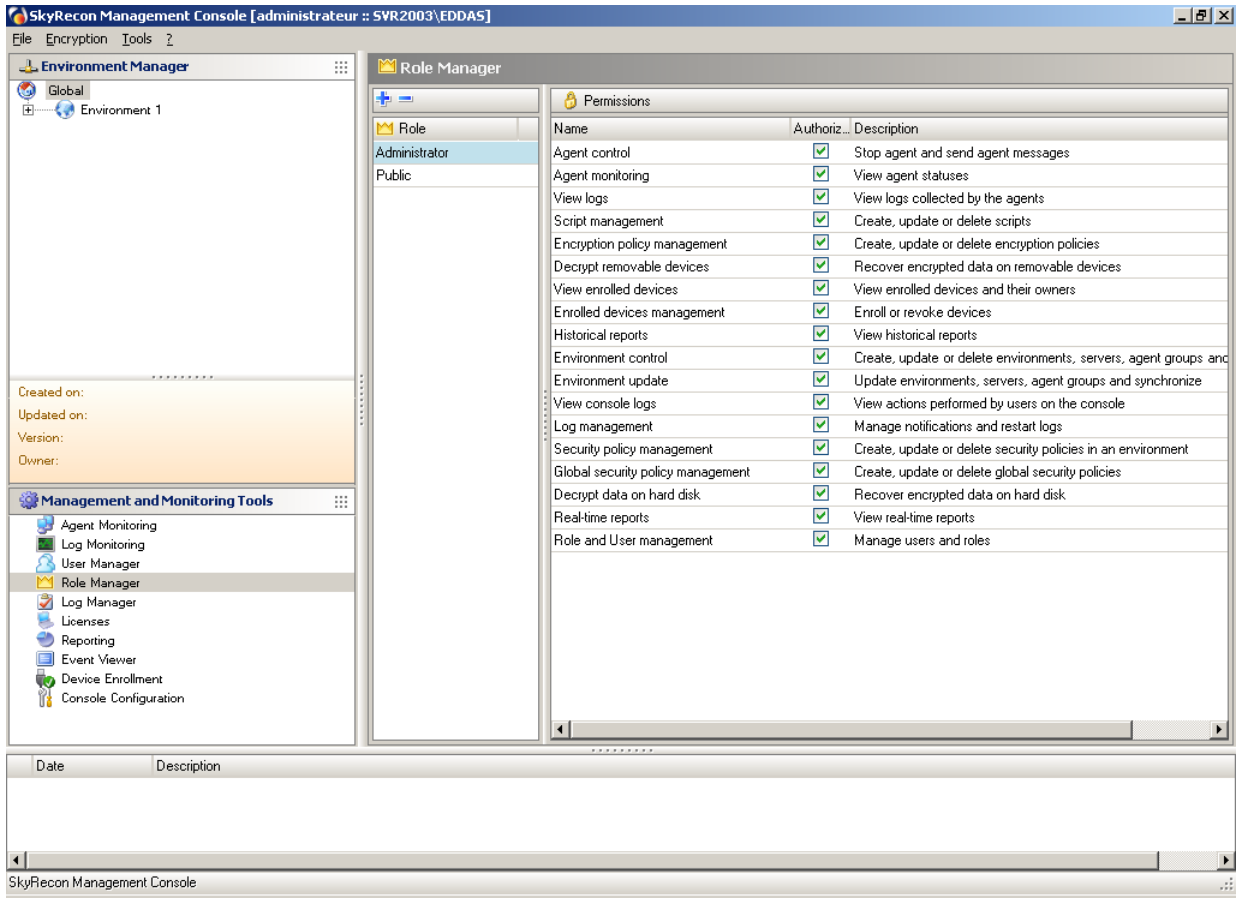


4. Select the role to be assigned to the user in the **Role** column.
5. Select the environment to be assigned to the user (if necessary) with the arrow.



6. Validate your modifications.

Role Manager



This area is used to create the roles assigned to SkyRecon management console users. These roles are assigned through the User manager.

The roles by default are the following:

- **Administrator**:

  Access rights to all operations in the console.

- **Public**:

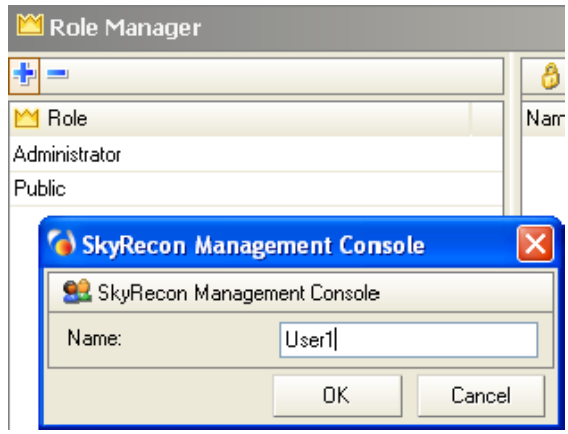
  Read-only access rights to Console Configuration, Environment Manager and Management and Monitoring Tools.

The role manager is used to create and name the users to which roles and environments are assigned.

To add a role, follow the steps below:

1. Click **Role Manager**.
2. Click .

3. Enter the **Name** of the new role and validate.



4. Click the role name in the **Role** column and check the appropriate boxes.

   Each permission can be enabled separately.

   The ExtendedXP Mode permission disables all the other permissions. When the ExtendedXP user connects to the administration console, he/she has access to a simplified console to be used with the ExtendedXP Service. For more information about the ExtendedXP mode, refer to chapter "Simplified management mode for ExtendedXP", page 233.

   If you have subscribed to the ExtendedXP Service, it is better to administrate machines of your environment with the ExtendedXP console. If settings in a security policy or an agent group are modified in the standard SkyRecon console, they will be automatically replaced when opening and editing from an ExtendedXP console.

5. Validate your modifications.

Log Manager

This area is used to customize log messages and agent notifications.

It is used to select how logs will be reported and where they will be stored:

- In a database.
- Via other applications.

Logs are systematically written into the local log file. The User Interface column is used to enable or disable their display on the agent.

Licenses

It is used to display information on:

- The number of agents deployed (taking into account the StormShield package that you have installed).
- The number of licenses that are still available.

Reporting

This area displays real-time and historical reports. These reports are used to collect information on:

- Agents.
- Servers.
- Policies.
- Configurations.
- Removable devices.
- Antivirus.

For more information, see "StormShield Reporting", page 557.

Event Viewer

This area displays the actions carried out by an administrator of the SkyRecon management console.

Actions such as the following are displayed:

- Sending configurations to the server.
- Renaming agent groups.
- Updating encryption policies.

For more information, see "Event Viewer", page 632.

Console Configuration

This area is used to modify and configure the SkyRecon management console.

For more information, see "Console Configuration panel", page 192.

CONSOLE CONFIGURATION PANEL

To display and configure the SkyRecon management console parameters, click **Console Configuration** in the Management and Monitoring Tools panel.

The Console Configuration panel includes two areas: **Options** and **Secure Connections**.

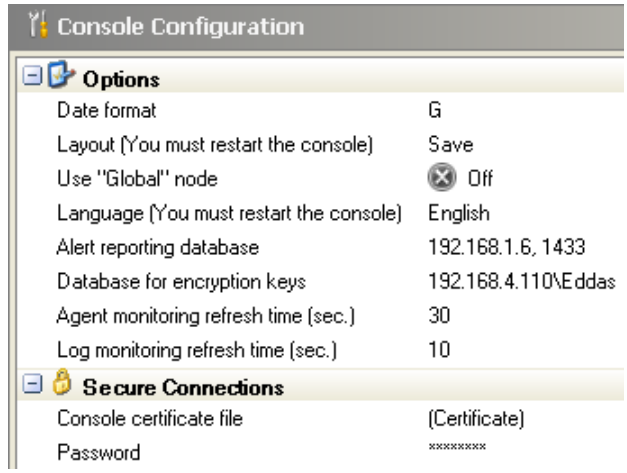


Fig. 4.4: Console Configuration panel

Options

In the **Options** area, the administrator can modify the following:

- **Date format**

  You can change the date format used throughout the console.

  You can use either of the following formats:

  - dddd/MM/yyyy.
  - dd/MM/yy.
  - dd/MM/yyyy.

- **Layout**

  You can adjust the size of panels and columns and save your modifications.

  You must restart the console for the new layout to take effect.

- **Language**

  You can change the console display language by using one of the following methods:

  - Double-click in the column on the right until the required language appears.
  - Click in the column on the right and the browse button ... and finally select the required language from the list.
  - You must restart the console for the new language to take effect.

- **Database for log monitoring**

  Select the SQL server instance that you want to use to monitor logs.

- **Database for encryption keys**

  Select the SQL server instance that you want to use to manage encryption keys.

- **Agent monitoring refresh time**

  Enter in seconds the refresh time to use for log monitoring (time interval between each refresh).

- **Log monitoring refresh time**

  Enter in seconds the refresh time to use for agent monitoring (time interval between each refresh).

Secure Connections

In the **Secure Connections** area, you can modify:

- The filepath used for the security certificates that protect communications between the console and the StormShield server.
- The password set when installing the server to prevent any illegal use of the certificates.

Chapitre 5

STORMSHIELD SERVER CONFIGURATION

ABOUT THIS CHAPTER

This chapter presents the StormShield server and its configuration editor.

It includes the following:

- Configuration editor
  - Server Roles
  - Network settings
  - Log Monitoring Configuration
  - Encryption
  - Antivirus Update
  - Cluster Settings
  - Software Updates Settings
  - Authentication Service

CONFIGURATION EDITOR

The configuration editor of the StormShield server includes the following areas:

- Server Roles.
- Network.
- Log Monitoring Configuration.
- Encryption.
- Antivirus Update.
- Cluster Settings.
- Software Updates Settings.
- Authentication Service.

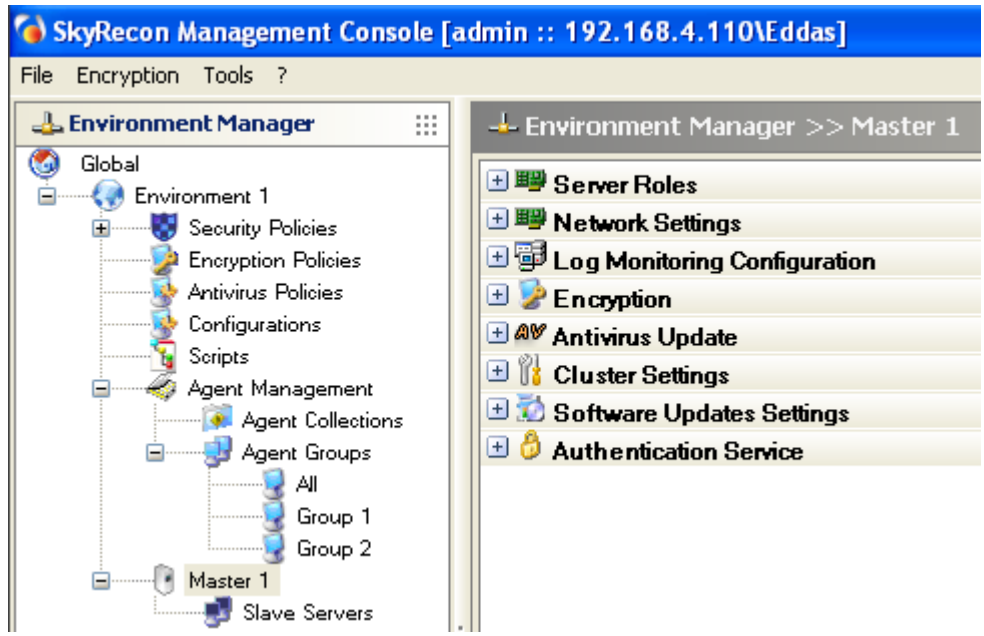


Fig. 5.1 : Configuration editor of the StormShield server

SERVER ROLES

The graphical interface of the Server Roles function is displayed as follows:

Fig. 5.2 : Master server: Server Roles

- **StormShield server**:

  This function is set to Enabled or Disabled.

  If the function is set to **Disabled**, the following parameters are disabled:

  - Encryption.
  - Cluster Settings.
  - Authentication Service.

- **Antivirus server**:

  This function is set to Enabled or Disabled.

  It enables or disables the antivirus server.

  If the function is set to Off, Antivirus Update remains disabled.

NETWORK SETTINGS

The graphical interface of the Network Settings function is displayed as follows:

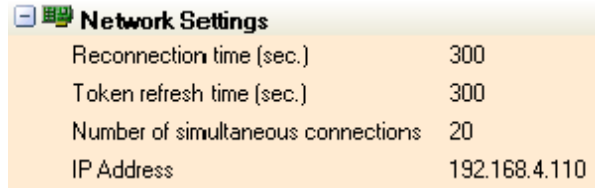


Fig. 5.3 : Master server: Network

- **Reconnection time (sec.)**:

  This is the time interval between each attempt to reconnect to the server, made by disconnected StormShield agents.

- **Token refresh time (sec.)**:

  This is the time interval between each token transmission made by the server to the agents.

- **Number of simultaneous connections**:

  This is the number of agents which can connect simultaneously to the StormShield server.

- IP Address:

  This is the server IP address.

LOG MONITORING CONFIGURATION

The graphical interface of the Log Monitoring Configuration function is displayed as follows:

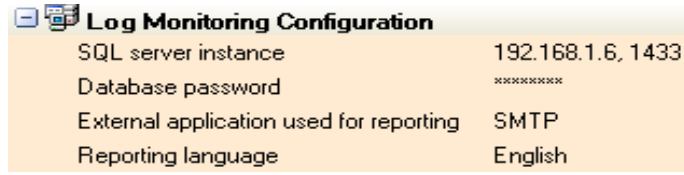


Fig. 5.4 : Master server: Log Monitoring Configuration

- **SQL server instance**:

  Enter the IP address of the SQL server instance used for the log database.

- **Database password**:

  This is the password used for the log database account.

  It was defined when installing the StormShield database.

- **External application used for reporting**:

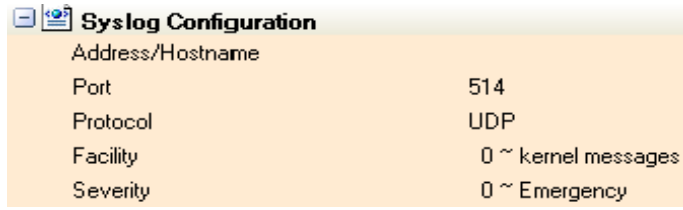
  You can select an application for exporting logs:

- **None**.

  If you choose **None**, the configuration editor of the master server will not bemodified.

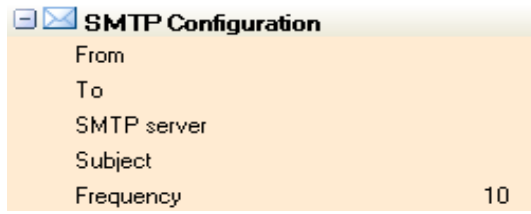
- **Syslog**.

  If you choose **Syslog**, the configuration editor of the master server will displaythe following section above Cluster:



- **SMTP**.

  If you choose **Syslog**, the configuration editor of the master server will displaythe following section above Cluster:



- **Reporting language**:

  This is the language used for log reporting.

ENCRYPTION

The graphical interface of the Encryption function is displayed as follows:

Fig. 5.5 : Master server: Encryption

- **Decrypt data at uninstallation**:

  Encrypted data on the agent computer will be automatically decrypted when uninstalling StormShield.

Only files encrypted with a computer key can be automatically decrypted.

- **Start date of allow uninstall**:

  It defines the date and time for starting the uninstallation of the StormShield agents.

- **End date of allow uninstall**:

  It defines the date and time for finishing the uninstallation of the StormShield agents.

- **SQL server instance**:

  Enter the IP address of the SQL server instance used for the key database.

- **Database password**:

  Enter the password of the key database.

ANTIVIRUS UPDATE

The graphical interface of the Antivirus Update function is displayed as follows:

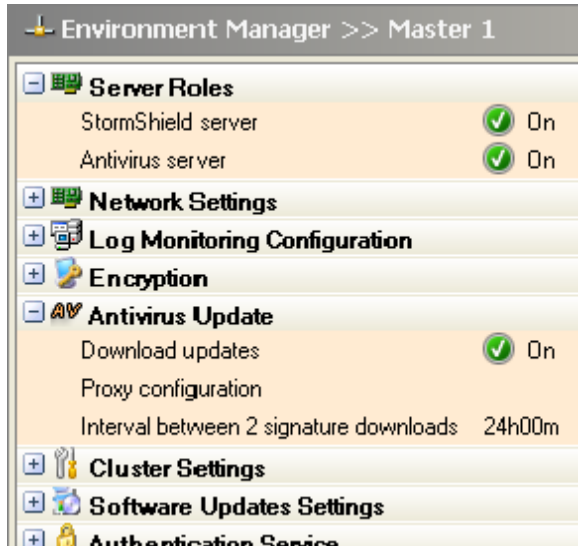


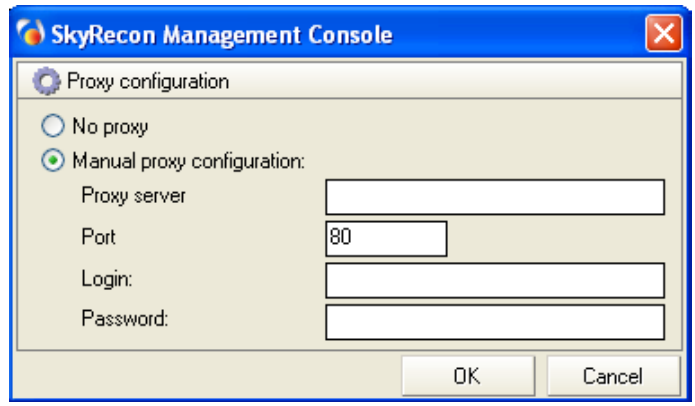
Fig. 5.6 : Master server: Antivirus Update

- **Download updates**:

  You can enable/disable the automatic update of the antivirus to the antivirus server.

- **Proxy configuration**:

  If necessary, enter the Proxy HTTP server parameters.



- **Interval between 2 signature downloads**:

  This is the time interval between two antivirus signature downloads.

  You can modify the interval for updating antivirus signatures.

  By default, this interval is set to 24 hours.

CLUSTER SETTINGS

The graphical interface of the Cluster Settings function is displayed as follows:

Fig. 5.7 : Master server: Cluster Settings

- **Monitoring interval**:

  The master server starts communicating with the slave servers and runs checks.

- **Communication timeout**:

  This is the time delay (30 seconds) after which a slave server is considered unavailable.

SOFTWARE UPDATES SETTINGS

The graphical interface of the Software Updates Settings function is displayed as follows:

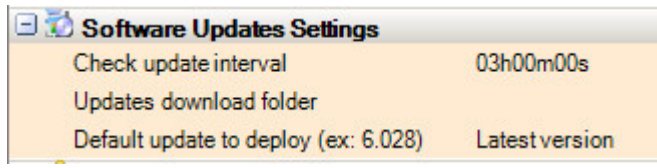


Fig. 5.8 : Master server: Software Updates Settings

- **Check update interval**.
- **Updates download folder**.
- **Default update to deploy**.

For more information, see section "Graphical interface", page 124.

AUTHENTICATION SERVICE

The graphical interface of the Authentication Service function is displayed as follows:

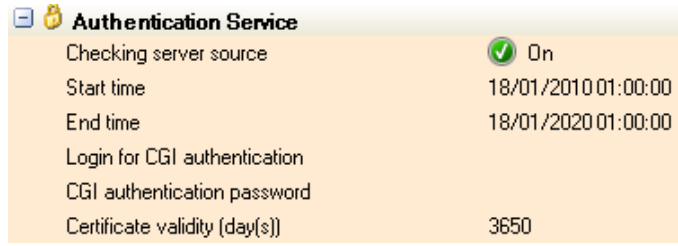


Fig. 5.9 : Master server: Authentication Service

- **Checking server source**:

  When set to **Enabled**, only the StormShield agents deployed from this server installation are authorized to connect to the servers of this environment.

  When set to **Disabled**, any StormShield agent can connect to the server.

- **Start time**:

  This is the date to start the certificate deployment.

- **End time**:

  This is the date to finish the certificate deployment.

- **Login for CGI authentication**:

  This is the login of the account used to download manually an agent certificate from webpage `https://[server IP address]/ssl/cgi`.

- **CGI authentication password**:

  This is the password of the account used to download manually an agent certificate from webpage `https://[server IP address]/ssl/cgi`.

- **Certificate validity** (day(s)):

  You can modify the period of validity assigned to agent certificates (by default 10 years).

Chapter 6

STORMSHIELD AGENT CONFIGURATION

ABOUT THIS CHAPTER

This chapter presents the StormShield agent and its configuration by the Administrator via the **Configuration Editor**.

It includes the following:

- Agent port configuration.
- Configuration Editor:
  - Agent Configuration.
    - Notification (pop-up).
    - Agent protection mode.
    - User interface.
    - Allow Stop Agent.
    - Enable logs.
  - Temporary Web Access.
    - Configuration from the console.
    - Configuration from the agent.
    - Send Network Interface Information.
  - Learning.
  - Antivirus Configuration.
    - Environment Manager.
    - Configuration Editor.
- Applying a configuration to an agent group.

AGENT PORT CONFIGURATION

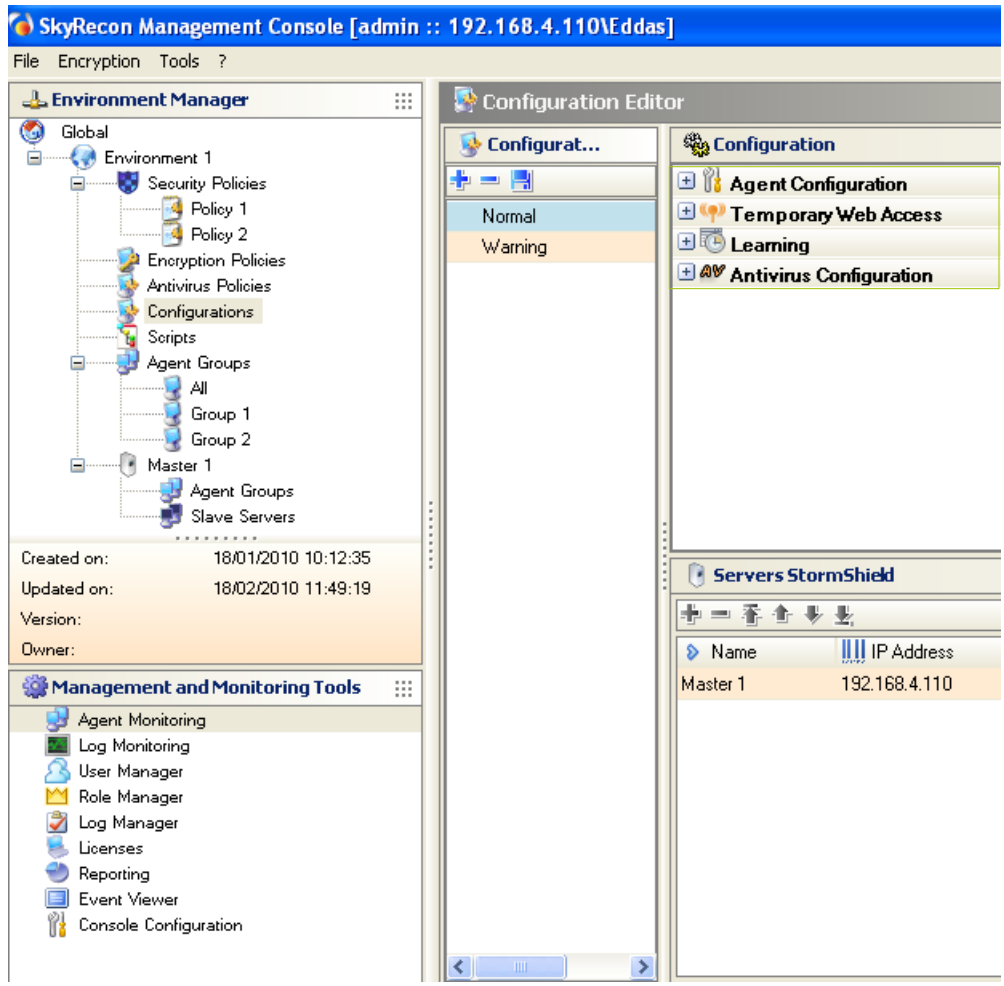
TCP ports 16005 and 16006 are reserved for the StormShield agent.

When testing agent/server communication, the agent will block any communication software from using these ports (example: `telnet`).

CONFIGURATION EDITOR

The Configuration Editor below Configuration includes **four** areas:

1. Agent Configuration.
2. Temporary Web Access.
3. Learning.
4. Antivirus Configuration.



AGENT CONFIGURATION

The graphical interface of the Agent Configuration function is displayed as follows:

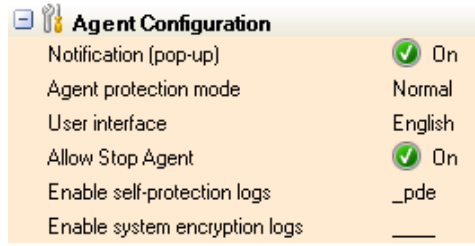


Fig. 6.1: Agent Configuration

Notification (pop-up)

This option enables/disables the pop-ups displayed on the StormShield agent.

Agent protection mode

The graphical interface of the Agent protection mode function is displayed as follows:

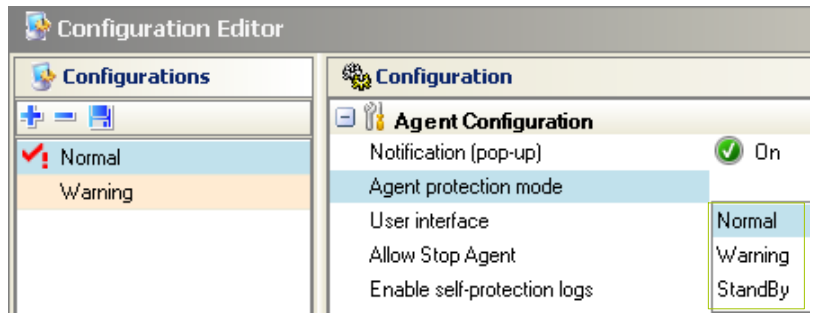


Fig. 6.2: Agent Configuration: Agent protection mode

There are **three** agent protection modes:

- **Normal**:

  The agent applies the policy.

  This mode blocks and logs.

  On the agent, this mode is indicated by the following StormShield Monitor icon:  .

- **Warning**:

  The agent does not apply the policy but it provides a warning log showing what is blocked by the policy.

  This option is used to see what the policy does in order to modify the latter if need be. This option can be used for simulation.

  This mode does not block but logs.

  On the agent, this mode is indicated by the following StormShield Monitor icon:  .

- **StandBy**:

  The agent applies no policy and keeps no warning log.

  It acts as a “pause” mode that can be used when you do not want to apply a specific policy (example: during server installation).

  This mode does not block and does not log either.

  On the agent, this mode is indicated by the following StormShield Monitor icon:  .

User interface

This option is used to select the user interface language on the StormShield agent.

Allow Stop Agent

The Allow Stop Agent option is handled in **five** stages:

1. Console settings.
2. If the Allow Stop Agent option is set to **On**.
3. If the Allow Stop Agent option is set to **Off**.
   - User procedure.
   - Administrator procedure.
4. If the user wants to uninstall the agent.
5. If the user wants to stop a temporary action in progress.

Console settings

In the Configuration Editor, the administrator can set **Allow Stop Agent** to **On** or **Off**.

- If this option is set to **On**, the user who has administrator rights on his workstation can stop the agent by simply running `stopagent.exe`.

  For more information, see "If the Allow Stop Agent option is set to ON", page 210.

  After the agent is installed but before certificates are downloaded, the default setting for **Allow stop agent** is **On**.

- If this option is set to **Off**, the user can request the administrator that the agent be temporarily stopped.

  For more information, see "If the Allow Stop Agent option is set to OFF", page 212.

  The user and the administrator will use the **challenge** procedure. For more information, see "Temporary action scripts", page 427.

Allow Stop Agent is to be used carefully since agent deactivation makes a workstation vulnerable to attacks of the virus or *keylogging* type.
Keylogging is used to capture keyboard events in order to steal passwords and other confidential information)

Nevertheless, it may be useful to stop the agent in a test environment.

If the Allow Stop Agent option is set to ON

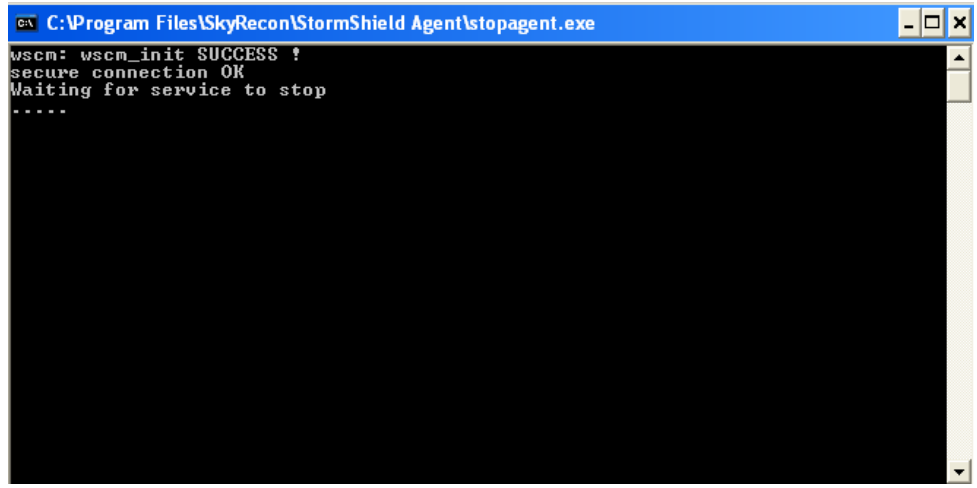
To stop the agent, the user must follow the steps below:

1. Go to the directory below:

   `[Program Files]\Skyrecon\StormShield Agent`

2. Double-click the `stopagent.exe` file.

3. Wait for the window to close:



4. Right-click the StormShield Monitor icon and select **Status** to check that the agent has effectively stopped.

5. To re-enable the agent, click **Activate** in the **Status** window.

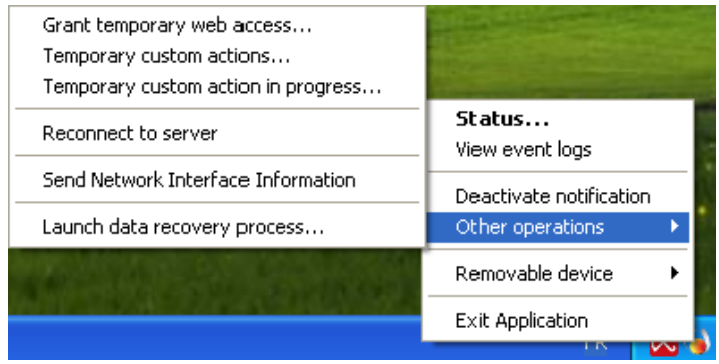
If the Allow Stop Agent option is set to OFF

To stop the agent, the user should ask the administrator to deactivate the agent on a temporary basis.

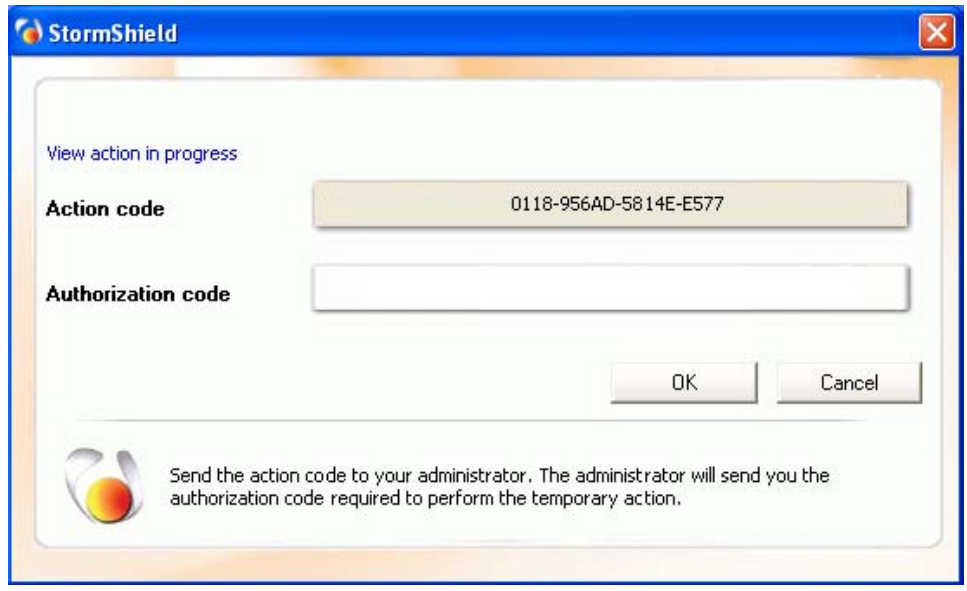
User procedure

The user must follow the steps below:

1. Click the StormShield Monitor icon and select **Other operations > Temporary custom actions**.

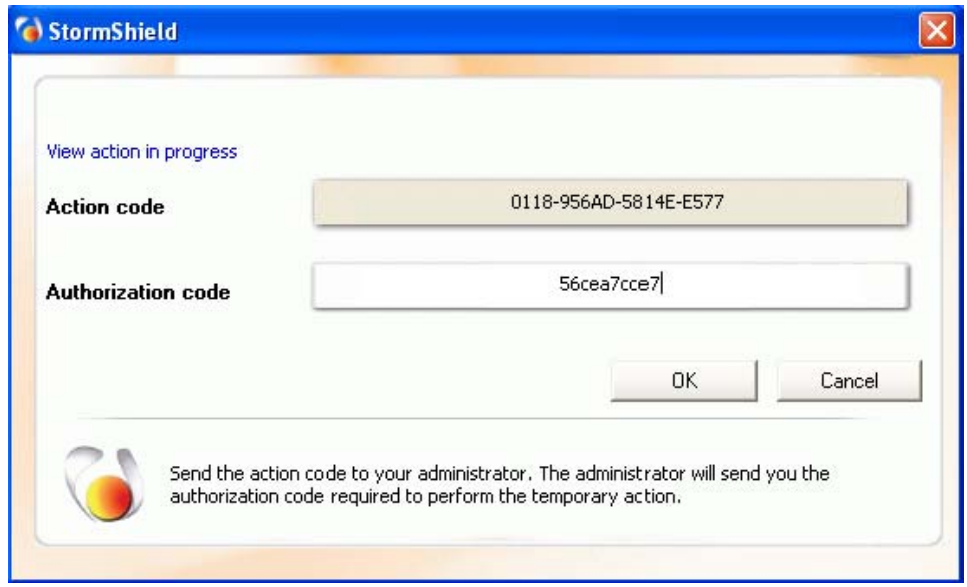


2. Send the **Action code** which is displayed to the administrator.



The administrator will send you the **Authorization code** which is displayed on his console.

3. In the **Authorization code** field, enter the code given by the administrator.



4. Click **OK**.

   The agent will be disabled for the time duration specified by the administrator.

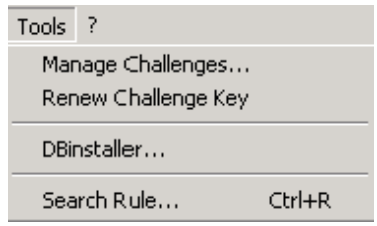
> If the action selected is **Disable Protections**, you must wait at least 30 seconds before agent protection stops. In other cases, the action selected takes effect immediately.

5. Right-click the StormShield Monitor icon and select **Status** to check that the agent has effectively stopped.

Administrator procedure

To answer the request sent by a user who wants to deactivate temporarily his StormShield agent, the administrator must follow the steps below:

1. On the SkyRecon management console, select **Tools > Manage Challenges**.



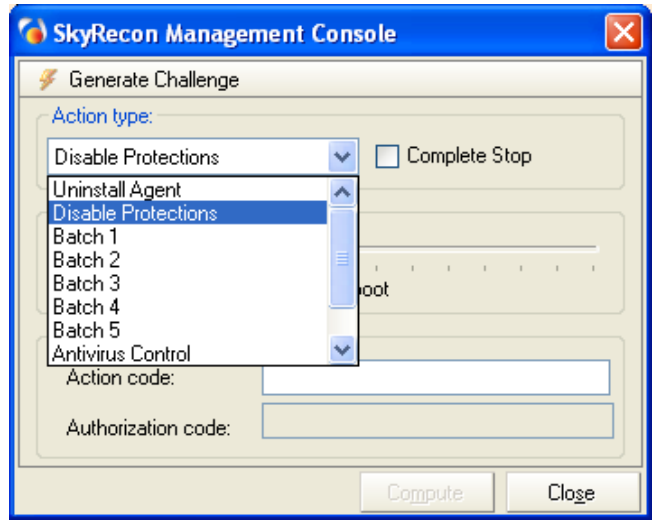
2. Define the following parameters:

   - **Action type** using to display the list of temporary actions.

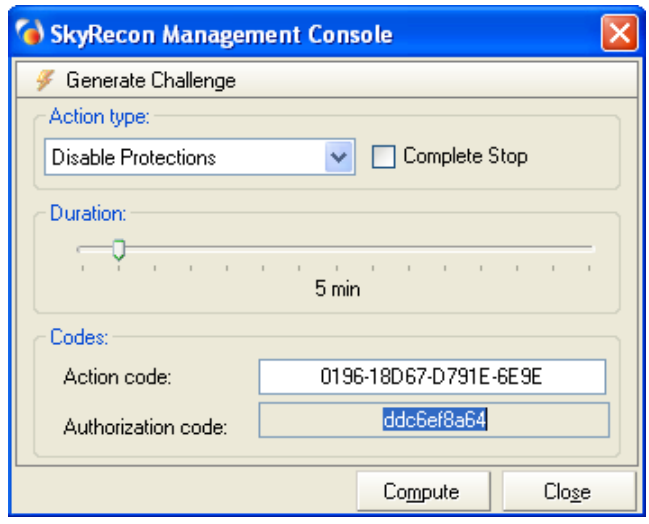
     If you check the **Complete Stop** box opposite Disable Protections, the agent will stop completely and will not switch to Activated - Stand-by mode.

     Therefore, no log will be sent and no policy will be applied.

   - **Duration** of the temporary action by sliding the cursor along the timeline.
   - Enter the **Action code** sent by the user.



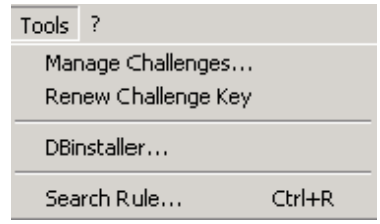
3. Click **Compute** to obtain the Authorization code.



4. Send this code to the user.

If the Administrator wants to renew the challenge code key, just click **Tools > Renew Challenge Key**.

It is recommended to renew the challenge key every fortnight when using challenges regularly.



If the user wants to uninstall the StormShield agent

On condition that the user has administrator rights to the agent computer and the **Allow stop agent** option is set to **On** on the console, the user can uninstall the agent by running `Srend.exe`.

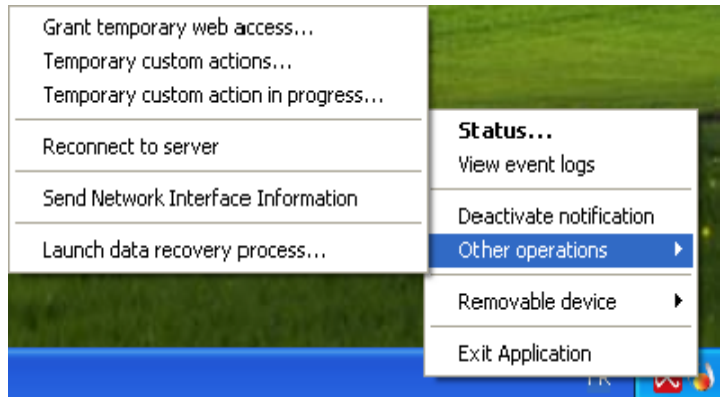
To uninstall the agent, the user must follow the steps below:

1. Go to the `[Program Files]\skyrecon\StormShieldAgent` directory.
2. Double-click the `Srend.exe` file.
3. Restart the computer to complete the agent uninstallation procedure.

If the user wants to stop a temporary action in progress

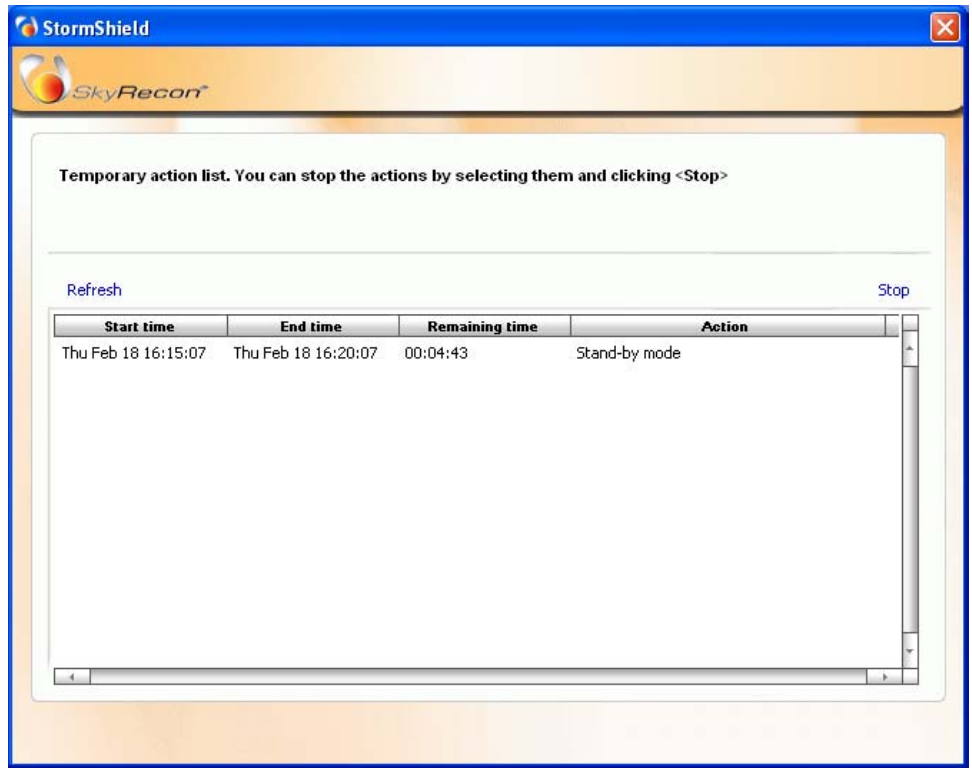
To stop a temporary action which is in progress on his workstation, the user must follow the steps below:

1. Right-click the StormShield Monitor icon and select **Other operations > Custom action in progress**.



2. The list of temporary actions which are in progress on the workstation is displayed.

   Click on the action to be interrupted.



3. Click **Stop**.

Enable logs

Overview

There are **two** types of Enable log options under **Agent Configuration** in the Configuration Editor:

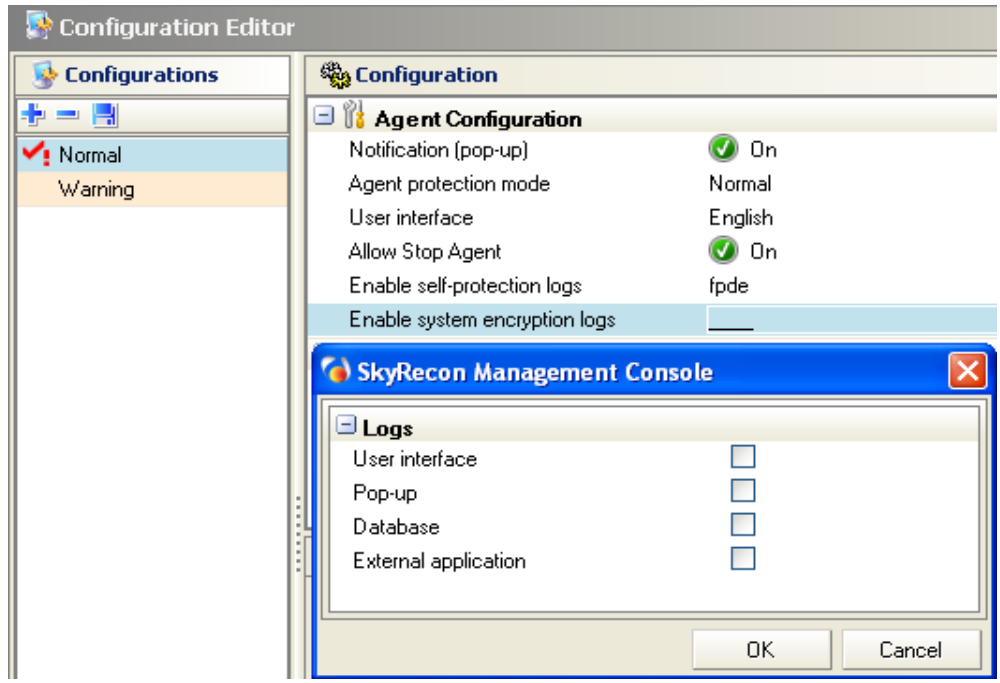
- **Enable self-protection logs**:

  This covers all the logs generated with RID=0.

- **Enable system encryption logs**:

  This covers all the encryption error logs.

Both options let you decide which StormShield logs are displayed and filtered in **Log Monitoring** (Management and Monitoring Tools panel).



Each log option contains the following parameters to save and consult logs:

- **User interface**:

  Logs are displayed on the user interface.

- **Pop-up**:

  Logs are displayed in a pop-up window.

- **Database**:

  Logs are sent to the database.

- **External application**:

  Logs are sent to an external system (examples: syslog or SMTP server).

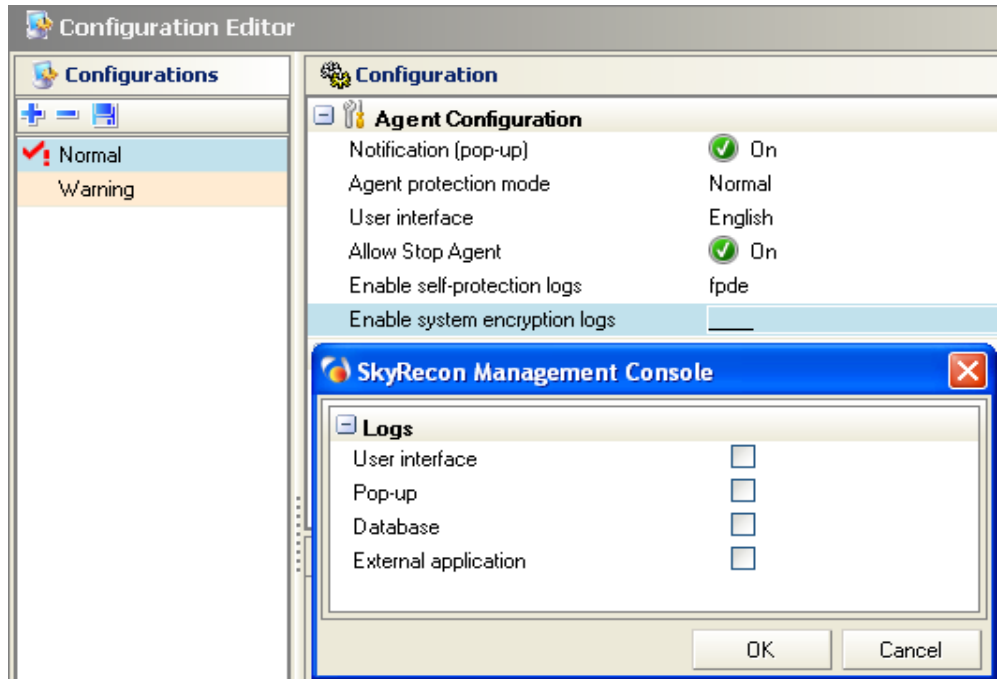
The default setting is set to `[empty]`.

For more information, see "Log Manager", page 620.

Settings for self-protection logs and system encryption logs

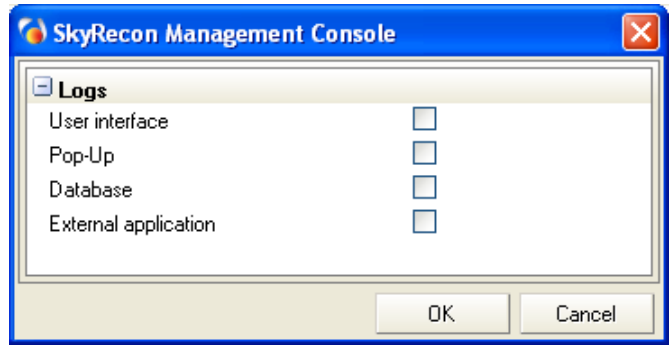
To apply settings to the logs, the administrator must follow the steps below:

1. In the Agent Configuration panel, click in the second column including **Enable self-protection logs** or **Enable system encryption logs**.



A pop-up list of logs is displayed in a window:

- User interface (F/f).
- Pop-Up (P/p).
- Database (D/d).
- External Application (E/e).



2. Select the options to be enabled or disabled.
3. Click **OK**.

Log status

The settings applied by the administrator to log statuses can be consulted and modified in the Security Policy Editor (Log column) and in the Log Manager.

Depending on your settings in Configurations > Agent Configuration, modified log statuses will be visible in the Security Policy Editor and in the Log Manager.

There are three log statuses available:

- **Enabled:**

  A green check ☑ is displayed in a box.

  In each log field, enabled logs are displayed in uppercase letters (examples: F, P, D, E).

  These logs are also visible in the Log Manager.

- **Disabled**:

  A red box ■ is displayed.

  In each log field, disabled logs are displayed in lowercase letters (examples: f, p, d, e).

  These logs are not visible in the Log Manager.

- **Empty**:

  If the box is left empty, the administrator can select a log to be displayed in the Log Manager.

  In each log field, a line in the form of an "underscore" is displayed (example: _pde).

  If the log is empty, the behavior will be the one defined in the Log Manager.

  For more information, see "Log Manager", page 620.

TEMPORARY WEB ACCESS

When access to WiFi is denied, Temporary Web Access allows the agent to establish an HTTP or HTTPS connection.

You can customize the ports enabled by this feature.

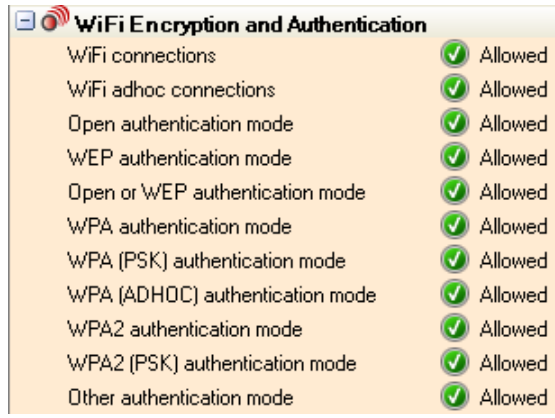
Example: A user working outside the company network will be able to use a WiFi HotSpot to connect to the company's VPN SSL server.

Configuration from the console

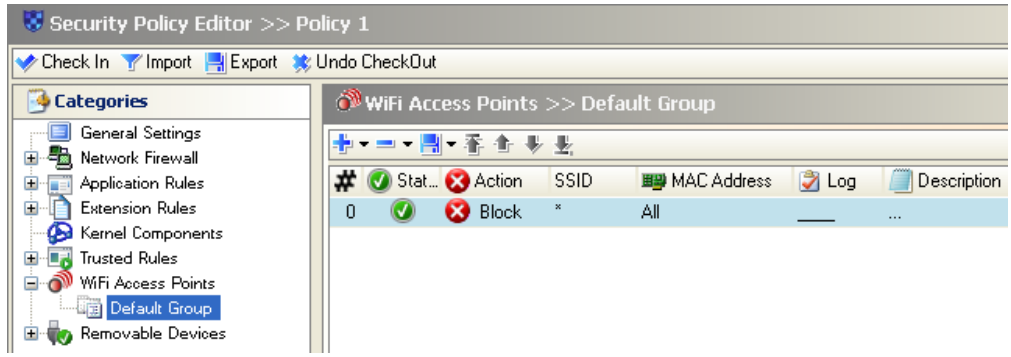
To deny access to WiFi access points and allow use of HotSpots, the administrator must configure the security policy as follows:

1. In the Security Policy Editor, go to Categories > General Settings > **WiFi Encryption and Authentication**.

2. Set **WiFi connections** and **WiFi adhoc connections** to **Allowed**.



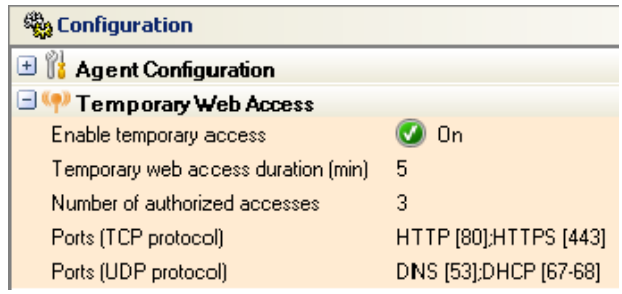
3. Under WiFi Access Points, deny access by creating a rule. Follow the steps below:
   - Edit the security policy.
   - Add a rule by clicking +.
   - Enter the following parameters:
     - SSID value: *****.
     - Action: **Block**.



The administrator can include a whitelist of authorized access points. It should be noted, though, that **WiFi Access Points** rules must be configured as follows:

- Rules with Action set to **Accept** are listed first.
- A final rule (with Action set to **Block** and SSID set to *****) is placed at the bottom of the list.

4. In the Configuration Editor, go to **Temporary Web Access** and set **Enable temporary access** to **On**.



5. Enter the Temporary web access duration in minutes.

   By default, this duration is set to 5 minutes, which is usually enough time for the user to connect to the HotSpot.

   The maximum duration is 30 minutes.

6. Enter the preferred **Number of authorized accesses**.

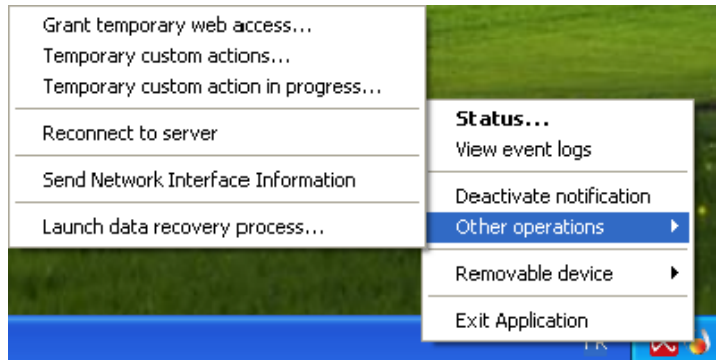
   By default, it is set to 3.

7. If necessary, change or add ports to the ports listed in the **Ports (TCP Protocol)** and **Ports (UDP Protocol)** fields.
   If you include a descriptive comment, you should then include the port number between brackets (example: `HTTP [80]`).

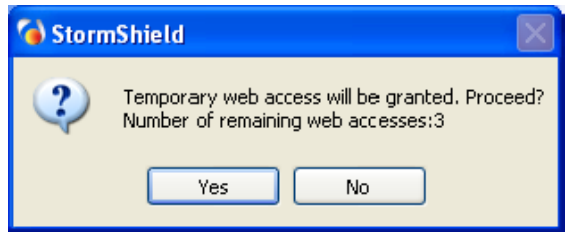
Configuration from the agent

To configure temporary web access from the agent, the user must follow the steps below:

1. Right-click the StormShield Monitor icon .
2. Select **Other operations** and click **Grant temporary web access**.



3. When prompted to proceed, click **Yes**.

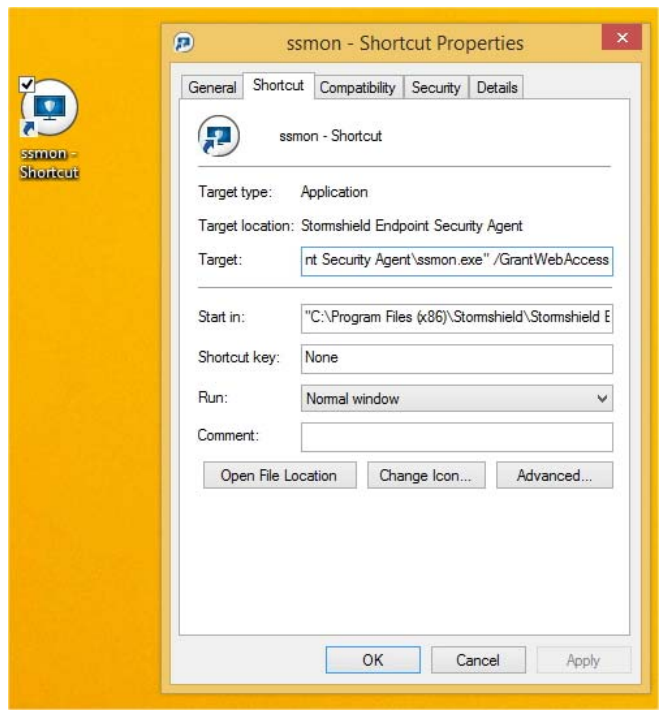


You can now access the web browser for the amount of time specified by the administrator.

The duration is usually long enough to use the browser to sign in to a hotspot or to connect to your company's VPN SSL server.

4. A window is displayed to show that temporary web access has expired.

The user may have the possibility to request temporary web access in a faster way. You can create a shortcut of the ssmon.exe executable file (graphical interface executable located in the agent repository) and place it on the users desktop. In the shortcut target, add the command line argument «/GrantWebAccess». Users just need to double-click the shortcut on their desktop to request temporary web access.



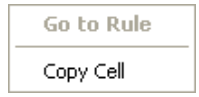
Send Network Interface Information

To retrieve the agent's network interface identifier for later use in the active network interface test (see "Network > Active Network Interface", page 400), follow the steps below:

1. Use a StormShield agent that belongs to the network to send network interface information to the server log:
   - Right-click the StormShield Monitor icon .
   - Select **Other operations** > **Send Network Interface Information**.
2. On the SkyRecon management console, select **Log Monitoring**.
3. Click the **Software** radio button.
4. Locate the log entry of the network interface ID.

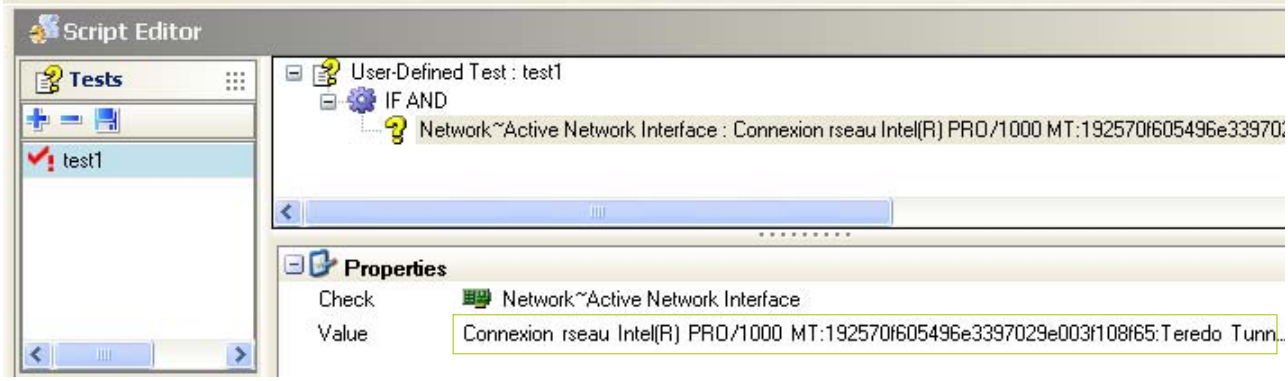
   The entry displays the following information:
   - **Date**.
   - **User Name**: Administrator.
   - **Action**: INFO.
   - **Status**: NET-INT.
   - **Type**: Agent.
   - **Mod. Name**: MODENFORCEMENT.
   - **Log**: Network interface ID.
   - **Agent Mode**.

5. Right-click the log entry.



6. Copy the network interface ID.

7. Paste the network interface ID into the **Value** field in the active network interface **Properties** under Scripts.



LEARNING

The graphical interface of the Learning function is the following:

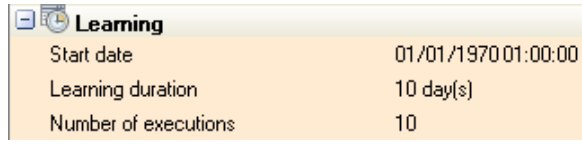


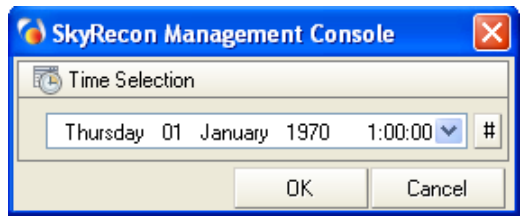
Fig. 6.3: Configurations: Learning

The learning function includes the following options:

1. **Start date**.

   To set the learning period start date, click ...

   Click # to set **Time Selection** to current date.



2. **Learning duration**.

   To define the learning period in days, just click on the field and enter the appropriate value.

3. **Number of executions**.

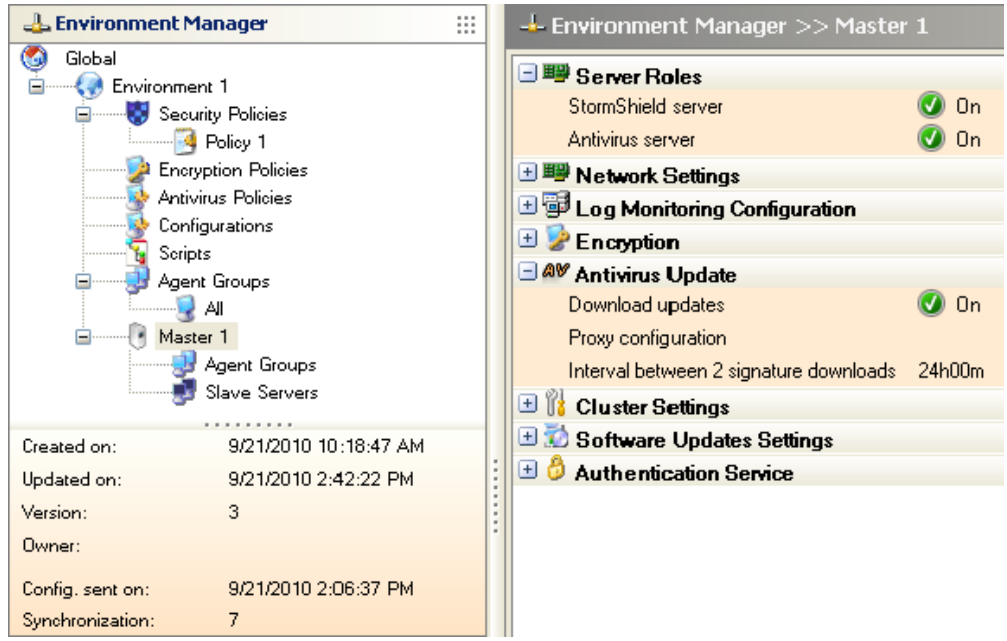
   To define the number of executions per process for creating an application-based profile, just click on the field and enter the appropriate value.

ANTIVIRUS CONFIGURATION

Environment Manager

The antivirus server IP address is set in the StormShield server configuration.

The **Antivirus server** option is enabled at the StormShield server level.

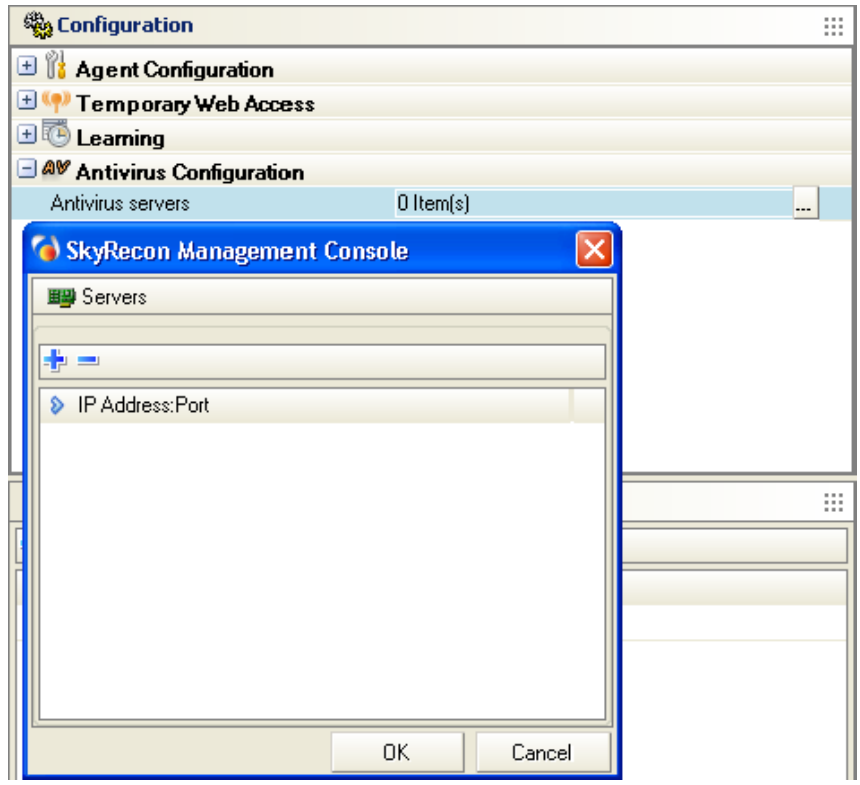


Configuration Editor

Antivirus servers

To configure the antivirus server, the administrator must follow the steps below:

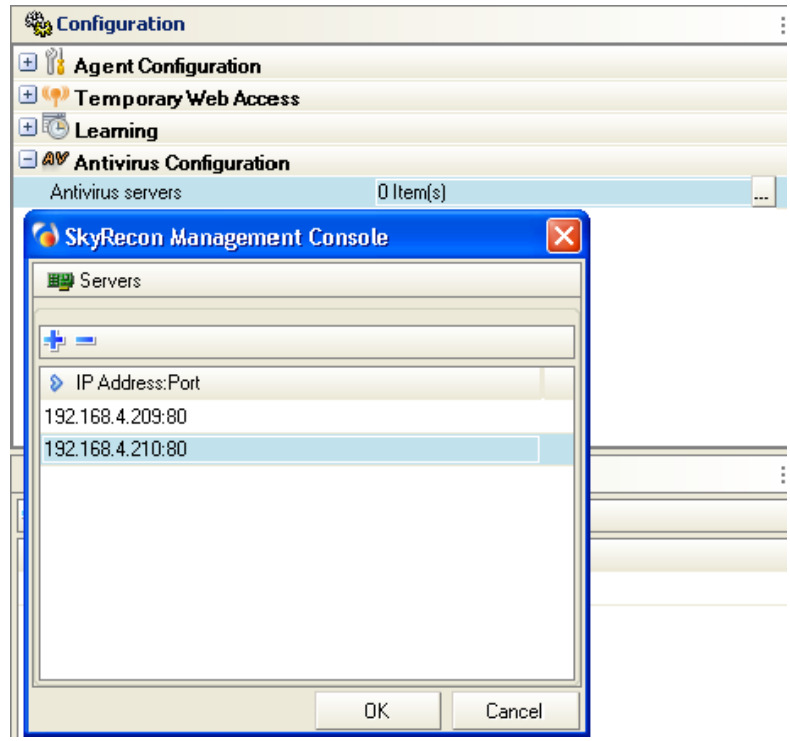
1. In the Antivirus Configuration area, select **Antivirus servers** and click ... .



2. Click + to add the IP address of an antivirus server.
3. Click - to remove an antivirus server from the list.
4. Click **OK** when you have finished.

The antivirus may have one or several servers.

The administrator must specify the port dedicated to each server. The port is the same as the one for the Apache web server.



Enable antivirus administration

The administrator can set Enable antivirus administration to **Enabled** or **Disabled**.

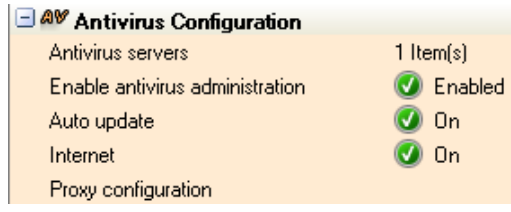
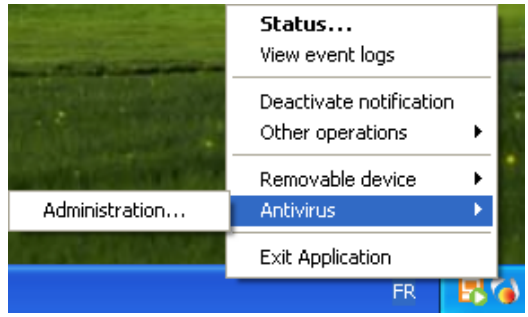


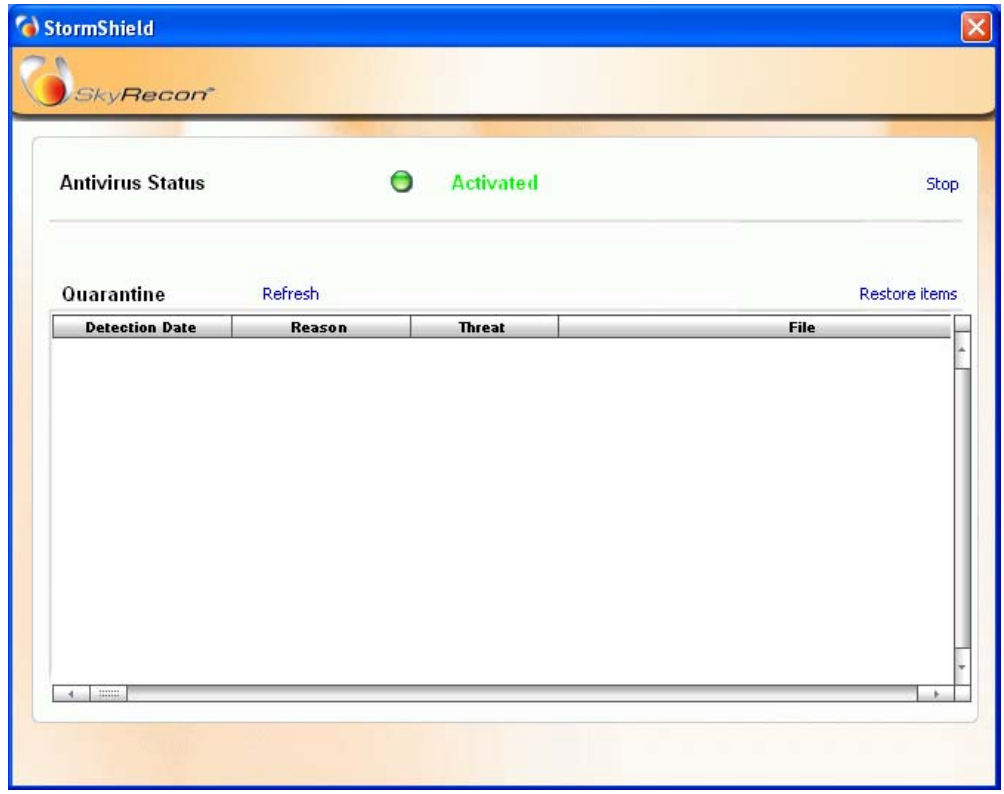
Fig. 6.4: Configurations: Antivirus Configuration

When Enable antivirus administration is set to **Enabled**, the antivirus administration mode on the StormShield agent is enabled.

When this mode is enabled on the agent, the user can access additional options by right-clicking the StormShield Monitor icon .



The user can enable or disable the antivirus protection, and restore quarantined files.



Auto update

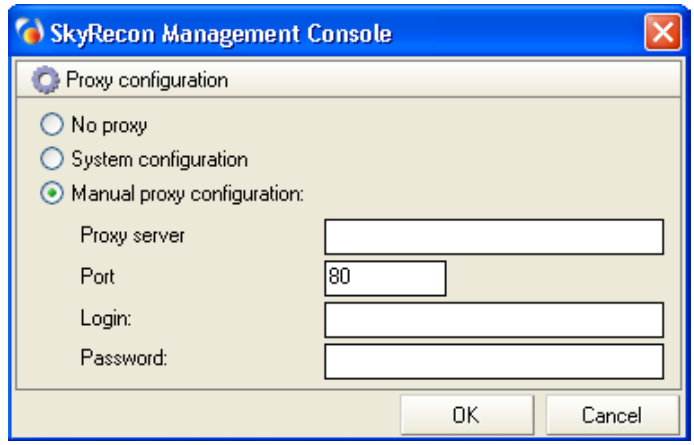
If the **Auto update** option is enabled, the agent automatically connects to the StormShield server to update the antivirus.

Internet

If the **Internet** option is enabled, the agent directly connects to the Avira servers to update the antivirus.

Proxy configuration

The administrator can define the **Proxy configuration** settings used when the agent updates the antivirus.

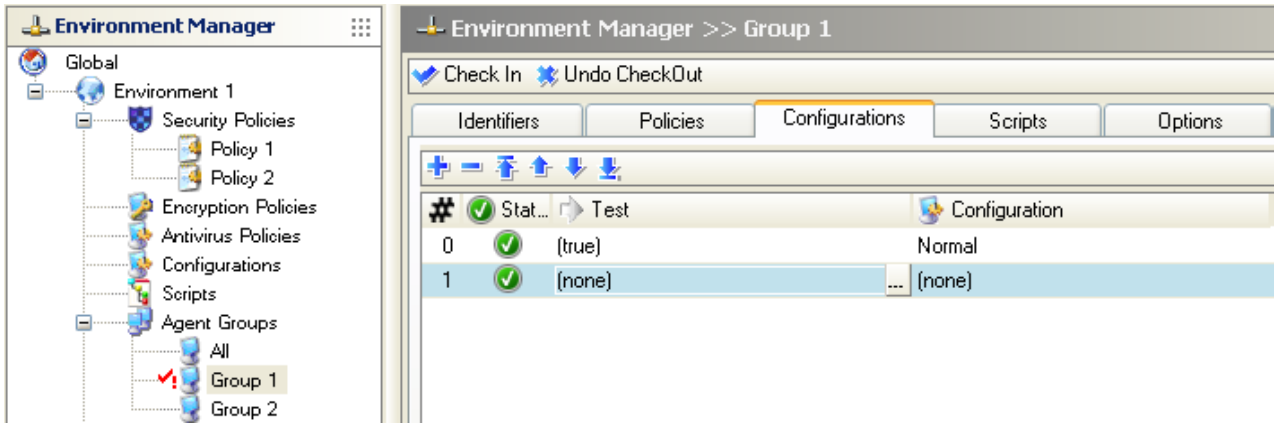


APPLYING A CONFIGURATION TO AN AGENT GROUP

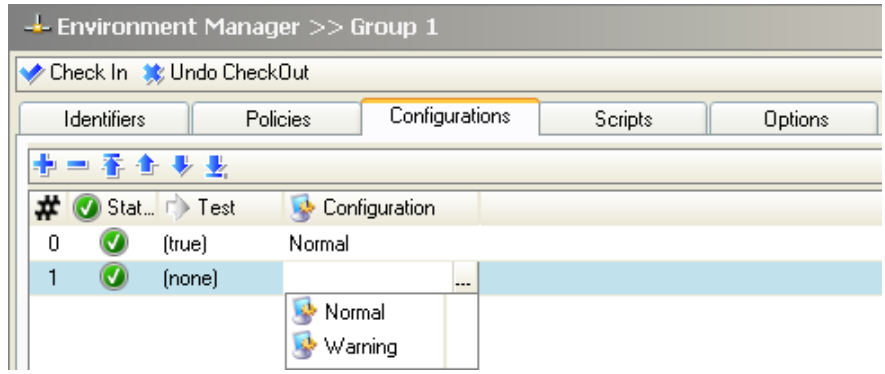
Configurations are assigned to agent groups.

To assign a configuration to an agent group, follow the steps below:

1. Click **Agent Groups** in the Environment Manager.
2. Click on the **Configurations** tab to display the configuration applied to the agent group.



3. To modify the configuration, click in the **Configuration** column to display ... .
   The drop-down list of the existing configurations is displayed.



4. Select the configuration to be applied to the agent group.
5. Validate your modifications.
6. Send the new configuration to the agent groups.

Chapitre 7

SIMPLIFIED MANAGEMENT MODE FOR EXTENDEDXP

ABOUT THIS CHAPTER

This chapter presents the simplified management mode of a StormShield environment for users of the ExtendedXP Service. This service is dedicated to the protection of Microsoft Windows XP operating system.

It includes the following:

- Enabling ExtendedXP mode
- Overview of the Environment Manager panel of the ExtendedXP console
  - Dashboard
    - Deployed agents status
    - Last events histogram
    - Workstations generating most events
    - More significant events over the last few days
  - Monitoring
    - Viewing events
  - Security Policies
    - Creating and removing security policies
    - Editing a security policy
    - Importing templates
  - Agent Groups
    - Creating and removing agent groups
    - Lost and Found group
    - Editing an agent group

ENABLING EXTENDEDXP MODE

To enable the ExtendedXP mode of the SkyRecon console and access the simplified interface, the user requires a specific role with the ExtendedXP permission.

The administrator creates and assigns the ExtendedXP role from the standard SkyRecon console.

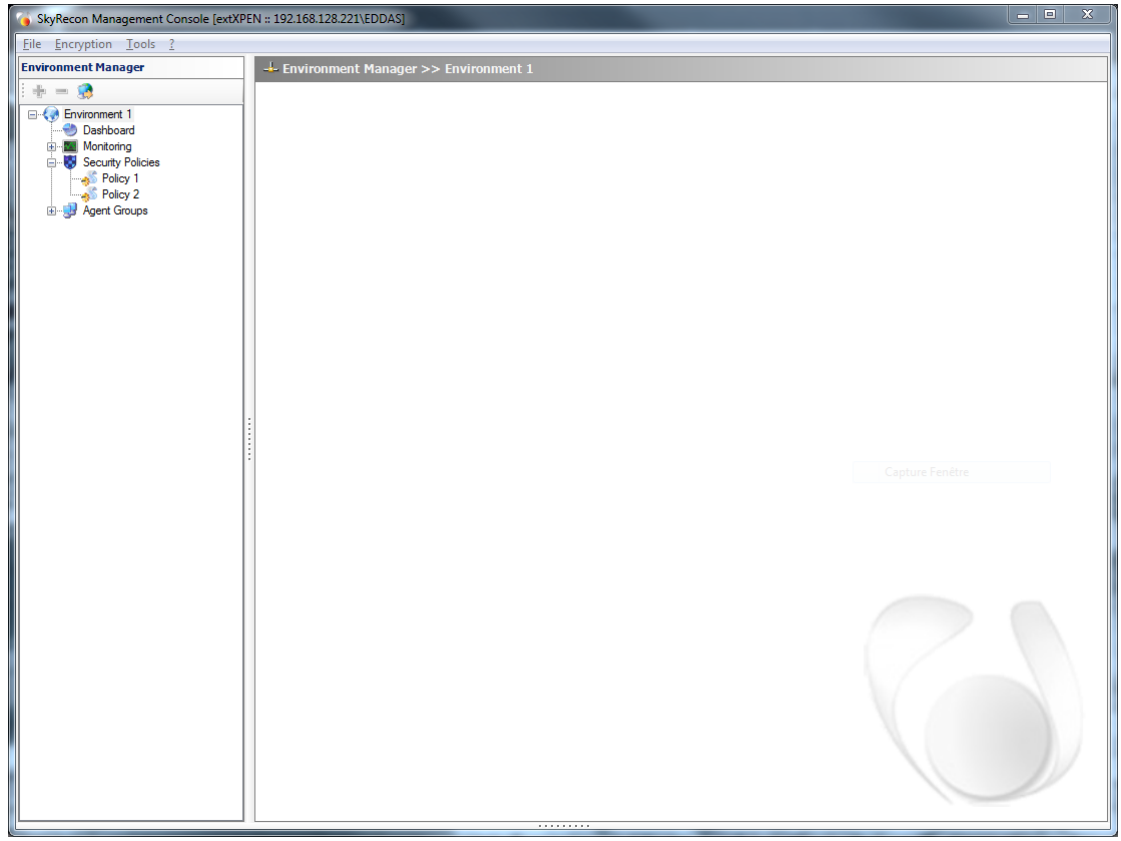
To create and assign the ExtendedXP role to a user, refer to sections "Role Manager", page 189 and "User Manager", page 187.

OVERVIEW OF THE ENVIRONMENT MANAGER PANEL OF THE EXTENDEDXP CONSOLE

When a user with an ExtendedXP role connects to the SkyRecon console, a simplified version of the interface opens.

This version allows the easy administration of Microsoft Windows XP workstations in order to protect this operating system against vulnerabilities.

From the **Environment Manager**, you can consult the dashboard and the logs monitoring. You can also configure security policies and agent groups.



The toolbar above the tree view of the **Environment Manager** allows the following:

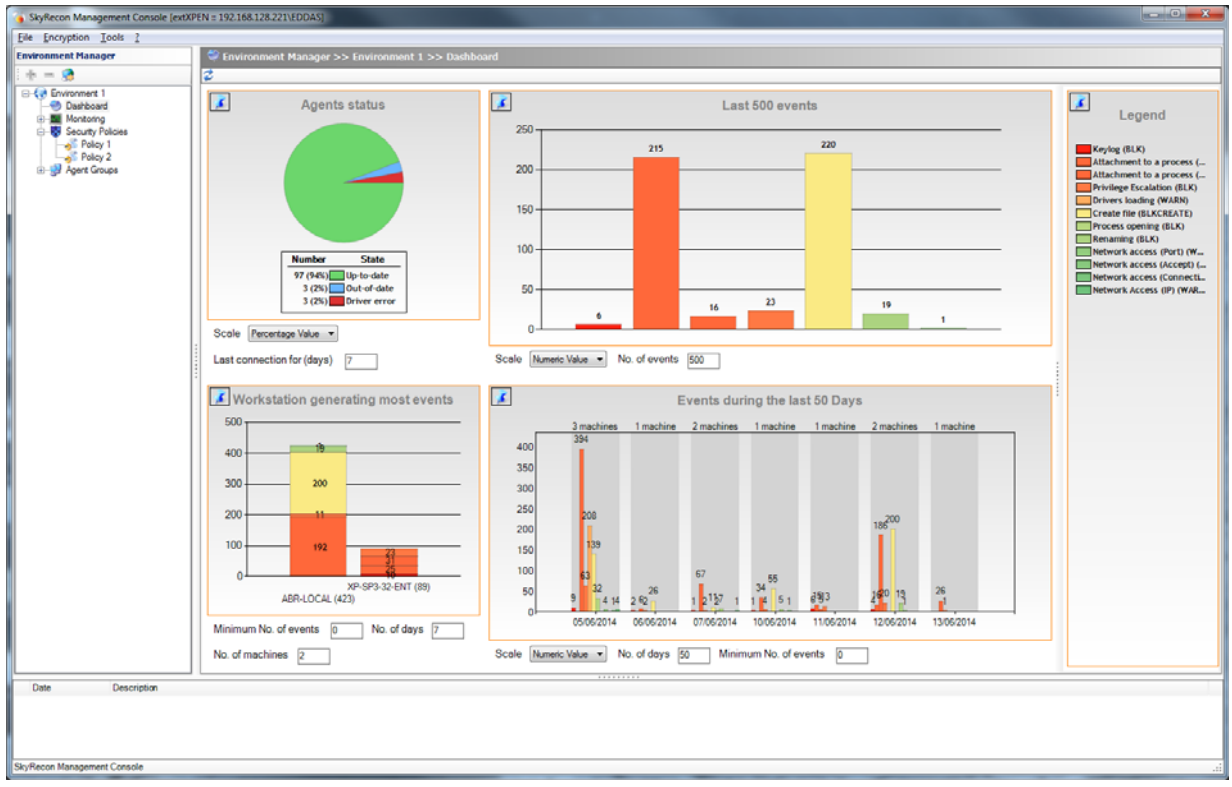
- The icon allows adding a security policy or an agent group depending on the object currently selected in the tree view.
- The icon allows removing a security policy or an agent group depending on the object currently selected in the tree view.
- The icon allows synchronizing the environment.

Synchronizing the environment means sending all data configured in the console (security policies and agent groups) to StormShield servers. Servers will send the information to the appropriate agents. They will then apply the security policy configured in the console.

DASHBOARD

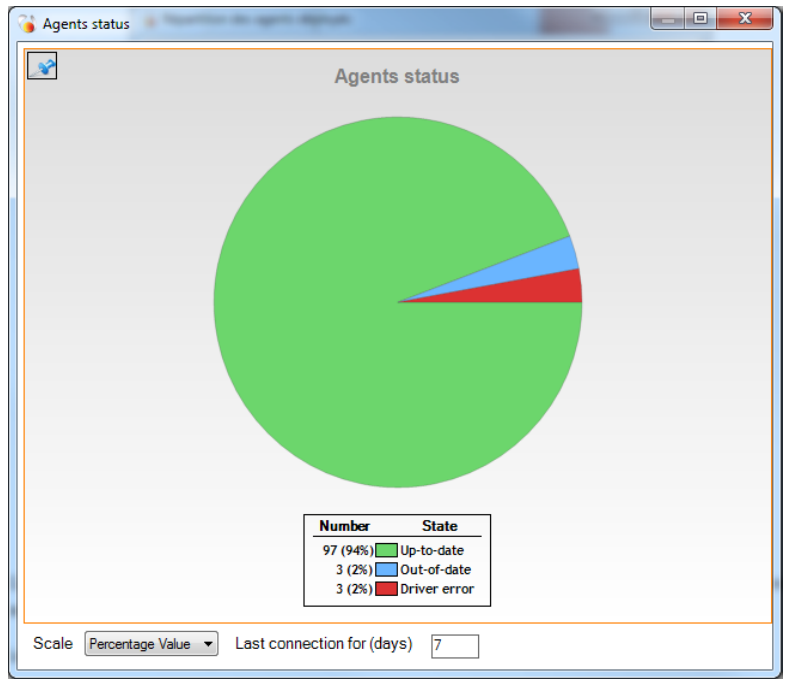
The **Dashboard** provides a global and up-to-date overview of workstations. It shows four configurable charts allowing the user to see various information at a glance.

Each chart can be undocked from the window by clicking the icon. You can browse the other panels of the console while keeping one chart or more undocked.



Deployed agents status

This chart displays the status of all StormShield agents: all agents which have been connected to a server are taken into account in this chart.



The possible statuses are:

- **Up-to-date**: the agent has been connected to a server for less than N days (refer to the chart settings below). The configuration and security policy of this agent are up-to-date and protections are functional.
- **Offline**: the agent has not been connected to a server for more than N days (refer to the chart settings below). The configuration and security policy of this agent are up-to-date.
- **Out-of-date**: the agent did not retrieve yet the last synchronized version of the configuration and security policy. Just after a synchronization of the environment, all the agents have this status, until their next connection to the server. Updating the configuration of an agent can take between a few hours and a few days according to the number of workstations and servers.
- **No Config**: no configuration is assigned to the agent, for example when it is installed on the workstation. It has to retrieve a valid configuration the next time it connects to servers.
- **Driver Error**: the agent cannot activate all protections because one of the drivers has not started or does not have any valid configuration. This is the case when the agent is installed and the machine has not been restarted yet. If the problem persists after restarting the agent, a re-installation will be required.

Chart settings

Scale

Select the type of scale:

- **Percentage Value**: angles are calculated according to the percentage of the total number of agents. This view presents the real distribution of the agents status.
- **Tendency**: angles are calculated according to the logarithm of the percentage of the total number of agents. This view keeps the order of values but allows pointing out small values which can sometimes hardly be seen on a linear scale.

Last connection for (days)

Define the number of days since the last connection agent-server for the agent to be considered as "offline" in the chart. In a local network client environment, the recommended value to identify offline workstations is one or two days.

Last events histogram

This chart displays the N last system events which occurred on agents. It provides an overview of recent activity on agents.

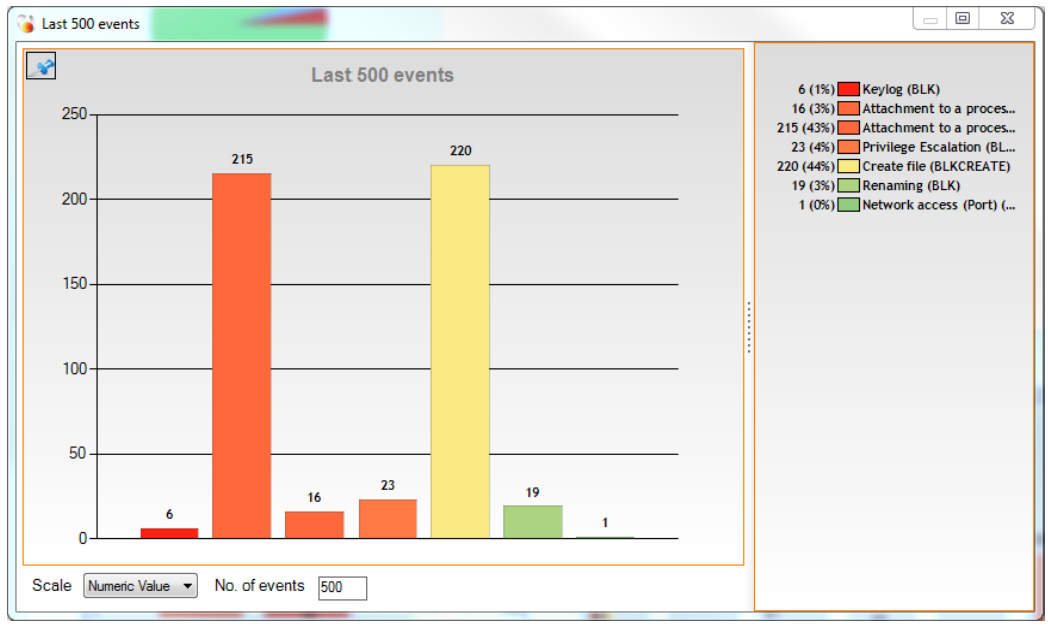


Chart settings

Scale

Select the type of scale:

- **Numeric value**: the height of bars is proportional to the number of events. This view presents the real distribution of events generated by the agents.
- **Tendency**: the height of bars is calculated according to a logarithmic scale. This view keeps the order of values but allows pointing out small values which can sometimes hardly be seen on a linear scale.

Number of events

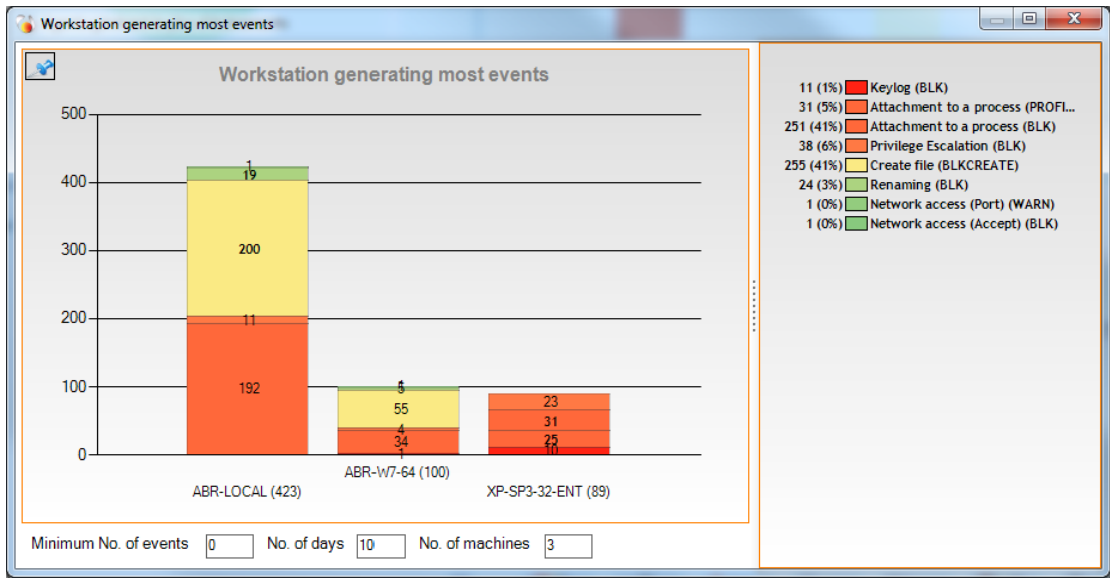
Define the total number of events to be displayed. Adjust the number according to the number of workstations and the log generation policy defined in order to get a precise view of the activity.

For less than 300 workstations, the value 50 is recommended.

For more than 1000 workstations, select a value between 100 and 500.

Workstations generating most events

This chart displays workstations which have generated the most events during the last days. It enables identifying possible attacks if many protection logs have been recently generated on some workstations.



Workstations are displayed in abscissa (X). Bars represent generated events. Events are divided by type and displayed by order of importance.

Chart settings

- **Minimum number of events**: define the minimum number of events a workstation must generate to be considered in this chart. This allows not displaying workstations with a too small amount of events to be considered as significant enough to be displayed.
- **Number of days**: define the number of days for which events have been generated. This allows restricting display to the recent activity of agents: an agent which has generated many old events is considered as less important than an agent which has recently generated events. The value 7 is recommended.
- **Number of machines**: define the maximum number of machines to be displayed. This chart is meant to display only machines which have generated the most events recently. It is thus useless to display too many machines in this chart. The value 10 is recommended.

More significant events over the last few days

This chart displays events generated over the last few days by all workstations. Events are grouped by day and displayed by order of importance.

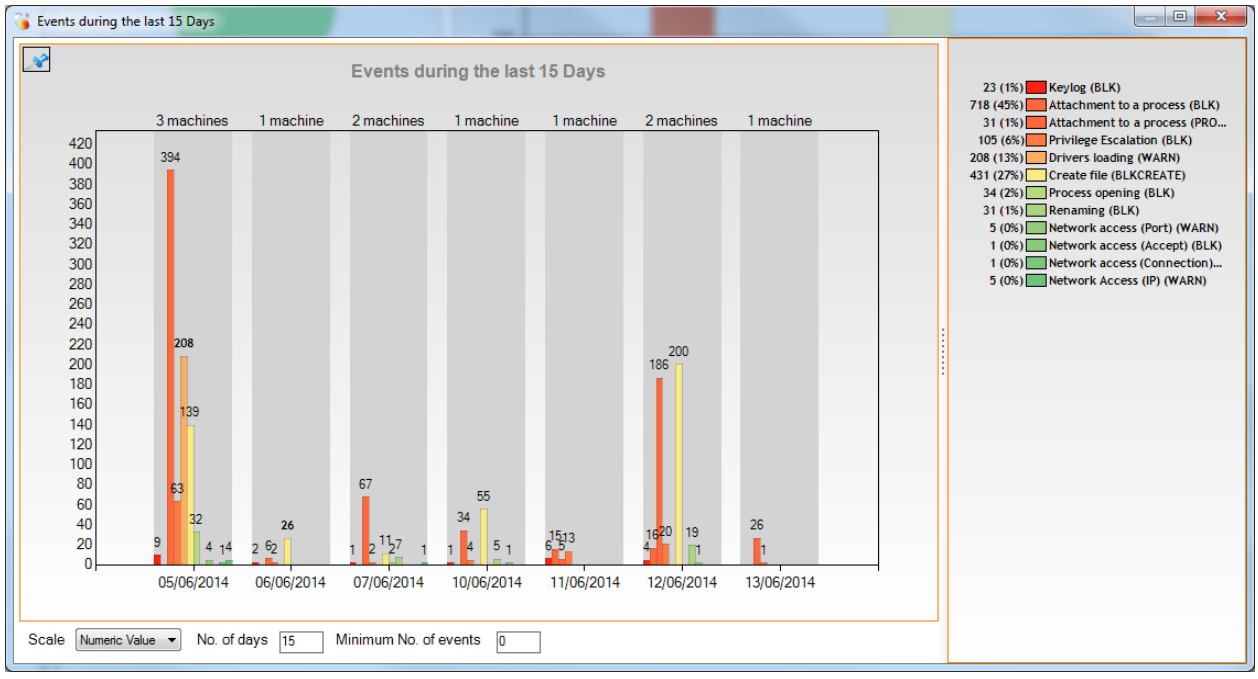


Chart settings

Scale

Select the type of scale:

- **Numeric value**: the height of bars is proportional to the number of events. This view presents the real distribution of events generated by the agents.
- **Tendency**: the height of bars is calculated according to a logarithmic scale. This view keeps the order of values but allows pointing out small values which can sometimes hardly be seen on a linear scale.

Number of days

Define the rolling day period (from the current day) during which events must be displayed.

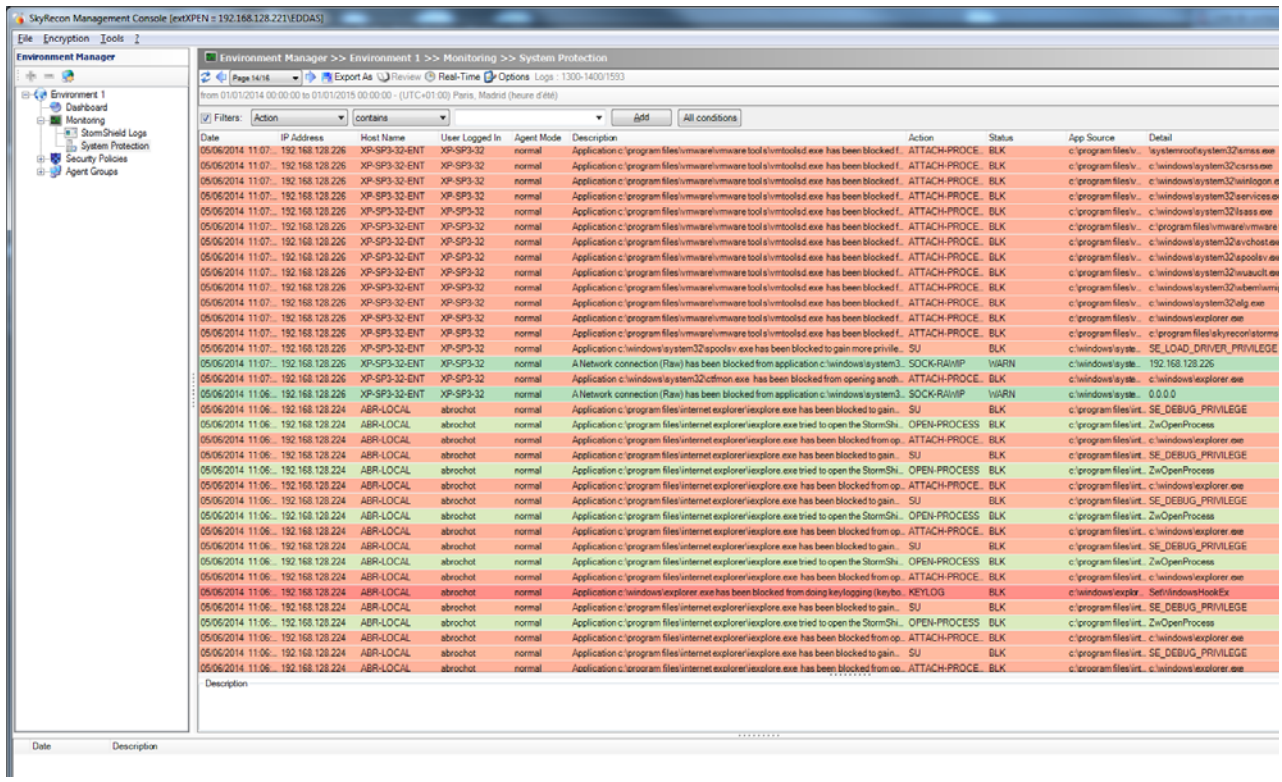
Minimum number of events

Define the minimum number of occurrences of an event on a particular day required to be displayed. Adjust the number according to the number of workstations and the log generation policy defined.

MONITORING

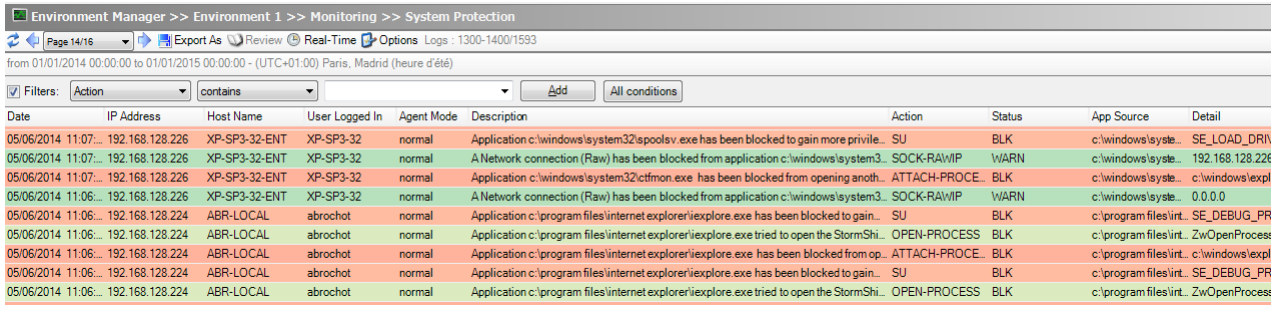
The **Monitoring panel** in the **Environment Manager** displays the different events reported by the StormShield agents. It is composed of two sections:

- **StormShield Logs**: reports events providing information about the operation of the product (policy update, installation, connection to the server, etc.).
- **System Protection**: reports events providing information about the activity of protections applied by the security policy (blocking, warning, etc.).



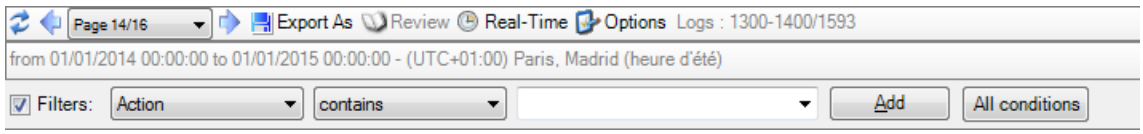
Viewing events

Both logs panels are similar for the two types of available events (**StormShield Logs** and **System Protection**). Only information columns defer.



Toolbar

The toolbar is the same for both event types. It allows browsing the event list, setting up the time period of events to be displayed and creating filters.



Click the  button to manually refresh the event list. Each time the list is refreshed, the log database is queried in order to create an up-to-date event list.

Use the page browser 

to change the page. Set up the number of logs per page in the **Options** menu.

The **Export as** button allows saving all logs (displayed on every pages) in a `txt`, `csv` or `xml` file. The `txt` format separates the columns with commas and the `csv` format with tabs. The `xml` format creates a node for each log and a sub-node for each column.

Select **Review** or **Real-Time** to choose the log display mode:

- **Review** displays logs according to filters and the start/end period selected in the options.
- **Real-Time** displays the latest hour logs and regularly updates the list (according to the period defined in the options).

In the **Options** menu, define the log period to be displayed in Review mode, the number of logs per page and the log monitoring refresh time.

With the filter bar, create a search filter on the different columns:

1. Check the box to activate the filter and enter a value in the search field.
2. Choose the column to be filtered with the first drop-down list.

3. The second drop-down list allows defining the type of comparison to be applied:
   - **contains**: a part of the text entered in the search field matches the text of the column.
   - **is**: the exact text entered in the search field matches the text of the column.
   - d**oes not contain**: the text of the column does not contain the text entered in the search field.
   - **is not**: the text entered in the search field does not exactly match the text of the column.
4. When the three parameters (column, comparison, text) are defined, click the **Add** button or press the Enter key to add the new filter.
5. If several conditions are defined, the **All conditions** button means that all the conditions must match to display a log.

   The **At least one condition** button means that at least one condition must match to display a log.

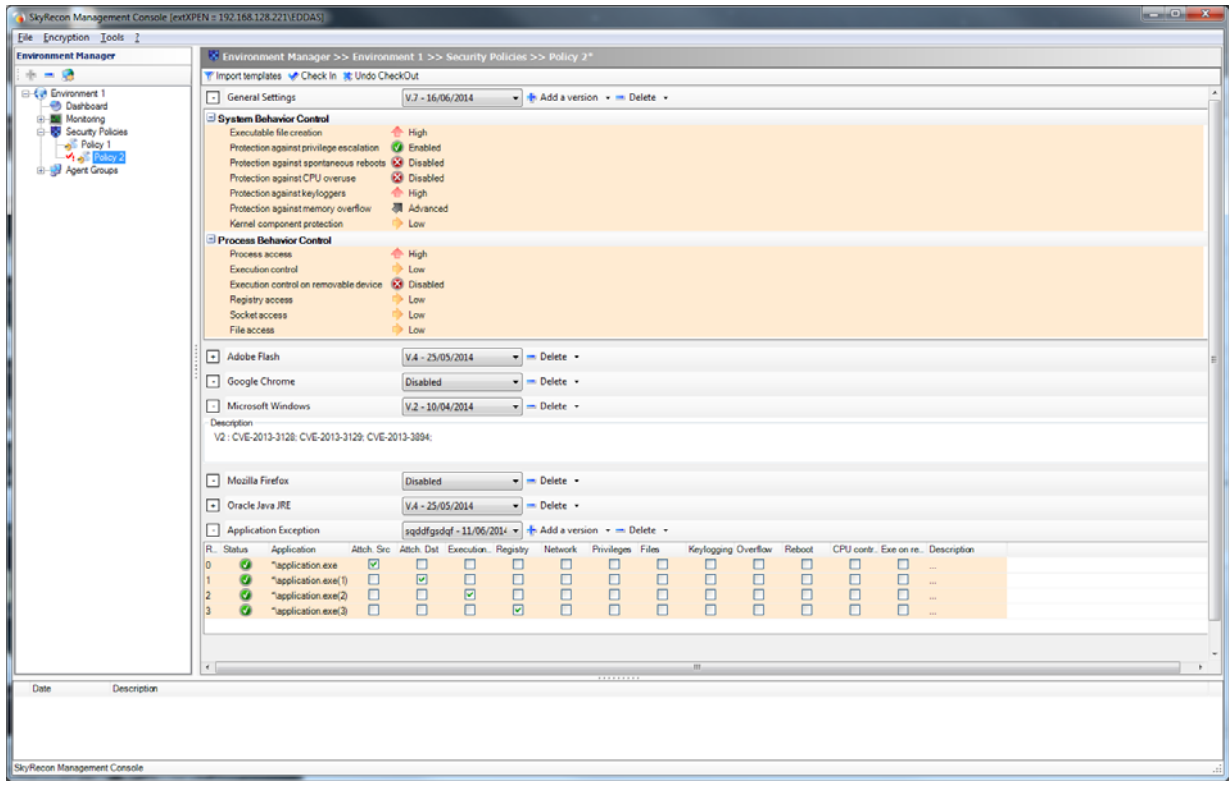
You can also quickly create a filter by selecting a log and right-clicking the line. Choose the inclusion or exclusion filter in order to show or hide logs according to the selected filter criteria.

SECURITY POLICIES

The **Security Policies** panel allows defining the protection level to be applied on workstations with the help of configuration templates provided with the ExtendedXP Service.

For each ExtendedXP templates (**General Settings**, **Application Exceptions**, **Microsoft Windows**, etc.), you can import the provided versions from the interface. Templates are provided in a sczip package. Each time templates are updated, a new version of the package is available.

After importing templates, this panel allows applying them and customizing some options.



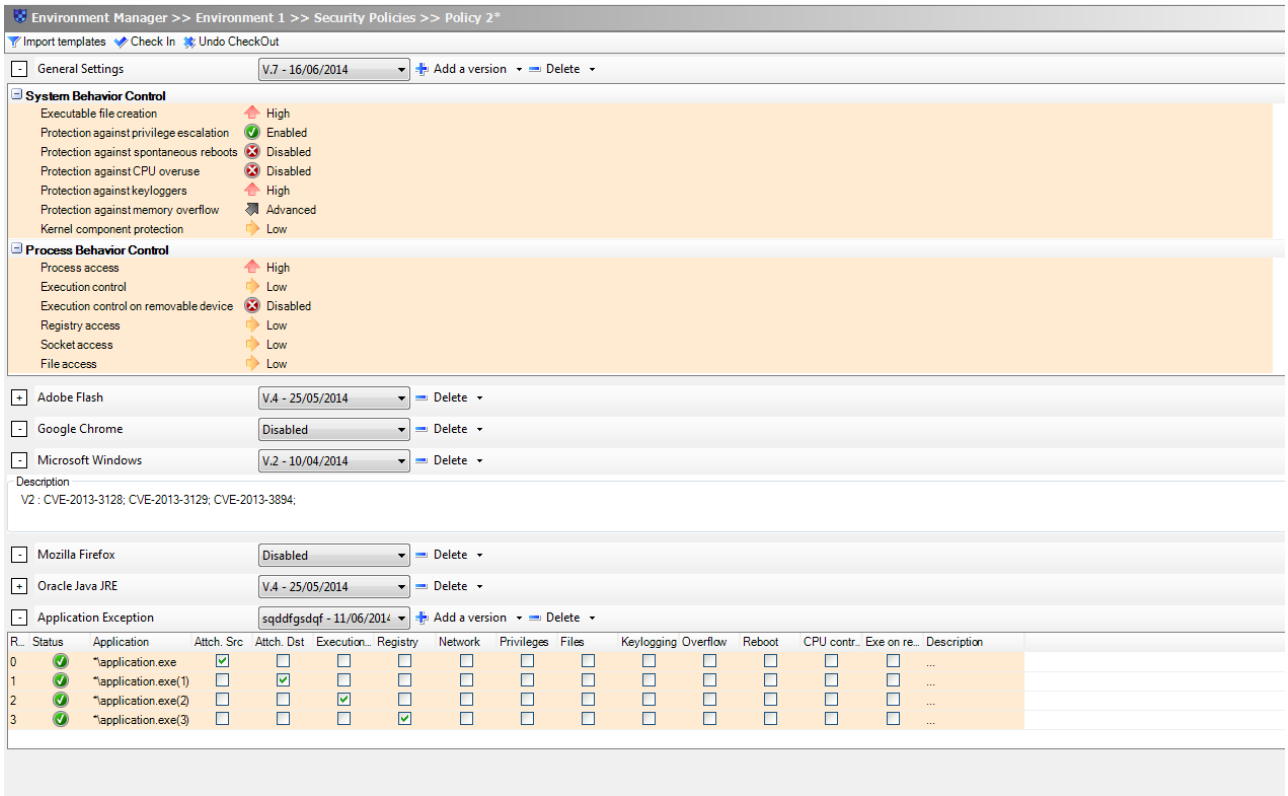
Creating and removing security policies

In the **Environment Manager** panel, create a new security policy by selecting the **Security Policies** node and click the button or right-click **Security Policies**: **New Policy**.

To remove a security policy, select the policy and click the button, or right-click the policy and select **Remove**. You can also press the Delete key.

Editing a security policy

When you select a security policy in the tree view, the settings panel displays on the right.



The editing mode of the security policy is automatically enabled when you change a setting: a red check is displayed in front of the policy node in the **Environment Manager**. To save your changes, validate the policy by clicking the **Check in** button above settings.

The Undo **CheckOut button** allows reloading the previous state of the policy.

Checking a policy does not mean it is applied to agents. To do so, synchronize the environment with the button located in the Environment Manager toolbar.

Importing templates

Click **Import templates** to load templates to be applied to the policy currently edited. Select the sczip package.

When importing a sczip file, ExtendedXP templates included in the package appear in the edition panel. Only some templates can be enabled depending on the offer you subscribed to. The **Disabled** option only is available in the drop-down list if the template is not authorized.

The template versions can be shared: versions imported in a security policy are available and can be applied in all the other policies of your environment.

Selecting a version

For each ExtendedXP template, select the version in the corresponding drop-down list. The versions are sorted by creation date. For more information about the content of a template version, refer to the description below each drop-down list and to the StormShield security advisory provided with the sczip.

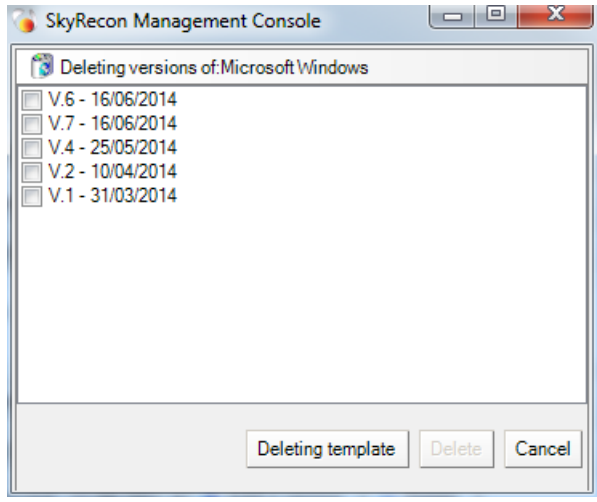
Removing a version and template

It is possible to remove some versions or all the versions of a template you do not need to clear the console interface.

To remove the selected version of a template, click the **Delete** button on the right of the drop-down list.

To remove several versions or the whole template, click the arrow on the right of the **Delete** button and select **Several versions**.

The following window is displayed.



Check the versions you want to delete and click **Delete**. To remove the template, click **Delete template**.

It is still possible to import again the template versions from a sczip. Keep the sczip if needed in the future.

Adding customized versions

For **General Settings** and **Application Exceptions** templates, you can add customized versions to adapt the policy to your environment.

You can create a new empty version or create a version from the version currently selected in the drop-down list. In the first case, click **Add a version** on the right of the drop-down list. In the second case, click the arrow on the right of the **Add a version** button and select the option **From "..."**.

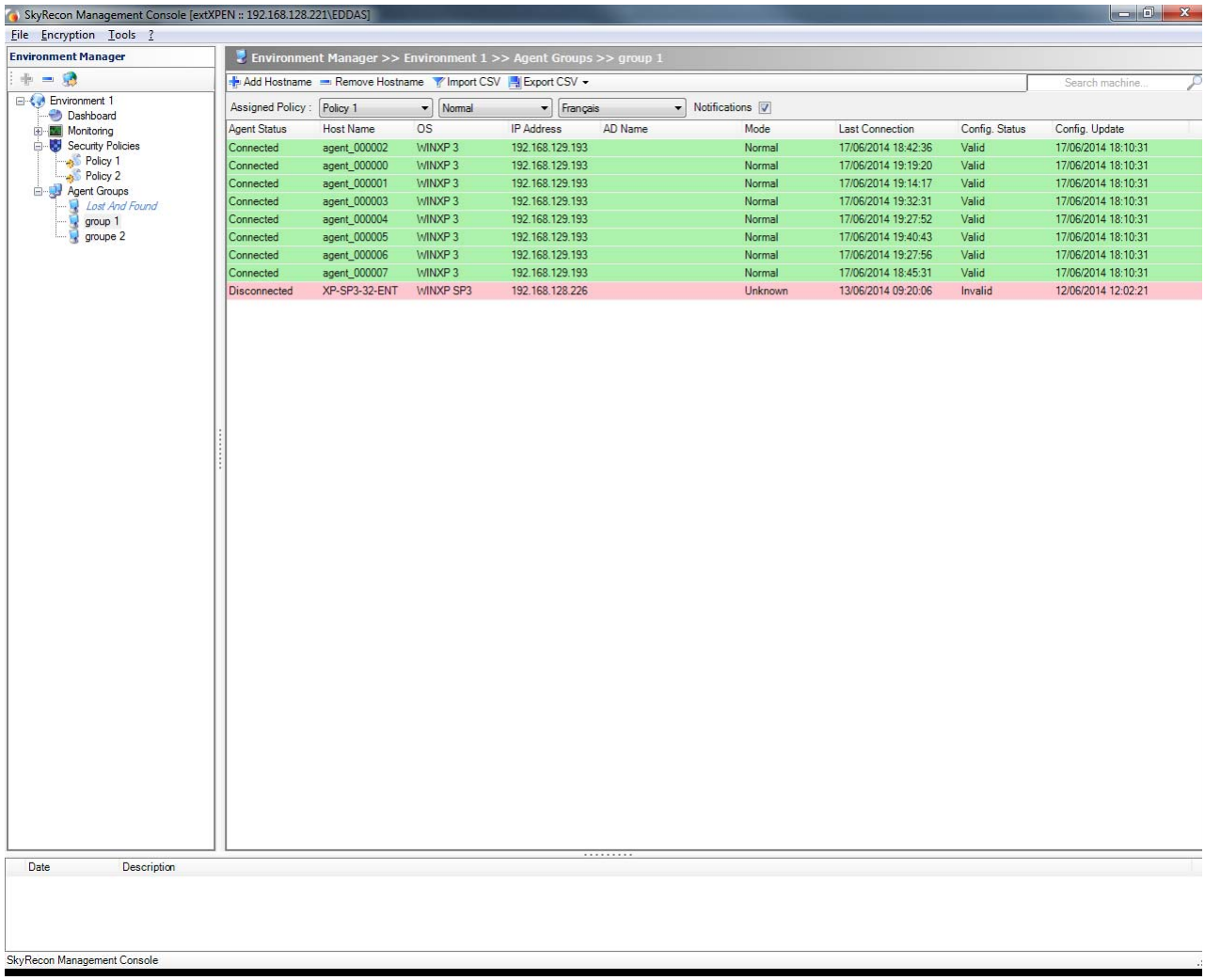
General Settings include the settings of the HIPS protection and the protection levels can be customized if they are too restrictive. For more information, refer to the section "Configuring automatic protections", page 260 of the chapter "System protection", page 253.

Reducing protection levels in general settings can make the product less efficient against some threats identified by the team providing the official template versions.

Exceptions on applications are about applications explicitly authorized to perform some operations. For more information, refer to the section "Trusted Rules", page 316 of the chapter "Rule-Based Protection", page 281.

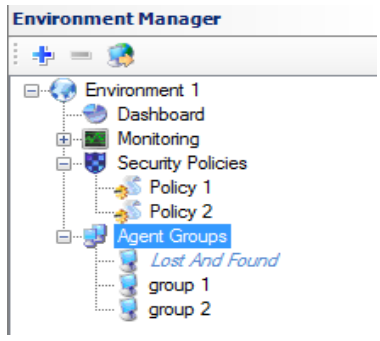
AGENT GROUPS

The **Agent Groups** panel allows classifying agents in different groups and thus applying different security policies, changing the language, etc.



Creating and removing agent groups

In the **Environment Manager** panel, create a new agent group by selecting the **Agent Groups** node and click the button or right-click **Agent Groups**: **New Agent Group**.



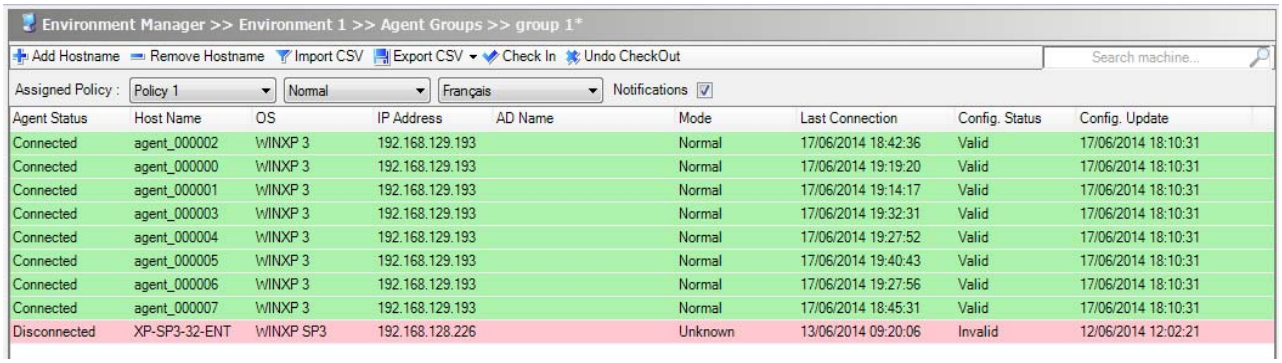
To remove an agent group, select the group and click the button, or right-click the group and select **Remove**. You can also press the Delete key.

Lost and Found group

The first group of the list cannot be removed or renamed. It is a default group which includes all the agents which do not belong to any other group. It is not possible to manually add or remove agents from this group: assigning an agent to another group will automatically remove it from the *Lost and Found* group. Removing an agent from a group will automatically move it to the *Lost and Found* group.

Editing an agent group

When you select an agent group in the tree view, the settings panel displays on the right.



Agent Status	Host Name	OS	IP Address	AD Name	Mode	Last Connection	Config. Status	Config. Update
Connected	agent_000002	WINXP 3	192.168.129.193		Normal	17/06/2014 18:42:36	Valid	17/06/2014 18:10:31
Connected	agent_000000	WINXP 3	192.168.129.193		Normal	17/06/2014 19:19:20	Valid	17/06/2014 18:10:31
Connected	agent_000001	WINXP 3	192.168.129.193		Normal	17/06/2014 19:14:17	Valid	17/06/2014 18:10:31
Connected	agent_000003	WINXP 3	192.168.129.193		Normal	17/06/2014 19:32:31	Valid	17/06/2014 18:10:31
Connected	agent_000004	WINXP 3	192.168.129.193		Normal	17/06/2014 19:27:52	Valid	17/06/2014 18:10:31
Connected	agent_000005	WINXP 3	192.168.129.193		Normal	17/06/2014 19:40:43	Valid	17/06/2014 18:10:31
Connected	agent_000006	WINXP 3	192.168.129.193		Normal	17/06/2014 19:27:56	Valid	17/06/2014 18:10:31
Connected	agent_000007	WINXP 3	192.168.129.193		Normal	17/06/2014 18:45:31	Valid	17/06/2014 18:10:31
Disconnected	XP-SP3-32-ENT	WINXP SP3	192.168.128.226		Unknown	13/06/2014 09:20:06	Invalid	12/06/2014 12:02:21

The editing mode of the agent group is automatically enabled when you change a setting: a red check is displayed in front of the group node in the **Environment Manager**. To save your changes, validate the agent group by clicking the **Check in** button above settings.

The **Undo CheckOut** button allows reloading the previous state of the group.

Checking an agent group does not update groups for agents. To do so, synchronize the environment with the button located in the Environment Manager toolbar.

Adding an agent

A group is a list of agents. To add an agent, several options are available:

- **Adding the hostname**: click **Add Hostname** in the toolbar at the top of the edition panel. If this agent has already been connected to a StormShield server, columns are instantly completed. Otherwise a new empty line displays with the **Unknown** status.
- **Importing a CSV file containing a hostname list**: Click **Import CSV** in the toolbar at the top of the edition panel. The CSV file must contain only one column. Each line must contain a NetBIOS name.
- **Moving an agent from a group to another (including from the *Lost and Found* group to another group)**: to move one or more agents from one group to another, select them in the tree view and drag and drop them to the node of the new group.

To move several agents, hold the Shift key pressed, select the agents and drag and drop them without releasing the key.

Removing an agent

Removing an agent from a group moves it back in the *Lost and Found* group except if this agent never connected to a server and its line remained empty.

To remove one or more agents, select them in the tree view and click **Remove Hostname** in the toolbar of the edition panel. You can also press the Delete key.

Exporting the agent list

You can export a part of the agents or all the agents of a group. By default, the **Export CSV** button exports all the agents of a group with the CSV format. To export only a part of the agents, select them, click the arrow on the right of the **Export CSV** button and select **Selection**.

Configuring an agent group

When the agent group is defined (the list of agents is created), you have to select the security policy to be applied by the group and the options of the agent configuration.

Security policy

Choose the security policy the agents of this group will apply when synchronizing the environment in the **Assigned Policy** drop-down list.

Configuration

The three options below allow configuring the agent:

- The first drop-down list allows selecting the agent mode:
  - **Normal**: the agent applies the policy. This mode blocks and logs. On the agent, this mode is indicated by the StormShield Monitor icon: .
  - **Warning**: the agent does not apply the policy but it provides a warning log showing what is blocked by the policy.

    This option is used to see what the policy does in order to modify it if need be. This option can be used for simulation.

    This mode does not block but logs.

    On the agent, this mode is indicated by the StormShield Monitor icon: .
  - **StandBy**: the agent applies no policy and keeps no warning log.

    It acts as a “pause” mode that can be used when you do not want to apply a specific policy (example: during server installation).

    This mode does not block and does not log either.

    On the agent, this mode is indicated by the StormShield Monitor icon: .
- The second drop-down list allows selecting the language of the agent interface. The supported languages are: French, English, Spanish, Portuguese and German.
- Select the **Notifications** check box if you want the agent to display notification messages to the user.

When the configuration of your environment is done, synchronize in order to apply the configuration to the agents.

Chapitre 8

SYSTEM PROTECTION

ABOUT THIS CHAPTER

This chapter describes the following:

- Protection mechanisms StormShield:
  - Profile-based protection.
  - Automatic protections.
  - Rule-based protection.
  - Order used to apply protection mechanisms.

- Profile-based protection :
  - Principles.
  - Automatic trust level assignment.
  - Correlation and weighting.
  - Learning.
  - Profile-based protection parameters.

- Automatic protections :
  - Principles.
  - Accessing automatic protections parameters.
  - Configuring automatic protections :
    - System Behavior Control.
    - Process Behavior Control.
    - Device Control.
    - WiFi Encryption and Authentication.
    - Network Activity Control.

- Rule-based protection :
  - Whitelists and blacklists.
  - Combining whitelists and blacklists.

PROTECTION MECHANISMS

To provide optimum protection, StormShield uses several protection modes that work in a coherent and complementary fashion.

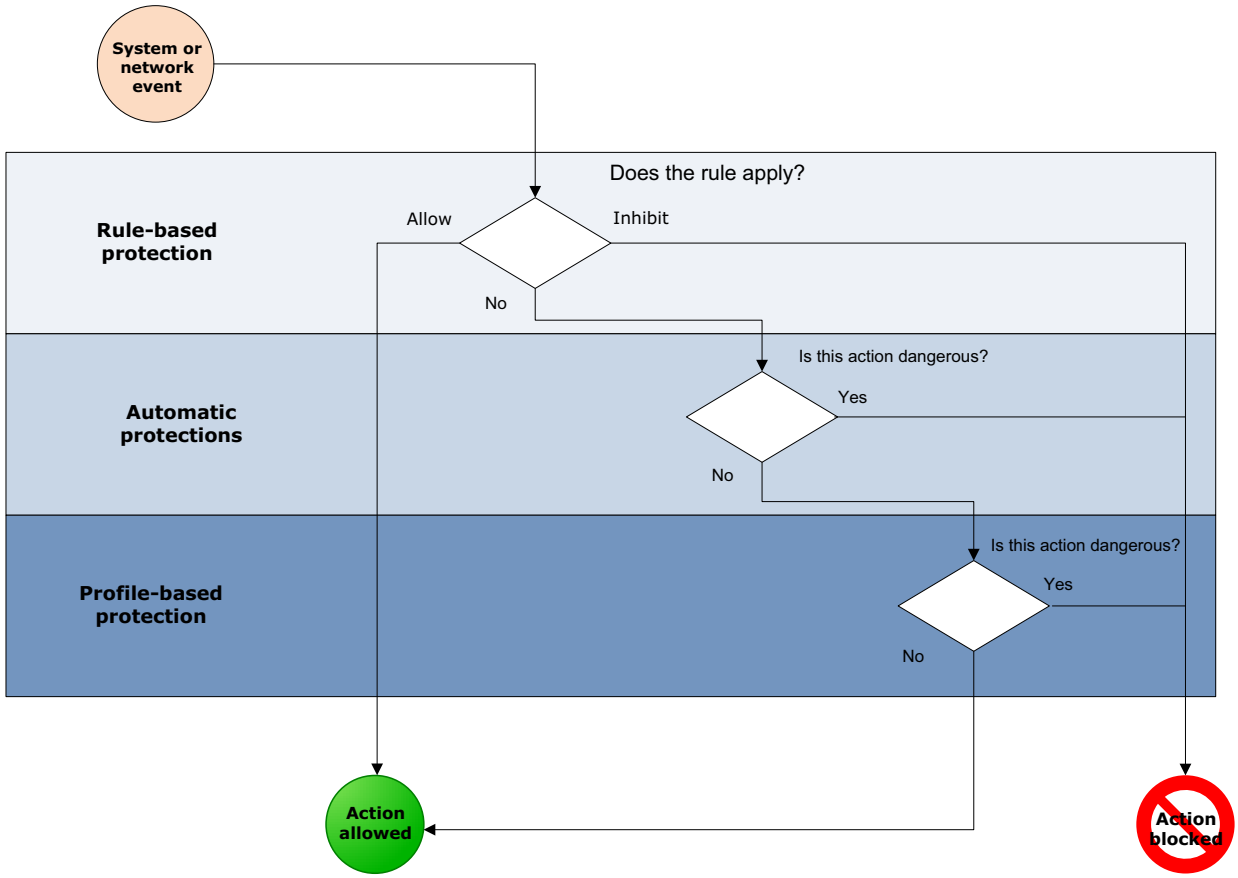


Fig. 8.1 : StormShield and its three protection mechanisms

PROFILE-BASED PROTECTION

Profile-based protection in StormShield:

- Monitors the applications being run.
- Alerts and blocks any process which behavior deviates from a reference profile.

For more information, see "Principles", page 258.

AUTOMATIC PROTECTIONS

Automatic protections cover system and network activities on the client workstation. They require no configuration from the administrator. The administrator can disable these protections partially or totally.

For more information, see "Configuring automatic protections", page 260.

RULE-BASED PROTECTION

Rule-based protection is used to define a specific policy in an organization. The administrator is in charge of implementing this policy by explicitly setting out permissions and bans on access to the client workstation resources.

For more information, see "Rule-Based Protection", page 281.

ORDER USED TO APPLY PROTECTION MECHANISMS

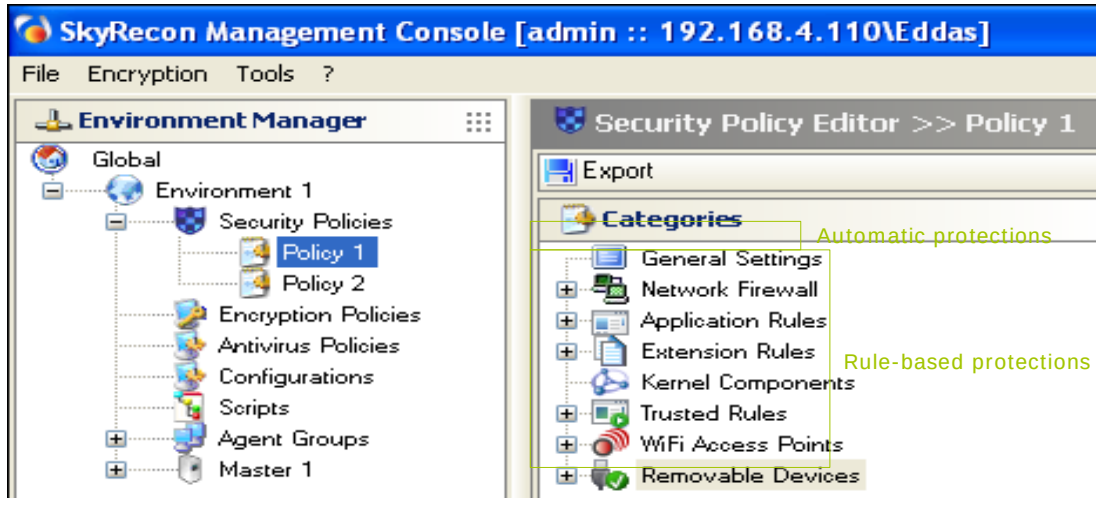
The three protection modes are applied in a specific order:

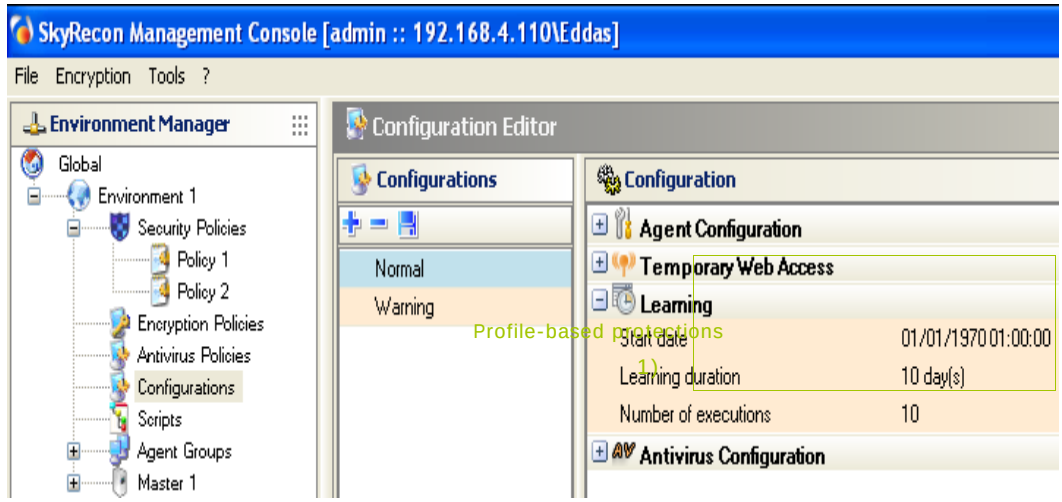
1. Rule-based protection.
2. Automatic protections.
3. Profile-based protection.

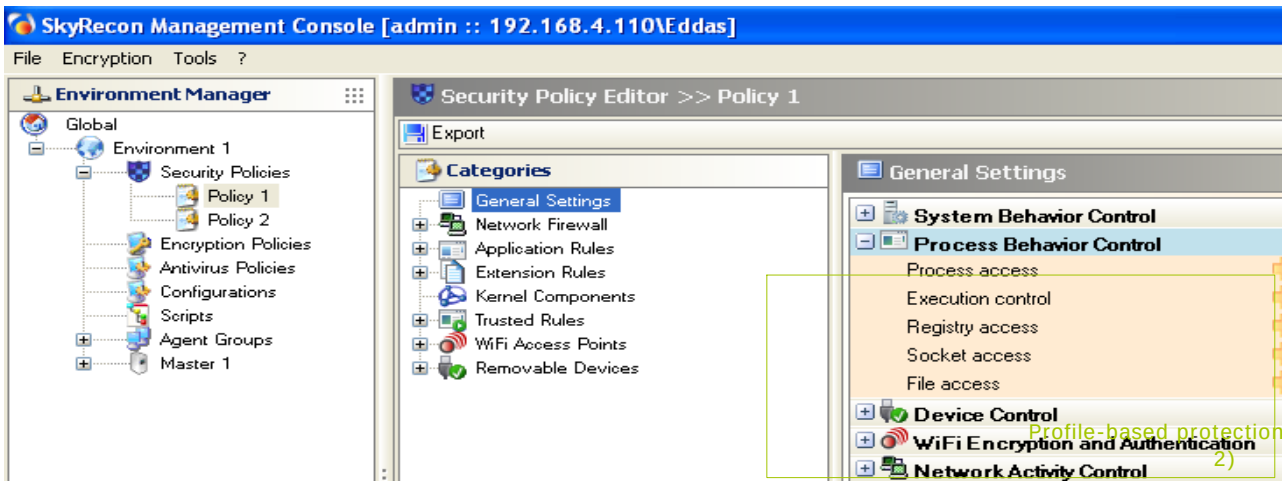
This order of precedence gives priority to the policy explicitly defined by the administrator (rule-based protection). Consequently, any ban or formal authorization expressed by the administrator is always applied. Human control always takes precedence over automation.

GRAPHICAL INTERFACE

StormShield protections are displayed on the SkyRecon management console asfollows:




SkyRecon Management Console [admin :: 192.168.4.110\Eddas]
File Encryption Tools ?
Environment Manager
Global
Environment 1
Security Policies
Policy 1
Policy 2
Encryption Policies
Antivirus Policies
Configurations
Scripts
Agent Groups
Master 1
Configuration Editor
Configurations
Normal
Warning
Configuration
Agent Configuration
Temporary Web Access
Learning
Start date 01/01/1970 01:00:00
Learning duration 10 day(s)
Number of executions 10
Antivirus Configuration
Profile-based protections 1)


SkyRecon Management Console [admin :: 192.168.4.110\Eddas]
File Encryption Tools ?
Environment Manager
Global
Environment 1
Security Policies
Policy 1
Policy 2
Encryption Policies
Antivirus Policies
Configurations
Scripts
Agent Groups
Master 1
Security Policy Editor >> Policy 1
Export
Categories
General Settings
Network Firewall
Application Rules
Extension Rules
Kernel Components
Trusted Rules
WiFi Access Points
Removable Devices
General Settings
System Behavior Control
Process Behavior Control
Process access
Execution control
Registry access
Socket access
File access
Device Control
WiFi Encryption and Authentication
Network Activity Control
Profile-based protection 2)

PROFILE-BASED PROTECTION

PRINCIPLES

Profile-based protection consists in evaluating application behavior by comparing it with a reference profile. Behavior analysis is based on monitoring the calls made by an application to the system:

- Opening ports.
- Accessing shared memory.
- Loading libraries.
- Reading registry keys, etc.

During the learning period, these calls are memorized to form an application standard profile. After this phase, the actions performed by the application while it is running are compared with its profile so as to detect any deviations that occur.

Learning is automatically restarted after:

- Any authorized modification to the application executable.
- Changing the learning period (date selected in the future).

AUTOMATIC TRUST LEVEL ASSIGNMENT

When a process is started, a trust level is automatically assigned. This trust level changes over time, depending on the deviations observed between the standard profile and true activity.

CORRELATION AND WEIGHTING

A slight deviation between the standard profile and the true activity of an application does not suffice to classify a code as dangerous. This is why profile-based protection also resorts to correlation and weighting mechanisms.

Correlation is used to compare several deviations (pertaining to different categories) so that the trust level can be changed accordingly. For example, injecting an unknown process correlated with the opening of a new port will indicate high attack risk.

Weighting is used to take into account the level defined by the administrator in the automatic protection parameters. As a result, a critical level combined with process injections will block any application that attempts to perform this operation (except for trusted applications in this category), regardless of the trust level assigned to the process.

LEARNING

The management console is used to activate learning using parameters that can be accessed from the Configuration Editor.

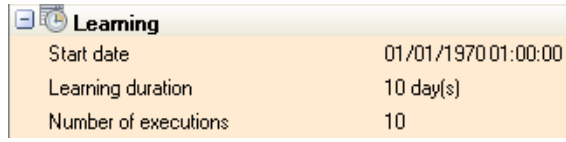


Fig. 8.2 : Learning parameters

The date indicates when learning will start on all the workstations assigned to the server. By default, the console displays 1/1/1970 1:00:00

The duration and/or number of executions of each process are used to set the learning phase parameters. If the learning duration is completed but the number of executions is inferior to that defined by the administrator, the learning phase continues.

PROFILE-BASED PROTECTION PARAMETERS

The general parameters for system protection presented in **Process Behavior Control** are also used for profile-based protection.

These parameters can be accessed in the **General Settings** panel of each securitypolicy:

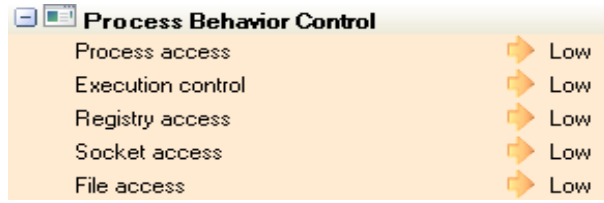


Fig. 8.3 : Profile-based protection parameters

AUTOMATIC PROTECTIONS

PRINCIPLES

Automatic protections in StormShield:

- Detect anomalies.
- Block anomalies.
- Require no configuration from the administrator.

However, the administrator can adjust StormShield's response to different event types. Depending on the administrator's settings, StormShield:

- Ignores the event.
- Generates an alert.
- Blocks the action in progress.

ACCESSING AUTOMATIC PROTECTIONS PARAMETERS

Automatic protection parameters belong to the **General Settings** category in the Security Policy Editor:

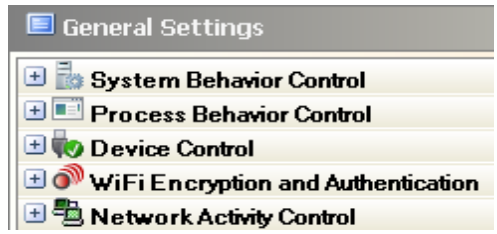


Fig. 8.4 : General Settings: Automatic protections

CONFIGURING AUTOMATIC PROTECTIONS

StormShield keeps on monitoring application and system activities. Collected information is used to protect your workstation from:

- Attempts to corrupt executable files.
- Attempts to access certain services or sensitive data in the system.

Depending on the type of anomalous activity detected and the response level defined by the administrator, StormShield can react in **real time** to protect the system.

Protection usually consists in refusing this malicious system call, while the application goes on running.

StormShield can also stop the process completely if system integrity is at stake.

Automatic protections can be fine-tuned for each security policy. The administrator can:

- Activate or deactivate a protection.
- Set the protection level.

These protection parameters are to be found in **General Settings**:

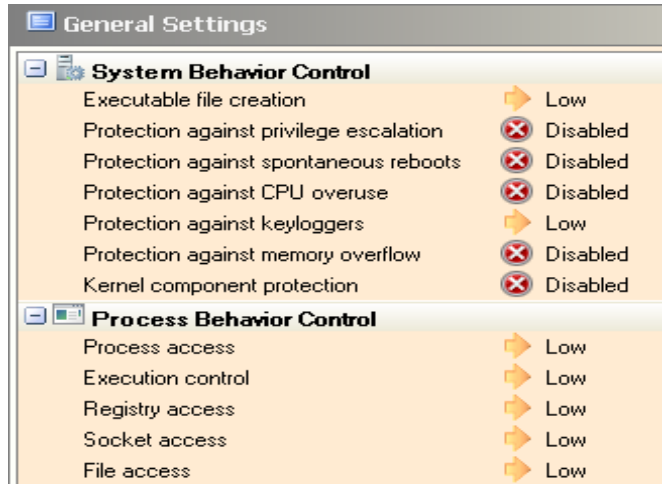


Fig. 8.5 : Partial example of automatic protection parameters

System Behavior Control

The System behavior control settings are the following:

- **Enabled/Disabled**.
- **High/Low/Critical/Advanced**.

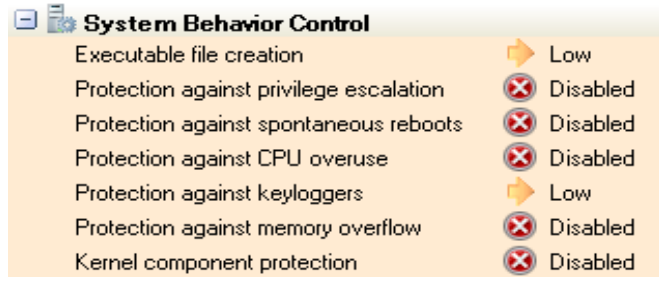


Fig. 8.6 : General Settings: System Behavior Control

- **Executable file creation**:

  Possible settings are the following:

  - **Low**:

    By default, this parameter is set to **Low**. It is actually disabled.

  - **High**:

    This parameter prevents the creation of the following executable files:

com	dll	exe	msi	mst	scr

  - **Critical**:

    This parameter prevents the creation of the following executable files:

bat	com	exe	mst	scr	vbs
cmd	dll	inf	pif	sys	ws
chm	drv	msi	reg	vbe	wsm

    You can use blacklists or whitelists to allow or prevent the installation ofspecific applications.

- **Protection against privilege escalation**:

  Possible settings are **Enabled** or **Disabled**.

  This parameter enables or prevents applications from letting a process gain administrator or system rights.

  The privileges requested by applications are saved in system logs.

- **Protection against spontaneous reboots**:

  Possible settings are **Enabled** or **Disabled**.

  It is usually the user who restarts the system but malicious software can trigger spontaneous reboots in order to:

  - Cause a denial of service.
  - Prevent patches from being downloaded.
  - Prevent antivirus signatures from being downloaded.

  This parameter prevents or allows applications to access privileges which permit system reboot.

  The privileges requested by applications are saved in system logs.

- **Protection against CPU overuse**:

  Possible settings are **Enabled** or **Disabled**.

  Some attacks tend to use up all CPU resources in order to:

  - Cause a denial of service.
  - Prevent patches from being downloaded.
  - Prevent antivirus signatures from being downloaded.

  This parameter prevents or allows applications to make an intensive use of CPU resources. These CPU-consuming applications are stopped by StormShield.

- **Protection against keyloggers**:

  Keylogging is used to capture keyboard events in order to steal passwords, confidential information, etc.

  Possible settings are the following:

  - **Low**:

    No blocking, no log.

  - **High**:

    Keylogging is blocked.

  - **Critical**:

    Best defense against graphical interface hooking (any event related to the graphical user interface is captured).

- **Protection against memory overflow**:

  Memory overflow occurs when programs attempt to write data beyond the allocated memory.

  These extra bytes replace valid data, and are executed as a program code.

  Possible settings are the following:

  - **Disabled**:

    No protection.

  - **Low**:

    KRP+RCP+HPP.

  - **High**:

    Low+NXP or BKP applied to network processes.

- **Critical**:

  This is a combination of the following options:

  - High+BKP applied to network processes if NXP is already enabled

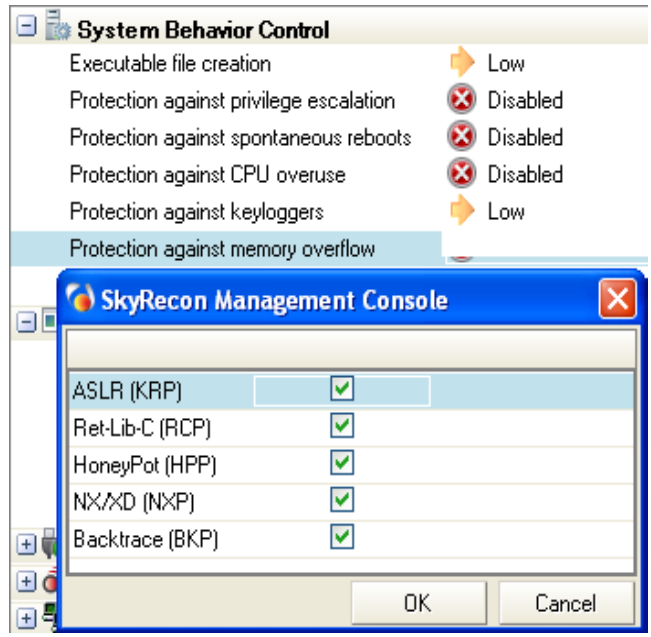
  or

  - High+BKP applied to all processes if NXP is disabled.

- **Advanced**:

  The administrator can disable one or several protection techniques in case of incompatibility.

  Possible options for **Advanced** are the following:



  - **ASLR (KRP)**:

    This option is used to randomize the base address of `kernel32.dll` when it is mapped into memory (under XP) on each reboot.

    Restart the computer for ASLR (KRP) activation/deactivation to be taken into account.

  - **Ret-Lib-C (RCP)**:

    This option blocks `return-into-lib(c)` attacks.

  - **HoneyPot (HPP)**:

    This option generates decoys which will be used by malicious code to find `kernel32.dll`.

- **NX/XD (NXP)**:

  First of all, you will have to enable this feature in the BIOS (Basic Input/ Output System) of your machine as well as the DEP (Data Execution Prevention) feature in Windows.
  This option in StormShield blocks the execution of processes based on memory addresses but does not kill the process in progress. There is a high risk of false positives, though.

  You can disable this option so as not to block the process in progress. It can prove useful when a legitimate process executes code in the memory addressing space.

- **Backtrace (BKP)**:

  This option is used to track the operations which led to the execution of untrusted code.

  This option can slow down the performance of your machine. If necessary, you can disable it.

In case of incompatibility between an application and StormShield's memory overflow protection, it is recommended to check that the application runs properly by disabling only protection options NX/XP (**NXP**) and Backtrace (**BKP**).

Should the problem persist, add a rule in **Trusted Rules**.

Some applications legitimately use mechanisms targeted by automatic protections.
For instance, the debugging function in a software development tool can legitimately use process injections whereas a remote control tool will perform keyboard event captures.
This is why StormShield has the ability to trust these applications, at each category level.
This feature is described in:

- "Trusted Rules", page 316.
- "Attributes", page 316.

PROTECTION	ASLR	RET-LIB-C	HONEYPOT	NX/XD	BACKTRACE
Disabled	off	off	off	off	off
Low	on	on	on	off	off
High	on	on	on	on	off
Critical	on	on	on	on	on
Advanced	on/off	on/off	on/off	on/off	on/off

Tableau 8.3 : Summary on Protection against memory overflow

NX/XD and Backtrace:

- When the **NX/XD** option is disabled or not present on your computer, the Backtrace option will then be enabled.
- The **Backtrace** option is always enabled when Protection against memory overflow is set to **Critical**.

- **Kernel component protection**:

  This parameter enables the administrator to activate or deactivate the detection of driver downloads.

  A learning period enables the kernel component protection to establish a list of legitimate drivers. After the learning period has expired, new drivers and suspect drivers will be blocked according to the protection level selected in the security policy (Enabled, Disabled, High, Low or Critical).

  Possible settings are the following:

  - **Disabled**:

    Kernel driver detection is disabled. No log is created on the StormShield server.

  - **Low**:

    New drivers and suspect drivers will not be blocked. They will only be detected. If the security policy prohibits certain drivers from being downloaded, these drivers will be blocked.

  - **High**:

    New drivers and suspect drivers are blocked on next boot. The drivers installed by Windows Update are automatically trusted.

  - **Critical**:

    Unknown drivers and suspect drivers are blocked on next boot. The drivers installed by Windows Update are automatically trusted.

Process Behavior Control

Process Behavior Control parameters can be set to **Low**, **High** or **Critical**.

The protection level selected by the administrator may have a direct impact on the agent behavior and on profile-based protection.

For more information, see "Profile-based protection", page 258.

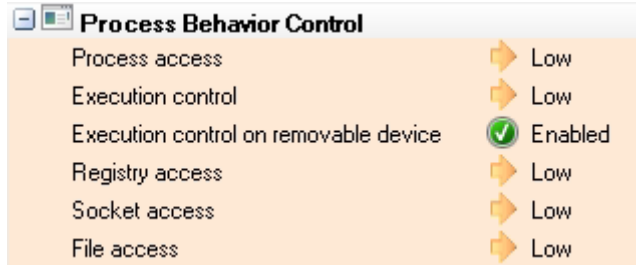


Fig. 8.7 : General Settings: Process Behavior Control

- **Process access**:

  The process injection mechanism is used by malicious code in order to:

  - Block another process from operating.
  - Corrupt the process being run.
  - Take control over the process being run.

  Possible settings are the following:

  - **Low**:

    No blocking, no log (the trust level changes marginally).

  - **High**:

    The trust level assigned to the application is affected by any unusual process injection. Only the process injections saved in the application profile during the learning period are authorized.

  - **Critical**:

    All process injections are blocked and profile-based protection is not used.

Some applications legitimately use mechanisms targeted by automatic protections.

For example, the UAC (User Account Control) under the Windows operating systems Vista and higher as well as the debugger of a software development tool may legitimately perform process injections. StormShield allows trusting these applications. For more information, see section "Trusted Rules", page 316.

- **Execution Control**:

  This mechanism monitors the execution of applications installed on the workstation. Malicious code may actually be hidden within authorized applications.

Possible settings are the following:

- **Low**:
  No blocking.
- **High**:
  Detects checksum mismatch errors in the application loaded in memory.
- **Critical**:
  Allows the execution of the binary files which are listed in the Windows system directory.
  Allows the execution of the binary files which extensions are listed in the table below:

com	dat	dll	drv	exe	msi
nls	scr	sra	srn	sro	sys
ocx					

- **Execution control on removable devices:**
  This control mechanism allows requesting a confirmation from the user when an application starts from a removable device connected to the agent.

  Possible settings are the following:

  - **Enabled**:
    A confirmation from the user is requested when an application tries to startfrom a removable device.
  - **Disabled**:
    No confirmation from the user is requested when an application tries to start from a removable device and the application can start.

  When this mechanism is used, a log message is created.

  The confirmation message directed at the user can be customized. In the Log Manager, choose the type System Logs and edit the notification message of the lines (#.)?EXE_ON_USB BLKEXECUTE et (#.)?EXE_ON_USB WARN. The message will display in a confirmation window on the agent.

- **Registry access**:
  This parameter which enables writing to the registry base, deactivates system protections and automatically starts any other program when rebooting the system.

Possible settings are the following:

- **Low**:

  No blocking (the trust level changes marginally).

- **High**:

  The application trust level is affected by any unusual operation in the registry base.

- **Critical**:

  The application trust level is severely affected by any unusual operation in the registry base.

- **Socket access**:

  Possible settings are the following:

  - **Low**: Blacklist policy.

    No network blockage except when explicitly banned. Profile-based protection is not applied: no deviation in socket use will affect the application trust level.

    All the application network connections which have not been explicitly authorized by the administrator (Application Rules or Trusted Rules) will be logged with the `[WARN]` keyword.

  - **High**: Whitelist policy.

    Only network access explicitly defined by the administrator and access detected during the learning period are authorized.

  - **Critical**: Whitelist policy in which no network access is allowed unless it has been explicitly declared.

    Data collected during the learning period is not taken into account.

- **File access**:

  This parameter is used to prevent the corruption and modification of executable file names. Any application declared in the rule-based protection is automatically protected against filename changes.

  Possible settings are the following:

  - **Low**:

    No blocking, no log (the trust level changes marginally).

  - **High**:

    The trust level assigned to the application is affected by any unusual process injection.

  - **Critical**:

    The application trust level is severely affected by any access to an unusual type of file. Any attempt to change the executable file is blocked.

The **Critical** value is a very powerful but also very restrictive tool. Updating an application requires that you first disable the protection or start another learning period.

It is highly recommended to use the Warning mode in order to adjust a policy.

Device Control

Device control can be set to **Allowed** or **Denied**.

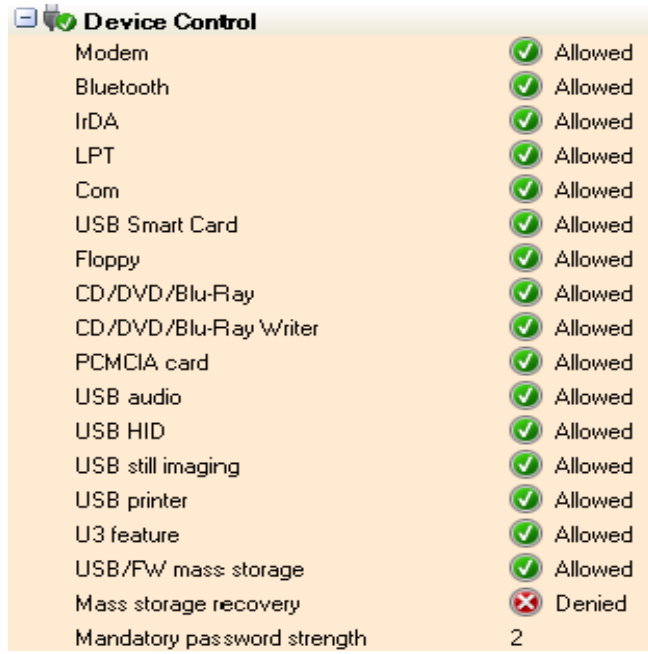


Fig. 8.8 : General Settings: Device Control

Device Control covers the following items:

- Modems (examples: RTC, 3G).
- Bluetooth.
- IrDA (Infrared Data Association) ports.
- LPT (parallel) ports.
- Comm ports.
- USB smart cards.
- Floppy disk drives (internal or external).
- CD/DVD/Blu-Ray.
- CD/DVD/Blu-Ray Writer.
- PCMCIA cards.
- USB audio cards.
- USB HID (Human Interface Device) keyboards or pointing peripherals (examples: mouse, graphics tablet, etc.).

- USB still imaging (examples: cameras, scanners, etc.).
- USB printers.
- U3 feature: It blocks autorun execution on U3 USB keys and CD-ROM readers.
- USB/FW mass storage: It consists of devices such as USB keys and hard disks, FireWire, etc.
- Mass storage recovery: Allows the user to decrypt mass storage devices which have been encrypted with StormShield.
- Mandatory password strength (2 by default): It is used to encrypt mass storage devices with StormShield.

The administrator can create policies applied to agent groups using removable devices. Settings will be more accurate. See "Creating an encryption policy to be applied to a group of devices", page 360.

For more information, see "Removable device encryption", page 355..

Devices with access set to **Denied** are blocked. This information is stored in Device Logs and the user receives an alert. For more information, see "Device Control", page 270.

WiFi Encryption and Authentication

WiFi Encryption and Authentication can be set to **Allowed** or **Denied**.

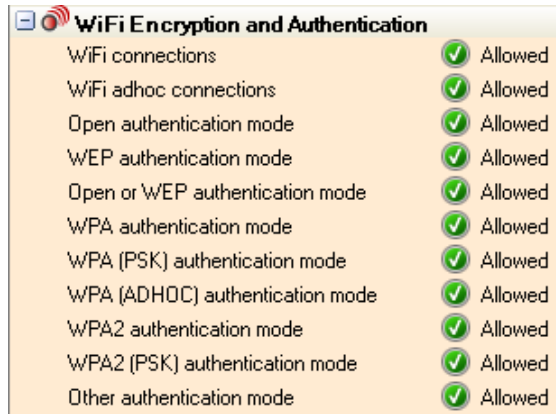


Fig. 8.9 : General Settings: WiFi Encryption and Authentication

WiFi Encryption and Authentication parameters are the following:

- **WiFi connections**:

  This parameter enables or disables the use of WiFi connections. When set to Denied, the network interface remains active but communications are blocked.

- **WiFi adhoc connections**:

  This parameter allows or denies the use of WiFi adhoc connections. This type of connection requires no base workstation and is limited to the duration of the session.

- **Open authentication mode**:

  When set to Allowed, no checks are performed during IEEE 802.11 OpenSystem authentication.

- **WEP authentication mode**:

  When set to Allowed, this mode uses specified IEEE 802.11 Shared Key authentication. This mode requires the use of a pre-shared *Wired Equivalent Privacy* (WEP) key for 802.11 authentication.

- **Open or WEP authentication mode**:

  When set to Allowed, this mode enables auto-switch mode. When using autoswitch mode, the device tries to use IEEE 802.11 *Shared Key* authentication. If Shared Key authentication fails, the device tries to use IEEE 802.11 OpenSystem authentication.

- **WPA authentication mode**:

  When set to Allowed, this mode enables the use of WPA version 1 *Security for Infrastructure* mode. Authentication is performed between the supplicant, authenticator and authentication servers via IEEE 802.1X.

  Encryption keys are dynamic and derived through the authentication process. While in authentication mode, the device will only associate with an access point whose beacon or probe response contains an (802.1X) authentication suite of type 1 within the WPA information element.

- **WPA (PSK) authentication mode**:

  When set to Allowed, this mode enables the use of WPA version 1 *Security for Infrastructure* mode. Authentication is performed between the supplicant, authenticator and authentication servers via IEEE 802.1X.

  Encryption keys are dynamic and derived through a pre-shared key used both by the supplicant and the authenticator.

  In this mode, the device only associates with an access point whose beacon or probe response contains the authentication suite of type 2 (pre-shared key) within the WPA information element.

- **WPA (ADHOC) authentication mode**:

  When set to Allowed, this mode enables the use of WPA version 1 *Security for adhoc* mode. This setting specifies the use of a pre-shared key without IEEE 802.1X authentication. Encryption keys are static and derived through the pre-shared key.

- **WPA2 authentication mode**:

  When set to Allowed, this mode enables the use of WPA version 2 *Security for Infrastructure* mode. Authentication is performed between the supplicant, authenticator and the authentication server via IEEE 802.1X.

  Encryption keys are dynamic and derived through the authentication process.

  In this mode, the device only associates with an access point whose beacon or probe response contains the authentication suite of type 1 (802.1X) within the RSN information element.

- **WPA2 (PSK) authentication mode**:

  When set to Allowed, this mode enables the use of WPA version 2 Security for Infrastructure mode. Authentication is made between the supplicant and the authenticator viaIEEE 802.1X.

  Encryption keys are dynamic and derived through a pre-shared key used both by the supplicant and the authenticator.

  In this mode, the device only associates with an access point whose beacon or probe response contains the authentication suite of type 2 (pre-shared key) within the RSN information element.

- **Other authentication mode**:

  When set to Allowed, this mode enables the use of other authentication modes.

Network Activity Control

StormShield protects network activity through an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS).

The interest of the IDS is multiple:

- The embedded IDS provides the client workstation with standalone attack detection capabilities, even when roaming away from the company's network protection systems.
- The IDS returns alerts that precisely identify recognized attacks.

The **IDS** is integrated with the firewall built into StormShield to form an Intrusion Prevention System (IPS).

The **IPS** alerts the administrator and blocks in real time attacks detected in incoming traffic.
Depending on the IDS sensitivity defined by the administrator, the alerts generated may trigger the dynamic application of a filtering rule by the firewall in order to temporarily cut off network access at affected port and protocol levels.

Network Activity Control settings are used to block network communications depending on the seriousness of the alert.

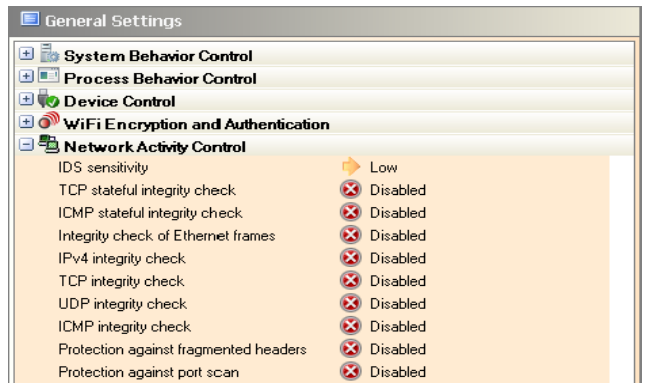


Fig. 8.10 : General Settings: Network Activity Control

The **Network Activity Control** parameters are the following:

- **IDS sensitivity**:

  Possible settings are the following:

  - **Low**:

    Any suspect network activity is logged.

  - **High**:

    Any illegal network activity is blocked.

  - **Critical**:

    Any illegal network activity is blocked. When enabled, this option is used during ARP cache analysis to block identity theft.

Correlation between IDS and IPS

The IDS sensitivity setting enables/disables the following IPS features:

- Protection against flooding.
- Protection against port scan.
- Protection against ARP cache poisoning.

A. Protection against flooding

It protects connections using the TCP protocol against flooding.

It monitors incoming connections and removes connections which remain too long in `SYN_RCVD` or`FIN_WAIT` state (~ 10 seconds).

If the IDS is set to **High**, and more than 20 connections are blocked in `SYN_RCVD` or `FIN_WAIT` state, these connections are removed.

Log excerpts:

```
[FLOOD]ÿ[CONNECTION_CLOSED]ÿ[(SYN_RCVD;16006;1533)]ÿ[192.168.42.121]ÿ[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAMEl]ÿ[20]ÿ[0]
```

```
[FLOOD]ÿ[CONNECTION_CLOSED]ÿ[(FIN_WAIT1;80;6218)]ÿ[192.168.42.122]ÿ[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ[20]ÿ[0]
```

If the IDS is set to **Critical**, and more than 10 connections are blocked in `SYN_RCVD` or `FIN_WAIT` state, these connections are removed and the firewall generates a rule to block the connections coming from the source IP address.

Log excerpt:

```
[FLOOD]ÿ[IP_BLOCKED]ÿ[0]ÿ[192.168.42.122]ÿ[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ[20]ÿ[0]
```

The number of connections in `SYN_RCVD` state per service is limited (port).

IDS LEVEL	PROTECTION AGAINST FLOODING
Low	Disabled

IDS LEVEL	PROTECTION AGAINST FLOODING
High	Connections are removed when exceeding 20 in number
Critical	◦ Connections are removed when exceeding 10 in number ◦ Source IP address is blocked

B. Protection against port scan

To use this protection, you must have enabled **Protection against port scan** in General Settings > Network Activity Control.

It consists in filtering:

- The `RST_ACK` packets of closed TCP ports.
- The `ICMP` packets of closed UDP ports.

An IP address is recognized as a scanner when a number of filtered packets is reached:

- Approximately 3 packets for rapid scans.
- Approximately 5 packets for slow scans.

If the IDS is set to **Low**, the agent detects port scans but no action is taken to block the IP address associated with the detected scanner.

Log excerpt when the IDS is set to **Low**:

```
[PORTSCAN]ÿ[SCAN_IN]ÿ[CHECKSCAN_MAX_QUICK_SUSPICIOUS_REACHED 4:
(TCP;8080)(TCP;8081)(TCP;8082)(TCP;8083)]ÿ[192.168.42.117]ÿ[0]ÿ[0]
ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ[0]ÿ[61710]
```

If the IDS is set to **High** or **Critical**, the agent blocks the IP address associated with the detected scanner.

Log excerpt indicating that incoming scans are blocked, when the IDS is set to **High**:

```
[PORTSCAN]ÿ[SCAN_IN]ÿ[CHECKSCAN_MAX_QUICK_SUSPICIOUS_REACHED 4:
(TCP;49154)(TCP;49157)(TCP;34313)(TCP;37792) (Blocked until
20h06m33s)]ÿ[192.168.42.117]ÿ[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ[777]ÿ[0]
```

SCAN_OUT logs are displayed if the host running the agent acts as a scanner:

```
[PORTSCAN]ÿ[SCAN_OUT]ÿ[CHECKSCAN_MAX_QUICK_SUSPICIOUS_REACHED 4:
(TCP;8080)(TCP;8081)(TCP;8082)(TCP;8083)]ÿ[192.168.42.1]ÿ[0]ÿ[0]ÿ[
0]ÿ[0]ÿ[HOSTNAME]ÿ[0]ÿ[61710]
```

IDS LEVEL	PROTECTION AGAINST PORT SCAN
Low	Filters
High	◦ Filters ◦ Blocks
Critical	◦ Filters ◦ Blocks

C. Protection against ARP cache poisoning

This protection detects:

- When the host running the agent attempts to steal the identity of another machine on the network.
- When any machine on the network attempts to steal the identity of another machine.

This protection includes:

- An ARP stateful inspection to filter the ARP replies which match no ARP request.
- A protection for gratuitous requests which are sent when the agent detects a machine which has stolen the identity of the agent's host. Gratuitous requests are used to correct entries in the ARP cache of the machines which are not equipped with StormShield.

IDS LEVEL	PROTECTION AGAINST ARP CACHE POISONING.
Low	Stateful inspection
High	◦ Stateful inspection ◦ Gratuitous ARP blocked
Critical	◦ Stateful inspection ◦ Gratuitous ARP blocked ◦ Protection against identity theft

Log excerpt:

```
[ARP_DELETE 00000005]ÿ[IN]ÿ[Request EthSrc=00:20:20:20:20:20
EthDst=00:16:17:2d:26:99 ArpHwSrc=00:20:20:20:20:20
ArpIpSrc=192.168.42.254 ArpHwDst=00:00:00:00:00:00
ArpIpDst=192.168.42.254]ÿ[192.168.42.254]ÿ[PORTSRC]ÿ[PORTDST]ÿ[PR
OTO1]ÿ[PROTO2]ÿ[]ÿ[0]ÿ[61710]
```

IDS	IPS		
	PROTECTION AGAINST FLOODING	PROTECTION AGAINST PORT SCAN	PROTECTION AGAINST ARP CACHE POISONING
Low	Disabled	Filters	Stateful inspection
High	Connections are removed when exceeding 20 in number	◦ Filters ◦ Blocks	◦ Stateful inspection ◦ Gratuitous ARP blocked
Critical	◦ Connections are removed when exceeding 10 in number ◦ Source IP address is blocked	◦ Filters ◦ Blocks	◦ Stateful inspection ◦ Gratuitous ARP blocked ◦ Protection against identity theft

Tableau 8.4 : Summary on the correlation between IDP and IPS

- **TCP stateful integrity check**:
  This parameter can be set to **Enabled** or **Disabled**.
  It verifies compliance with protocol RFC 793.
- **ICMP stateful integrity check**:
  This parameter can be set to **Enabled** or **Disabled**.
  It verifies compliance with protocol RFC 792.
- **Integrity check of Ethernet frames**:
  This parameter can be set to **Enabled** or **Disabled**.
  It verifies compliance with protocol RFC 894.
- **IPv4 integrity check**:
  This parameter can be set to **Enabled** or **Disabled**.
  It verifies compliance with protocol RFC 791.

- **TCP integrity check**:

  This parameter can be set to **Enabled** or **Disabled**.

  It verifies compliance with protocol RFC 793.

- **UDP integrity check**:

  This parameter can be set to **Enabled** or **Disabled**.

  It verifies compliance with protocol RFC 768.

- **ICMP integrity check**:

  This parameter can be set to **Enabled** or **Disabled**.

  It verifies compliance with protocol RFC 792.

- **Protection against fragmented headers**:

  This parameter can be set to **Enabled** or **Disabled**.

  It protects against network attacks using header fragmentation as a way to bypass network firewall filtering rules.

- **Protection against port scan**:

  This parameter can be set to **Enabled** or **Disabled**.

  It blocks incoming packets from the source address if a port scan is detected.

RULE-BASED PROTECTION

Rule-based protection lets the administrator define which actions are authorized or banned at system and network level (examples: access to files, registry bases or network protocols).

Rules represent the finest granularity of administrator-defined security policies. They are organized by category in the Security Policy Editor.

These categories are the following:

- Network Firewall
- Applicative Rules.
- Extension Rules.
- Kernel Components
- Trusted Rules.
- WiFi Access Points
- Removable Devices.

For more information, see "Rule-Based Protection", page 281.

WHITELISTS AND BLACKLISTS

Rule-based protection can be used in a whitelist or blacklist approach.

A **whitelist** approach consists in banning everything that is not explicitly authorized.

A **blacklist** approach consists in authorizing everything that is not explicitly banned.

COMBINING WHITELISTS AND BLACKLISTS

Both approaches can be combined depending on the environment in which the rules are applied.

It is possible to use a whitelist for everything relating to network access and a blacklist when dealing with applications that users can legitimately use.

Chapter 9

RULE-BASED PROTECTION

ABOUT THIS CHAPTER

This chapter details the rule-based protection configuration at network firewall and system firewall level.

It includes the following:

- Relationships between security policy components:
  - Rules.
  - Rule groups.
  - Rule categories.

- Security policy types:
  - Empty policy.
  - Standard policy.
  - Advanced policy.

- Security Policy Editor.

- Rule categories:
  - Network Firewall.
  - Application Rules.
  - Extension Rules.
  - Kernel Components.
  - Trusted Rules.
  - WiFi Access Points.
  - Removable Devices.

- Rule management:
  - Adding a rule.
  - Importing a rule.
  - Importing a rule group.
  - Deleting a rule.
  - Setting the rule priority order.
  - Enabling/Disabling a rule group.
  - Displaying more details on rules.

- Handling conflicts between rules:
  - Rule priority order.
  - Examples.

- Writing conventions:
  - Application entry format.
  - Environment variables.

- Configuration templates:
  - Overview.
  - Predefined groups and configuration rules.

RELATIONSHIPS BETWEEN SECURITY POLICY COMPONENTS

The figure below reviews the relationships between:

- Rules.
- Rule groups.
- Rule categories.

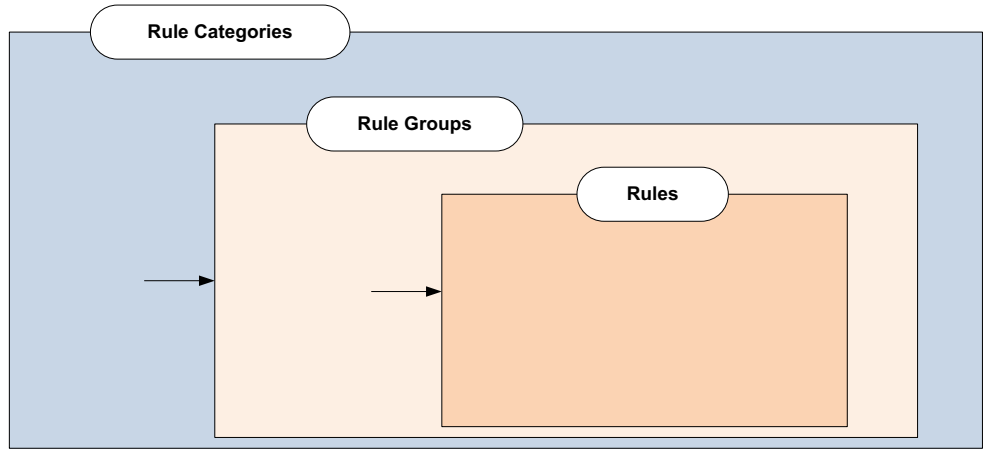


Fig. 9.1: Relationships between security policy components

Fig. 9.2: Security policy components: Categories, Groups and Rules.

RULES

Rule-based protection lets the administrator define and ensure the application of an explicit security policy. A security policy is defined by formal rules set out to allow or ban access to given services or data.

Rules represent the finest granularity of administrator-defined policies. They are organized in the **Security Policy Editor**.

RULE GROUPS

Rules are gathered in rule groups to facilitate their use by the administrator.

Here are some examples of rule groups which feature in the files provided by SKyRecon Systems.
These rule groups are generated when importing SkyRecon Systems' files, or when creating an advanced security policy after checking the appropriate groups:

- Default Group.
- Base System.
- Base Network.
- Web Browsers.
- Email Clients.
- P2P.
- Instant Messaging.
- Multimedia.
- Antivirus (AVP option only).

RULE CATEGORIES

Rule groups are gathered in rule categories.

Rule categories are the following:

- General Settings.
- Network Firewall.
- Application Rules.
- Extension Rules.
- Kernel Components.
- Trusted Rules.
- WiFi Access Points.
- Removable Devices.

SECURITY POLICY TYPES

When adding a new security policy, the administrator has the option to choose among **three** policy types:

- Empty policy.
- Standard policy.
- Advanced policy.

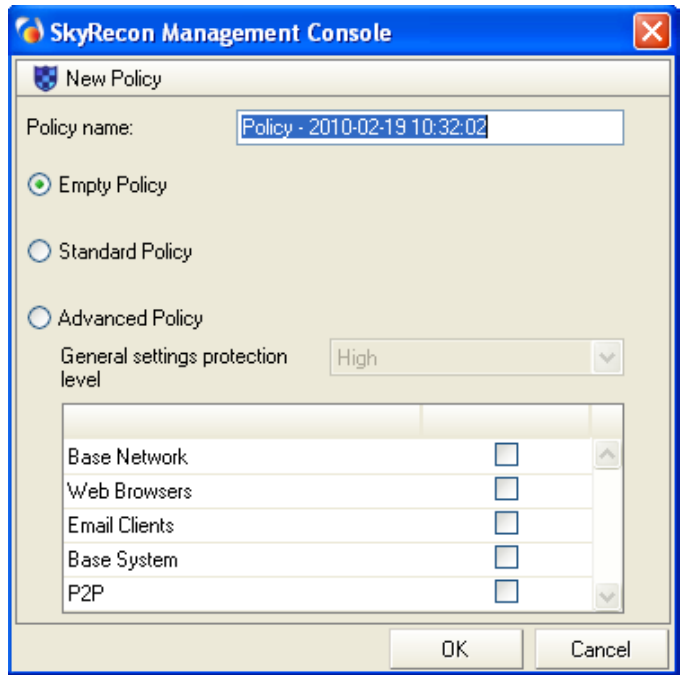


Fig. 9.3: Security policy types

EMPTY POLICY

An empty security policy contains the default rule group that can be configured by the administrator.

The security policy shown below includes an **Antivirus** rule group in **Trusted Rules**.
However, the Antivirus rule group is only included if the user has installed the antivirus option.

For more information, see "Packages, option and licenses", page 47.

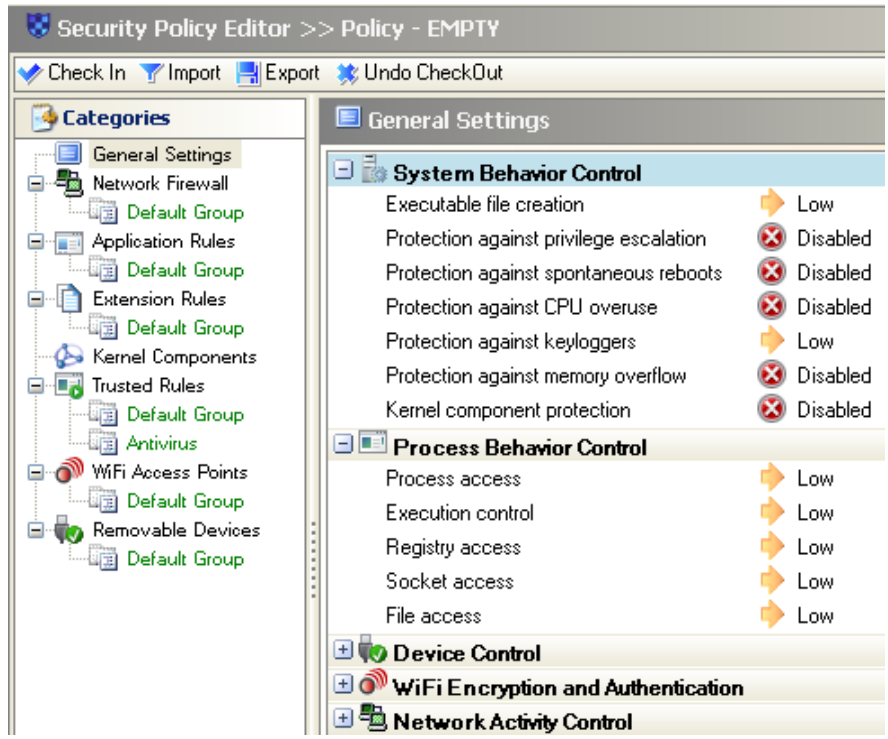


Fig. 9.4: Security Policy Editor: Empty policy sample

STANDARD POLICY

Besides having the default rule groups, a standard security policy contains the following rule groups:

- **Base Network**:

  This is a set of firewall rules used for standard services on workstations.

- **Base System**:

  This is a set of system rules used for standard services on workstations.

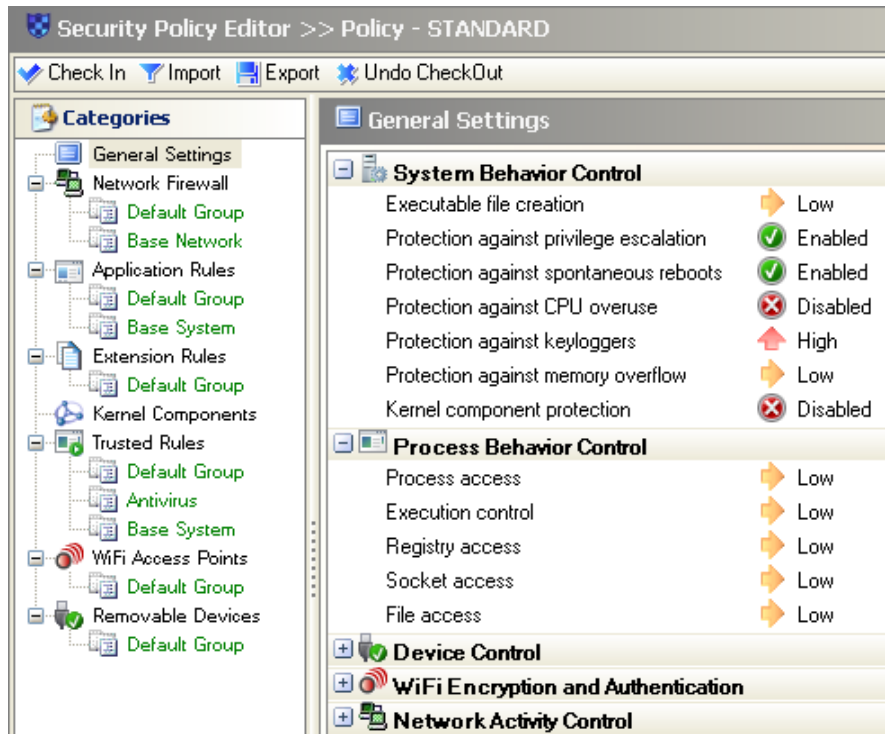


Fig. 9.5: Security Policy Editor: Standard policy sample

ADVANCED POLICY

When creating an advanced security policy, the administrator can choose to add other rule groups to the default rule groups.

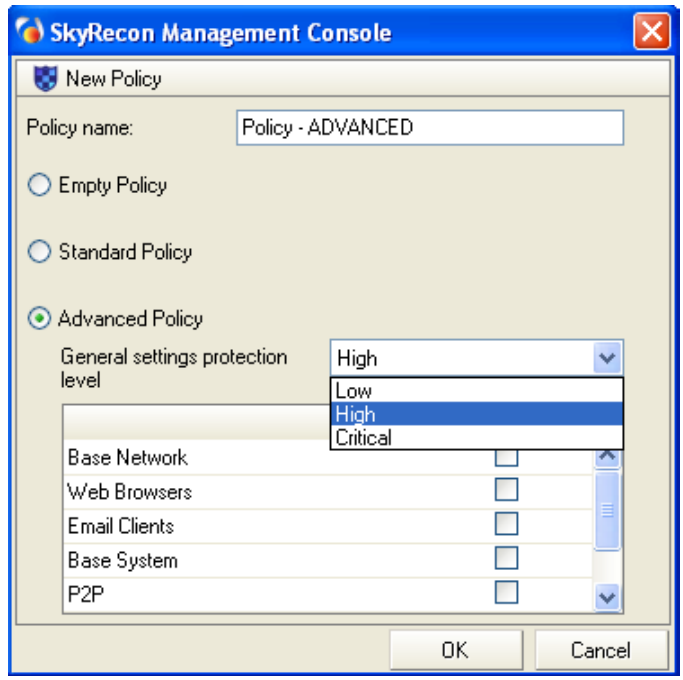


Fig. 9.6: Advanced security policy options

The administrator can choose among the **seven** rule groups:

- **Base Network**:

  Rule group used to control DNS, netbios and workstation management.

- **Web Browsers**:

  Rule group used to control or restrict the standard Web browser.

- **Email Clients**:

  Restrictive rule group for standard e-mail clients which controls access to POP3, SMTP and HTTP. It also restricts access to `VBS` and `exe`.

- **Base System**:

  Rule group for main Windows services and programs such as `svchost`, `explorer` and `rundll`.

- **P2P**:

  Restrictive rule group used to deny access to peer-to-peer applications (P2P).

- **Instant Messaging**:

  Restrictive rule group for standard instant messaging clients (network restrictions to the server and extension restrictions to sharing file).

- **Multimedia**:

  Restrictive rule group for multimedia players and file formats.

For more information, see "Predefined groups and configuration rules", page 342.

SECURITY POLICY EDITOR

Security policies include rules that the administrator can configure in the **Security Policy Editor** on the SkyRecon management console.

The editor panel includes the following categories in a tree view.

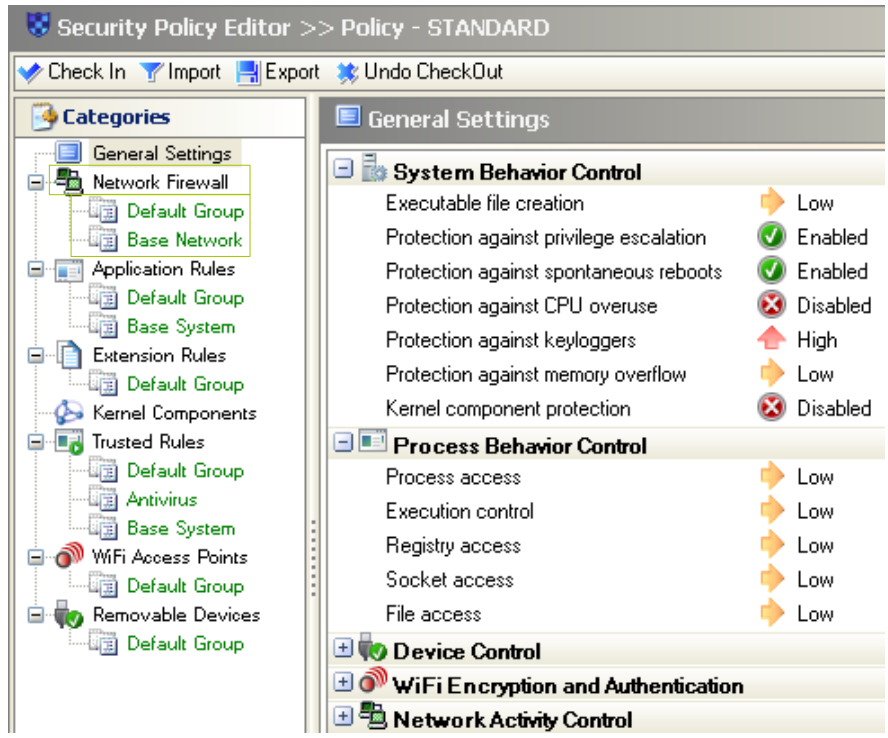


Fig. 9.7: Security policy in a tree view including categories (in black) and rule groups (in green)

For more information, see "Packages, option and licenses", page 47.

RULE CATEGORIES

To open a rule category, click on the node under Categories in the three view.

There are **eight** categories:

- **General Settings:**

  This category is located at the first level under Categories in the tree view. These settings determine automatic protections.

- **Network Firewall**:

  This category enables static and dynamic control of the network firewall.

- **Application Rules**:

  This category covers:

  - All the rules relating to running applications.
  - All the rules relating to modifying applications.
  - Application access rights to network, files and registries.

- **Extension Rules**:

  This category is used to define rules according to file type regardless of the application that accesses the file.

- **Kernel Components**:

  This category provides kernel protection by enabling control over driver loading and detecting suspect drivers.

- **Trusted Rules**:

  This category is used to free certain applications from any check to avoid irrelevant blocking.

- **WiFi Access Points**:

  This category provides network protection by enabling control over WiFi access points that can be accessed by workstations.

- **Removable Devices**:

  This category provides removable device protection by enabling control over the devices that can be used by the workstations.

To ban the use of removable devices, WiFi and/or WiFi adhoc connections, go to **General Settings > WiFi Encryption and Authentication > [parameter]** to set the parameter to **Denied**.

NETWORK FIREWALL

StormShield integrates a network firewall that is controlled:

- Statically (by administrator rules).
- Dynamically (by reacting to embedded IDS alerts).

Static firewall operation is defined by rules.

Dynamic network firewall operation is defined by IDS sensitivity and the seriousness of IDS alerts.

For more information, see "Rule management", page 336.

Rules are displayed in a tabular form:

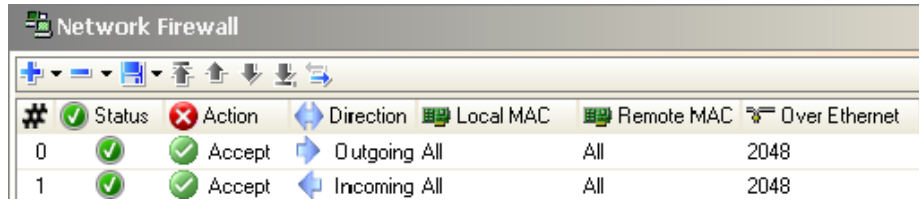


Fig. 9.8: Network Firewall rules

Network interfaces in bridge mode on virtual machines are not filtered by the firewall.

Attributes

The network rules attributes are the following:

- **#**:

  This attribute is used to define the order in which rules are evaluated so as to avoid conflicts between them.

  The network firewall uses the first rule which matches.

- **Status**:

  This attribute can be set to Enabled or Disabled.

  A disabled rule is retained in the configuration but not evaluated when processing the network event.

  The **Enabled** icon is .

  The **Disabled** icon is .

- **Action**:

  This attribute blocks or accepts the data flow.

  The **Accept** icon is  .

  The **Block** icon is  .

- **Direction**:

  This attribute is used to define whether the data flow is filtered on the way **in** or on the way **out**.

  Rules on TCP, ICMP and UDP traffic are stateful. This means that only the direction of the first packet needs to be defined. A rule to allow response data to flow will be dynamically generated by the firewall. In other cases (non-stateful), the administrator needs to define two rules: one rule for the way in and one rule for the way out.

- **Remote IP**:

  This attribute is used to restrict data flow destination address.

  This address can be:

  - An IP address.
  - An IP address list.
  - An IP address range.

  By default, no host is specified. This means that the rule applies to all addresses.

- **Over IP**:

  This attribute defines to which IP protocol the rule is applied.

- **Stateful**:

  This attribute activates/deactivates the stateful processing of TCP, UDP or ICMP flows.

  Stateful rules retain the communication session status while the firewall automatically generates the rule required by the response data flow.

- **Local Port:**

  This attribute defines the local host service port number (for TCP and UDP) or the local code (for ICMP).

  The administrator can define:

  - A port number.
  - A port list.
  - A port range.

- **Remote Port**:

  This attribute defines the remote host port number (for TCP and UDP) or code (ICMP).

  The administrator can define:

  - A port number.
  - A port list.
  - A port range.

- **Log**:

  This attribute is used to save log files.

- **Description**:

  This attribute is used to add a comment to the rule.

- **Group**:

  This attribute shows the group to which the rule belongs. This indication is only visible in the root overview mode of each category.

Additional attributes

The administrator has access to more options by clicking on the network firewall toolbar. Additional columns are displayed.

The additional rule attributes are following:

- **Local MAC**:

  This attribute is sued to restrict the data flow source address.

  This address can be:

  - A MAC address.
  - A MAC address list.
  - A MAC address range.

  By default, no host is specified. This means that the rule applies to all addresses.

- **Remote MAC**:

  This attribute is used to restrict the data flow destination address.

  This address can be:

  - A MAC address.
  - A MAC address list.
  - A MAC address range.

  By default, no host is specified. This means that the rule applies to all addresses.

- **Over Ethernet**:

  This attribute defines the protocol over Ethernet to which the rule applies.

- **Local IP**:

  This attribute is used to restrict the data flow source address.

  This address can be an IP address or an IP address list.

  By default, no host is specified. This means that the rule applies to all addresses.

Local and remote MAC attributes are taken into account only under Windows XP.

Attribute configuration

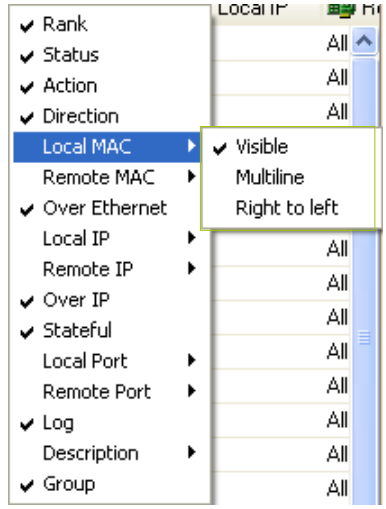
Graphical interface

By default, the Network Firewall settings are set to **All** and Status is set to **Accept**.

You can select the columns to be displayed by right-clicking any header.

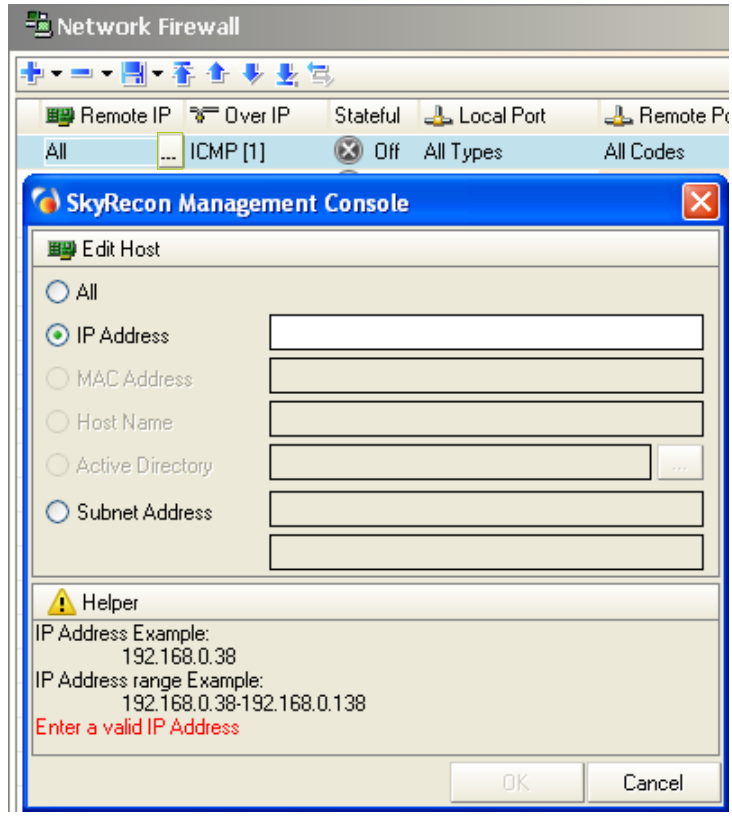
Choose the headers you wish to display from the list.

You can customize the display of some attributes to make reading easier:



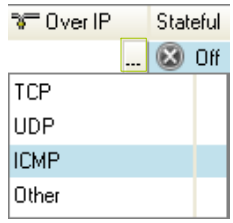
Remote IP

To modify settings, click ... to display the following window and proceed with modifications:



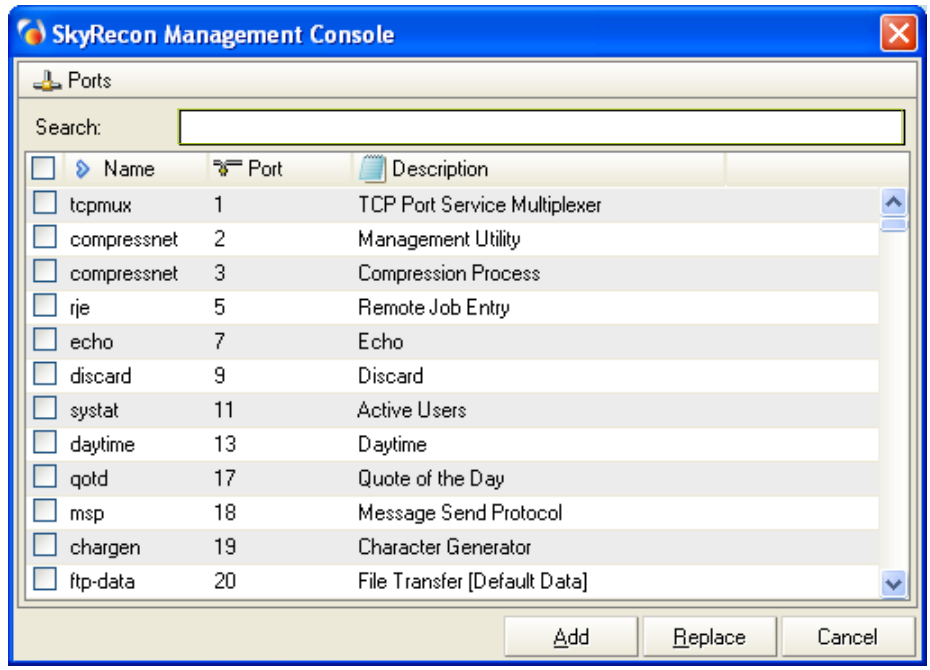
Over IP

To modify settings, click ... to display the following window and proceed with modifications:



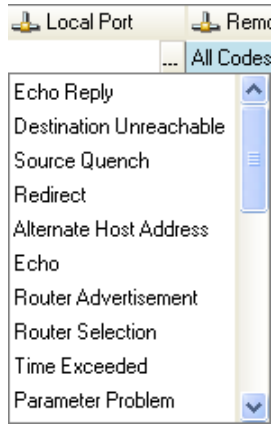
Local Port

To modify **TCP** and **UDP** settings, click ... to display the following window and proceed with modifications:



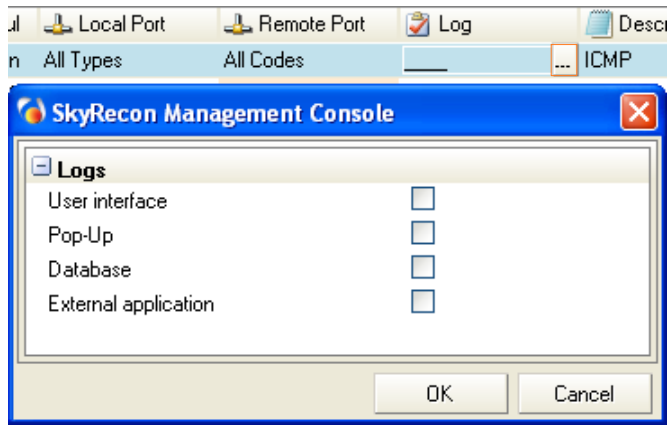
1. Select the required services by clicking in the check boxes.
2. Enter the characters in the **Search** field to reduce scrolling through the list.
3. Click **Add** after making your selection.

To modify **IMCP** settings, click ... to display the following window and proceed with modifications:



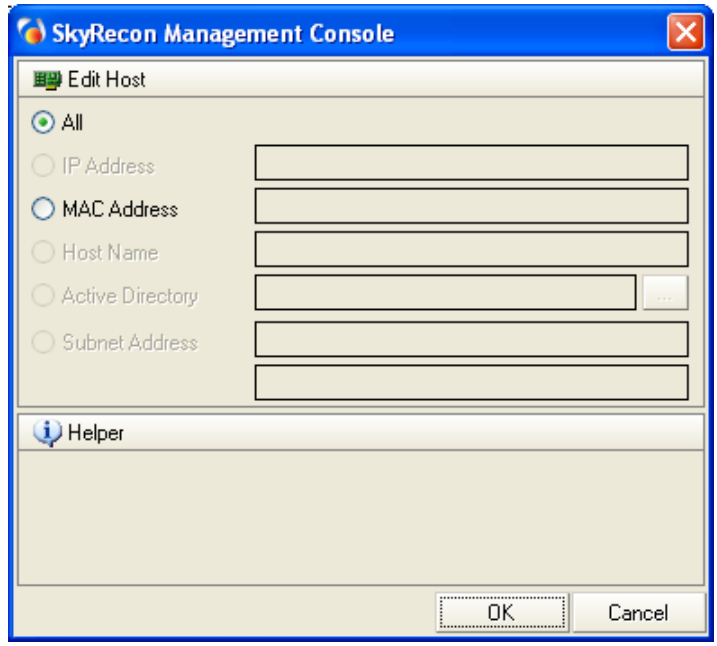
Log

To modify settings, click ... to display the following window and proceed with modifications:



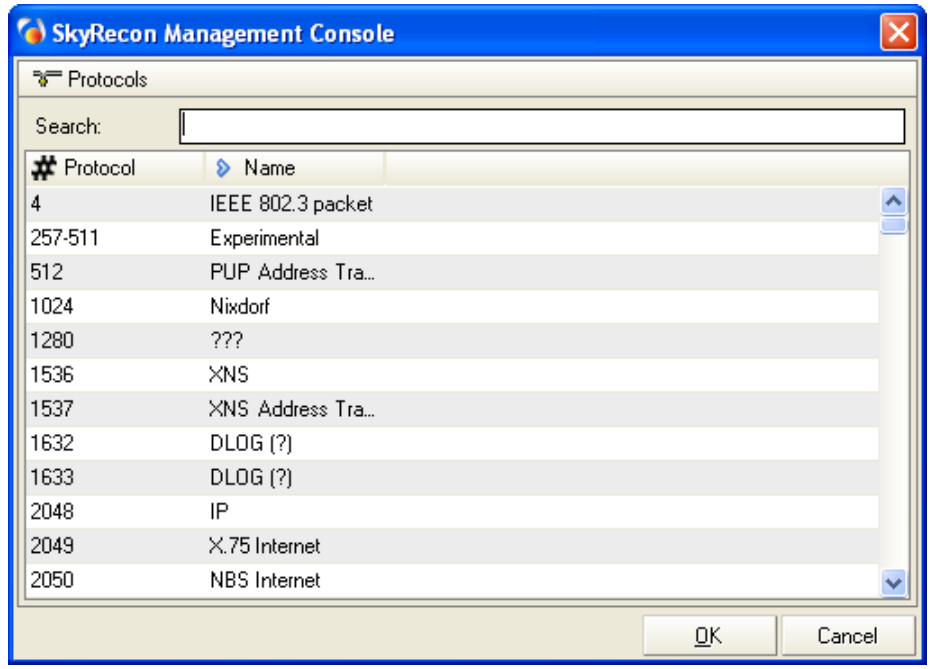
Local MAC

To modify settings, click ... to display the following window and proceed with modifications:



Over Ethernet

To modify settings, click ... to display the following window and proceed with modifications:



1. Enter the characters in the **Search** field to reduce scrolling through the list.
2. Select the appropriate protocol.
3. Click **OK**.

APPLICATION RULES

Here is an example of Application Rules:

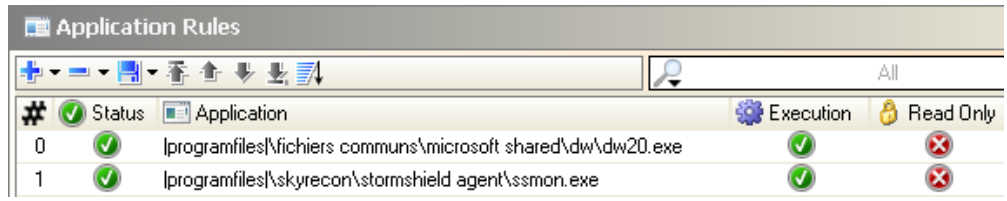


Fig. 9.9: Application Rules

Attributes

The Application Rules attributes are the following:

- **Status**:

  This attribute defines the rule status which is set to Enabled or Disabled.

  A disabled rule is retained in the configuration but is not evaluated when processing the network event.

  The **Enabled** icon is .

  The **Disabled** icon is .

- **Application**:

  This attribute defines the application to which the rule applies. Using a wildcard at the end of the path lets you set a rule that covers all executables in a given path.

  Example: `|programfiles|\Internet Explorer\*`

- **Execution**:

  This attribute allows or denies access to the application.

- **Read Only**:

  This attribute protects the application executable. When set to Enabled, you cannot:

  - Modify
  - Move
  - Rename
  - Create
  - Delete the application.

- **Files**:

  This attribute shows the application rights to access the files:

  - Read Only (execute).
  - Access Denied.
  - Allow (execute).
  - Create Denied.
  - Execute Denied.

- **Network**:

  This attribute controls the application rights to access the network.

- **Registry**:

  This attribute controls the application rights to access the registry base.

- **Copy/Paste**:

  This attribute controls the copy/paste feature in your applications.

- **Log**:

  This attribute defines the settings for saving and viewing log files.

- **Description**:

  This attribute is a freeform comment.

- **Group**:

  This attribute shows the group to which the rule belongs. This indication is only visible in the root overview mode of each category.

Toolbar

The following toolbar (on the upper part of the window) is used to:

- Add
- Import
- Save
- Delete
- Sort rules.

The **Search** field is used to reduce scrolling through the list of rules.

For more information, see "Rule management", page 336.

Attribute configuration

Network

Double-click in the **Network** column to open the Network Access window.

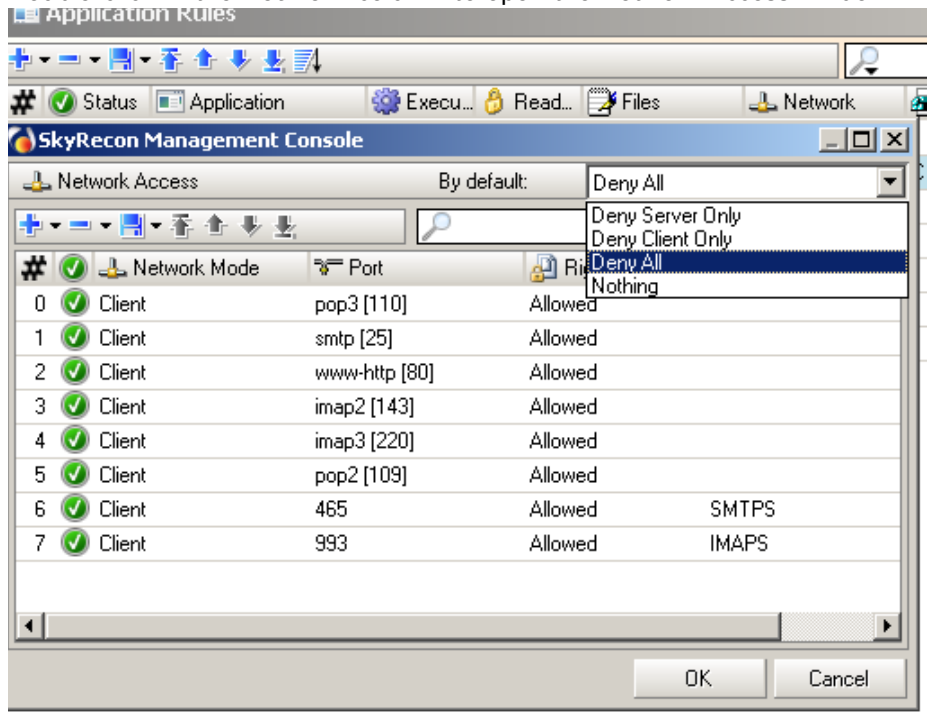


Fig. 9.10: Network Access window

Overall management of access rights to the network

Access rights to an application are managed with an overall or detailed basis.

Overall access rights are defined in the **By Default** field. This field is used to restrict application communication.

Four options are available:

- **Deny Server Only**:

  The application cannot listen to a port. It can only operate in Client mode, which means that only the application can initiate a connection to a given service.

- **Deny Client Only**:

  The application can only operate in Server mode. It can only respond to connections initiated by client programs.

- **Deny All**:

  The application is not allowed to connect to the network.

- **[Empty]**:

  No behavior is applied by default except for the global security level (High, Low or Critical) and associated rules.

  Local sockets are not controlled by network access rules.

Detailed management of access rights to the network

The network access attributes are the following:

- **Status**:

  This attribute can be set to Enabled or Disabled.

  Just like other items that require activation, a disabled access right is retained in the configuration but is not evaluated when processing the system event.

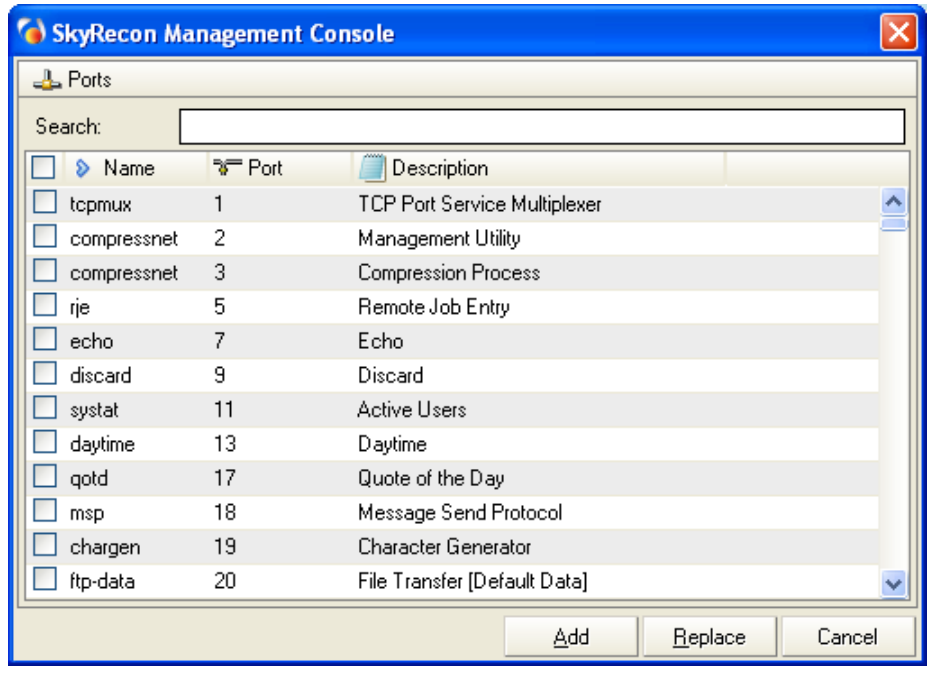
- **Network Mode**:

  Possible values are the following:

  - Client.
  - Server.
  - Client and Server.
  - [None]: no behavior is applied by default.

- **Port**:

  Use the selection button to choose from the list of predefined services. You can define port lists and ranges.



- **Rights**:

  This attribute can be set to Allowed or Denied.

- **Description**:

  This attribute is a freeform comment to facilitate identification.

Files

Double-click in the **Files** column to open the Files access window:

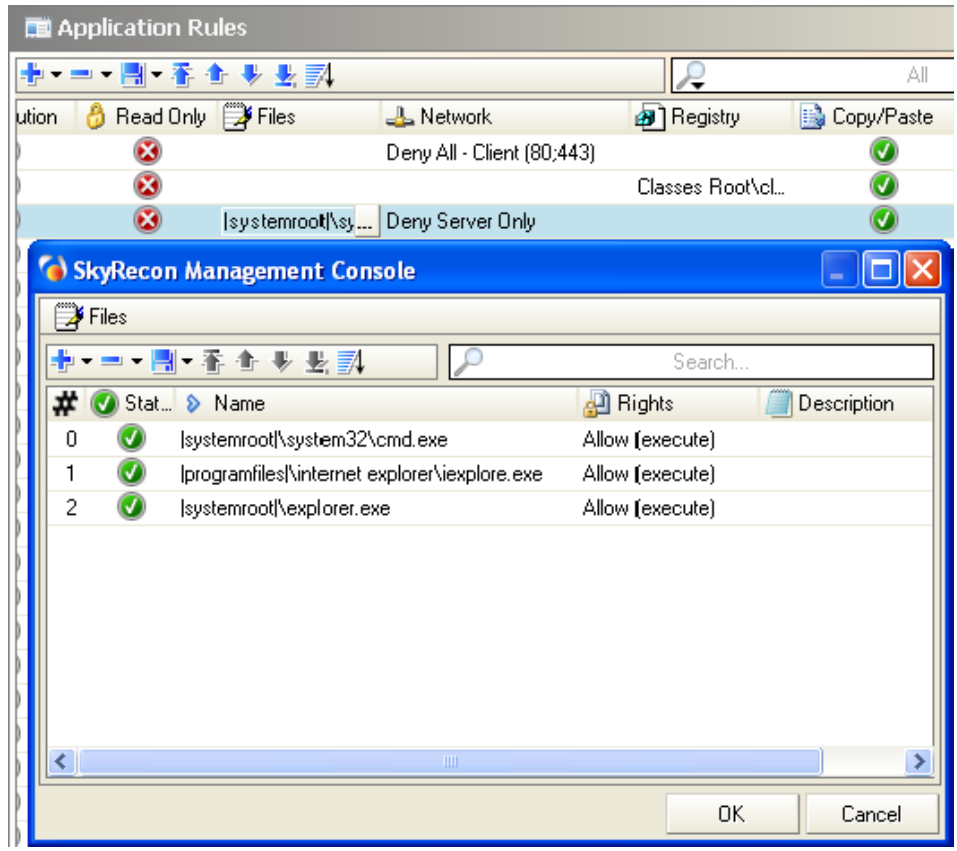


Fig. 9.11: File Access window

The file access attributes are the following:

- **Status**:

  This attribute can be set to Enabled or Disabled.

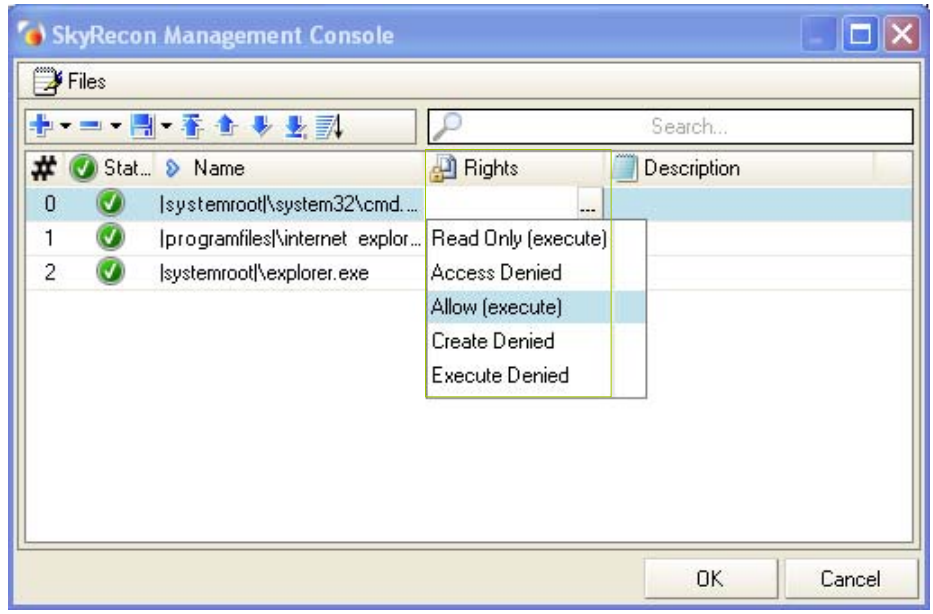
  Just like other items that require activation, a disabled access right is retained in the configuration but is not evaluated when processing the system event.

- **Name**:

  This attribute is the filename which may include one or several * wildcards.

- **Rights**:

  Possible values are the following:



- **Description**:

  This attribute is a freeform comment to facilitate identification.

Registry

Double-click in the **Registry** column to open the Registry Access window:

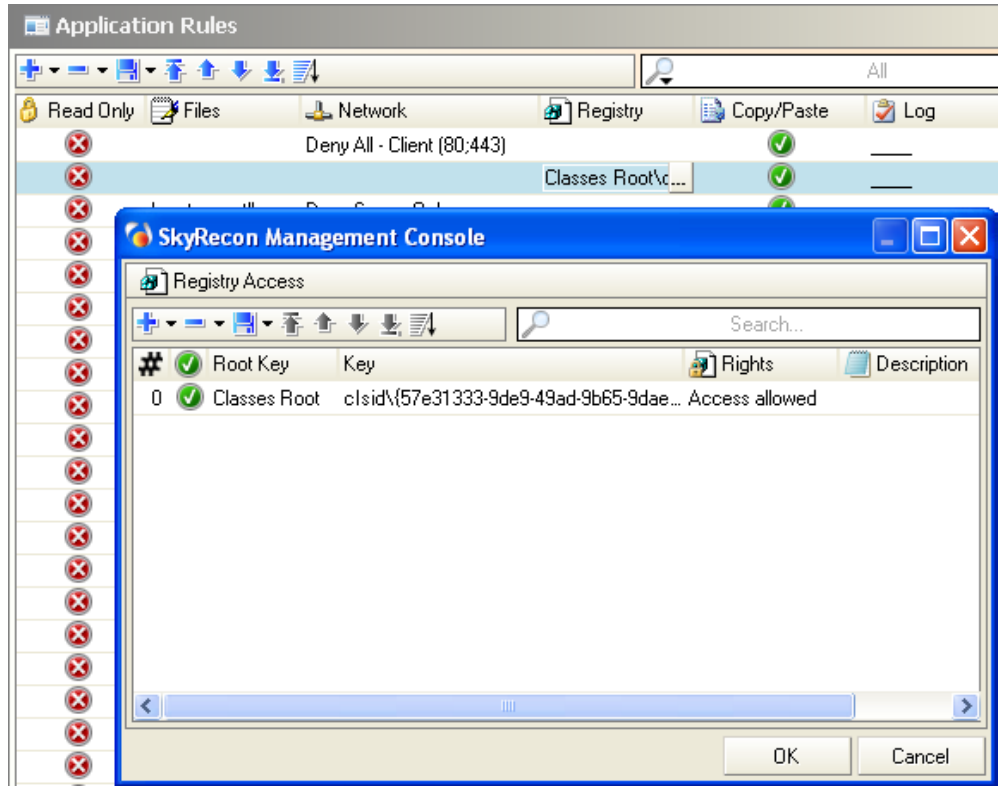


Fig. 9.12: Registry Access window

The registry access attributes are the following:

- **Status**:

  This attribute can be set to Enabled or Disabled.

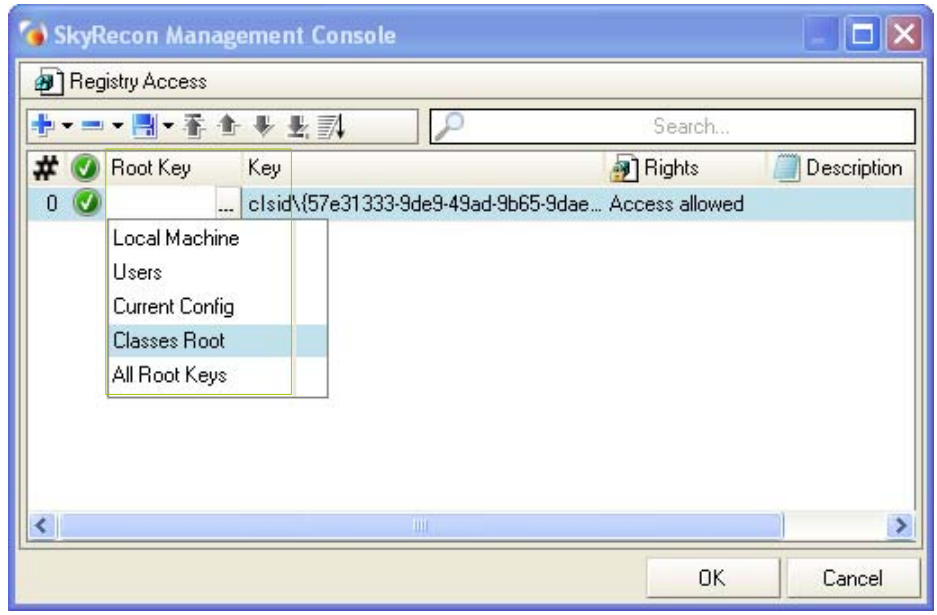
  Just like other items that require activation, a disabled access right is retained in the configuration but is not evaluated when processing the system event.

- **Root Key**:

  Possible values are the following:

  - Local Machine.
  - Users.
  - Current Config.

- Classes Root.
- All Root Keys.



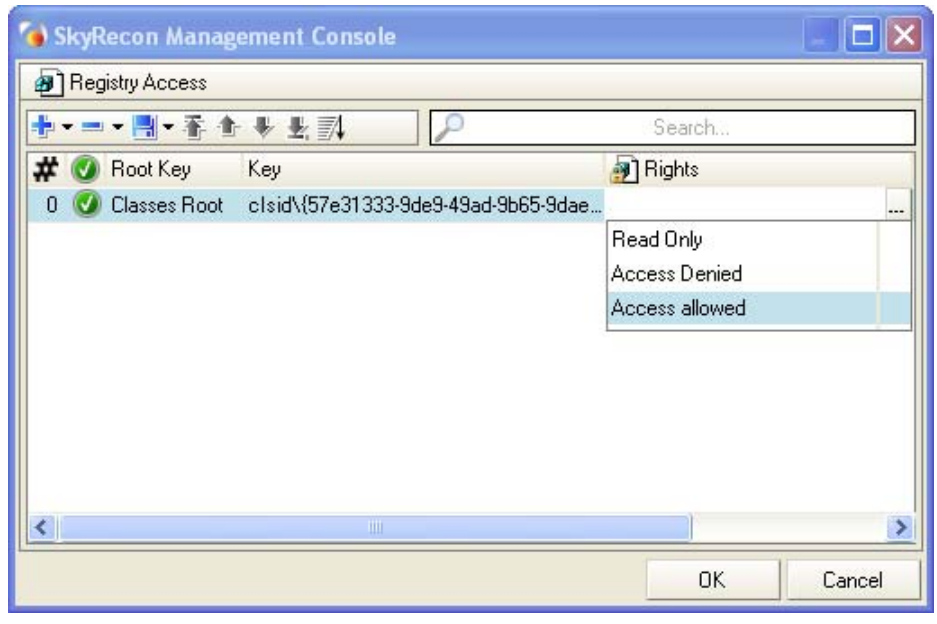
- **Key**:

  This attribute is the name of the key to be specified for registry access.

- **Rights**:

  Possible values are the following:

  - Access denied.
  - Access allowed.
  - Read Only.



- **Description**:

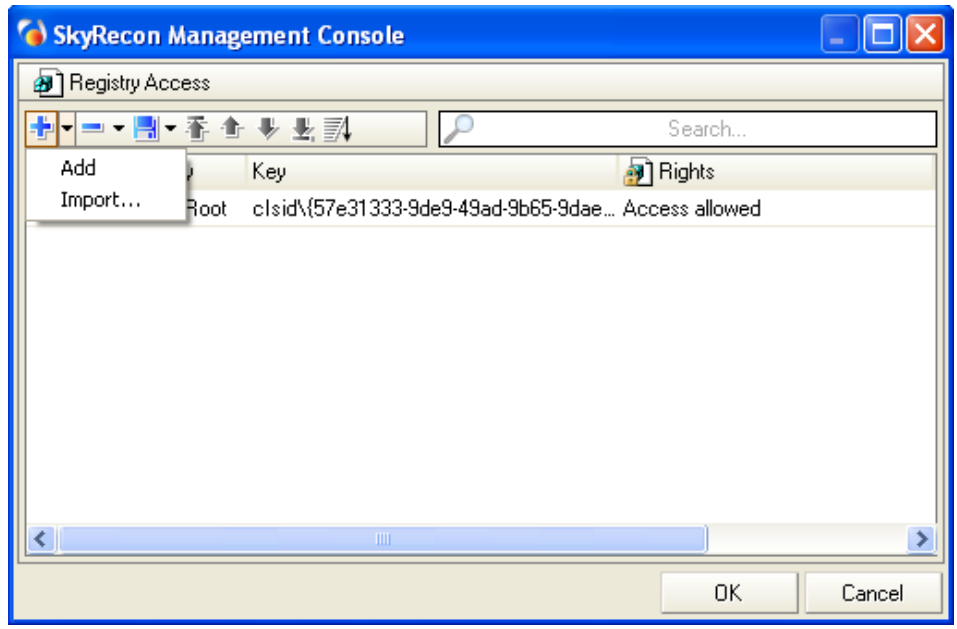
  This attribute describes the key type used for registry access so as to facilitate identification.

Lists of predefined registry access rights

To facilitate the definition of security policies, StormShield is supplied with a list of predefined registry access rights.

To import this list of predefined registry access rights, click  and **Import**.

A search window opens to allow you to browse for the file to be imported.



The **`registry_protection.srxml`** file is a read-only file listing the registry base keys. Malicious programs can use these keys for their installation on workstations.

Once the list is loaded, you can change it to your specifications by:

- Adding lines.
- Deleting lines.
- Changing access rights.

These modifications will not be reflected on the imported file unless you save it using  .

EXTENSION RULES

Extension Rules are used to create a whitelist of extensions and specify the applications that can use them.

For each extension specified, you will need to define which applications are allowed to access this extension. By default, defining a rule for an extension will ban all applications from accessing the corresponding files.

Extension Rules are presented in a tabular form:

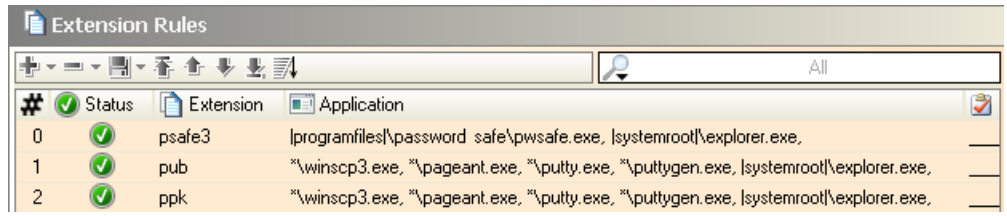


Fig. 9.13: Extension Rules

`.srx`, `.sro`, `.sra` and `.srn files are` protected by StormShield: no application can thus access them. However, it is possible to allow an application to access `.srx` files by adding an extension rule for the `srx` extension.

Attributes

The Extension Rules attributes are the following:

- **Status**:

  This attribute can be set to Enabled or Disabled.

  Just like other items that require activation, a disabled access right is retained in the configuration but is not applied.

  Status has no effect on whether or not the application can access files with an extension specified in the Extension column.

  When Status is set to **Disabled**, the application will not be treated as part of the whitelist until Status is re-enabled.

- **Extension**:

  This attribute defines the extension to which the rule applies. Only the extension is to be entered. There is no need to enter a dot **.** or a wildcard *****.

  For more information, see "Extension Rules", page 310.

- **Application**:

  This attribute indicates which applications can access the files corresponding to the extension specified.

For example, in Fig. 9.13:"Extension Rules", page 310, Outlook Express has access to the files whose extension is `.wab`. No other application can access these files unless they have been included in the extension rules.

If you do not include **|systemroot|\explorer.exe** in the program list, you will not be able to access files via Explorer.

- **Log**:

  This attribute indicates the log where messages are saved when an application not specified in the whitelist tries to access a file covered by the extension rule.

  Log messages will be saved/displayed on/in:

  - The user interface.
  - A pop-up.
  - A database.
  - An external system.

- **Description**:

  This attribute is a freeform comment to facilitate identification.

- **Group**:

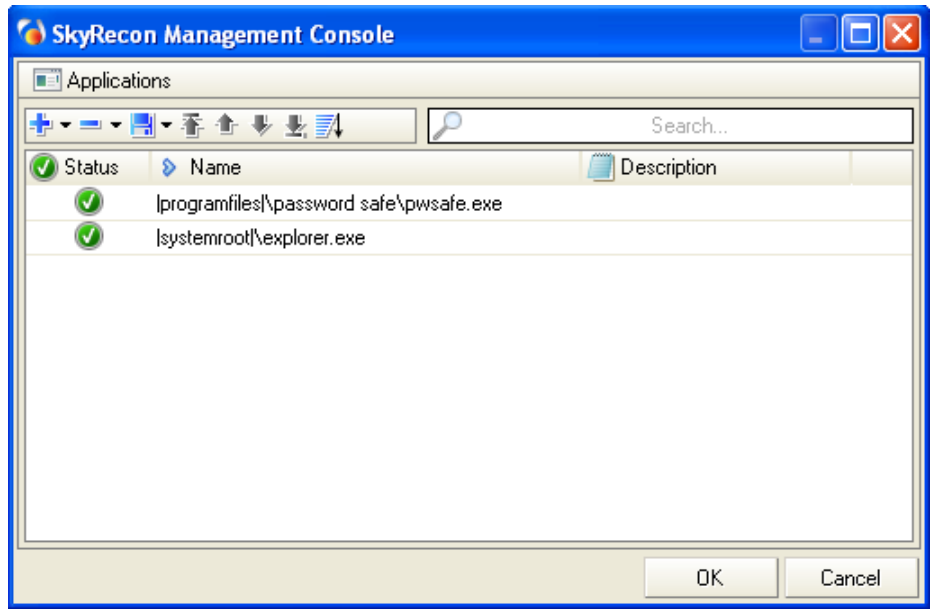
  This attribute shows the group to which the rule belongs. This indication is only visible in the root overview mode of each category.

Attribute configuration

Applications

Double-click in the **Applications** column to open a dialog box.

This dialog box enables you to specify the applications with the right to access files corresponding to this extension.



To remove temporarily an application from the extension rule, double-click the **Status** field to disable it.

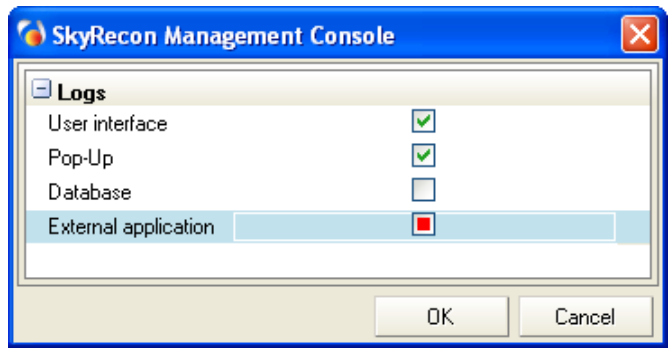
If no application is specified, the extension rule will apply to all applications. Therefore, no application will be able to access files with the extension specified.

Logs

Whenever an extension rule is enforced, a log entry is added to the system log.

To specify where to store the log entries when an extension rule is applied to a particular extension:

- Click the Log field associated with each extension to display the **Logs** window.
- Check the log(s) that you want to use.



KERNEL COMPONENTS

Attributes

This category enables control over driver loading and detects suspect drivers.

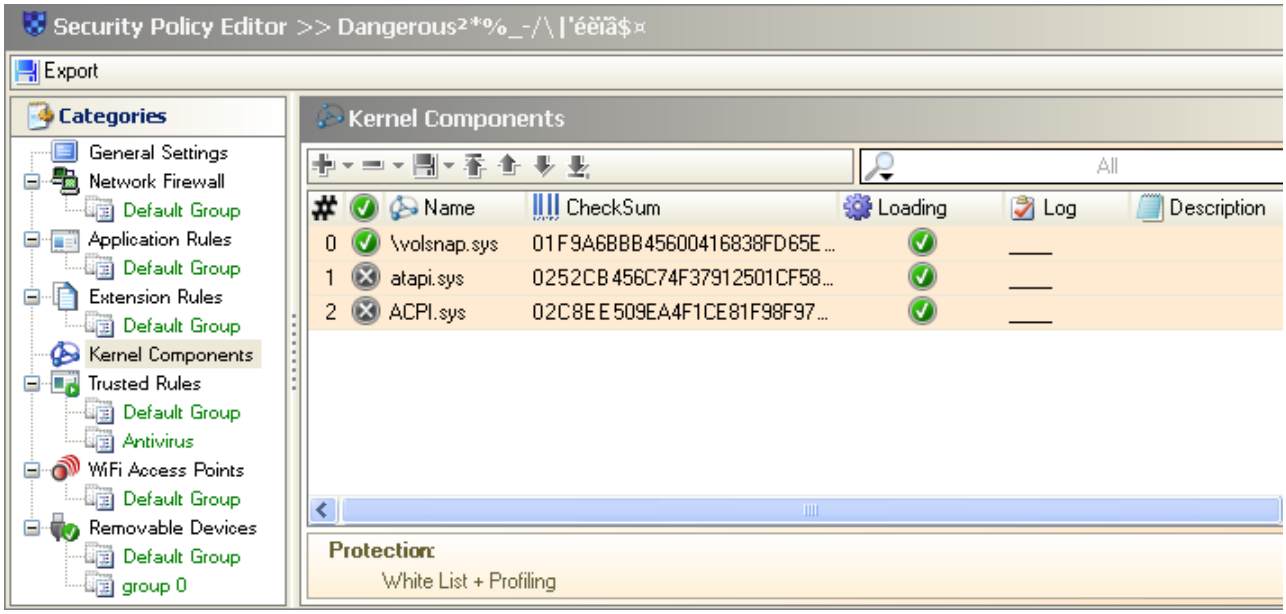


Fig. 9.14: Kernel Components

The Kernel Components attributes are the following:

- **Status**:

  This attribute can be set to Enabled or Disabled.

- **Name**:

  This attribute is the driver name.

- **CheckSum**:

  This attribute is the driver hash.

  The list cannot include twice the same hash but two drivers can have the same name with a different hash.

- **Loading**:

  This attribute can be enabled or disabled.

- **Log**:

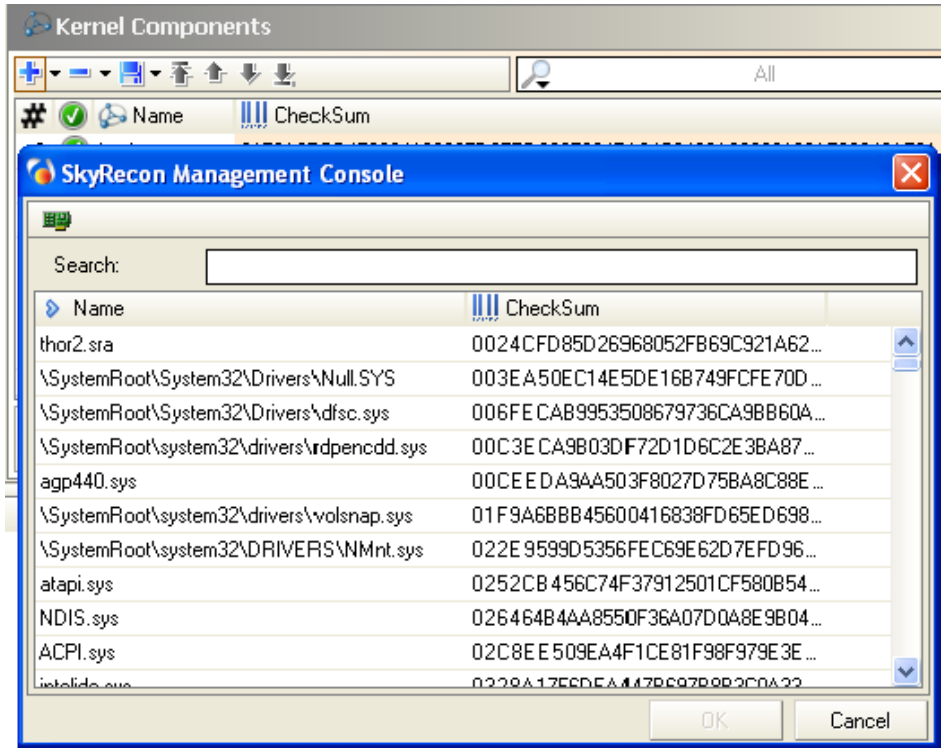
  This attribute defines the settings for saving and viewing log files.

- **Description**:

  This attribute is a freeform comment.

Attribute configuration

To add a driver to the list of kernel components, click in the toolbar. The following window is displayed:



The list of kernel components is automatically generated from the drivers loaded on the workstations on which the agent has been installed.
The protection must be set to Low level at the minimum for the loaded drivers to be listed.

You can use the **Search** field to make sure that a driver or its hash is not already present in the list.

TRUSTED RULES

Defining applications in the Trusted Rules category releases these applications from certain checks so that they can continue to execute actions banned by these checks.

Here are a few examples:

- A remote control application may legitimately use keylogging functions if the **Keylogging** box is checked.
- A debugging tool must be able to attach itself to processes if the **Attach. Src** box is checked.

Attributes

Trusted Rules attributes are displayed in a tabular form:

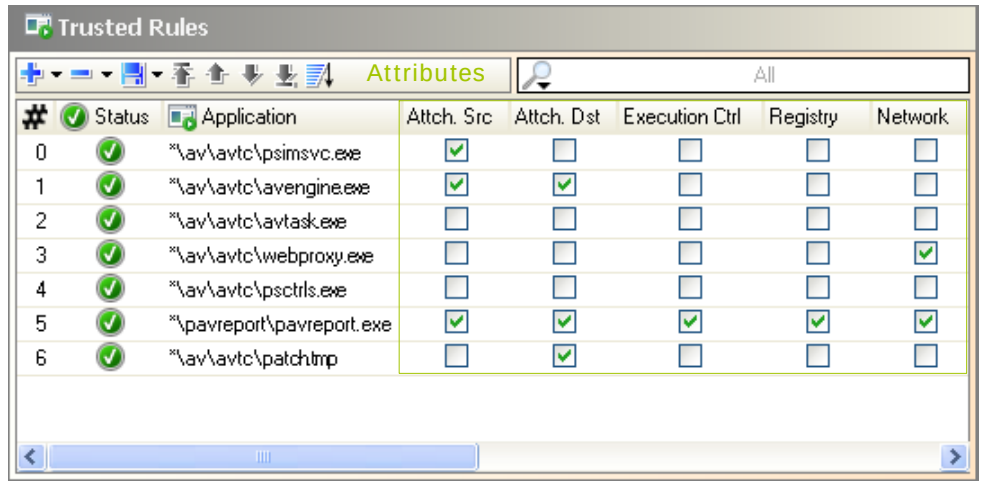


Fig. 9.15: Trusted Rules

The Trusted Rules attributes are the following:

- **Status**:

  This attribute can be Enabled or Disabled.

  A disabled rule is retained in the configuration but is not evaluated when processing the system event.

- **Application**:

  This attribute defines the application to which the rule applies.

- **Domains**:

  This attribute specifies the domains in which the application is trusted.

  The **checked** box means that the application can be trusted in the specified domain. All actions relating to this domain that are normally blocked or indicated by the automatic protections or profile-based protection will, in this case, be considered legitimate.

  The **unchecked** box means that the application is not trusted in the assigned domain.

- **Description**:

  This attribute is a freeform comment.

- **Group**:

  This attribute shows the group to which the rule belongs. This indication is only visible in the root overview mode of each category.

Trusted domains

The trusted domains used are the following:

- **Attach.Src** (attachment source):

  If the box is checked, the application is allowed to attach itself to one or more processes.

- **Attach.Dst** (attachment destination):

  If the box is checked, other processes are allowed to attach themselves to the application.

- **Execution Ctrl**:

  If the box is checked, access to binary files is allowed.

- **Registry**:

  If the box is checked, the application is allowed to access the registry base.

- **Network**:

  If the box is checked, the application is allowed to use sockets.

- **Privileges**:

  If the box is checked, the application allows for escalation of privileges.

- **Files**:

  If the box is checked, the application is allowed to access protected files.

- **Keylogging**:

  If the box is checked, the application is allowed to capture keyboard events.

- **Overflow**:

  If the box is checked, the application is allowed to perform memory overflow.

  Data Execution Prevention (DEP) must be enabled to limit false positives.

- **Reboot**:

  If the box is checked, the application is allowed to reboot the workstation.

- **CPU control**:

  If the box is checked, the application allows for CPU overload.

- **Exe on removable device**:

  If the box is checked and if the option **Execution control on removable device** in the process behavior control is enabled, the application can start from a removable device connected to an agent without confirmation from the user.

The trusted domains correspond to the General Settings defined for automatic protections and profile-based protection.

WIFI ACCESS POINTS

Overview

The WiFi Access Points rules allow you to accept or block WiFi access points:

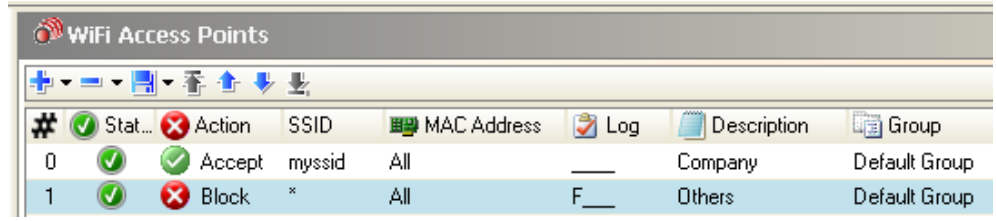


Fig. 9.16: WiFi Access Points

Blocked actions on WiFi Access Points are recorded into the Device log.

WiFi Access Points rules define a whitelist of authorized access points which StormShield-protected workstations can connect to.

To create a whitelist, you must create or modify a policy so that it includes the following:

1. In General Settings, set **WiFi connections** to **Allowed** (under WiFi Encryption and Authentication).
2. Select the appropriate WiFi Access Points rules with the names of the allowed **SSID**s and set **Action** to **Accept**.
3. Add a final WiFi Access Points rule with **SSID** set to ***** and **Action** set to **Block** at the bottom of the list.

WiFi Access Points rules must be ordered so that:

- Rules with **Action** set to **Accept** are listed first.
- A final rule with **Action** set to **Block** and **SSID** set to ***** is placed at the bottom of the list.

Attributes

The WiFi Access Points attributes are the following:

- **Status**:

  This is the rule status (enabled or disabled).

- **Action**:

  This option can assume the following values: Accept or Block.

- **SSID**:

  This stands for the Service Set IDentifier.

- **MAC Address**:

  This is the MAC address of the access point.

- **Log**:

  This attribute defines the settings for saving and viewing log files.

- **Description**:

  This is a freeform description.

- **Group**:

  This the group to which the rule applies. It is visible only in the WiFi Access Points root.

Toolbar

The following toolbar is used to:

- Add
- Import
- Delete
- Save
- Sort rules.

For more information, see "Rule management", page 336.

REMOVABLE DEVICES

Using groups of removable devices strengthens data security.

You can tailor each group of removable devices to ensure enforcement of the company's usage guidelines relating to devices. For example, you can create separate groups of devices based on employees' job requirements, their hierarchical position in the company, etc.

A group of removable devices for R&D engineers might contain fewer restrictions than an administrative group.

Overview

Removable Devices rules are used to create groups of removable devices:

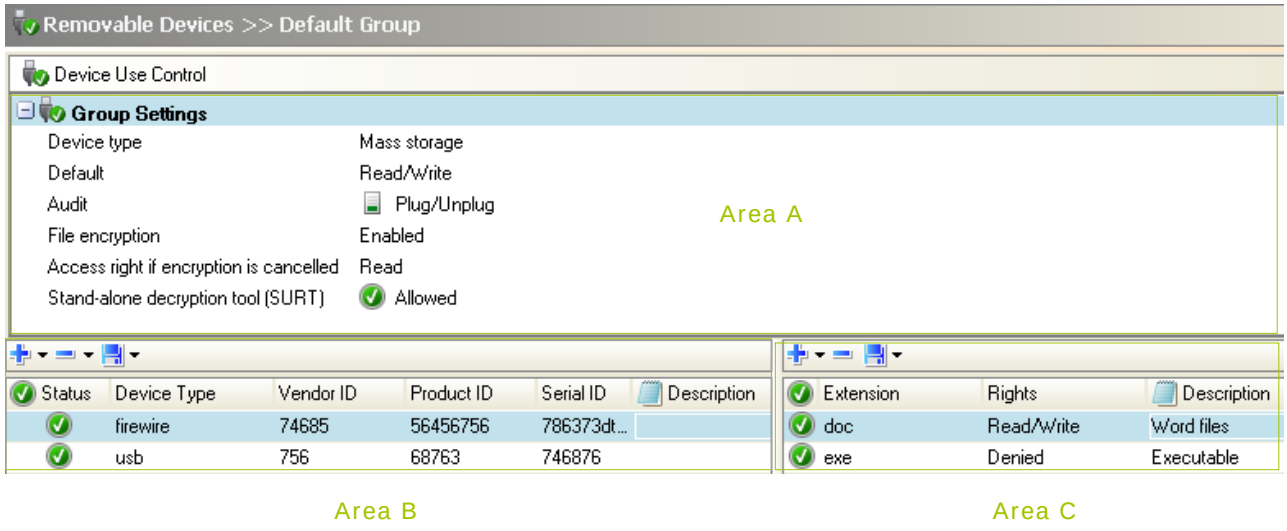


Fig. 9.17: Removable Devices

The Removable Devices panel include three areas:

- **Area A**: **Group settings**

  These settings are applicable to all removable devices in the group.

- **Area B**: **Individual device settings**

  This is the list of devices which constitute the group.

- **Area C: Exceptions by file extension**

  For removable mass storage devices (USB or FireWire), you can specify exceptions to default access rules according to file extension.

  Example: You can set the default access rule to **Denied** for a given device or device type but allow Read access to Excel or Word files.

Group settings

Group settings apply to **all** removable devices in the group.

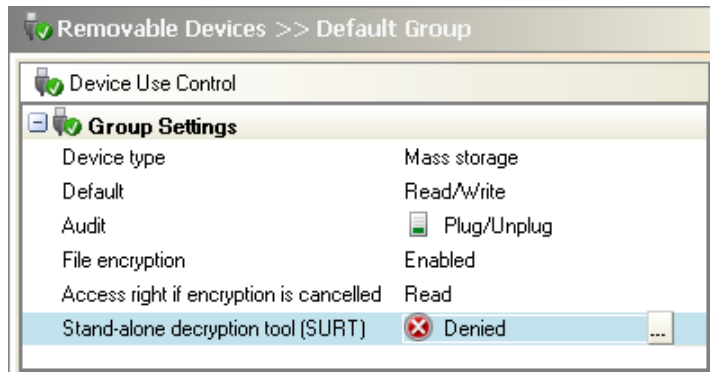


Fig. 9.18: Removable Devices: Group settings

Group settings include **six** items:

- Device type.
- Default (access).
- Audit.
- File encryption.
- Access right if encryption is cancelled.
- Stand-alone decryption tool (SURT).

Device Type

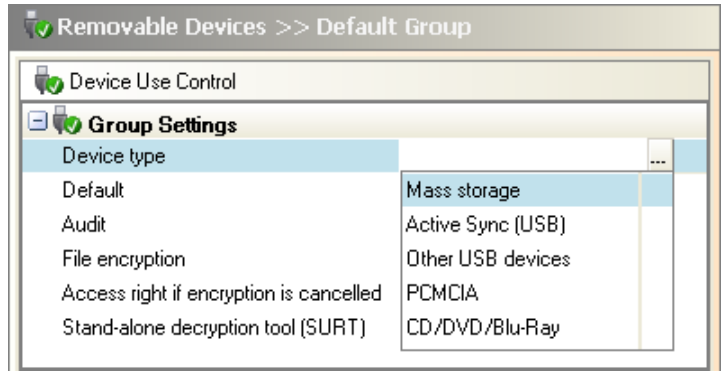


Fig. 9.19: Removable Devices: Device Type

This parameter defines the device type. It can assume the following values:

- **Mass storage**.
- **ActiveSync (USB)**:

  It is used to synchronize with mobile phones (Windows).
- **Other USB devices**:

  It is used for all other types of USB devices.
- **PCMCIA:**

  It enables the user to insert PCMCIA cards for easy transfer and sharing of information.
- **CD/DVD/Blu-Ray**.

After selecting a device type, the data related to this value is updated and set as default. Updated data consists of:

- **Default**:

  For more information, see "Default (access)", page 323.

- **Audit**:

  For more information, see "Audit", page 324.

- **Encryption**:

  For more information, see "File encryption", page 325.

Default (access)

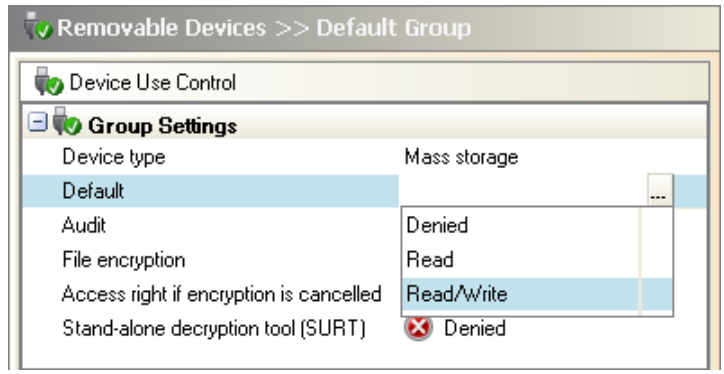


Fig. 9.20: Removable Devices: Default (access)

This parameter can assume the following values:

- **Denied:**

  By default, the user has no access rights to the devices in the list.

  If default access for the device group is set to **Denied**, when the user tries to read or write to a device pertaining to this group, the action will be blocked and the event entered into the Device log.

- **Read**:

  By default, the user has read access rights to the devices in the list.

  If the user tries to write to any device listed, the action will be blocked and the event entered into the Device log.

- **Read/Write**:

  By default, the user has both read and write access rights to all devices in the list.

You can add a list of files which will be excepted from the **Default access** settings.

This list is defined in Area C called **Exceptions by file extension.**

Difference between Access Denied from General Settings and from Removable Devices

When access to a removable device is denied from the security policy under **General Settings > Device Control**, the volume appears on your workstation but not its content.

When access to a removable device is denied from the Removable Devices category under **Removable Devices > Group Settings > Default**, the volume appears on your workstation.
Furthermore, you can list the volume files and folders even if access is denied. Creating empty folders is also possible but not new files.

Audit

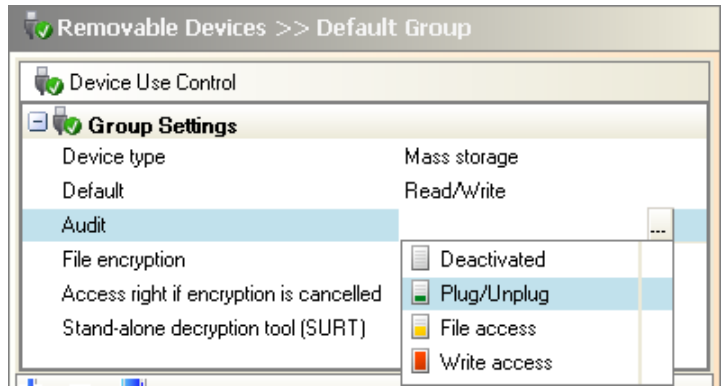


Fig. 9.21: Removable Devices: Audit

This parameter is used to enable the audit of a specific group of mass storage devices.

This parameter allows you to track device use without blocking device actions. You can gather information on how devices are being used. Whenever an audit is enabled, it is recorded in the Device log.

The StormShield agent does not notify the user when an audit is triggered. However, the user can view auditing activity in Log Monitoring > Device > **Information**.

It can assume the following values:

- **Deactivated**:

  Auditing is disabled.

- **Plug/Unplug**:

  An audit entry is written into the Device log when a device in the list is plugged into or unplugged from the computer.
  This entry includes the device size and storage capacity.

- **File access**:

  An audit entry is generated into the Device log when:

  - A device in the list is plugged into or unplugged from the computer.
  - A file on the device is either created, renamed or deleted.

- **Write access**:

  An audit entry is generated into the Device log when:

  - A device in the list is plugged into or unplugged from the computer.
  - A file on the device is either created, renamed, modified or deleted.

Auditing **records** actions in the Device log. It does **not block** unauthorized use.

Blocking unauthorized use is controlled by the **Default** access settings and the list of exceptions under Removable Devices > **Exceptions by file extension**.

File encryption

This parameter enables the encryption of the files stored on a USB or FireWire device. It can be set to **Enabled** or **Disabled**.

For more information, see "Encrypting a file", page 511.

Access right if encryption is cancelled

This parameter can assume the following values:

- Denied
- Read (only)
- Read/Write (access),

if the user chooses not to encrypt the device when prompted to create an encryption password.

Stand-alone decryption tool (SURT)

This parameter allows or denies the use of the SURT decryption tool to enable file decryption on removable devices, for systems not running StormShield.

If this option is enabled, the SURT application will be copied onto the removable devices encrypted by StormShield.

USB Parameters

USB parameters apply to USB devices of the group.

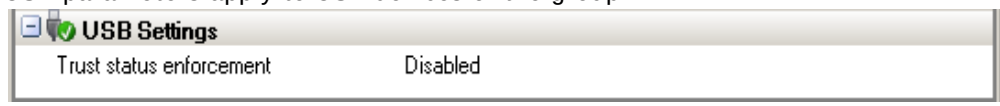


Fig. 9.22: USB parameters definition window

USB parameters include the following element :

- Trust status enforcement

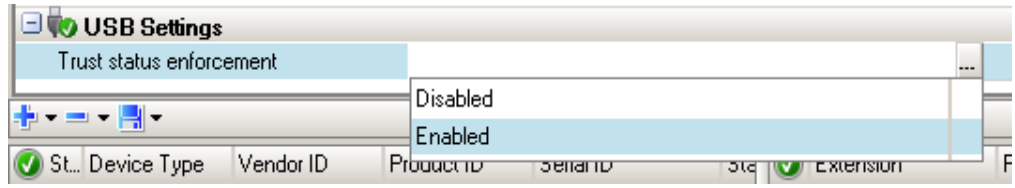


Fig. 9.23: Activation of the trust status enforcement

This parameter applies only if the device is enrolled.

When this option is enabled and if there is an antivirus installed on the workstation, files added or modified out of the perimeter controlled by StormShield are checked by the antivirus in order to verify there is no risk in their content.

Adding individual devices to a group

Overview

You can create a group of devices by adding individual devices and their parameters.

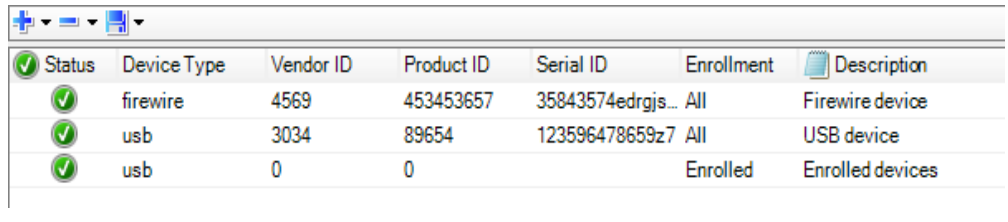


Fig. 9.24: Removable Devices: Individual devices and their parameters

Individual devices include specific details (device types, vendor identifiers, etc.).

The individual devices added to the list must include part or all of the following information:

- **Status**:

It indicates whether the rule status is enabled or disabled (compulsory field).

- **Device Type**:

  It can assume the values USB or FireWire.

- **Vendor ID**:

  This is the identification number of the device vendor.

- **Product ID**:

  This the product code of the device.

- **Serial ID**:

  This is the serial number of the device. Enter this number if you want to assign parameters to an individual device, otherwise leave the field blank.

- **Enrollment**:

  This parameter is specific to USB devices. The following values are available:

  - All: the rule applies to all devices.
  - Enrolled: the rule applies only to devices enrolled by an administrator.
  - Trusted: the rule applies only to devices enrolled by an administrator and which have not been modified from a workstation not protected by StormShield.

Consult "Delegation of the removable device administration", page 349 for more information on this feature.

- **Description**:

  You can add a comment about the device (optional).

You can use a wildcard to create a rule to include any USB or FireWire device.

To do this, in the device window (area B), set all fields to * except for the **Serial ID** which should be left blank.

This information can be added manually or by automatic device detection. For more information, see "Overview", page 330 (Step 4).

Procedure

There are two ways to control removable devices on the console:

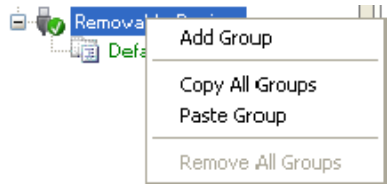
- Either from **General Settings > Device Control** in the Security Policy Editor.

  For more information, see "Device Control", page 270.

- Or from the **Removable Devices** category by creating a group of devices.

To control the use of removable devices by creating a group of devices, follow the steps below:

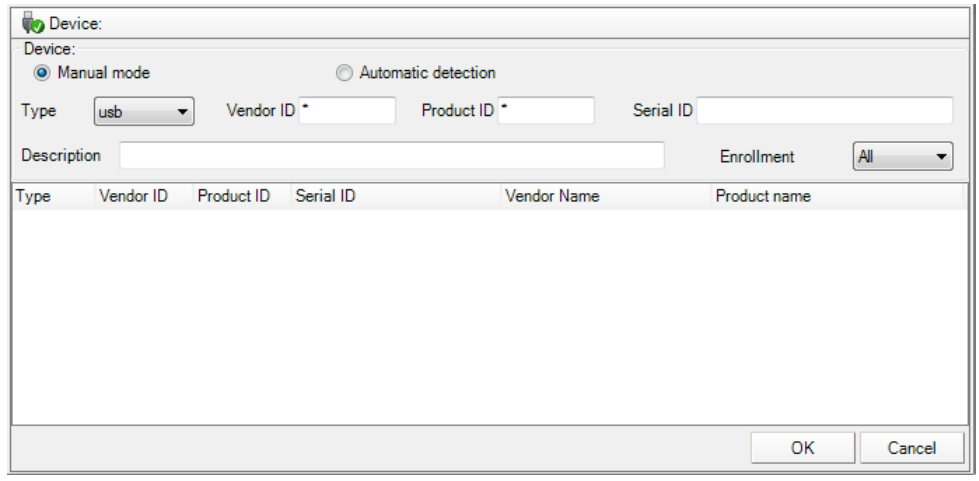
1. Under Categories, right-click Removable Devices and click **Add Group**.



To change the default group name:
- Select the name.
- Press F2.
- Enter a new name.

2. Under Group Settings, select the **Audit** and **Default** access settings that you want to apply to the entire group of devices.

3. Click . The **Device** window is displayed:



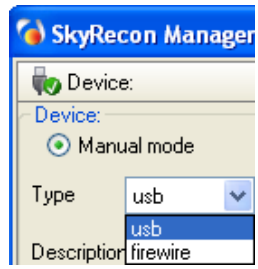
4. Add a device to the list manually or automatically. To do so, click on the **Manual mode** or **Automatic detection** radio button. Repeat the operation with each device.

   If you select automatic detection, you will need to plug in each device to be added.

Depending on how you want to use the device group, you may not want to provide specific information for each category.
For example, you may want to include all the devices from one vendor.

In this case, you would not include the Serial ID.

- If you click on the **Manual mode** radio button, follow the steps below:
  - In the Type field, select **usb** or **firewire** from the dropdown menu.



  - Enter the following information as appropriate:
    - Vendor ID.
    - Product ID.
    - Serial ID.
    - Description.
    - Enrollment.
- If you click on the **Automatic detection** radio button, in the Type field, select **usb** or **firewire** from the dropdown menu.

  StormShield will detect any device currently plugged into the USB port and add them to the group.

  The Device window then automatically refreshes and displays the new information.

  The new device is automatically selected. You can deselect it by clicking on its line.

  If necessary, you can delete any unwanted device from the group.

5. Enter a **Description** (optional).
6. Click **OK**.

   The removable device is added to the device group.
7. Edit device information as needed.
8. Create a list of file exceptions (optional).
   For more information, see "Procedure", page 330.

Exceptions by file extension

Overview

You can specify exceptions to the default group settings. These exceptions are based on file extensions.

For example, Group Settings Default access rights can be set to Denied but you can allow `txt`, `rtf`, `jpg`, etc. files to be read in **Exceptions** (area C) by setting the **Rights** field to **Read**.

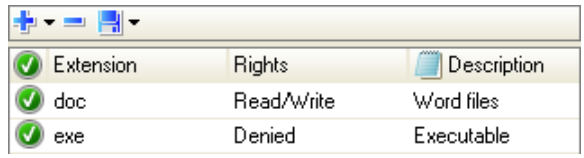


Fig. 9.25: Removable Devices: Exceptions by file extension

This parameter can assume the following values:

- **Denied:**

  If a user tries to read from or write to a denied file (which is stored on a device pertaining to the group), the action will be blocked even if Group Settings Default access rights are set to Read/write or Read.

- **Read**:

  The user can read from “excepted” files on devices even if Group Settings Default access rights are set to Denied.
  Even if Group Settings Default access rights are set to Read/write, the user can read but not write into these “excepted” files.

- **Read/write**:

  The user can read from and write to an “excepted” file on listed devices even if Group Settings Default access rights are set to Denied.

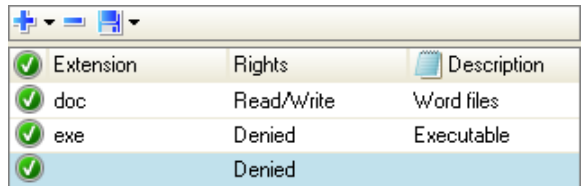
File extension exceptions apply to all devices in the device group.

Procedure

To create a list of exceptions by file extension, follow the steps below:

1. Under Removable Devices, above the **Extension** column (area C), click + to add a rule.

By default, rights are set to **Denied**.



2. Double-click in the **Extension** column field.
3. Enter a file extension (example: `doc`).

> To add an extension, you only need to enter the letters that indicate the extension. No wildcard is needed. For example, you do not need to enter *.doc, doc is enough.

4. In the **Rights** column, enter the access rights assigned to the file extension.
5. Enter a **Description** (optional).

Examples

The following three examples illustrate how you might use device group policies to reinforce your company's usage standards.

Example 1

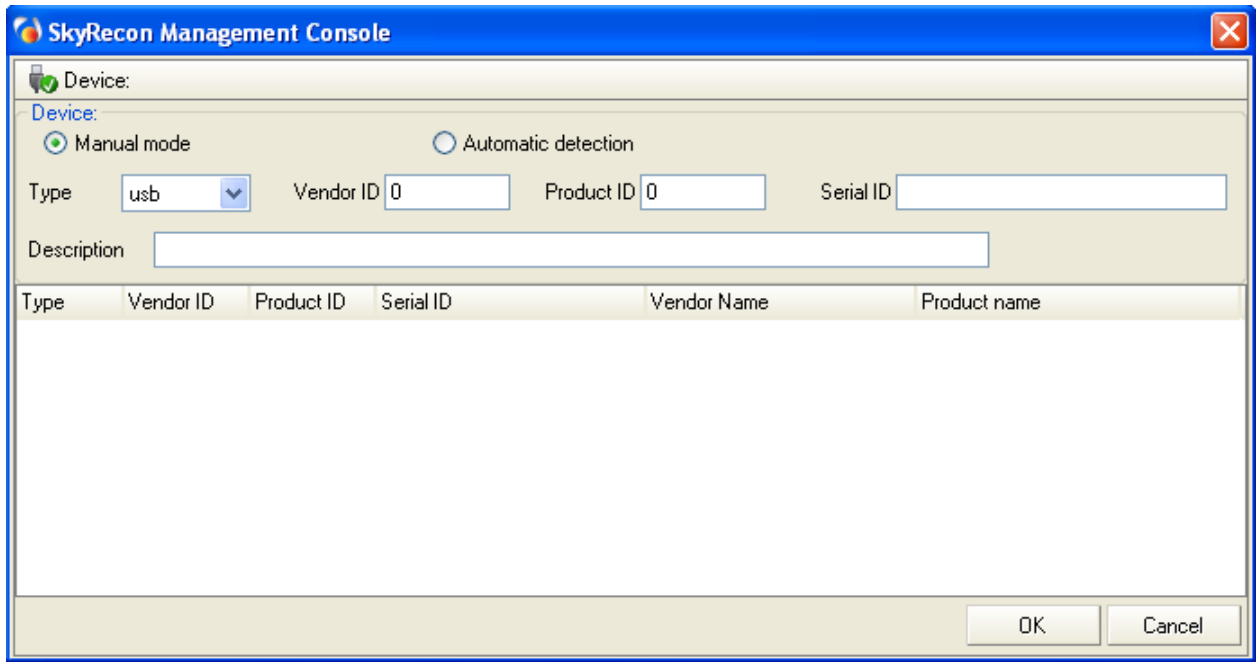
In this example, a device group rule called "Minimal Access" is created to handle any device not specified in any other rule.

Example 1 is the most restrictive example.

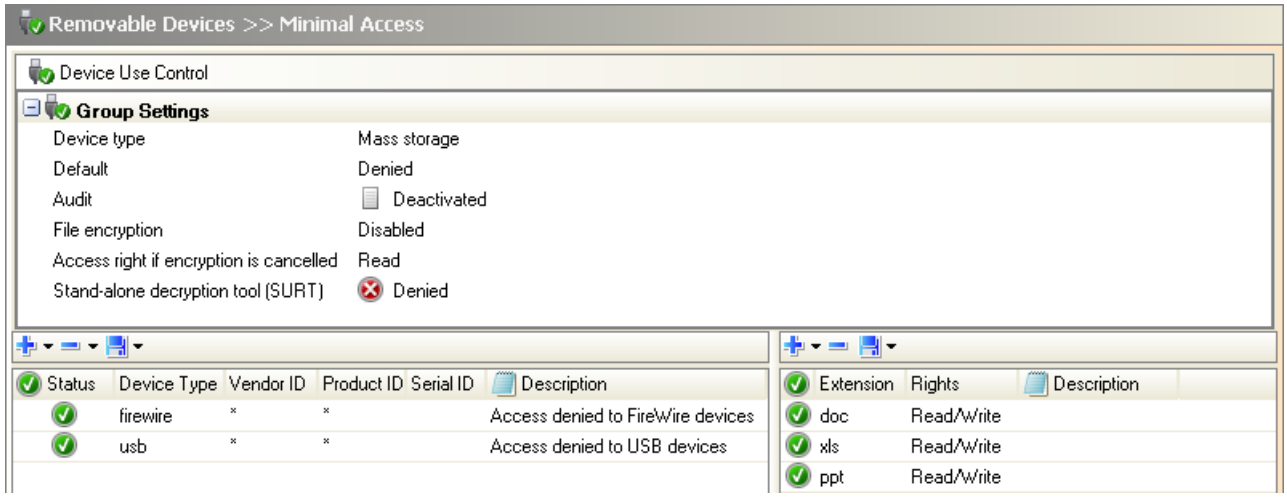
This group denies default access to all devices while file exceptions grant Read/write access to Microsoft Word, Excel and PowerPoint files.

1. Set default group access to **Denied**.
2. Click + to add a rule.
3. In the Device window, create a **USB** device group:
   - Select **Manual mode**.
   - Set Type to usb.
   - Enter **0** in the Vendor ID and Product ID fields.
   - Leave the Serial ID blank. This acts as a wildcard.
     The result is that all devices are blocked by default.
   - Enter a **Description** (optional).

- Click **OK**.



4. Repeat Step 3 to create a **FireWire** device group.
5. Set the access rights for the “excepted” files (`doc`, `xls` and `ppt`).
6. The device list area should look similar to this example.



Example 2

In this example, a “VIP” group is created to handle specific devices used by high-ranking company officials.
Access is unrestricted but devices are listed individually.
Vendor, Product and Serial IDs are included so that only individually-identified devices can be used. The Serial ID is especially important in specifying a unique device.

An unidentified device would be treated under the “Minimal Access” group rule created in Example 1.

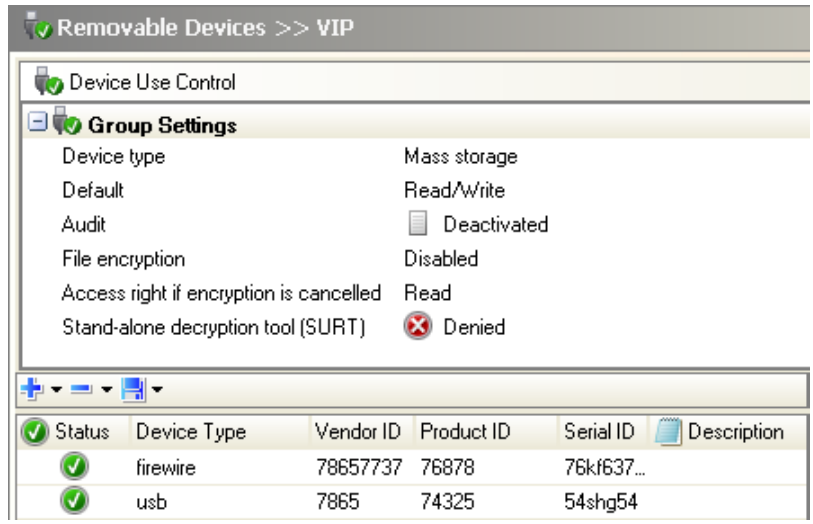
To create this example, follow the steps below:

1. Set Default access set to **Read/Write**.
2. Click to add a rule for **USB** devices.
   - Define the usb settings:
     - Type.
     - Vendor ID.
     - Product ID.
     - Serial ID.
     - Description (optional).
   - Click **OK**.
3. Repeat Step 2 to add a **FireWire** rule.

In this example, we grant read/write rights on all devices.

That is the reason it is highly recommended to fill in the information fields - in particular the serial number field - available for each device.

4. The result should look similar to this:



Example 3

In this example, an “Employee” group is created.

Access is:

- Less restricted that in the “Minimum Access” group in Example 1.
- More restricted than in the “VIP” group in Example 2.

The “Employee” group does not list individual devices but lists groups of devices.

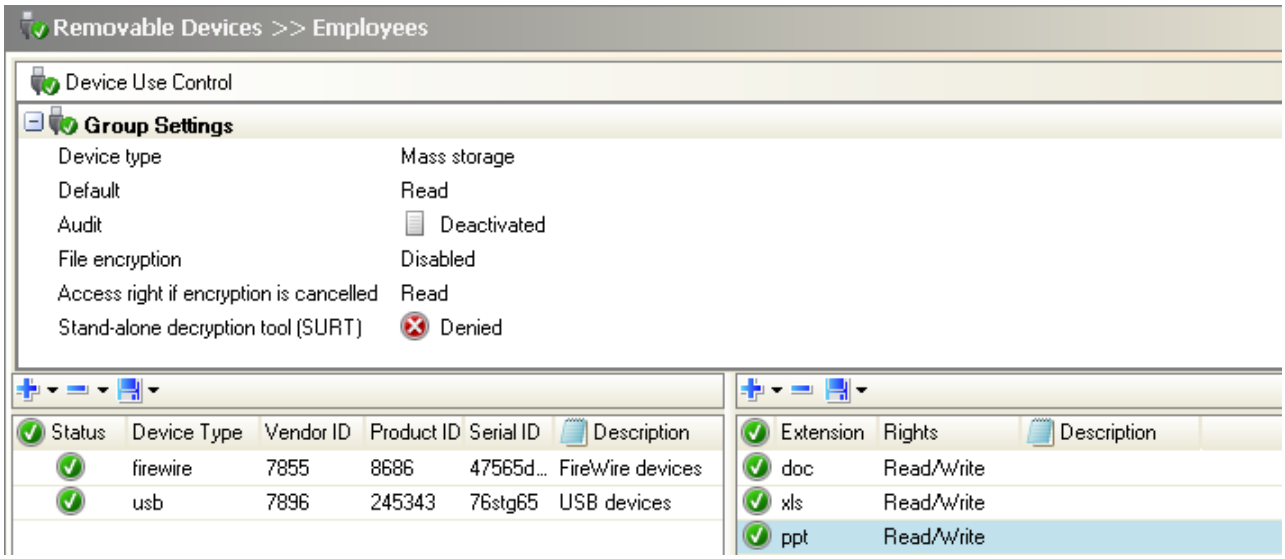
This is useful for restricting devices to company-issued devices that use particular Vendor and Product IDs.

Default access and audit settings, and file exceptions will then apply to any device that matches both the Vendor and Product IDs of one of the devices listed.

To create this example, follow the steps below:

1. Define Default access to **Read**.
2. Click to + add a rule.
3. In the Device window, create a device group:
   - Select the detection mode: **Manual mode** or **Automatic detection**.
   - Select the device type: **usb** or **firewire**.
   - Set the following parameters:
     - Device Type.
     - Vendor ID.
     - Product ID.
     - Description is optional.
   - Leave Serial ID blank.
   - Click **OK**.

4. The result should look similar to this:



RULE MANAGEMENT

The following toolbar is used to:

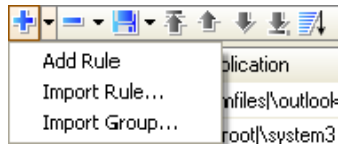
- Add
- Import
- Delete
- Save
- Sort rules.

The **Search** field is used to reduce scrolling through the list of rules.

ADDING A RULE

To add a rule, follow the steps below:

- Just click or click to display the dropdown menu.
- In the second case, click **Add Rule**.



- Define the rule settings.

IMPORTING A RULE

To import a rule, follow the steps below:

- Click to display the dropdown menu.
- Select **Import Rule**.
  A search window opens to allow you to browse for the rule file.

IMPORTING A RULE GROUP

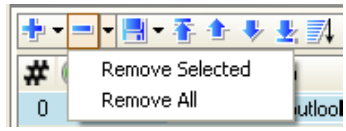
To add a rule group, follow the steps below:

- Click to display the dropdown menu.
- Select **Import Group**.
  A search window opens to allow you to browse for the rule group file.

DELETING A RULE

To delete a rule, follow the steps below:

- Select the rule to be deleted.
- Click directly to remove the rule or to display the drop-down menu.



- In the second case, click **Remove Selected** or **Remove All** to delete all the group rules.

To delete more than one rule at a time, press **Ctrl** while clicking to select the rules.

SETTING THE RULE PRIORITY ORDER

Three buttons are available to set the rule priority order:

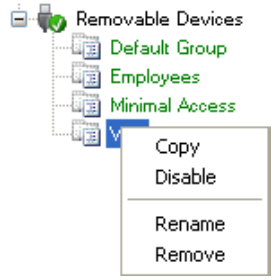
- Click or to change the rank of the rule selected.
- Click or to set the rule selected at the top/bottom of the list.
- Click to sort automatically the rules according to the following criteria:
  - Full path.
  - Full path including environment variables.
  - Full path without environment variables, ending with a *.
  - Full path including environment variables, ending with a *.
  - Path starting with a *.

It is recommended to use when there is a large number of rules to be sorted.

ENABLING/DISABLING A RULE GROUP

To enable/disable a rule group, follow the steps below:

- Right-click the appropriate rule group in the Categories tree structure.
- Select **Disable/Enable** from the dropdown menu.



To disable a rule group, that is to keep it in the configuration while inhibiting its application, just right-click the rule group and select **Disable**.

To disable a single rule, just double-click on the rule in the corresponding column.

DISPLAYING MORE DETAILS ON RULES

This option only applies to the network firewall toolbar.

You can access additional attributes by clicking .

HANDLING CONFLICTS BETWEEN RULES

RULE PRIORITY ORDER

The order for evaluating rules depends on the rule order defined manually by the administrator, the rule category and its scope of action.

The check sequence for rule categories is the following:

1. Trusted Rules.
2. Extension Rules.
3. Application Rules.

For Application Rules, simply defining a rule for a particular application frees it from any other rules applicable to a set of applications, as regards:

- Network environment.
- Files.
- Registries.

EXAMPLES

Here are three examples showing how rule collisions are handled.

Example 1

Let us consider the following situation:

- No application (`*.exe`) is allowed to access a text file (`*.txt`).
- Windows Notepad (`*\notepad.exe`) is allowed to access text files (`*.txt`)

In this case, the second rule takes precedence, as it is the most specific. It will therefore be possible to open a text file using Notepad.

Example 2

Let us consider the following situation:

- No application (`*.exe`) is allowed to access text files (`*.txt`).
- Internet Explorer is explicitly allowed to access the network using certain ports.

The Internet Explorer rule takes precedence over the generic rule. There is no conflict as the filed of application of the two rules is different:

- The first rule applies to files.
- The second rule applies to network access.

Example 3

Let us consider the following situation:

- No application (`*.exe`) is allowed to access text files (`*.txt`).
- Internet Explorer is explicitly forbidden to access MP3 files (`*.mp3`).

As the Internet Explorer rule takes precedence over the generic rule, this application will have the right to open text files.

To inhibit this behavior, it will be necessary to specify both .txt and .mp3 access rules for this application.

WRITING CONVENTIONS

APPLICATION ENTRY FORMAT

The full application path can be specified. One or several * wildcards can also be used.

Example 1

Here is an example of an application identified by its full path:

```
C:\program files\Internet Explorer\iexplore.exe
```

Example 2

This example shows how to identify an application regardless of the drive where it is located or its access path:

```
*:\program files\Internet Explorer\iexplore.exe
*\iexplore.exe
```

ENVIRONMENT VARIABLES

There are three environment variables used to specify rules independently of differences in naming and organization proper to Windows system directories.

These variables are defined using pipe separators (|), at the beginning or end of the string:

|programfiles|

This the default installation directory for applications. It is usually:

```
c:\program files
```

|systemdrive|

This is the root of the drive where the system is installed. It is usually:

```
c:\
```

|systemroot|

This is the primary directory for operating system files. For Windows XP, it is usually:

```
c:\windows
```

CONFIGURATION TEMPLATES

OVERVIEW

StormShield includes basic policy templates and a set of predefined packages that should be used for accelerating the implementation of your own security policies.

These templates are designed to be enhanced over time. We will therefore only provide references to some basic preset configurations here.

Before implementing these configurations, check with your reseller or on SkyRecon Systems' extranet site (`http://extranet.skyrecon.fr`) for the availability of new templates.

PREDEFINED GROUPS AND CONFIGURATION RULES

Following are some of the predefined groups and configuration rules supplied with StormShield 6.0 (in addition to those included in the base configuration).

They are installed by default in the `Sample` subfolder under:

```
C:\Program Files\skyrecon\SkyRecon Management Console\
```

Base policies

StormShield is supplied with several base policy templates. Base policies are meant to be used as a quick-start template for building your own policies.

Base policies include a number of network and system rules that have been defined to prevent the product from blocking legitimate basic Windows operations.

When your policy rules are complete, you should increase the automatic protections security levels in **General Settings**.

The base policies consist of the following files:

- `base_policy.scep`:
  Example of base policy for a standard workstation.
- `advanced_base_policy.scep`:
  Example of reinforced base policy for a standard workstation.

The `Sample` subfolder also contains a `base_policy` folder which includes three files:

- `base-network.scep`:
  Example of network firewall rules for a standard workstation.
- `base-system_applications_rules.scep`:
  Example of application rules for a standard workstation.
- `base-system_trusts_rules.scep`:
  Example of trusted rules for a standard workstation.

Application rules

The predefined application rules consist of:

- Rules for protecting Outlook, Outlook Express and ThunderBird (limiting abnormal code execution, filtering network communication, protecting address books):
  - `e-mail_applications_rules.scep`:
    Application Rules.
  - `e-mail_applications_extensions.scep`:
    Extension Rules.
  - `e-mail_applications_trusts.scep`:
    Trusted Rules.
- Rules for protecting Internet Explorer and Firefox (filtering network communication, stopping the browser from opening executable files):
  - `web-browsers_application_rules.scep`:
    Application Rules.
- Rule group banning P2P applications (blacklist):
  - `P2P_application_rules.scep`:
    Application Rules.
- Rule group banning instant messaging applications (blacklist):
  - `Instant_Messaging_applications_rules.scep`:
    Application Rules.
- Rule group banning the use of multimedia files on the system:
  - `multimedia_files_extensions.scep`:
    Extension Rules.
- Rules for protecting the user and local machine registry base:
  - `registry_protection.scep`:
    List of registry keys for application rules.
  - `advanced_registry_protection.scep`:
    List of advanced registry keys for application rules.
- Rules for protecting system files:
  - `system_files.scep`.

Predefined object list

StormShield also offers two lists of file types that are useful for blacklists. These lists are included in the following files:

- `multimedia_files.scep`:
  List of the main multimedia, audio and video file extensions.
- `active_content_files.scep`:
  List of the main executable file extensions.

Chapitre 10

REMOVABLE DEVICE ADMINISTRATION

ABOUT THIS CHAPTER

This chapter presents the administration and enrollment of removable devices.

It includes the following:

OVERVIEW

StormShield enables to enroll removable devices used on the organization's workstations in order to control them. It ensures the security of the workstation on which the device is connected and facilitates the management of devices.

An enrolled removable device is uniquely identified and configured by the device management tool. It must be associated to a single user who is the owner.

An enrolled device is trusted as long as its content has not been modified out of the perimeter of the organization. It can be used on any workstation of the secured perimeter. If a modification of the content is detected, it is possible to configure an antivirus check on the device to be trusted again.

A control agent installed on each workstation and server of the organization allows access only to enrolled removable devices complying with the controls defined in security policies.

StormShield supports all USB 2.0 device drivers. However it supports only 3.0 USB devices using the following drivers:

- usbhub (Microsoft Generic)
- usbhub20
- vusb3hub (Via)
- nusb3hub (Nec Electronics, Renesas Electronics)
- iusb3hub (Intel)
- asmthub3 (AS Media)
- usbhub3 (Microsoft Generic Window 8)
- amdhub30 (AMD)

An enrolled device cannot be encrypted.

PREPARATION OF THE REMOVABLE DEVICE ENROLLMENT

To enroll removable devices, you must satisfy the following prerequisites:

- a unique identifier, specific to the organization
- an access to the organization LDAP directory

The organization identifier is automatically generated when installing StormShield. The value of the identifier can be manually modified, for example to reuse the identifier of a previous installation.

By default, the StormShield console automatically detects the Active Directory forest of which the workstation is a member. This Active Directory allows to identify the owners of the enrolled keys.

The connection parameters to the LDAP directory can be manually configured to connect to a specific zone of the directory or to another directory for example.

These parameters are stored in the [db_properties] table of the StormShield configuration SQL base.

This table can include the following properties:

Key	Value
enrollment-organizationGuid	The value of this property must be specific to the organization. The identifier format is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx where x is a hexadecimal digit. It is initialized during the installation with a random value.
enrollment-ldapGuidAttribute	This property contains the name of the LDAP attribute including users GUID. The default value is `objectguid`. On other LDAP directories, it can be `entryuuid`.
enrollment-ldapBaseDN	This property defines the branch of the directory from which users are searched for. By default, it is the Active Directory root.
enrollment-ldapServer	This property contains the address and the port of the LDAP server. The current Active Directory is used by default.
enrollment-ldapUser	Login used to authenticate and search for users in the directory. This property can be empty when an anonymous or Active Directory connection is used.
enrollment-ldapPwd	This property contains the connection password to the directory.

enrollment-IdapAuthType	The possible values of this property are `Anonymous` for an anonymous connection, `Basic` or `Digest` for a classic LDAP directory, and `Negotiate` for an Active Directory.
enrollment-IdapUserFilter	This property contains the LDAP filter listing the directory users. The default filter corresponds to the active users of the Active Directory: `(&(!(useraccountcontrol:1.2.840.113556.1.4.803:=2))(objectcategory=person))` For a classic LDAP directory, the filter can be `(objectclass=inetorgperson)`.
enrollment-IdapAutoCompleteFilter	LDAP filter used when automatically completing the name of a user. The default value is `(cn={0}*)`. The attribute used as users RDN must be used. This filter can be replaced by `(uid={0}*)` for example.
enrollment-IdapAdministratorFilter	This property contains the LDAP filter enabling to find the LDAP account of the administrator connected to the console from his/her StormShield identifier. The default value is `(&(userprincipalname={0}@*)(objectcategory=person))`. We recommend naming StormShield users with the same name as their account in the directory. On some LDAP repositories, the value can be `(&(uid={0})(objectclass=inetorgperson))`.
enrollment-IdapSearchUserFilter	This property contains the LDAP filter used by the console for the advanced search of names. It can be applied to all attributes containing a part of the name of the searched user. The default value is `(l(cn=*{0}*)(displayname=*{0}*)(mail=*{0}*))`.
enrollment-IdapSearchDepartmentFilter	This property is used as a LDAP filter by the console for the advanced search of names. It can be applied to all attributes containing a part of the service or the site of the searched user. The default value is `(l(ou=*{0}*)(department=*{0}*)(l=*{0}*))`.

To modify these properties, you must edit the [db_properties] table of the StormShield configuration SQL base thanks to an SQL Server client like `sqlcmd` or SQL Management Studio.

DELEGATION OF THE REMOVABLE DEVICE ADMINISTRATION

OVERVIEW

If a security policy applies to several devices, it can be tedious to add new devices. You need to deploy a new configuration when modifying the list of devices.

In order to simplify these scenarios, the rules of the security policy rely on the enrollment status of the device. The status is one of the rules configuration settings.

The console enables to assign a status to a device. Agents configuration does not depend on the devices status. The advantages are the following:

- StormShield administrators having access to the enrollment management features do not have to be the same that administrators able to modify agents configuration.

  The number of enrollment administrators can be much higher than the number of agents administrators.

- The status of the same device can change. A device is considered as trusted if it is used only on the organization network. It can lose this status if it is modified on a workstation out of the network.

- The owner is known when enrolling the device. The logs generated by the agent mentions the name of the owner.

The installation of StormShield may need to be customized as described in the section "Preparation of the removable device enrollment", page 347 to use this enrollment feature.

The device administration delegation features are detailed in the following sections.

DEVICE ADMINISTRATION PERMISSIONS

The devices administration is divided into two features. Each one is controlled by a specific permission in the roles management window.

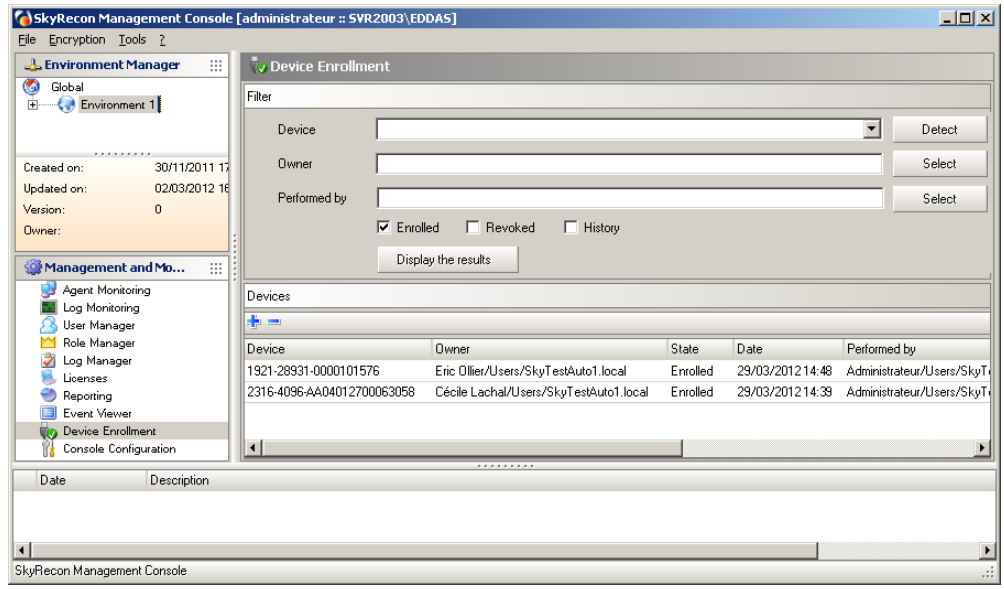
View enrolled devices	☑	View enrolled devices and their owners
Enrolled devices management	☑	Enroll or revoke devices

The permission **View enrolled devices** is compulsory for all devices administrators. It enables to consult the current enrollment status of a device, to find devices associated to a person and to access the complete history of actions. It is a read-only access.

The permission **Enrolled devices management** allows administrators to enroll or revoke a device. The scope of the administrators includes all the devices and all the owners. It is not possible to limit the management of enrolled devices to a sub-set of the organization. However, all the administration actions are traced and it is possible to audit each administrator's operations.

ENROLLED DEVICE CONSULTATION

All the devices administration functions are in the **Device enrollment** window.

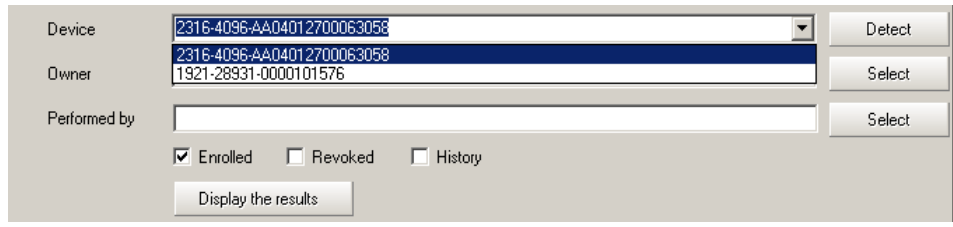


The **Filter** panel enables to filter the list of devices in order to consult the enrollment status of a specific device, of a particular person or to know the list of enrollment operations performed by a particular console administrator.

The list of devices in the lower panel details enrollments and in particular the name of the administrator who enrolled or revoked the device.

Device selection

Administration screens automatically detect devices connected to the workstation.

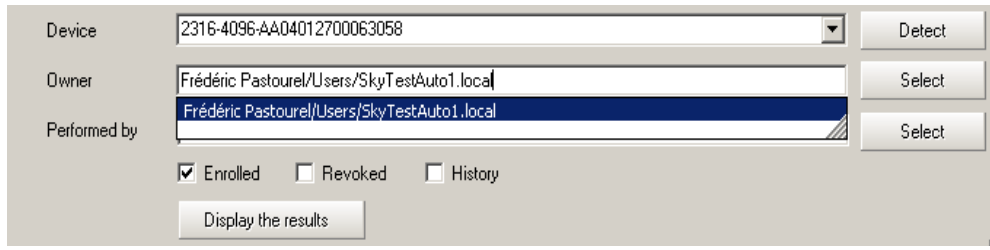


Click the **Detect** button to display the devices identifiers in the **Device** drop-down list.

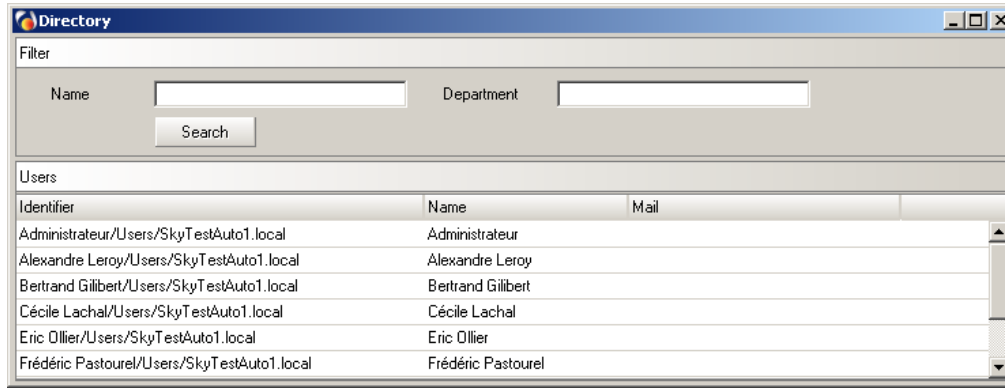
Directory

In the **Owner** and **Performed by** fields, select the owner of a device or the administrator who performed the enrollment operation from the organization directory.

The automatic completion of names based on the first letters enables a quick selection.



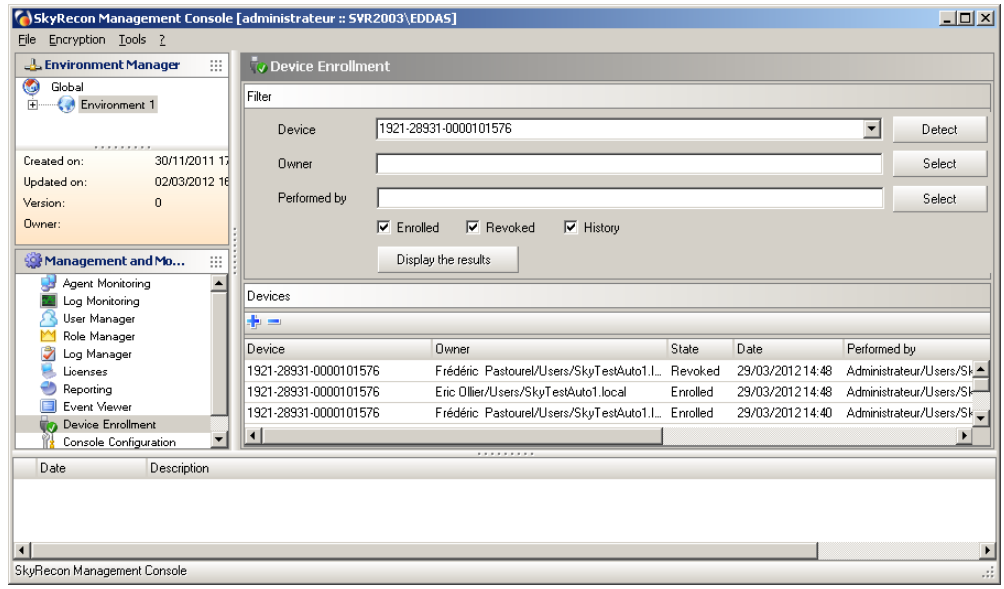
If it is not possible to search a person with his/her name, click the **Select** button to open the advanced search form. Enter any letter of the name, the location or the department of a person to filter the users list.



Events history

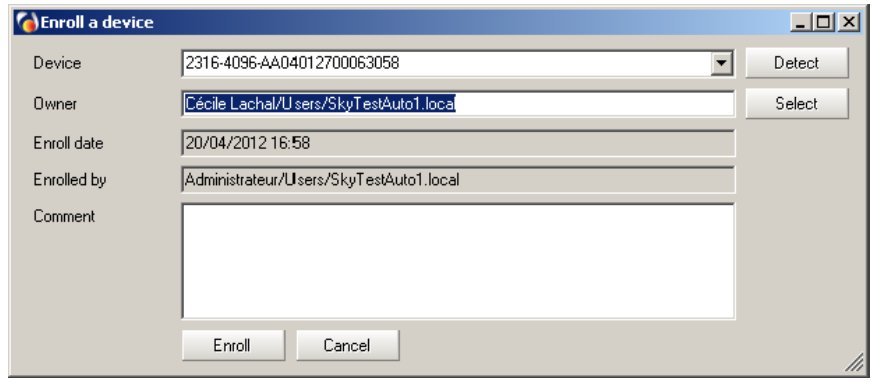
In the **Filter** panel, if the **History** checkbox is unchecked, the **Device** list only displays the current status of the device or of the person selected in the filters.

If it is checked, the list also displays past events.

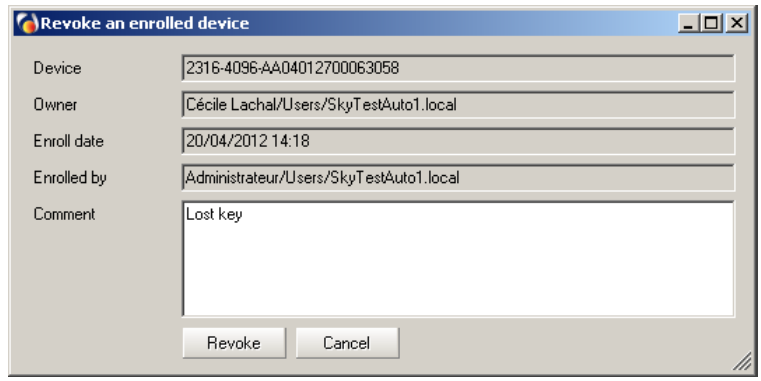


DEVICE ENROLLMENT AND REVOCATION

An administrator can enroll a device by clicking the icon on the main panel. The **Enroll a device** window displays. He/she can select the device, the owner and enter a comment.



When an enrolled device is listed in the main panel, the administrator can revoke it by selecting it in the list and by clicking the icon. The **Revoke an enrolled device** window displays. He can then view the details of the device and add a comment about the revocation.



Administration events are systematically traced in the StormShield base and can be viewed in the history.

Chapitre 11

REMOVABLE DEVICE ENCRYPTION

ABOUT THIS CHAPTER

This chapter presents the encryption/decryption of removable devices.

It includes the following:

- Overview :
  - Purpose.
  - Characteristics :
    - Advanced Encryption Standard.
    - Password protection.
    - Encryption password.
    - Secure erasure.
  - Supported operating systems.
  - What can be encrypted.
  - Unencrypted partitions.
  - Encryption key.
  - Synchronizing.
  - Symbology.

- Creating an encryption policy to be applied to a group of devices :
  - Two-level settings :
    - Removable Devices
    - General Settings

- Connecting a removable device :
  - Password.
  - Synchronizing.
  - Access to the device without password.
  - Access to encrypted data.
  - Behavior when modifying the encryption policy.
  - Using encrypted devices on other computers :
    - Sharing encrypted files.
    - Systems not running StormShield.
    - Other systems running StormShield.
  - Removing SD cards.
- Decrypting a removable device :
  - Administrator side.
  - Agent side.
- Passwords :
  - Administrator side.
  - Agent side.
- Repairing a corrupted encryption key.

OVERVIEW

PURPOSE

Removable Device Encryption provides an extra layer of protection by encrypting data stored on USB or FireWire devices
with a password-protected key.

Removable device encryption is **not** related to the StormShield encryption feature.

An enrolled device cannot be encrypted.

CHARACTERISTICS

Advanced Encryption Standard

The StormShield encryption feature (for USB and FireWire devices) is based on the Advanced Encryption Standard (AES).
This system has been approved by the U.S. Government for use with both classified and non-classified documents.

The size of device encryption keys is limited to 256 bits.

Password protection

By password-protecting the encrypted data stored on these devices, sensitive company data is further protected from theft.

Encryption password

The password used to open encrypted files is also encrypted. It is therefore as secure as the encryption applied on files.

Secure erasure

When encrypting a device already containing files, StormShield first generates an encrypted copy of old data before performing a secure erasure. When creating new files on a device encrypted by StormShield, this erasure operation is not required.

For this reason, the encryption of a device already containing files takes more time than the copy of the same amount of data on an already encrypted device. The number of passes required for a secure erasure depends on the device type: magnetic (external hard disk) or flash memory (USB key) type.

SUPPORTED OPERATING SYSTEMS

USB and FireWire encryption is supported by:

- 32-bit Windows XP SP3.
- 32-bit Windows Vista SP2.
- 32-bit Windows 7.

Removable device encryption-related menus are hidden on the agents that are installed on PCs running unsupported operating systems.

WHAT CAN BE ENCRYPTED

You can opt to automatically encrypt entire USB and FireWire devices.

For more information, see "Creating an encryption policy to be applied to a group of devices", page 360.

The device encryption policy is applied to the entire device group. The Access Control List (ACL) defined in **General Settings** is applied as part of the encryption policy.

For more information, see "Purpose", page 357 and "Access to the device without password", page 363.

UNENCRYPTED PARTITIONS

For devices with partitions, such as external hard disks, you can omit a partition from the encryption policy after the first plug-in.

There is no password prompt for an unencrypted partition.

Partitions must be created before the device is encrypted.

ENCRYPTION KEY

The encryption key is stored in a file called `sr_id.` in the key root directory. There is one `sr_id.` file per partition. Each partition can be protected by a different password.

The StormShield server contains a copy of the data stored in the `sr_id.` file. If this file is **corrupted** on the removable mass storage device, a copy of the data is automatically downloaded from the server in order to restore the file. This is invisible to the user.

If however, the server is not available, the user will receive a message indicating that:

- `sr_id.` is corrupted.
- Encrypted files are inaccessible.

The user can either request a new encryption key from the administrator or replace the `sr_id.` file with a backup copy (if the user has previously made one).

For added assurance, the user should also make a backup of the encryption key using the **Export** function in the StormShield Agent monitor menu.

For more information, see "Exporting an encryption key", page 380.

SYNCHRONIZING

The first time a device is plugged in after a device encryption policy is applied, it goes through a synchronization process encrypting the entire device.

A progression bar is displayed throughout the process.

SYMBOLOGY

An orange lock is displayed at "My Computer > Devices with Removable Storage" level to indicate that there is at least one encrypted file stored on the device.

CREATING AN ENCRYPTION POLICY TO BE APPLIED TO A GROUP OF DEVICES

TWO-LEVEL SETTINGS

You can define removable device encryption at **two** levels in the security policy:

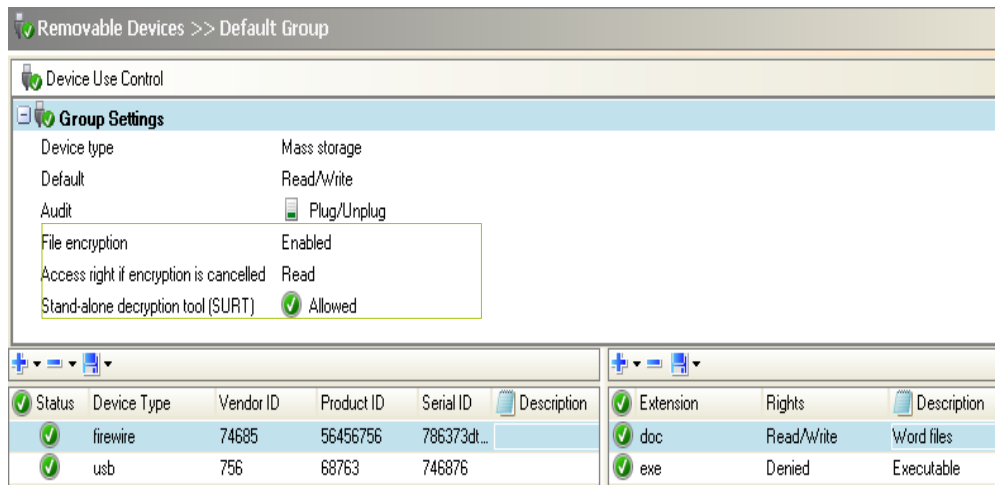
- Removable Devices.

  For more information, see "Removable Devices", page 320.
- General Settings.

  For more information, see "Device Control", page 270.

Removable Devices

The device encryption settings under **Removable Devices** > Device Use Control > Group Settings are the following:



- **File encryption**
  - Disabled:
    No file encryption.
  - Enabled:
    This option encrypts the entire device or a device partition.

- **Access right if encryption is cancelled**:
  This option enables:
  - Read-only,
  - Read/Write,
  - Denied access,

  to unencrypted files if the user chooses not to encrypt the device when prompted to create an encryption password.

- **Stand-alone decryption tool (SURT)**:
  This option allows or denies use of the SURT encryption tool to enable file decryption on systems not running StormShield.

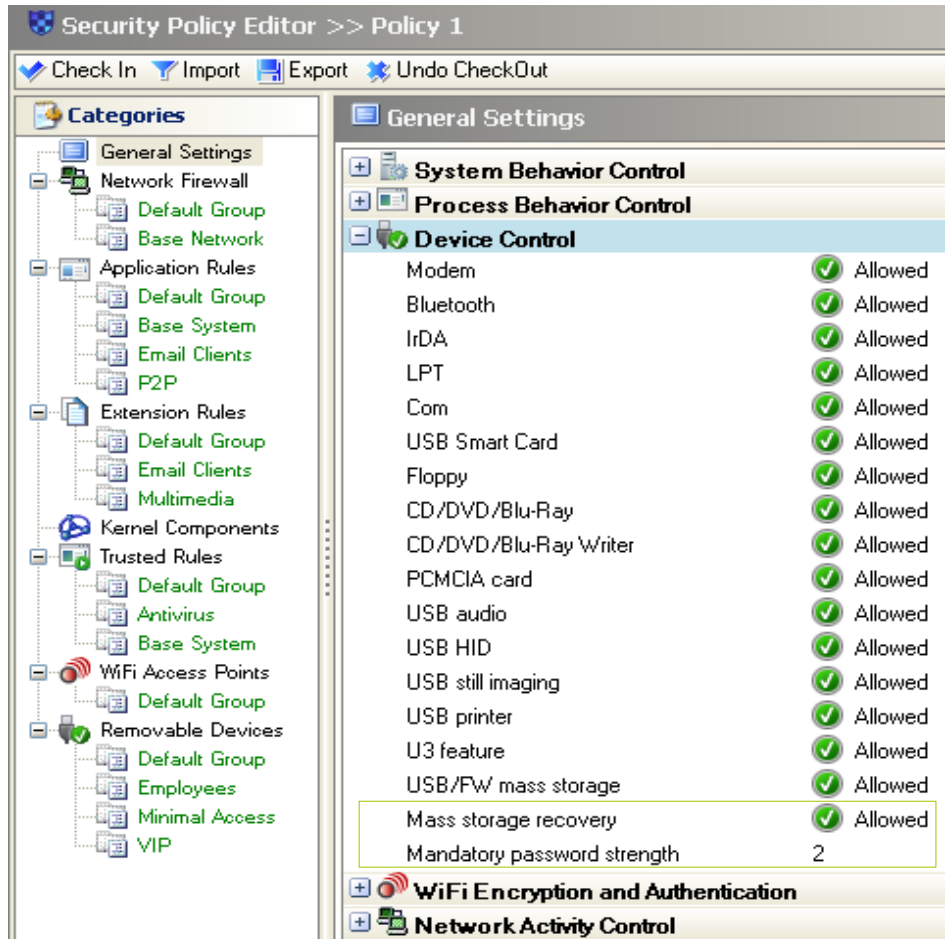
Encryption settings also apply to all devices in the device group.

If **Default** access to the device group is set to **Denied**, the device will not be able to access the workstation on which the agent is installed.

Access will remain denied whatever the encryption policy applied to devices.

General Settings

The device encryption settings under **General Settings > Device Control** are the following:



- **Mass storage recovery**:

  This option allows or denies the user to decrypt the removable device.
- **Mandatory password strength**

  This option defines the password strength used for device encryption.

  The value is set to 2 by default.

CONNECTING A REMOVABLE DEVICE

PASSWORD

The first time a user plugs in a device with an encryption policy, a window:

- Opens.
- Prompts you to enter the new password.
- Prompts you to confirm the password.

If a USB or FireWire device uses an encryption policy, a pop-up window prompts for the password each time the device is plugged in.

The mandatory password strength is set by the administrator in **General Settings > Device Control**.

For more information, see "Passwords", page 370.

SYNCHRONIZING

The first time a device is plugged in after a device encryption policy is applied, it goes through a synchronization process encrypting the entire device.

A progression bar is displayed throughout the process.

During the synchronization process, the user should not leave the computer for a large period of time.
If the computer automatically locks or goes into standby mode after a period of time, the synchronization process will stop. The user will then have to enter the device encryption password to relaunch the process.

Default access control is bypassed. This means that all files on the device will be encrypted even if **Default** access is set to Denied or Read only.

ACCESS TO THE DEVICE WITHOUT PASSWORD

If, when prompted to enter the password, the user clicks **Cancel**, the device is locked to prevent unencrypted data from being written to the device.

In this case, access rights depend on the **Access right if encryption is cancelled** in Removable Devices > Device Control > Group Settings.

Access rights can assume the following values:

- Read (only).
- Read/Write.
- Denied.

> It should be noted that **Default** access and **Exceptions by file extension** settings also apply to the device group.
>
> Therefore, if default access to the device is set to **Denied**, the user cannot access the device.

If the user tries to access an encrypted file without setting the password, information contained in the file will be displayed as encrypted text.

> The Access right if encryption is cancelled option is valid only for this session. Next time the user plugs in the device, the password prompt will be displayed again.

ACCESS TO ENCRYPTED DATA

As long as the correct password is entered, there is no difference to the user between reading encrypted and unencrypted data.

Data is encrypted whenever it is written to a device with encryption enabled. If a file is copied, created or modified on the device, its data is encrypted.

BEHAVIOR WHEN MODIFYING THE ENCRYPTION POLICY

When the encryption policy changes, this change does not take effect until the next time the device is plugged in.

The next time the device is plugged in:

- he new files will be encrypted.
- The encrypted device will remain encrypted.

  In this case, the user must manually decrypt the device which will then remain unencrypted in accordance with the new encryption policy.

USING ENCRYPTED DEVICES ON OTHER COMPUTERS

Sharing encrypted files

Encrypted files on a device can be shared on condition that:

- The device is plugged into another computer running a StormShield agent.
- The encryption policy on the computer includes **Read** or **Read/Write** access.
- The user knows the encrypted device password.

Systems not running StormShield

If an encrypted device is plugged into a computer that is not running a StormShield agent:

- Encrypted files can be opened but their content will be displayed as encrypted text.
  If the device contains an unencrypted partition with files, these files can be used as normal.
- New files can be added onto the device. They will not be encrypted though.
- Files can be copied from the device but they will remain encrypted.
- If the SURT encryption tool is enabled in the device Group Settings of the security policy, the user can encrypt and decrypt files simply by dragging anddropping files to the SURT icon .

  This standalone encryption tool can also be downloaded from SkyRecon Systems website.

  For more information, see "SURT", page 509.

Other systems running StormShield

If an encrypted device is plugged into a computer that is running a StormShield agent:

- The encrypted device will be unaffected by the computer encryption policy.
- The user will need to enter the encrypted device password in order to access the files.
- The computer audit and access policies will be applied to the device.

REMOVING SD CARDS

When removing an SD card from the reader, `odin` (removable device control driver) is not notified.

If you remove an SD card from the reader, the system will not detect the action and the card volume label will still be displayed in Windows Explorer.

As a consequence, if you install a new SD card, StormShield will not prompt you to enter any password. Instead StormShield will use the password of the previous SD card. The user will not be able to access existing files because the key used to decrypt them is not correct and new files will be encrypted with the wrong key.

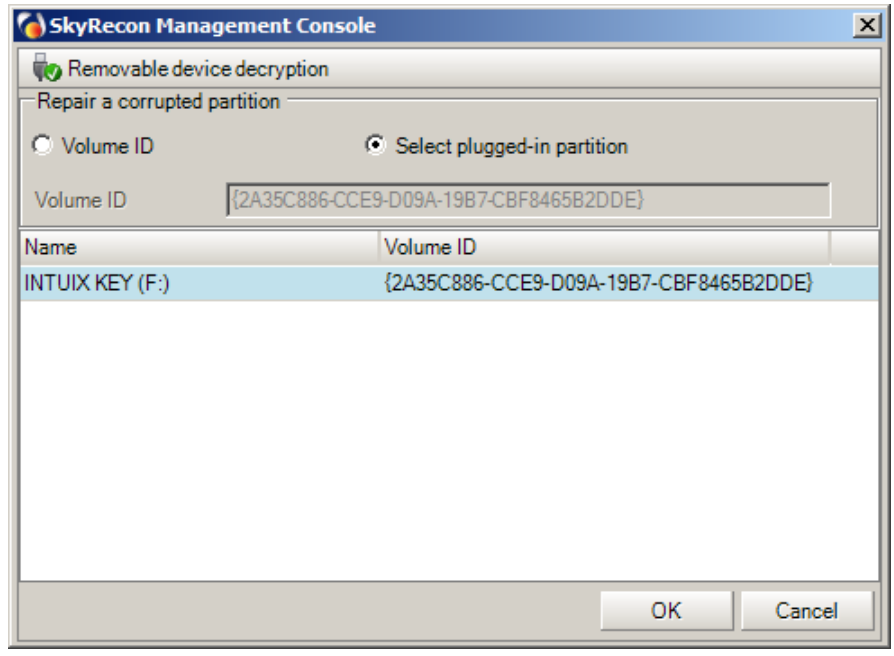
Before removing an SD card, it is imperative to use the eject function in Windows (right-click the reader and click **Eject**).

DECRYPTING A REMOVABLE DEVICE

ADMINISTRATOR SIDE

To decrypt a removable device, the administrator must follow the steps below:

1. Connect the removable device to the computer where the SkyRecon management console is installed.
2. Click the **Encryption** menu.
3. Select **Decrypt Removable Devices**.
4. Enter the console certificate password.
5. Select a device from the list.



6. Click **OK**.

AGENT SIDE

Any StormShield agent user can decrypt a device on condition that **General Settings > Device Control > Mass storage recovery** is set to Allowed in the security policy.

During the decryption process, the user should not leave the computer for a large period of time even if the device has a large disk space.
If the computer automatically locks or goes into standby mode after a period of time, the synchronization process will stop.

The user will then have to enter the device encryption password to relaunch the process.

To decrypt a removable device, the user must follow the steps below:

1. Right-click the StormShield Monitor icon to display the menu below:

2. Click **Removable device** and **Decrypt a removable device**.
   The Decrypt protected data window is displayed.

3. Select the device from the list.
4. Enter the device encryption password.

5. Click **OK**.

PASSWORDS

If a user forgets the encryption password, a new one can be provided by the administrator.

The procedure requires action by both the user and the administrator.

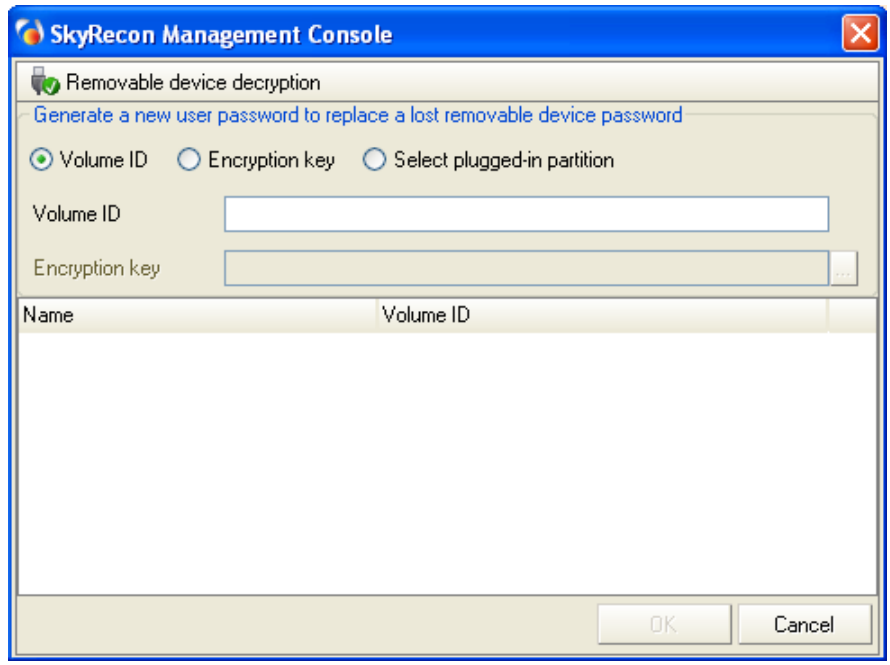
ADMINISTRATOR SIDE

Replacing a lost password

To replace a lost password, the administrator must perform the steps below:

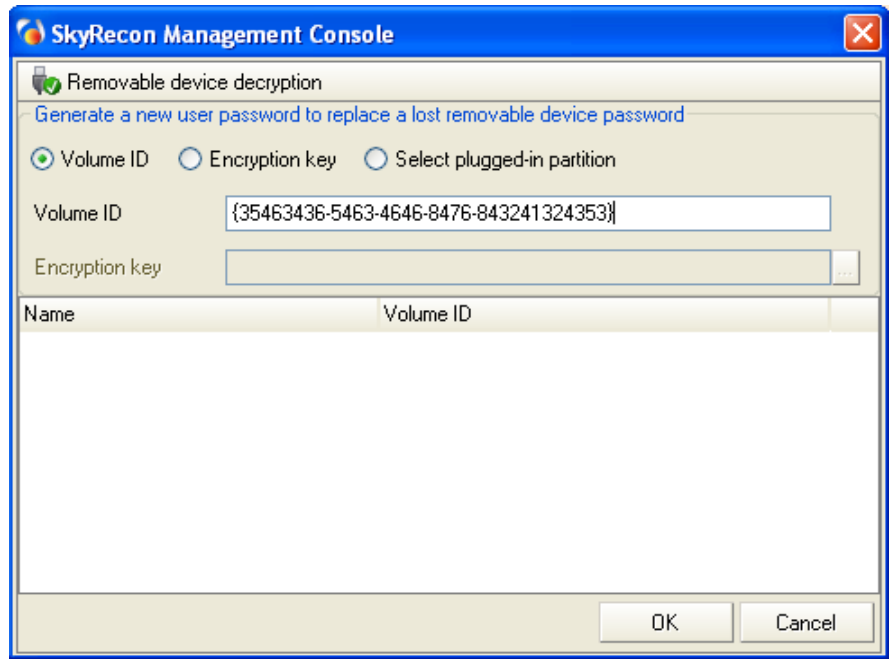
1. Click **Encryption > Generate New Removable Device Password**.
2. Enter the console certificate password.

3. Select how to generate a new password:

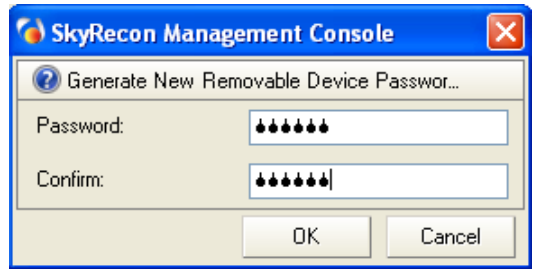


- By **Volume ID**:
  - Click the **Volume ID** radio button.
  - Enter the volume ID sent by the user and click **OK**.

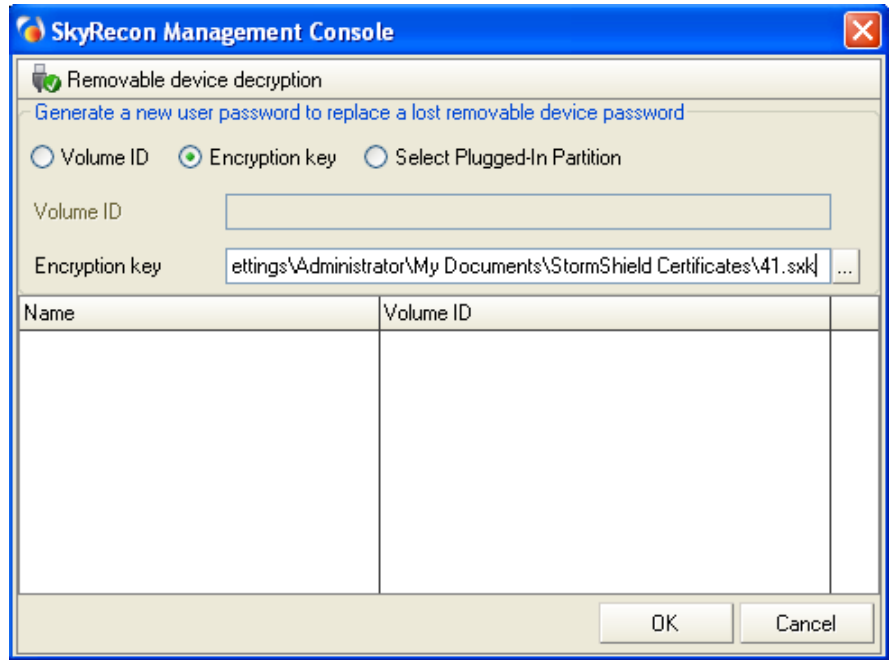
    The **OK** button will be activated as soon as the volume ID is recognized.



- Enter the new password.
- Confirm the password.
- Click **OK**.

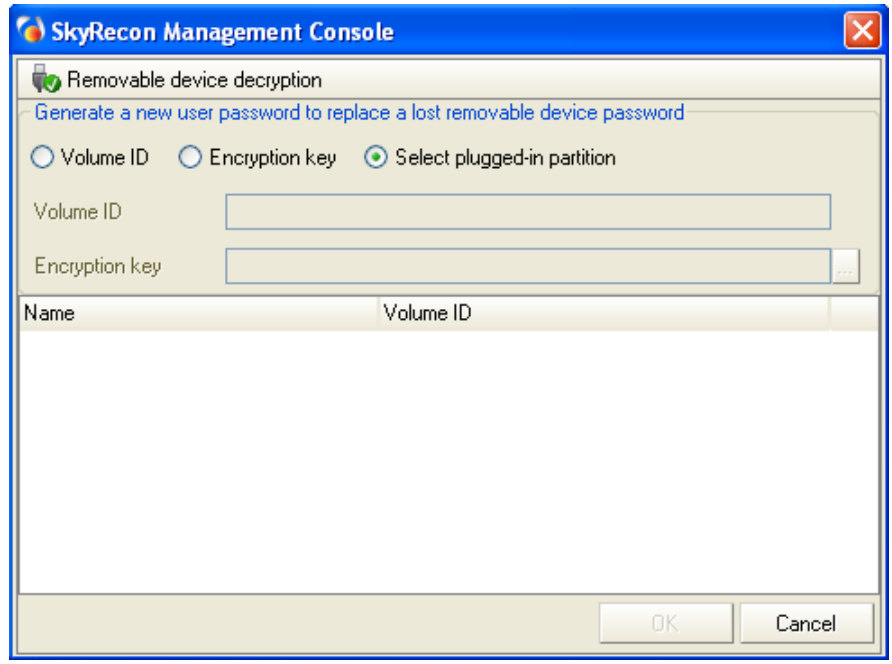


- By **encryption key**:
  - Click the **Encryption key** radio button.
  - Select the encryption key file from your system by clicking the Browse button ... .



  - Click **OK**.
  - Enter the new password.
  - Confirm the password.
  - Click **OK**.

- By **Select plugged-in partition**:
  - Click the **Select plugged-in partition** radio button.
  - Select the removable device partition.



  - Enter the new password.
  - Confirm the password.
  - Click **OK**.

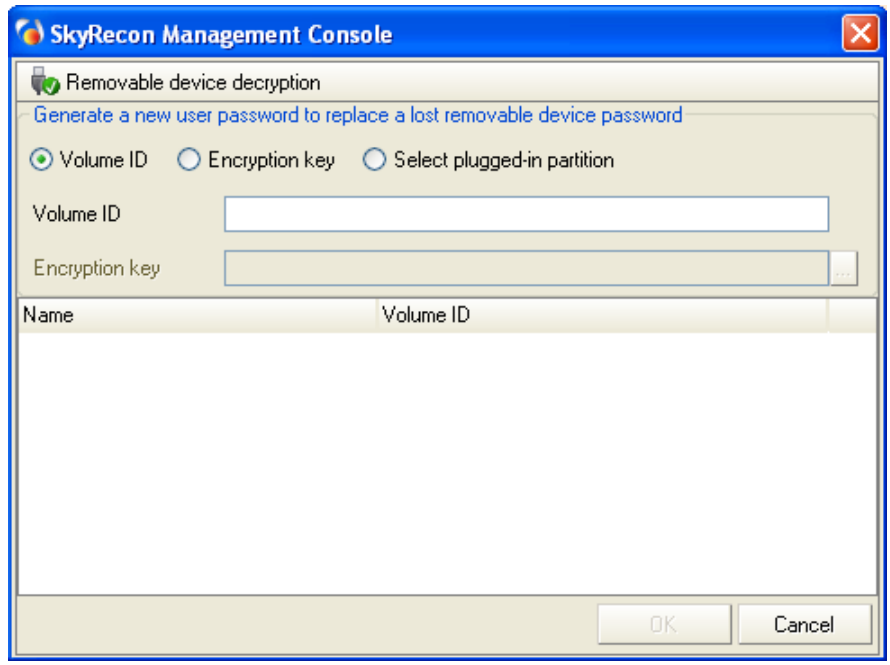
If the action selected fails to generate the key, try another option.

Exporting an encryption key

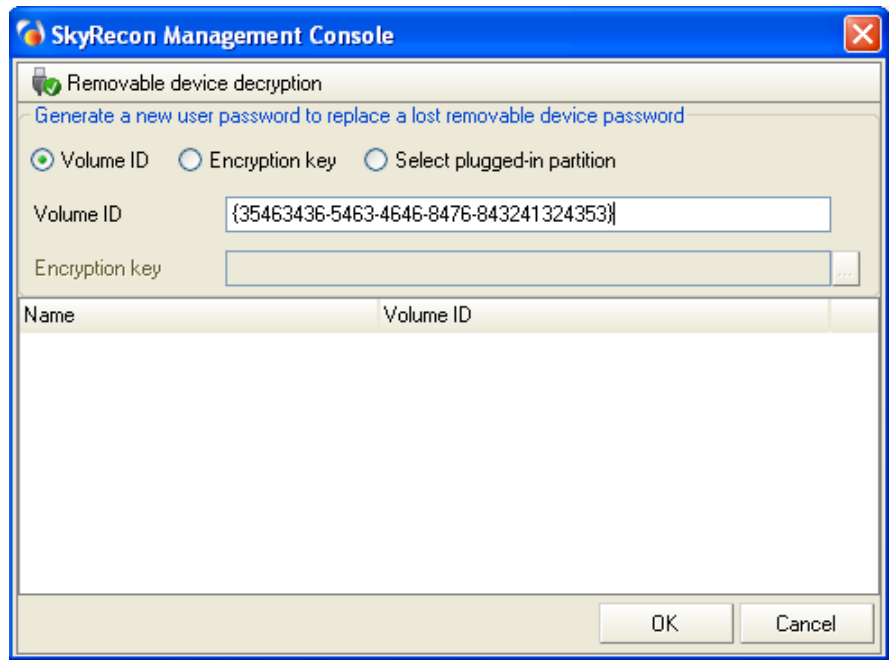
After generating a new password for the user, the administrator will export the encryption key. To do so, he must follow the steps below:

1. Click **Encryption > Generate New Removable Device Password**.
2. Enter the console certificate password.

3. Select how to generate a new password:

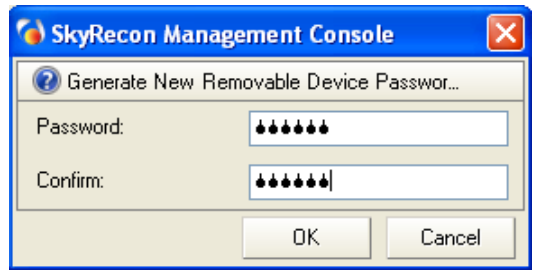


- By **Volume ID**:
  - Click the **Volume ID** radio button.
  - Enter the volume ID sent by the user and click **OK**.
    The **OK** button will be activated as soon as the volume ID is recognized.

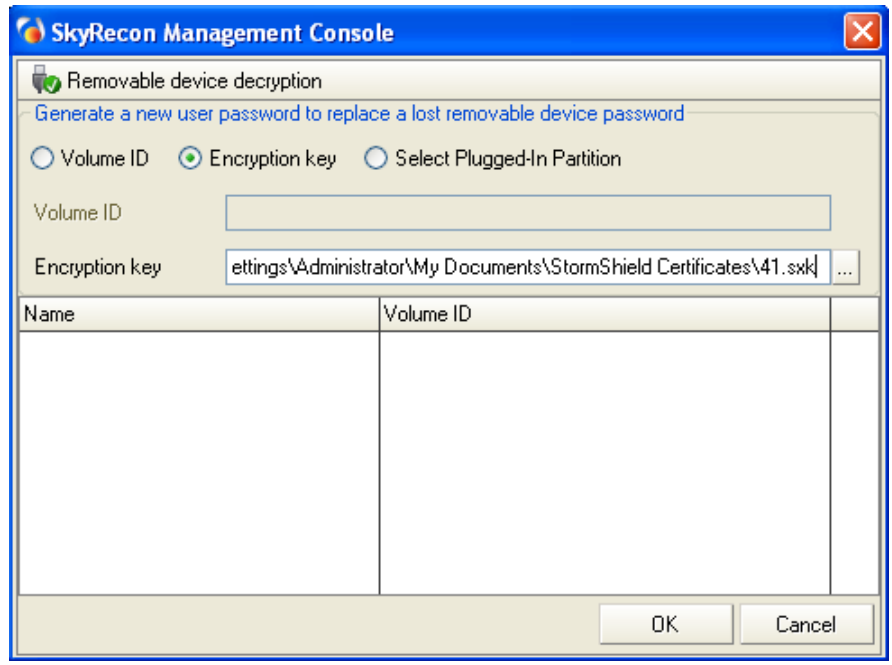


  - Enter the new password.
  - Confirm the password.

- Click **OK**.

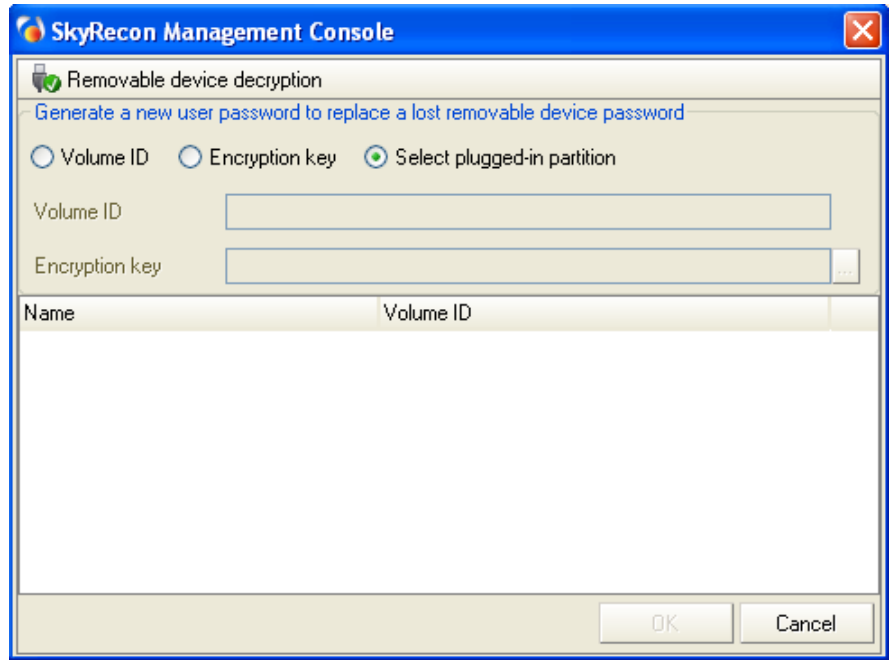


- By **encryption key**:
  - Click the **Encryption key** radio button.
  - Select the encryption key file from your system by clicking the Browse button ... .



  - Click **OK**.
  - Enter the new password.
  - Confirm the password.
  - Click **OK**.

- By **Select plugged-in partition**:
  - Click the **Select plugged-in partition** radio button.
  - Select the removable device partition.



  - Enter the new password.
  - Confirm the password.
  - Click **OK**.

  If you choose this option, the encryption key file `ExportKey.sxk` will be directly exported to the connected device.

4. After entering the new encryption key password, save the `ExportKey.sxk` file.
5. Notify the user of the new key location. The user can then import the new key.

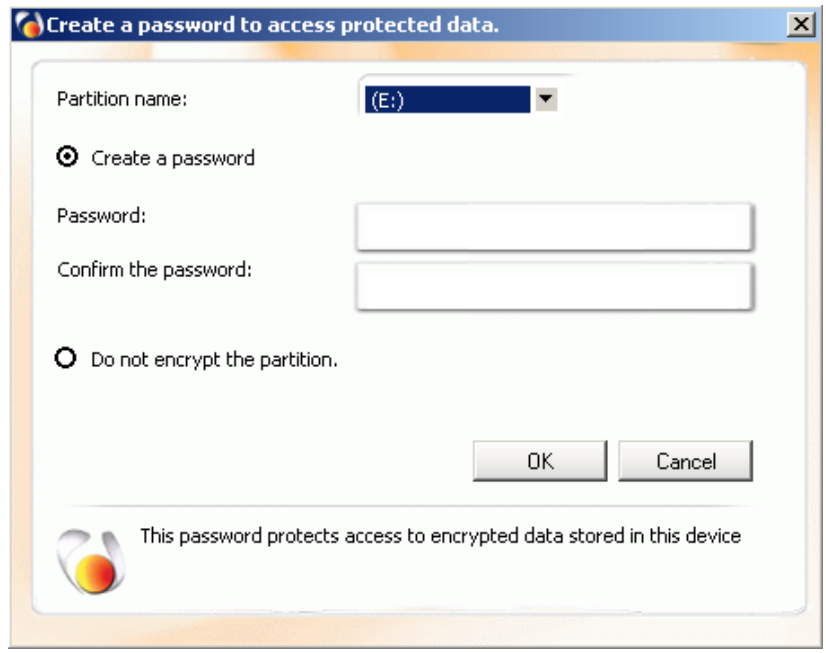
AGENT SIDE

Creating a password

To create a password, the user must follow the steps below:

1. Right-click the StormShield Monitor icon and click **Removable device > Create a password**.

A window is displayed that prompts you to create your password to access protected data.



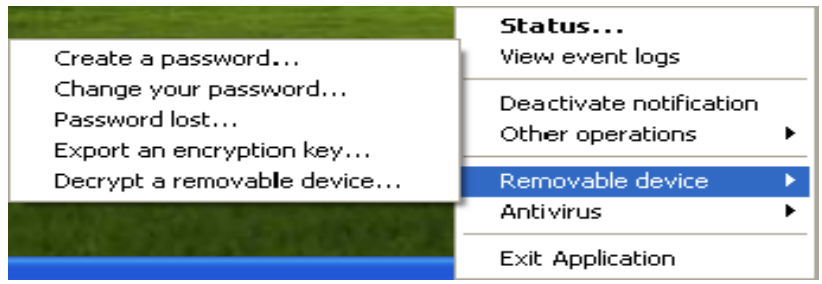
2. Select the volume from the list.
3. Enter the required information.
4. Click **OK**.

Changing a password

Users can change their own password by clicking in the StormShield Monitor menu.

The user must follow the steps below:

1. Right-click the StormShield Monitor icon and click **Removable device > Change your password**.



   A window is displayed that prompts you to change your password to access protected data.

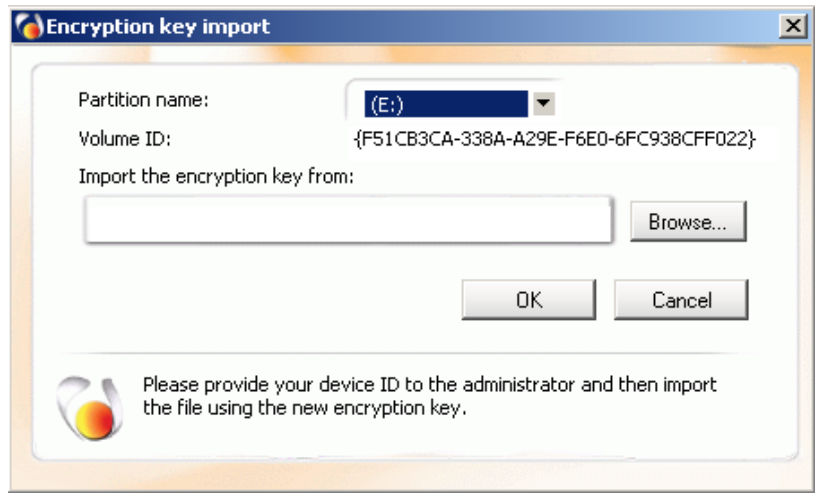
2. Select the volume from the list.
3. Enter the required information.
4. Click **OK**.

Lost password

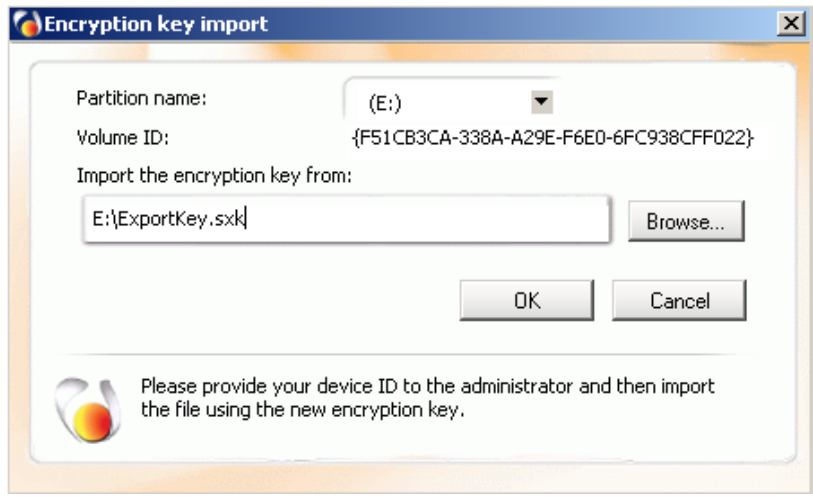
To obtain a new password from the administrator, users must follow the steps below:

1. With the device plugged in, right-click the StormShield Monitor icon and click Removable device.
2. Click **Password lost**.

A partition name and volume ID (key ID) are displayed.



3. Send the volume ID to the administrator (by email or by copying it to a server, etc.).
4. If the administrator sends you the encryption key, you must import it:
   - Click **Import the encryption key from** field.
   - Enter the path and filename (or click the **Browse** button to locate the encryption key).
   - Click **OK** to import the replacement file.



Exporting an encryption key

StormShield agent users can export a **copy** of the encryption key for backup purposes. Exporting an encryption key can be useful when there is no network access.

To export an encryption key, the user must follow the steps below:

1. With the device plugged in, right-click the StormShield Monitor icon and click Removable device.
2. Click **Export an encryption key**

The encryption key export window is displayed.

3. Click **Export the encryption key to** field.
4. Enter the path and filename (or click the Browse button ... to locate the encryption key).

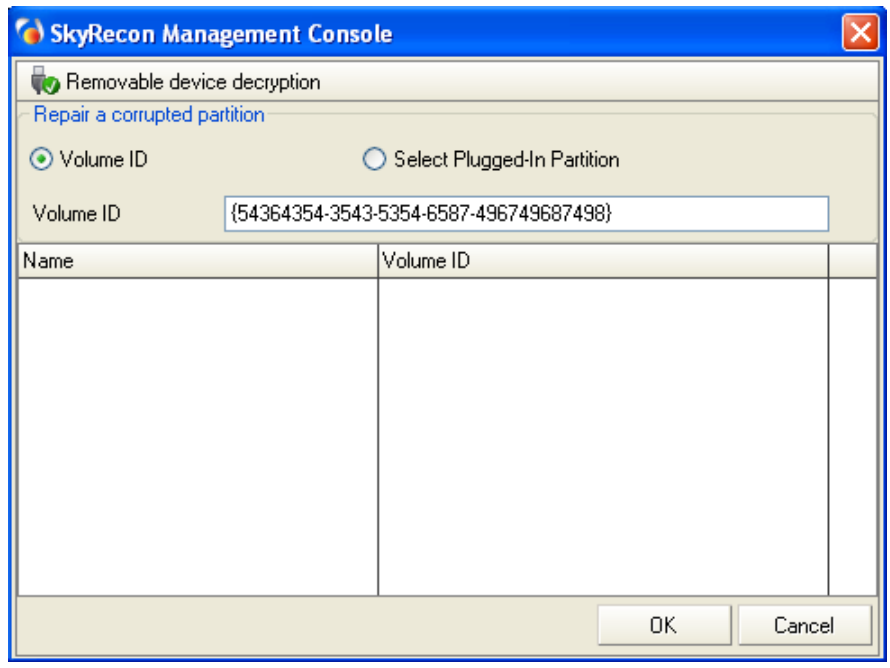
5. Click **OK** to export the file.

REPAIRING A CORRUPTED ENCRYPTION KEY

To repair a corrupted encryption key, the administrator must follow the steps below:

1. Select **Encryption > Repair Removable Device Encryption Key**.

2. Select how to repair the encryption key.

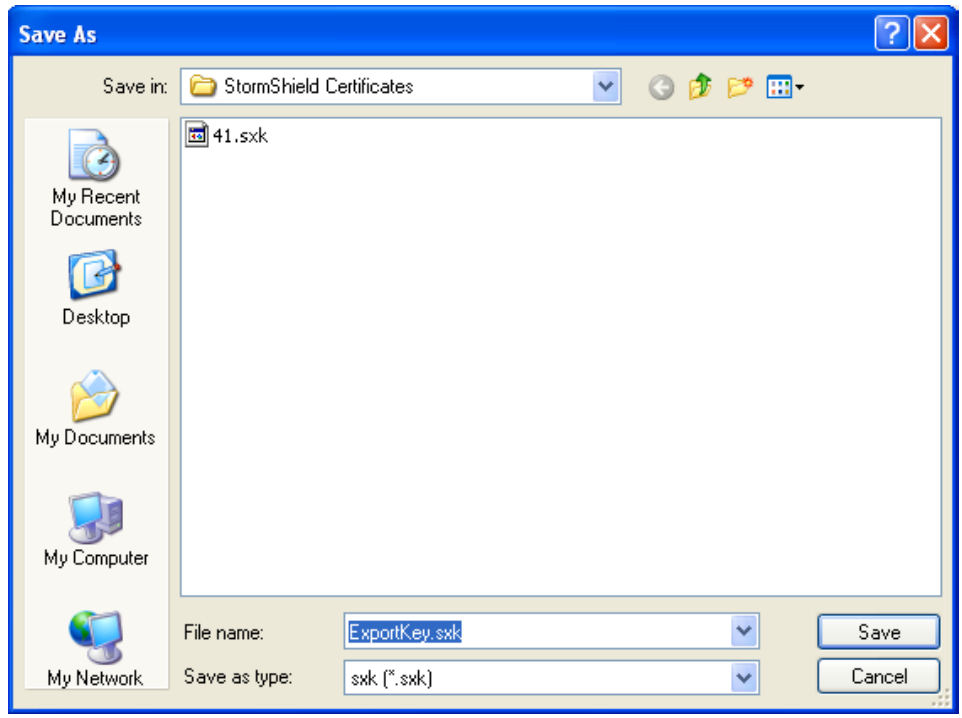


   - If you choose **Volume ID**, enter the volume ID in the text field.
   - If you choose **Select Plugged-In Partition**, select the appropriate volume.

3. Click **OK**.

   The **OK** button will be activated only if the volume ID is correct or if the removable device is detected.

4. Save your new encryption key.



Chapter 12

SCRIPTS

ABOUT THIS CHAPTER

This chapter describes StormShield's **Scripts** feature and how to create and implement your own scripts.

It includes the following:

- Overview:
  - Scripts feature.
  - Script types:
    - Test scripts.
    - Action scripts.
    - Batch scripts.

- Script Editor.

- Test scripts:
  - Overview.
  - Statements.
  - Built-in tests.
  - User-defined tests.
  - Creating a test script.

- Action scripts:
  - Overview.
  - Built-in actions.
  - User-defined actions.
  - Creating an action script.
- Batch scripts:
  - Overview.
  - TRUE/FALSE results.
  - Creating a batch script.
- Temporary action scripts.
- Uploading files from the master server.

OVERVIEW

SCRIPTS FEATURE

StormShield can be used to create scripts that control the automatic and autonomous reconfiguration of StormShield agents.

The use of scripts enables the administrator to define conditions for applying policies and configurations based on:

- The status of the workstation.
- The connection used.
- The identity of the user.

Dynamic Policy Enforcement makes it possible to modify security policies in real time and enforce workstation conformity.
The latter is highly important before allowing user workstation access to the corporate network.

SCRIPT TYPES

There are three script types:

1. Test scripts.
2. Action scripts.
3. Batch scripts.

Script types are detailed hereafter.

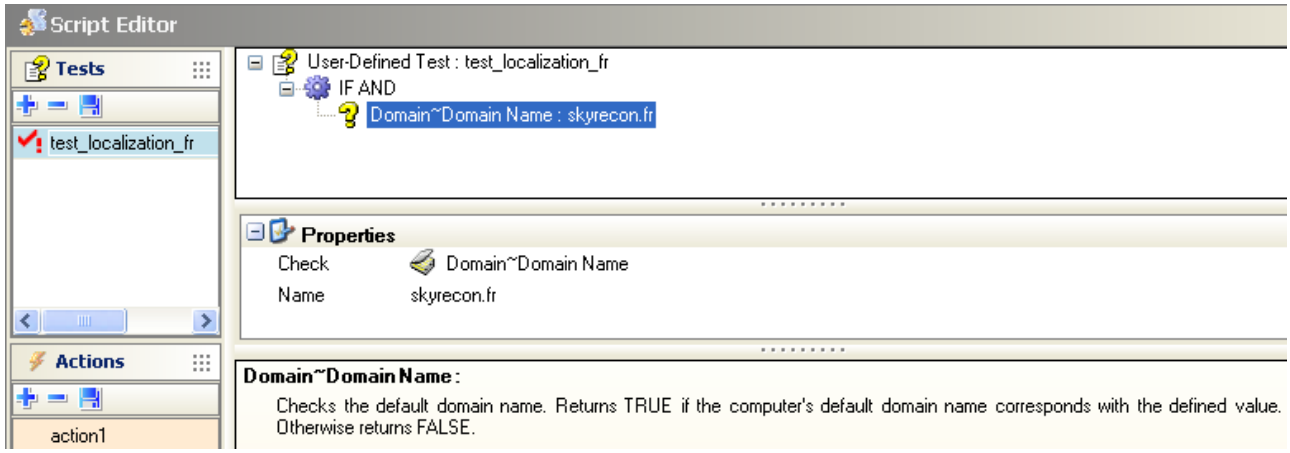
Test scripts

Test scripts may include the following:

- Built-in tests (predefined).
- User-defined tests.
- Boolean logic operators.

The test script icon is .

Here is an example of test script including a user-defined test based on a domain name:



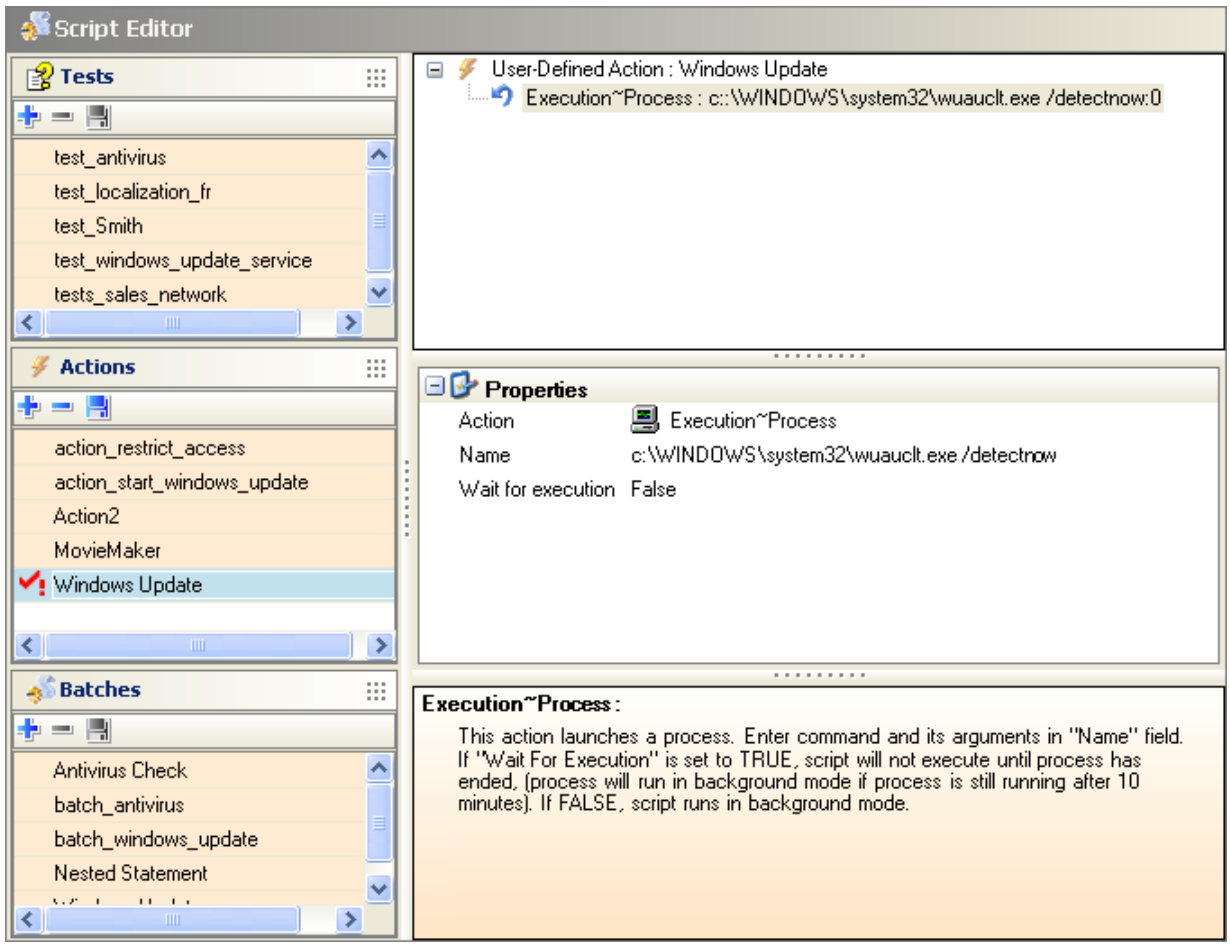
Action scripts

Action scripts may include the following:

- Built-in actions.
- User-defined actions.

The action script icon is .

Here is an example of action script including a user-defined action:



Batch scripts

Batch scripts may include the following:

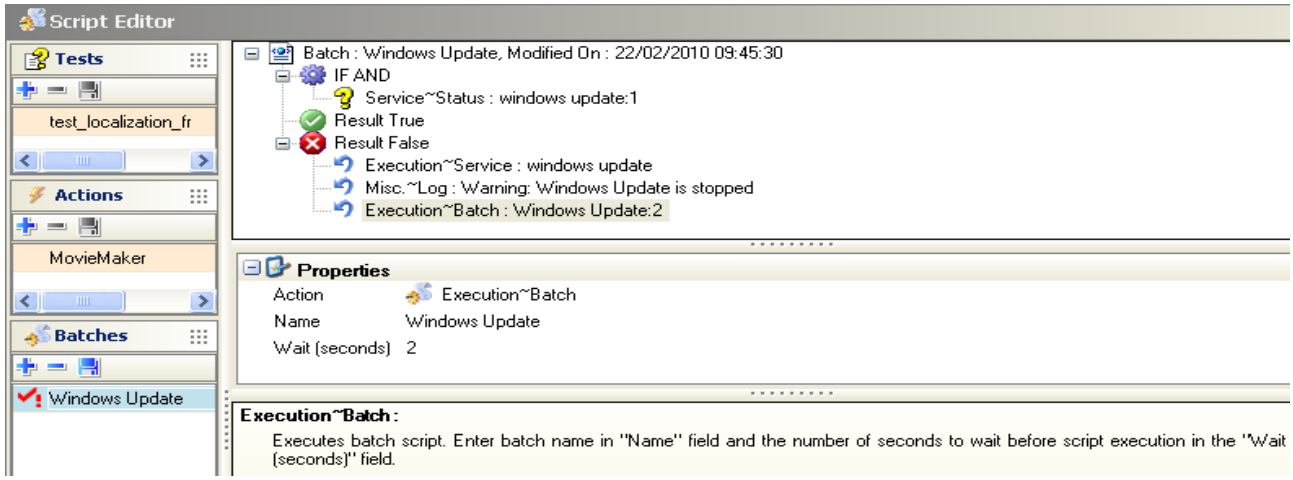
- Test scripts.
- Action scripts.
- Boolean logic operators.
- Results.

The batch script icon is .

The TRUE result icon is .

The FALSE result icon is .

Here is an example of batch script based on the verification of the execution of Windows Update service. If the service is not active, it will be relaunched:



You will find in this chapter, a section called "Temporary action scripts", page 427.

Temporary action scripts do not belong to the standard script category. These scripts fulfill a specific function upon user's request that is to run:

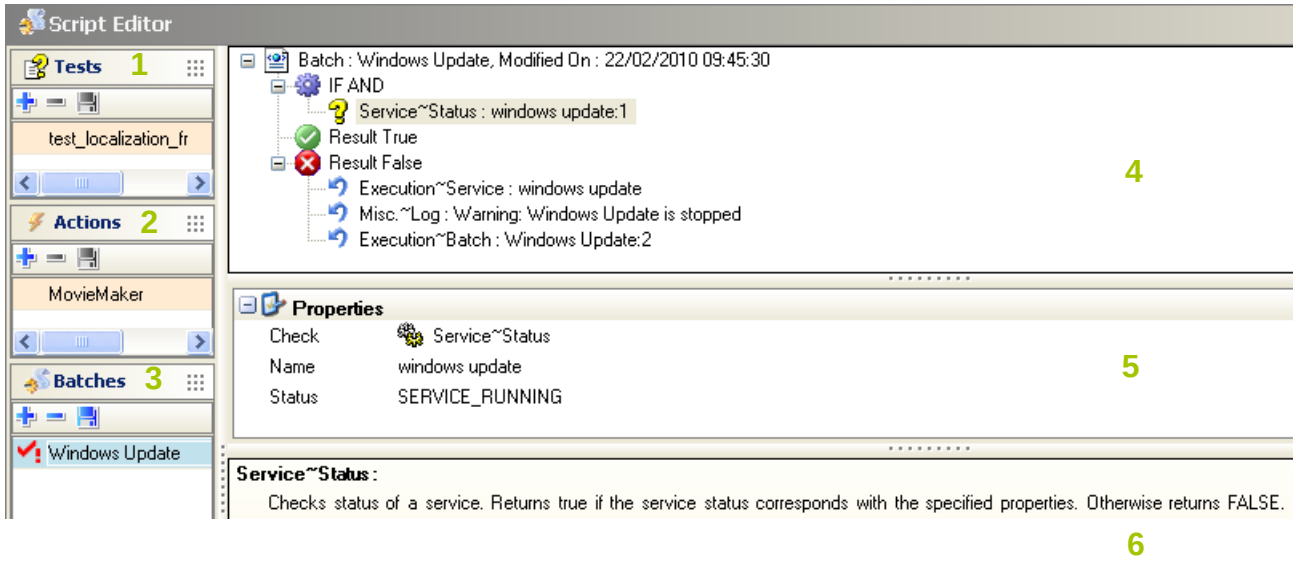
- Rest scripts,
- Action scripts,
- Batch scripts,

on the StormShield agents on a temporary basis.

These scripts are configured on the SkyRecon management console.

SCRIPT EDITOR

The **Script Editor** panel is where you build your scripts.



1. **Tests**:
   This area displays available tests.
   You can add tests by:
   - Right-clicking on this area and selecting **Add** from the drop-down menu.
   - Clicking directly .

   You can also check out existing tests.
   For more information, see "Test scripts", page 393.
2. **Actions**:
   This area displays available actions.
   You can add actions to the list.
   You can also check out existing actions.
   For more information, see "Action scripts", page 407.
3. **Batches**:
   This area displays available batches.
   You can add batches to the list.
   You can also check out existing batches.
   For more information, see "Batch scripts", page 416.

4. **Work area**:

   This area displays the contents of the selected script. This is where you actually build or edit your scripts.

5. **Properties**:

   This area displays the properties associated with a test or an action.

   You can double-click the field next to the property to change it.

6. **Message area**:

   This area displays a description of the selected test or action.

When creating or modifying scripts, you can move items (examples: statements, built-in tests or user tests) by a simple drag-and drop.

For more information, see:

- "Test scripts", page 393.
- "Action scripts", page 407.
- "Batch scripts", page 416.

TEST SCRIPTS

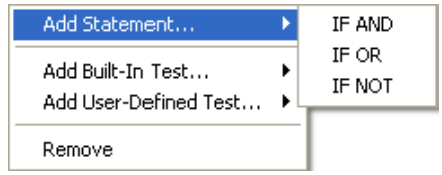
OVERVIEW

The test script components are the following:

- **Statements**:
  Boolean logic operators (Example: IF AND).
- **Built-in tests**:
  Predefined tests (Example: used to check the execution of a process).
- **User-defined tests**:
  Tests that you or another administrator have previously created.

STATEMENTS

Statements use the Boolean logic operators IF AND, IF OR and IF NOT.



Statement definitions

Statements return **TRUE** or **FALSE** values depending on the statement and the test results.

STATEMENT	RETURNS...
IF AND	• TRUE if all tests return TRUE. • FALSE if any test returns FALSE.
IF OR	• TRUE if at least one test returns TRUE. • FALSE if all tests return FALSE.
IF NOT	• TRUE if all tests return FALSE. • FALSE if any test returns TRUE.

Table 12.5: Statement definitions

Example of tests using logic operators

Following is an example of the components that make up a simple test:

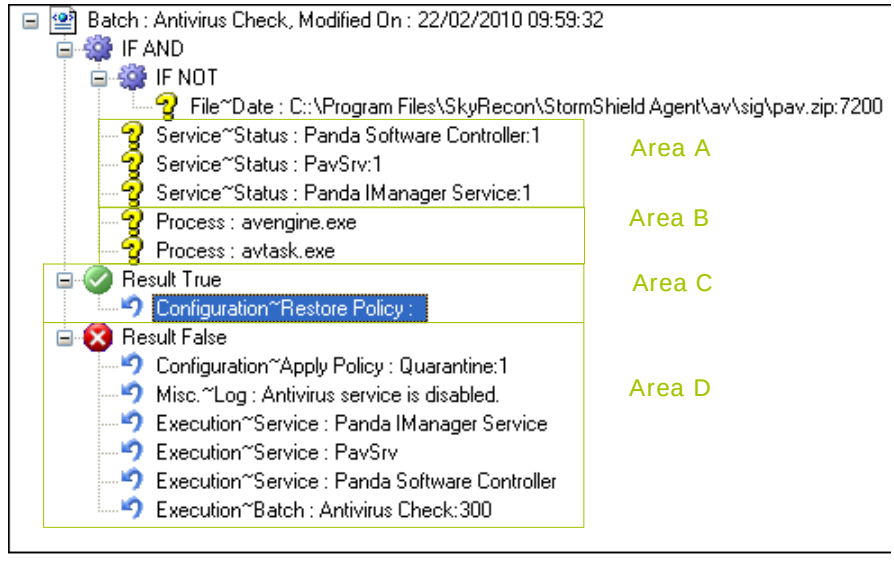
```
IF NOT
   \
  IF AND
     \
    mytest1
      |
     mytest2
```

- If **mytest1** and **mytest2** both return **TRUE**:
  - Statement IF AND returns TRUE.
  - Statement IF NOT returns FALSE.
- If **mytest1** returns **TRUE** and **mytest2** returns **FALSE**:
  - Statement IF AND returns FALSE.
  - Statement IF NOT returns TRUE.

Nested statements

You can nest statements to form more powerful and complex tests.

Here is an example of batch test including nested statements:



The purpose of this example is to test if the antivirus service is running on the workstation.

The agent will check if:

- The three services have been launched (Area A).
- The two executable files are present on the workstation (Area B).

If the test returns **TRUE**, the agent will restore the previous permanent policy on the workstation (Area C).

If the test returns **FALSE** (Area D):

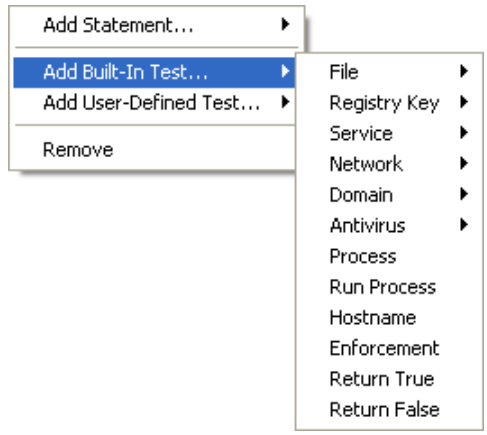
- A quarantine policy will be applied temporarily to prevent any risk as long as the antivirus service is disabled.
- A log will be sent indicating that the antivirus service is disabled.
- The three services will be relaunched.
- The batch will be reloaded after 300 seconds.

BUILT-IN TESTS

A built-in test is a predefined test that you can use in your script.

First level

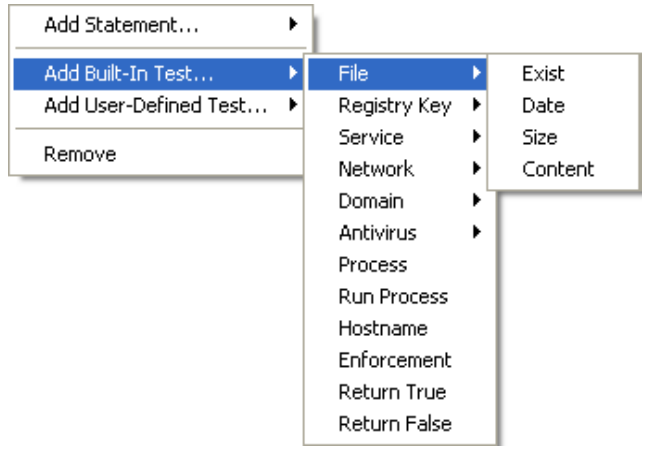
Here is the first-level list of built-in tests available in StormShield:



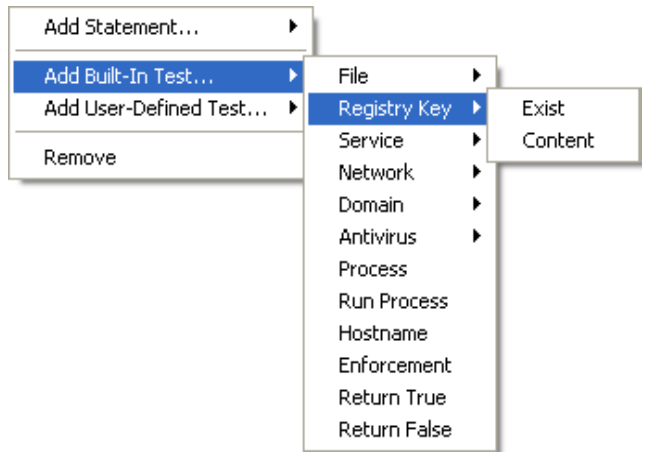
Second level

Here is the second-level list of built-in tests available in StormShield:

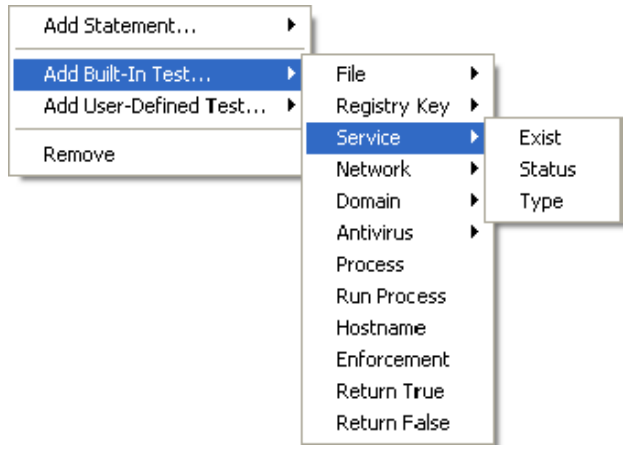
- Under **File**, you will find the following built-in tests:



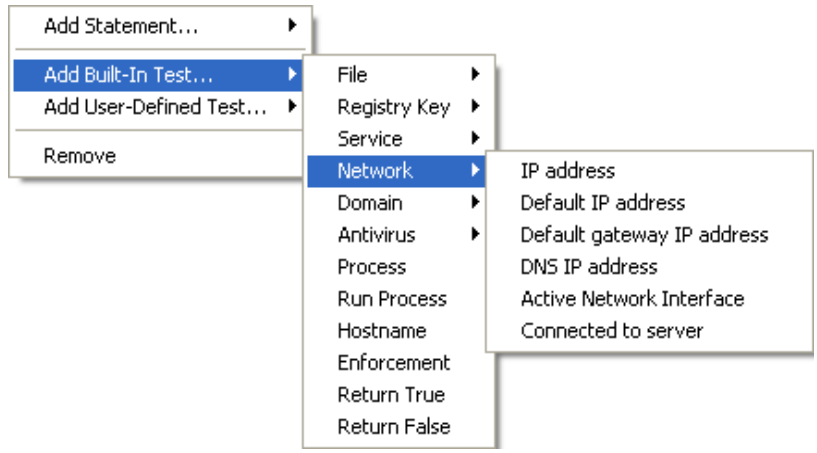
- Under **Registry Key**, you will find the following built-in tests:



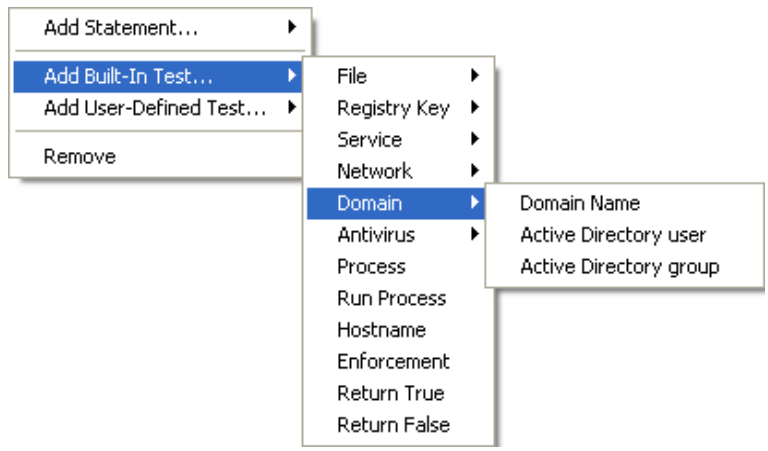
- Under **Service**, you will find the following built-in tests:



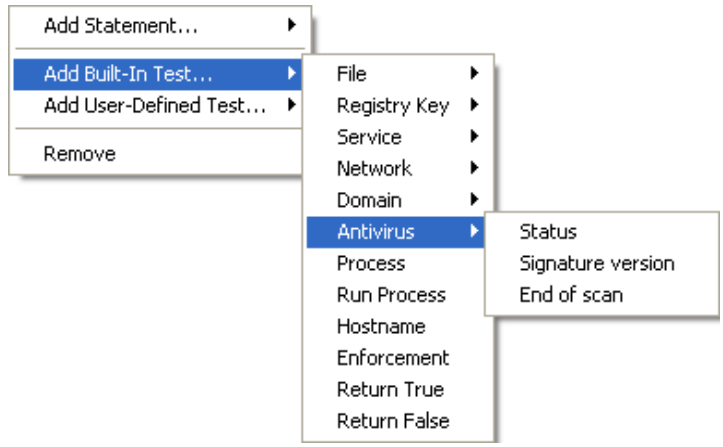
- Under **Network**, you will find the following built-in tests:



- Under **Domain**, you will find the following built-in tests



- Under **Antivirus**, you will find the following built-in tests:



Definition of built-in tests

A built-in test performs commonly used tests that you can run as part of your own scripts.

TEST	DESCRIPTION	PROPERTIES
File > Exist	Checks for named file on agent system. Returns **TRUE** if named file exists. Otherwise, returns **FALSE**.	Enter filename and path: ◦ `Name: c:\programs\acme software\acme software update.exe`
File > Date	Checks the modification date of the named file on agent system to determine its age. Returns **FALSE**: ◦ either if modification date and specified age are greater than or equal to the current date, ◦ or if named file does not exist. Otherwise, returns **TRUE**.	Enter filename and path: ◦ `Name: c:\Programs\antivirus\update.exe` Enter the duration that will be added to the file modification date to define the time basis for the test: ◦ `Time (sec.): 120`
File > Size	Checks the size of a specific named file on agent system. Returns **FALSE**: ◦ either if the file size is different from the size specified, ◦ or if named file does not exist. Otherwise, returns **TRUE**.	Enter filename and path: ◦ `Name: c:\test\file.png` Specify the size of the filename in bytes: ◦ `Size (bytes): 20`

Table 12.6: Built-in test definitions (Sheet 1 of 5)

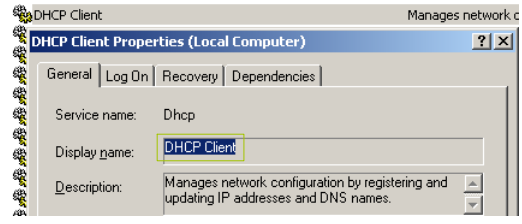
TEST	DESCRIPTION	PROPERTIES
File > Content	Checks the content of the named file. Returns **TRUE** if file contains the character string specified. Returns **FALSE**: ◦ either if the named file does not exist, ◦ or if the character string is not found, ◦ or if the file size exceeds 5 MB.	Enter filename and path: ◦ `Name: c:\test\file.txt` Define the character string to be searched: ◦ `Content: antivirus test log`
Registry Key > Exist	Checks for registry key in registry database. Returns **TRUE** if the registry key exists. Otherwise, returns **FALSE**.	Choose registry path: ◦ `Root: HKEY_LOCAL_MACHINE` Enter the registry key path: ◦ `Path: Software\Microsoft Office 11.0`
Registry Key > Content	Checks the content of the named registry key in the registry database. Returns **TRUE** if the key contains the character string specified. Otherwise, returns **FALSE**.	Enter registry path: ◦ `Root Key: HKEY_CLASSES_ROOT` ◦ `Key: SYSTEM\CurrentControlSet\Services\TCPip\Parameters` ◦ `Name: [Hostname]` ◦ `Content type: REG_DWORD` ◦ `Content: COMPUTER1`
Service > Exist	Checks for a service. Returns **TRUE** if the service exists. Otherwise, returns **FALSE**.	Follow the steps below: ◦ Enter `services.msc` in **Start > Run** or in a command prompt. ◦ Select the appropriate service. ◦ Right-click the service. ◦ Click **Properties** to view the service name and its writing conventions (uppercase/lowercase). ◦ Conform to writing conventions when entering the service name in the built-in test (see frame):  - `Name: Dhcp`

Table 12.6: Built-in test definitions (Sheet 2 of 5)

TEST	DESCRIPTION	PROPERTIES
Service > Status	Checks the service status. Returns **TRUE** if the service status matches specified properties. Otherwise, returns **FALSE**.	Enter service status: ◦ `Name: Dhcp` Define the service status: ◦ `Status: SERVICE_RUNNING`
Service > Type	Checks the service type. Returns **TRUE** if service type matches specified properties. Otherwise, returns **FALSE**.	Enter service name: ◦ `Name: Dhcp` Enter service type: ◦ `Type: SERVICE_AUTO_START`
Network > IP address	Checks the IP address of the host specified. Returns **TRUE** if the IP address is that configured on the host. Otherwise, returns **FALSE**.	Enter the IP address and subnet mask: ◦ `IP/Netmask: 172.16.36.21/32`
Network > Default IP address	Checks the default IP address. Returns **TRUE** if the IP address is that configured on the host. Otherwise, returns **FALSE**.	Enter the IP address and subnet mask: ◦ `IP/Netmask: 172.16.36.21/32`
Network > Default gateway IP address	Checks the default gateway IP address. Returns **TRUE** if the IP address is that configured on the host. Otherwise, returns **FALSE**.	Enter the IP address and subnet mask: ◦ `IP/Netmask: 172.16.36.254/32`
Network > DNS IP address	Checks the main DNS server IP address that is configured on the host. Returns **TRUE** if the IP address matches the main DNS IP address. Otherwise, returns **FALSE**.	Enter the IP address and subnet mask: ◦ `IP/Netmask: 172.16.36.254/32`
Network > Active Network Interface	Checks the network interface specified. Returns **TRUE** if the active network interface matches the one specified. Otherwise, returns **FALSE**.	After clicking in the **Value** field in the Properties area, make a selection from the dialog box to display the list of active network interfaces.
Network > Connected to server	Checks that the agent can connect to the StormShield server.	
Domain > Domain Name	Checks the default domain name. Returns **TRUE** if the domain name on the host matches that of the DNS server. Otherwise, returns **FALSE**.	Enter domain name to be tested: ◦ `Name: domain.com`

Table 12.6: Built-in test definitions (Sheet 3 of 5)

TEST	DESCRIPTION	PROPERTIES
Domain > Active Directory User	Checks the Active Directory user in the current interactive session. Returns **TRUE** if the user logged onto the current interactive session corresponds to the one specified. Otherwise, returns **FALSE**.	Enter user Distinguished Name (DN): ◦ `Name: CN=john, OU=Users,DC=skyrecon,DC=fr` Remark: This built-in test only works in Connected mode.
Domain > Active Directory Group	Checks that a particular user belongs to the Active Directory Group in the current interactive session. The first parameter is the domain name in NETBIOS format. The second parameter is the group name. Returns **TRUE** if the user logged onto the current interactive session belongs to the group specified. Otherwise, returns **FALSE**.	Enter the domain name in NETBIOS format: ◦ `Domain: SKYRECON` Enter the AD group name: ◦ `Name: users` Remark: This built-in test only works in Connected mode.
Antivirus > Status	Checks the antivirus status. Returns **TRUE** if the antivirus is enabled. Otherwise, returns **FALSE**.	Only if you have installed the AVP option.
Antivirus > Signature version	Checks the age of the antivirus signature database. Returns **TRUE** if the age of the antivirus signature database is ≤ number of days specified. Otherwise, returns **FALSE**.	Only if you have installed the AVP option. The antivirus signature database is considered obsolete when it is 3 days old. You may increase this value.
Antivirus > End of scan	Checks that the antivirus scan is over. Returns **TRUE** if the antivirus scan is over. Otherwise, returns **FALSE**.	Only if you have installed the AVP option.
Process	Checks for a running process. Returns **TRUE** if the process is running. Otherwise, returns **FALSE**.	Enter process name: ◦ `Name: update.exe`

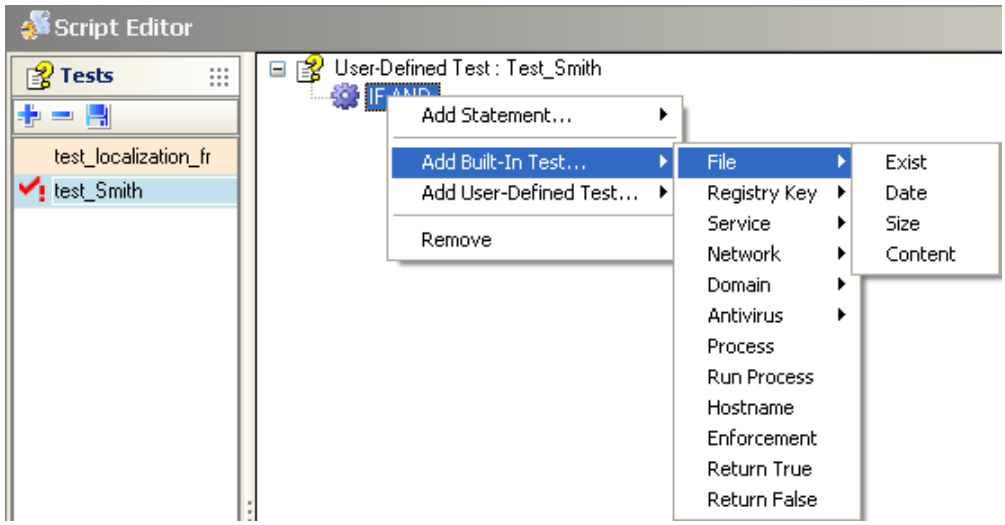
Table 12.6: Built-in test definitions (Sheet 4 of 5)

TEST	DESCRIPTION	PROPERTIES
Run Process	Launches and checks the execution of a process. If **Wait for execution** is set to **TRUE**, the script will wait for the end of process execution before executing another action. If process execution exceeds 10 minutes, the script will be run in parallel. If **Wait for execution** is set to **FALSE**, the script continues in parallel. Returns **TRUE** if process terminates properly. Otherwise, returns **FALSE**.	Enter process name and path: ◦ `Name: c:\program files\antivirus\update.exe` Enable/Disable **Wait for execution**: ◦ `Wait for execution: False`
Hostname	Checks the hostname. Returns **TRUE** if hostnames correspond. Otherwise, returns **FALSE**.	Enter hostname: ◦ `Name: Computer1`
Network Enforcement	Assigns a value to the "Network Enforcement" variable. Can be used by TNC clients (Trusted Network Connect) such as Odyssey Access Clients on Juniper Networks (R).	Set Network Enforcement status to either of the following options: • Allow, • Isolate, • No access, • No recommendation.
	For more information on Juniper's UAC, see How to install Juniper's "Unified Access Control" module?	
Return True	Always returns **TRUE**.	
Return False	Always returns **FALSE**.	

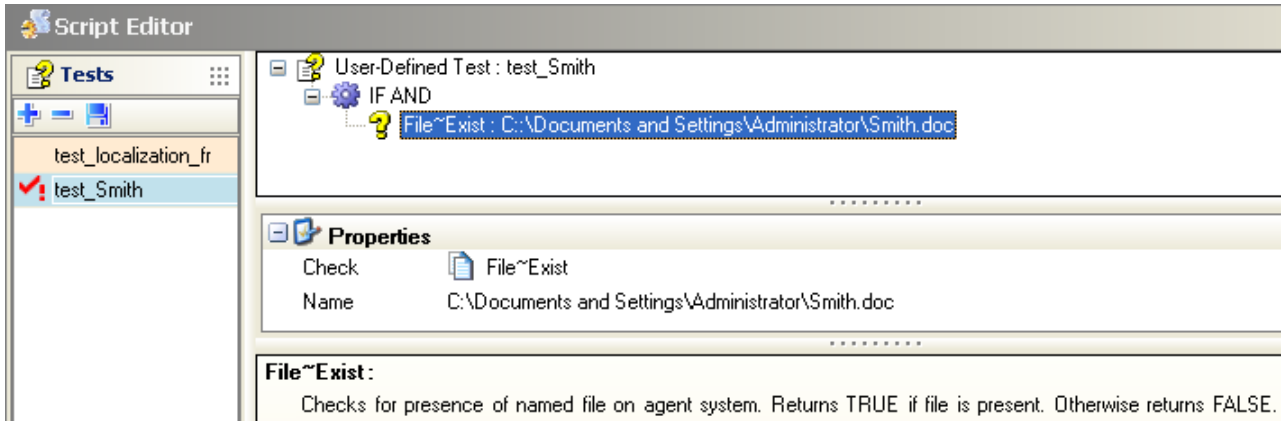
Table 12.6: Built-in test definitions (Sheet 5 of 5)

Example of built-in tests

Here is an example of built-in test (**File>Exist**) that is designed to check for the `Smith.doc` file on the agent workstation:



You can also specify the file pathname. If the file exists, the test returns TRUE.



USER-DEFINED TESTS

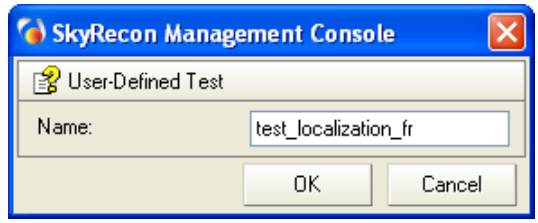
A user-defined test is a test that you or another administrator have created. You can include user-defined tests in your scripts.

CREATING A TEST SCRIPT

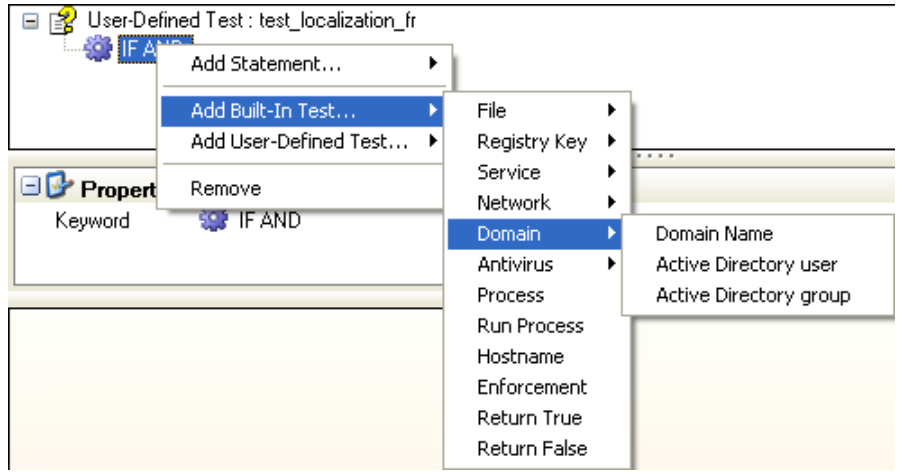
To create a test script, follow the steps below:

1. In the **Tests** area in the Script Editor:
   - Right-click in the area.
   - Select **Add** from the dropdown menu or just click the + icon on the toolbar.

   - Name the user-defined test script.

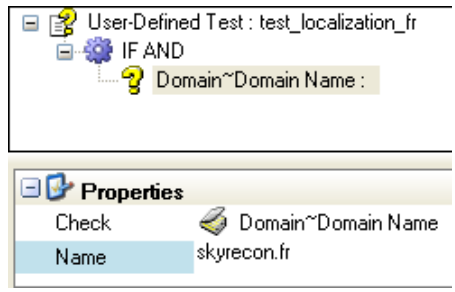


2. Right-click the statement displayed by default **IF AND** and click one of the following items:
   - Add Statement.
   - Add Built-In Test.
   - Add User-Defined Test.



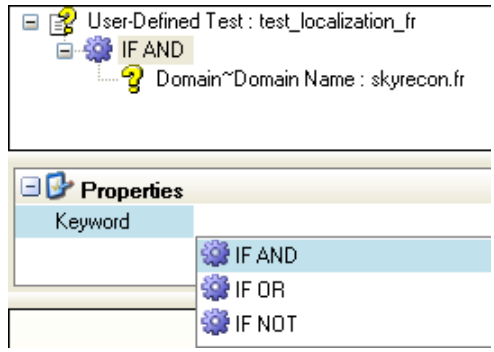
3. When adding a **test**, specify its properties.

   To display and fill in the **Properties** panel:
   - Click the newly created test.
   - Fill in the **Name** field to define the domain name.



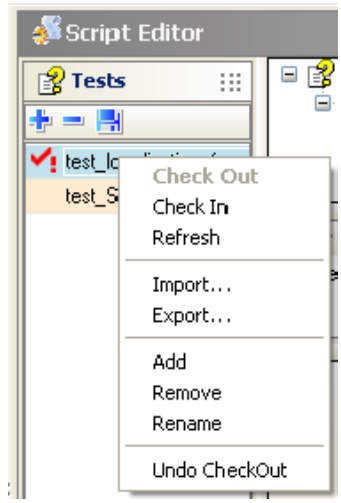
4. To change the **statement** displayed by default (IF AND) or to add another statement:
   - Click the IF AND statement in the upper panel.
   - Click the statement in the **Properties** panel.
   - Click ... to browse the statement list.

- Select the appropriate statement from the dropdown menu.



If several tests are included in the test script, you have to enter and/or select required information using the Browse button ....

5. When you have finished creating the test script:
   - Right-click the test script in the **Tests** panel.
   - Select **Check In**.



For more information, see "Definition of built-in tests", page 398.

ACTION SCRIPTS

OVERVIEW

An action script may include two types of action:

- **Built-in actions**:

  These actions are standard actions supplied with StormShield.
- **User-defined actions**:

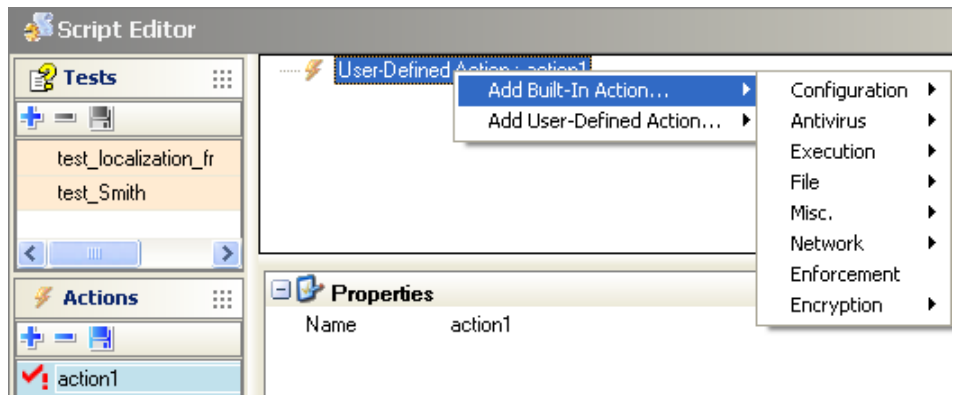
  These actions are the ones that you create or that are created by another administrator.

BUILT-IN ACTIONS

A built-in action is a predefined action used in your scripts. You can add numerous built-in actions as part of your scripts.

First level

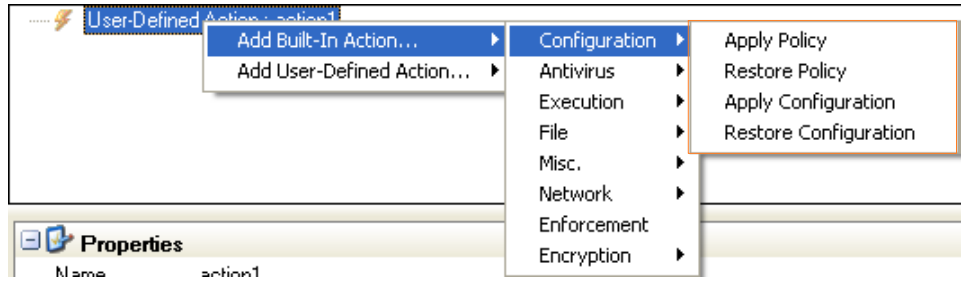
Here is the first-level list of built-in actions available in StormShield:



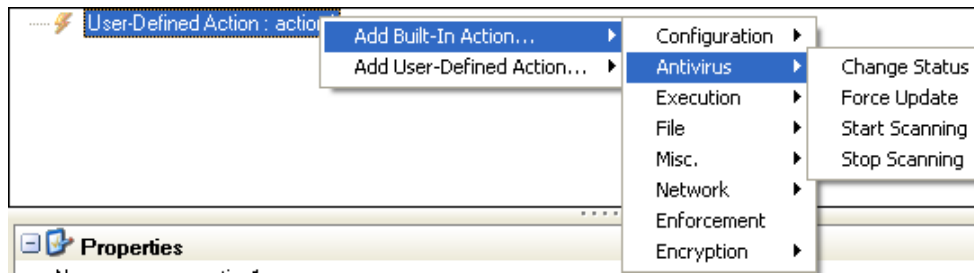
Second level

Here is the second-level list of built-in actions available in StormShield:

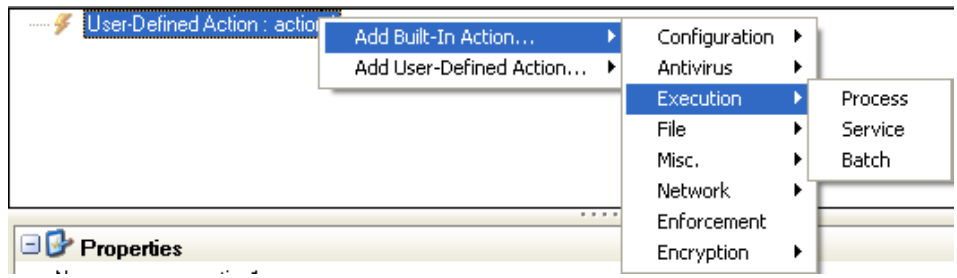
- Under **Configuration**, you will find the following built-in actions:



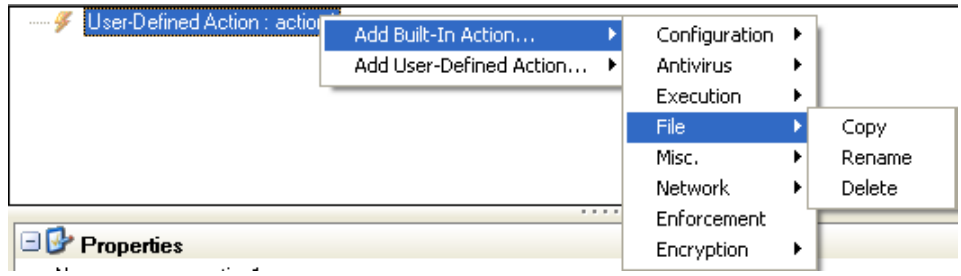
- Under **Antivirus**, you will find the following built-in actions:



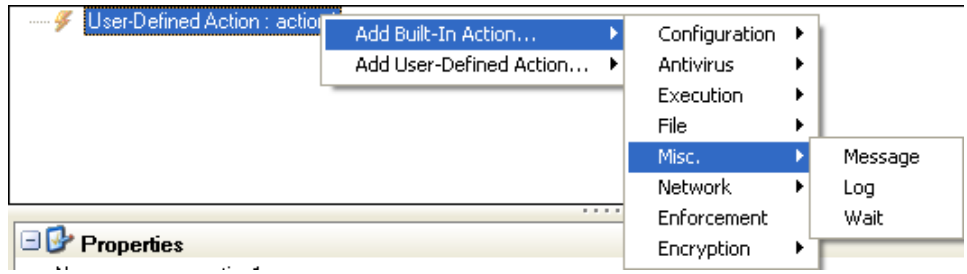
- Under **Execution**, you will find the following built-in actions:



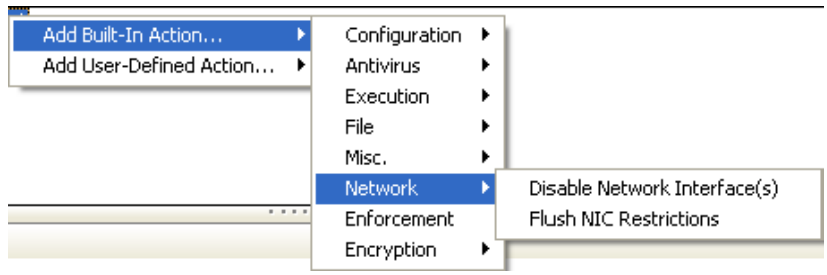
- Under **File**, you will find the following built-in actions:



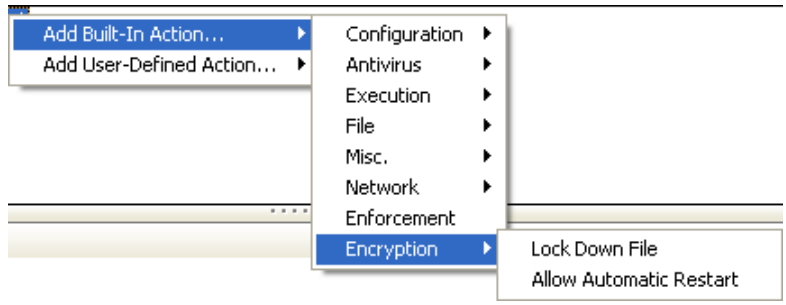
- Under **Misc.**, you will find the following built-in actions:



- Under **Network**, you will find the following built-in actions:



- Under **Encryption**, you will find the following built-in actions:



Definition of built-in actions

Built-in actions perform commonly used actions that you can run as part of your own test or batch scripts.

ACTION	DESCRIPTION	PROPERTIES
Configuration > Apply Policy	Applies a security policy.	Select a security policy: ◦ `Name: Policy 1` ◦ `Type:` - `Temporary`: If you apply a "Restore Policy" action, the permanent security policy will be restored. - `Permanent`: If you apply a "Restore Policy" action, the permanent security policy will be restored even though one or several temporary policies have been applied in the meantime (scripts).
Configuration > Restore Policy	Restores the security policy previously in effect. The policy which is restored is that defined at Agent groups level.	
Configuration > Apply Configuration	Applies a configuration.	Enter configuration name. ◦ `Name: Paris Office` ◦ `Type:` - `Temporary`: If you apply a "Restore Configuration" action, the permanent configuration will be restored. - `Permanent`: If you apply a "Restore Configuration" action, the permanent configuration will be restored even though one or several temporary configurations have been applied in the meantime (scripts).
Configuration > Restore Configuration	Restores the previous permanent configuration. The configuration which is restored is that defined at Agent groups level.	
Antivirus > Change Status	Enables/Disables the antivirus.	
Antivirus > Force Update	Forces the antivirus update.	
Antivirus > Start Scanning	Enables/Disables the antivirus scan.	
Antivirus > Stop Scanning	Stops the antivirus scan.	

Table 12.7: Built-in action definitions (Sheet 1 of 3)

ACTION	DESCRIPTION	PROPERTIES
Execution > Process	Launches applications or processes.	Enter process name and path, and the **Wait for execution** parameter (if any): ◦ `Name: c:\Programs\antivirus\update.exe` ◦ `Wait for execution:` - `True`: The rest of the script is not executed until process ends. - `False`: The script is running in background mode. The process is executed with SYSTEM user privileges.
Execution > Service	Launches a service.	Enter service name: ◦ `Name: wuauserv`
Execution > Batch	Launches a batch.	Enter batch name: ◦ `Name: AntiVirus Check` Enter the number of seconds before launching the batch: ◦ `Wait (seconds): 30`
File > Copy	Copies a file.	Enter name and path of the file to copy: ◦ `Name: c:\Account1` Enter name and path of the file copy: ◦ `Name: c:\Account2`
File > Rename	Renames a file.	Enter name and path of the original file: ◦ `Name: c:\programs\acme software\myfile1.txt` Enter name and path of the new file: ◦ `New Name: c:\programs\acme software\myfile2.txt`
File > Delete	Deletes a file.	Enter path and filename: ◦ `Name: c:\document.txt`
Misc. > Message	Displays a StormShield message popup to the user.	Enter the message text to be displayed in the popup. `Message: You must update your antivirus signature database.`
Misc. > Log	Generates a new INFO log on the agent. This log is displayed in the **Logs: Software** part under **Log Monitoring** (in the Management panel) on the console. The log filename on the agent is `software.sro`.	Enter the log message to be displayed in the **Value** field.

Table 12.7: Built-in action definitions (Sheet 2 of 3)

ACTION	DESCRIPTION	PROPERTIES
Misc. > Wait	Pauses the script execution.	Enter pause length in seconds.
Network > Disable Network Interface(s)	Disables an agent network interface.	Select how to disable network interfaces: ◦ `Type`: - `Whitelist`: All network interfaces are disabled excepting those mentioned on the list. This action remains active until the next full review of the batches on the agent or an explicit call in a batch file of the "Flush NIC Restrictions" action. - `Blacklist`: Only the listed network interfaces are disabled. ◦ `Values`: network card hash. To disable all network interfaces in the Whitelist, a value of the type 0:000000000 must be entered. After clicking **Values** in the **Properties** panel, make a select from the dialog box. Network interfaces can be added by the administrator or imported from the database.
Network > Flush NIC Restrictions	Cancels the "Disable network interface" action. The network interface is not automatically re-enabled.	
Enforcement	Sets the status of a variable. Can be used by TNC clients (Trusted Network Connect) such as Odyssey Access Clients on Juniper Networks (R).	Set **Status** to: ◦ Allow, ◦ Isolate, ◦ No access, ◦ No recommendation.
	For more information on Juniper's OAC, see How to install Juniper's "Unified Access Control" module?	
Encryption > Lock Down File	Enables/Disables encrypted file lockdown. When files are locked, no user (even authenticated) will access encrypted files.	
Encryption > Allow Automatic Restart	Enables/Disables automatic restart (without compulsory password entry) for full disk encryption.	

Table 12.7: Built-in action definitions (Sheet 3 of 3)

USER-DEFINED ACTIONS

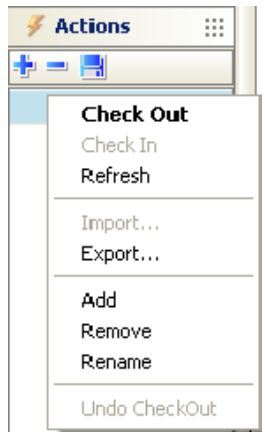
User-defined actions are actions previously created by you or another administrator.

You can include user-defined actions in test and batch scripts.

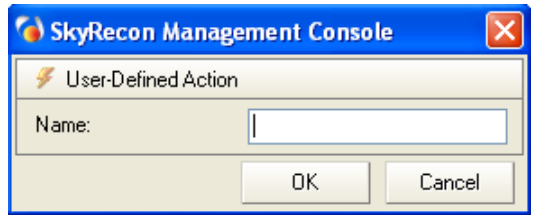
CREATING AN ACTION SCRIPT

To create an action script, follow the steps below:

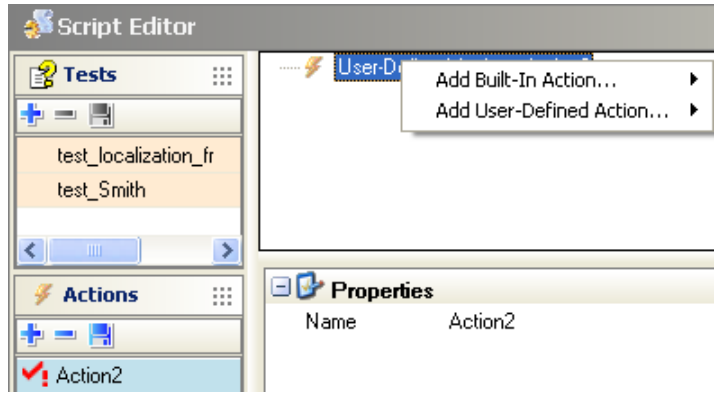
1. In the **Actions** area in the Script Editor.
   - Right-click in the area.
   - Select **Add** from the dropdown menu or just click the + icon on the toolbar.



   - Name the user-defined action script.

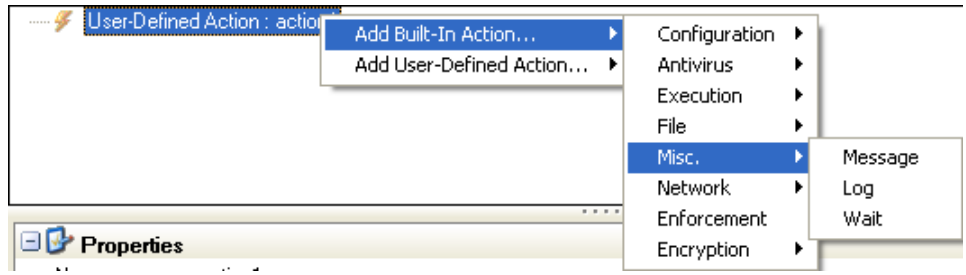


2. In the work area, right-click the Action icon to display the **Add** dropdown menu.



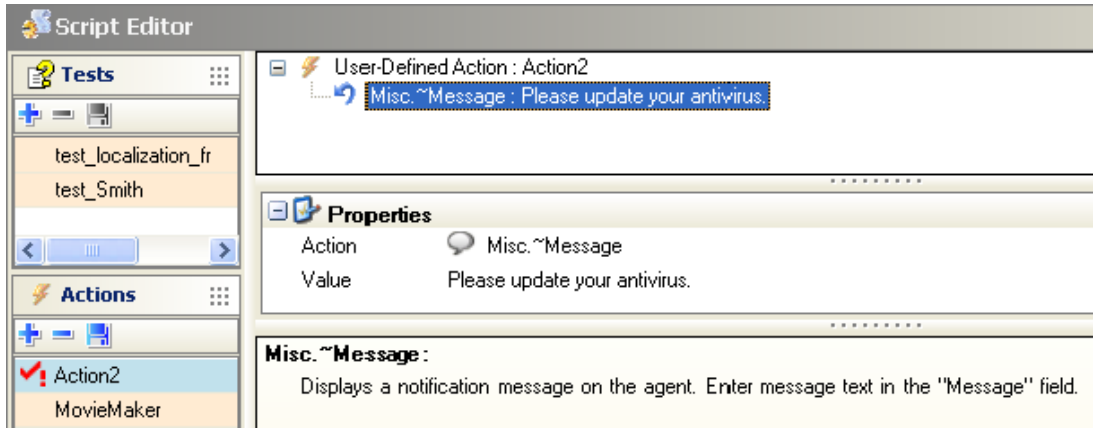
3. To display the first-level actions which are available, select either of the following:
   - Add Built-In Action.
   - Add User-Defined Action.

4. Select a second-level action (Example: Misc. > Message).

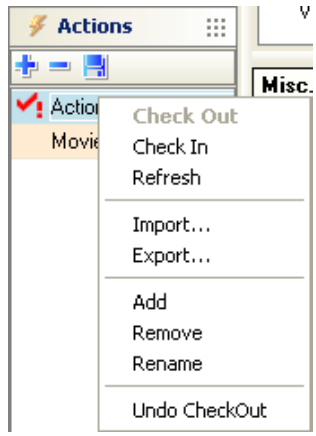


The action is added to the script. You now have to specify its properties.

5. Click the appropriate action to display its **Properties**. Enter and/or select the information required using ... .



6. When you have finished creating the action script:
   - Right-click the action script in the **Actions** panel.
   - Select **Check In**.



BATCH SCRIPTS

OVERVIEW

Batch scripts enable you to combine tests and actions in order to create more complex and powerful scripts that can be applied to network policies and configurations.

Batch scripts include the following:

- **Statements**:

  Statements use the Boolean logic operators IF AND, IF OR and IF NOT.

- **Built-in tests**:

  Built-in tests are commonly used tests supplied with StormShield (Example: "Process" used to check the execution of a process).

- **User-defined tests**:

  User-defined tests are tests that you create or that are created by another administrator.

  They consist of:

  - Statements.
  - Built-in tests.
  - Other user-defined tests.

- **Built-in actions**:

  Built-in actions are commonly used actions supplied with StormShield (Example: "Run Process" to start a process).

- **User-defined actions**:

  User-defined actions are actions that you create or that are created by another administrator.

  They consist of:

  - Statements.
  - Built-in actions.
  - Other user-defined actions.

TRUE/FALSE RESULTS

When you add a new batch, the **Result True** and **Result False** settings are automatically added.
Add actions under Result True or Result False according to the action that you want applied based on the result returned.

You can create a batch script to check that any workstation trying to log onto the network has antivirus software. If this is not the case, the batch will be configured to refuse network access.

The batch will contain tests and actions to be executed based on the test results returned.

The administrator is not allowed to remove a script (test, action or batch) used by another script.

For more information, see:

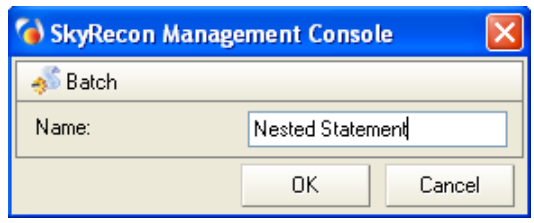
- "Batch scripts", page 416.
- "Creating a batch script", page 417.

CREATING A BATCH SCRIPT

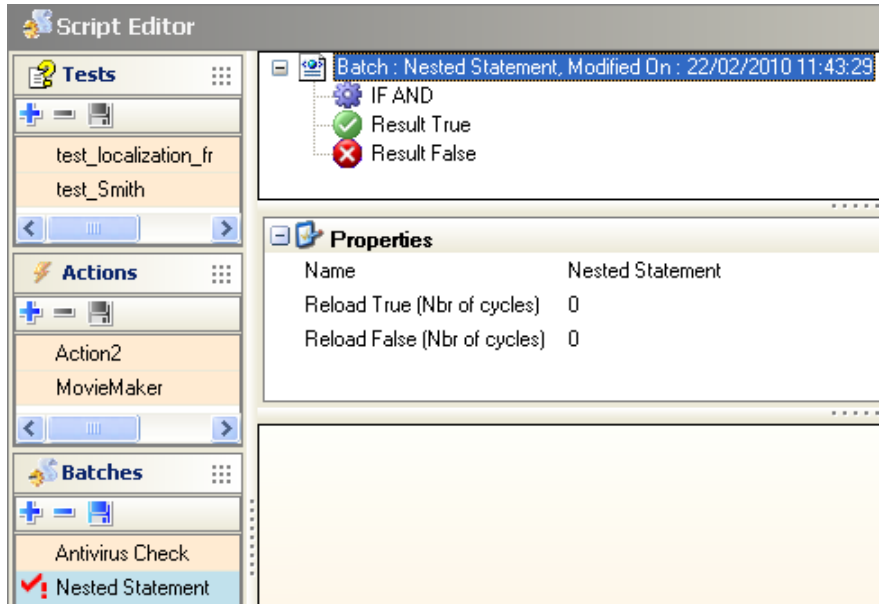
To create a batch script, follow the steps below:

1. In the **Batches** panel in the Script Editor:
   - Right-click in the Batches area.
   - Select **Add** from the dropdown menu or just click the icon on the toolbar.

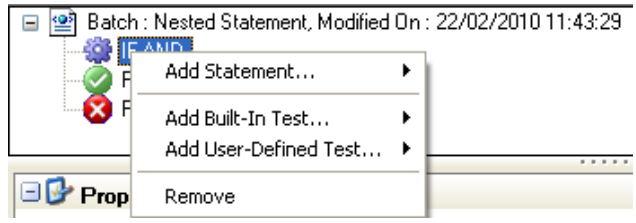
   - Enter a name for the batch.



You can modify the batch name by double-clicking the field opposite **Name** in the **Properties** panel.



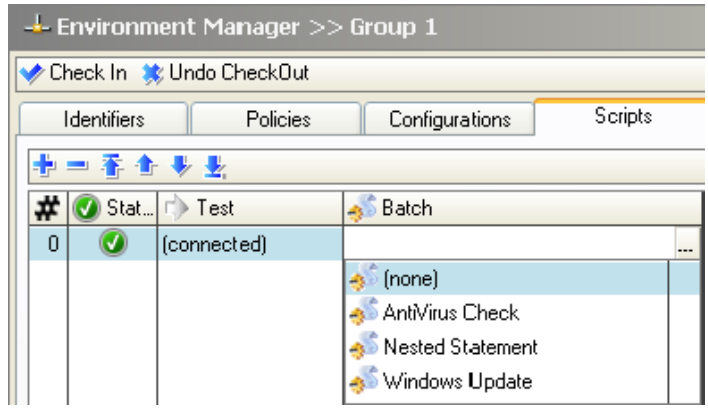
2. Right-click the statement displayed by default (**IF AND**) and click either of the following options:
   - Add Statement.
   - Add Built-In Test.
   - Add User-Defined Test.



3. To change the **statement** displayed by default (IF AND) or to add another statement:
   - Click the IF AND statement in the upper panel.
   - Click the statement in the **Properties** panel.
   - Click ... to browse the statement list.
   - Select the appropriate statement from the drop-down menu.

4. If you have added a **test**, specify its properties.
5. Right-click the **Result True** icon or the **Result False** icon to display the list of actions to be associated with the result returned.

   Both result icons are generated by default when creating the batch.
6. Add required actions, tests and statements to your batch script (Example: Windows Update.)
7. To apply your batch to an agent group:
   - Go to **Agent Groups** in the Environment Manager.
   - Edit the agent group to be associated with the batch.
   - Click the **Scripts** tab.
   - Select the test to be applied to the agent group (`connected`, `disconnected` and `true` are present by default).
   - Select the batch to be applied to the agent group.



   - Validate your modifications.

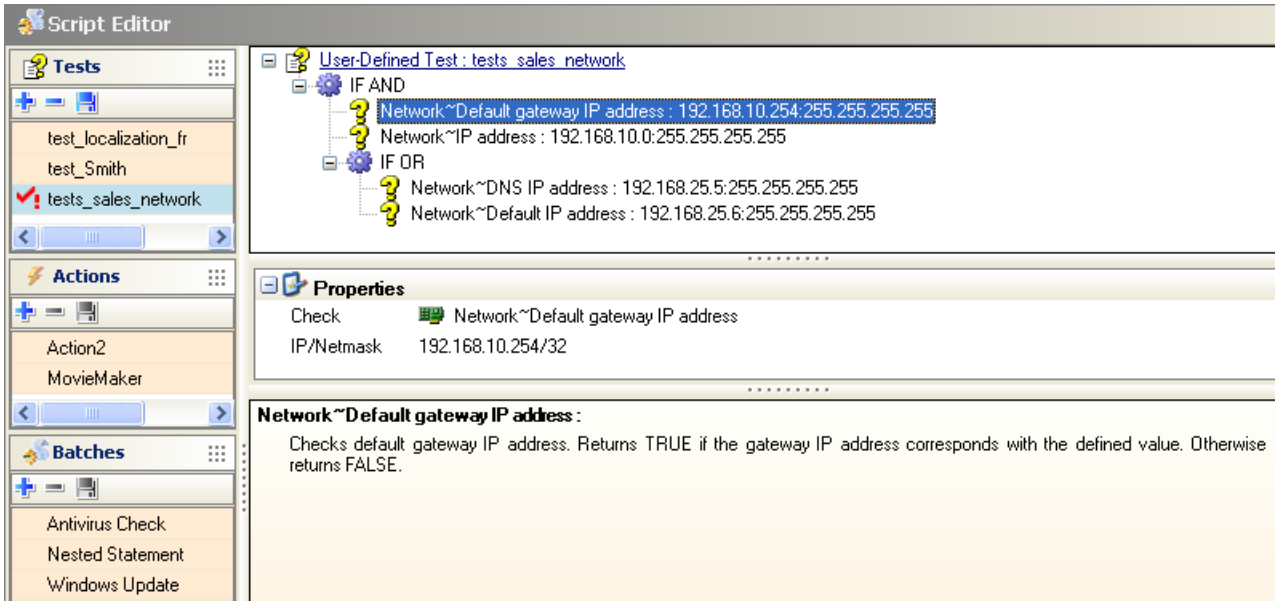
Example 1

Creating a test to check that a workstation is on the network

To check that a workstation is on the network, follow the steps below:

1. Create a test script called "`test_sales_network`" to check if the computer is on the network:
   - Add an **IF AND** statement.
   - Add the **Default Gateway IP Address** built-in test.

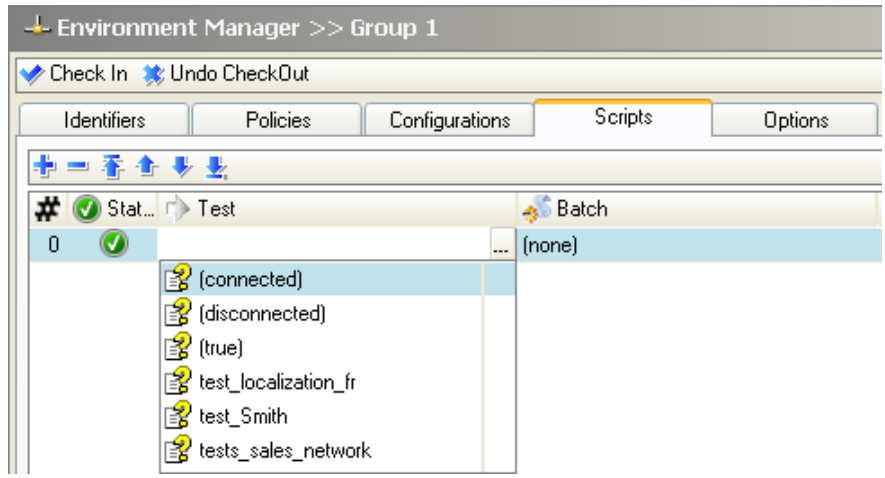
- In the Default Gateway IP Address properties, specify:
  - The gateway IP address of the Sales Network.
  - The network IP address.



- Add an **IF OR** statement.
- Add a **DNS IP Address** built-in test.
- Add another **DNS IP Address** built-in test.
- In the DNS server properties of each DNS server, specify:
  - The DNS IP address.
  - The subnet mask.

2. To apply the test to the agent group:
   - Go the Environment Manager.
   - Select and edit the agent group to be tested.
   - Click the **Scripts** tab:
     - Click .

- In the **Test** column, select the test to be applied to the agent group.



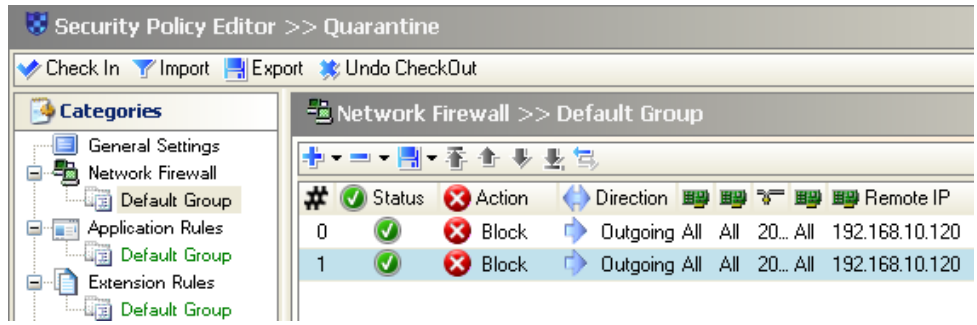
- Validate your modifications.

Example 2

Applying a quarantine policy

To apply a quarantine policy, if the antivirus is no longer operating, follow the steps below:

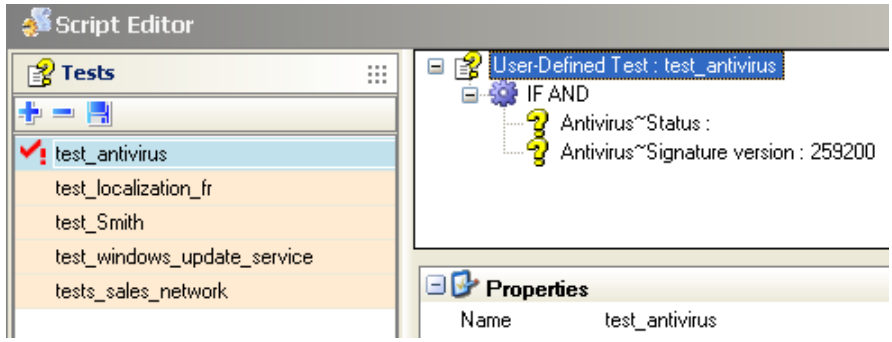
1. In the Policy Editor > Categories > Network Firewall, create a **Quarantine** policy to restrict network access to the antivirus server and to ban network access to sensitive servers and networks.



You can apply restrictions to any element in the same way as for a security policy (Example: forbid the execution of specific programs).

2. Create a test called "`test_antivirus`" to check that when a host connects to the company server:
   - The antivirus is running.

- The signature file is not older than 2 days.

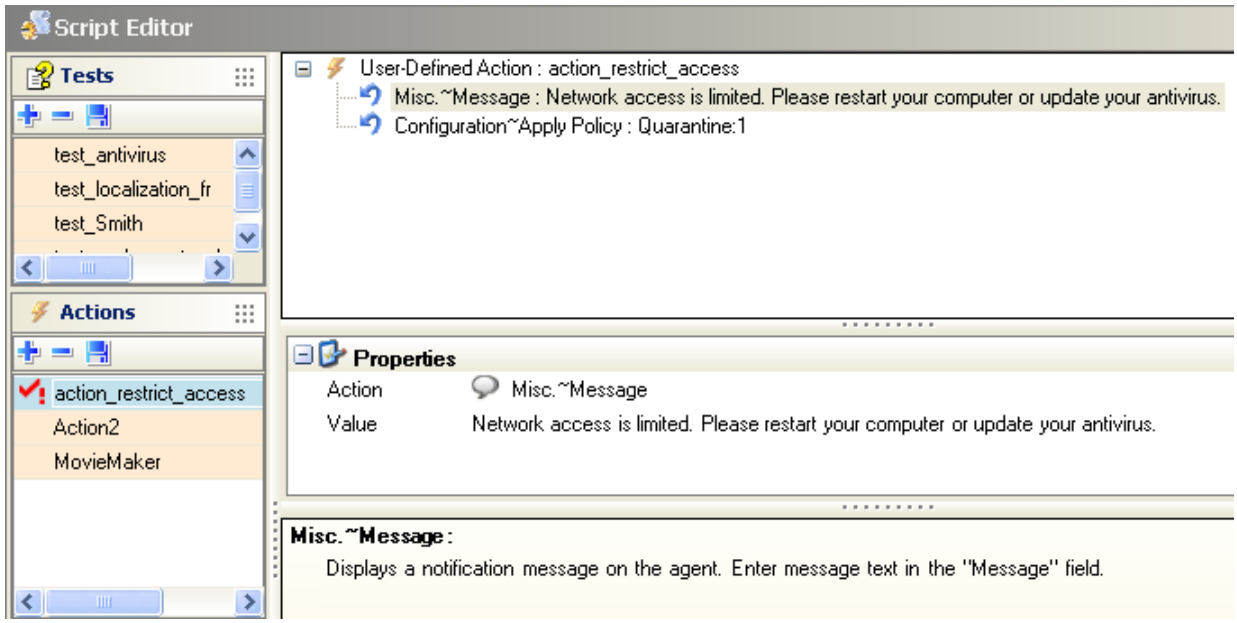


3. Under **Script Editor > Tests**, follow the steps below:
   - Add an **IF AND** statement.
   - Inside the IF AND statement, add the two following tests:
     - **Antivirus > Status:**

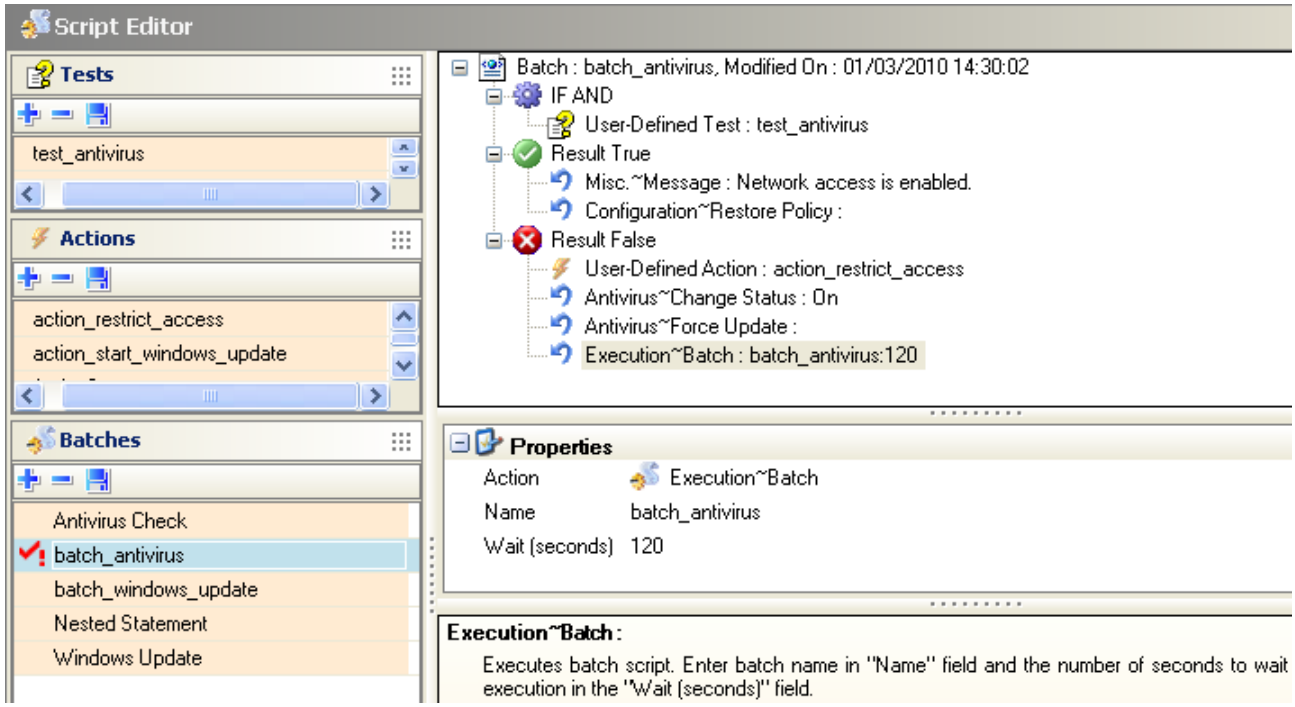
       In order to check the status of your antivirus software (enabled/disabled).
     - **Antivirus > Signature version:**

       In the Properties panel, enter the duration after which the antivirus is considered obsolete. In this example, 3 days is converted into seconds (`259200` seconds in the upper section of the user-defined test).
4. Under **Script Editor > Actions**, create a new action called "`action_restrict_access`".

   You will use this action to apply the **Quarantine** policy.

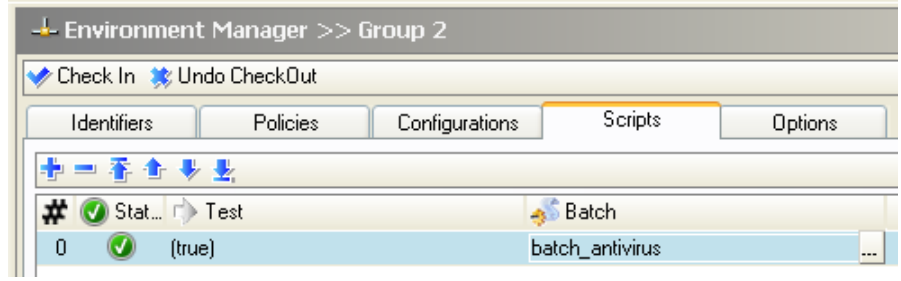


5. In the user-defined action "`action_restrict_access`", follow the steps below:
   - Add a Misc. > **Message** action to inform the user of the action required.
   - Add a Configuration > **Apply Policy** action:
     - Select the Quarantine policy that you have created in Step 1.
     - Select the **Temporary** type.
       If you disconnect your computer, the permanent security policy is reapplied.
6. Under **Script Editor > Batches**, create a batch to associate required actions with the test:



   - Add an **IF AND** statement.
   - Add the user-defined test "`test_antivirus`" that you have created in Step 2.
   - Add in **Result True** the actions to be executed if the test returns **TRUE**:
     - A Misc. > **Message** action to indicate that the access to the network is allowed.
     - A Configuration > **Restore Policy** action to restore the permanent policy.
   - Add in **Result False**:
     - The user-defined action "`action_restrict_access`" to apply the Quarantine policy.
     - The built-in action **Antivirus > Change Status**. Specify **ON** in the Properties panel.
     - The built-in action **Antivirus > Force Update**.
     - An Execution > **Batch** action to restart the test every 2 minutes (120 s).

7. To apply the batch to the agent group, follow the steps below:
   - Go to the Environment Manager.
   - Select and edit the agent group.
   - Click the **Scripts** tab:
     - In the **Test** column, select (true).
     - In the **Batch** column, select the batch to be applied to the agent group.



   - Validate your modifications.

Example 3

Checking that the Windows Update service is running

To check that the Windows Update service is running, you will create three scripts:

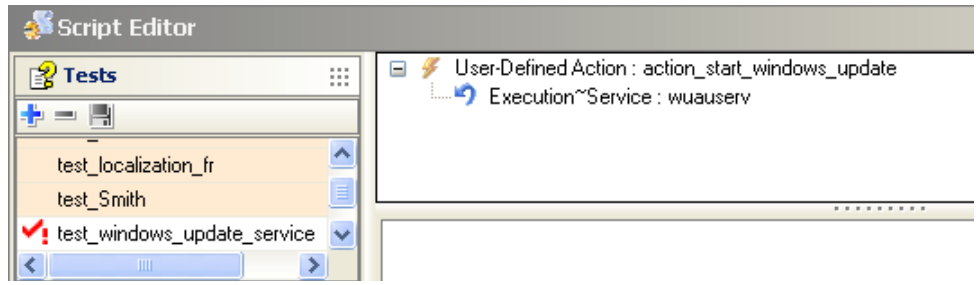
- A test script
- An action script
- A batch script.

Your script should include the case when the service is not running and force Windows Update to restart.

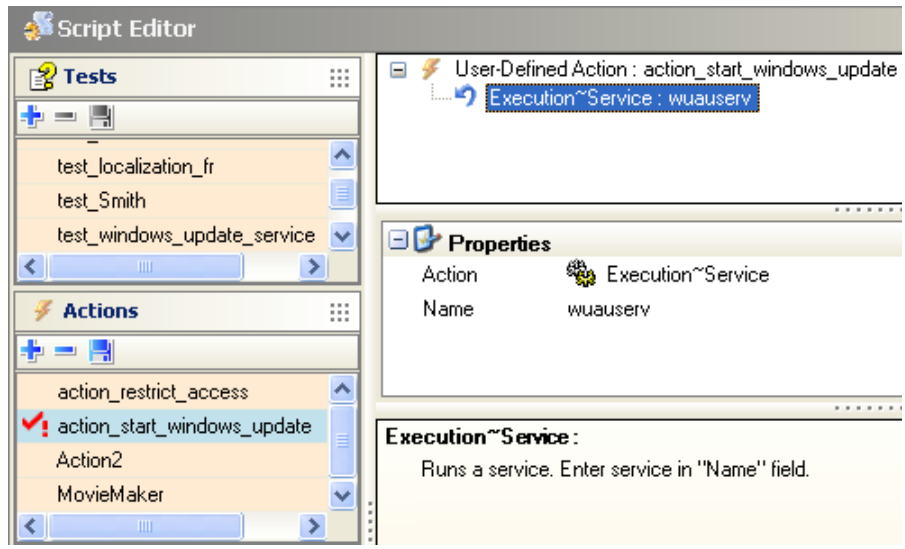
To check that the Windows Update service is running, follow the steps below:

1. Under **Script Editor > Tests**, create a new test called "`test_windows_update_service`".
   - Add an **IF AND** statement.
   - Inside this statement:
     - Add the Service > **Status** test.
     - Enter the name of the Windows Update service: `wuauserv`.

The test returns **FALSE** if the service has not started.

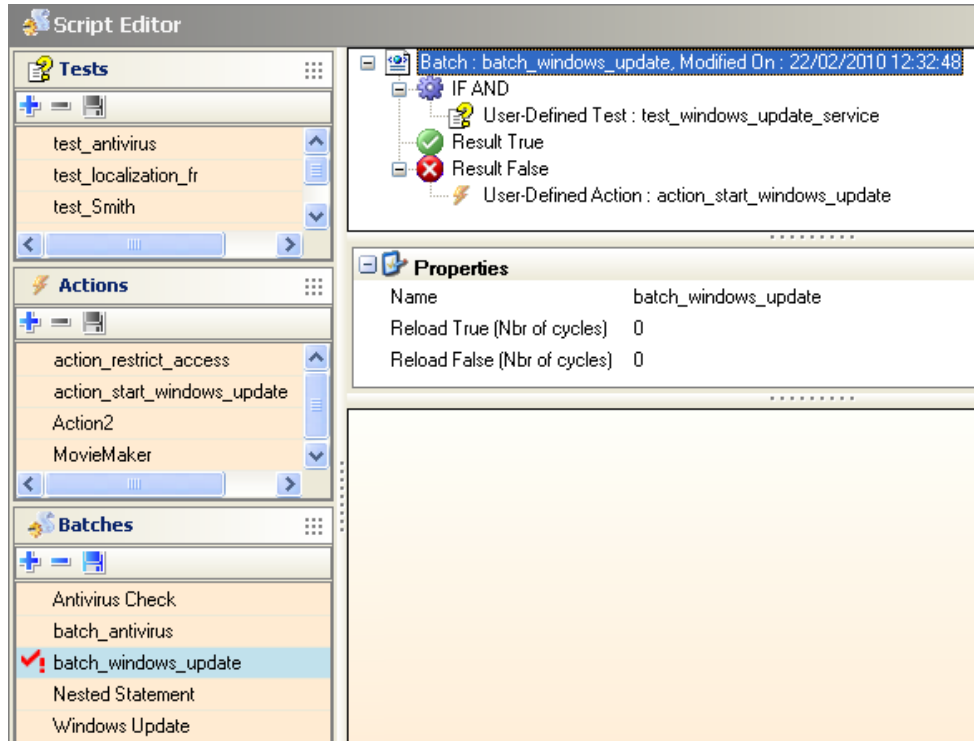


2. Under **Script Editor > Actions**, create a new action called "`action_start_windows_update_service`".
   - Add an Execution > **Service** action.
   - Enter the name of the Windows Update service: `wuauserv`.

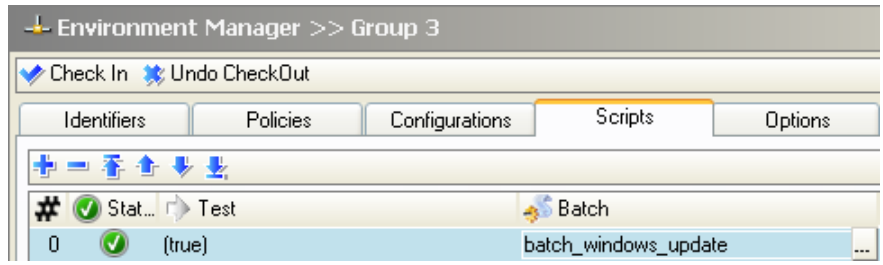


3. Under **Script Editor > Batches**, create a new batch:
   - Add an **IF AND** statement.
   - Inside the IF AND statement, add the user-defined test "`test_windows_update_service`" that you have created in Step 1.

- In Result False, add the user-defined action "`action_start_windows_update_service`" that you have created in Step 2.



4. To apply the batch to the agent group:
   - Go to the Environment Manager.
   - Select and edit the agent group to be associated with the batch.
   - Click the **Scripts** tab:
     - In the **Test** column, select (true).
     - In the **Batch** column, select the batch to be applied to the agent group.



   - Validate your modifications.

TEMPORARY ACTION SCRIPTS

OVERVIEW

Temporary actions are scripts configured on the SkyRecon management console. A temporary action script is applied to a StormShield agent on a temporary basis.

Users request the execution of temporary actions via **challenges**. The administrator manages challenges from the SkyRecon management console.

Applying a temporary action script via a challenge request will in no way replace the conventional application of a policy or a configuration through a batch defined by the administrator and dedicated to a specific environment.
A policy defined in a specific environment cannot be restored using a temporary action script.

Batch scripts and temporary action scripts (including batches) are initiated by the **administrator**.
Only temporary action requests are initiated by the **user**.

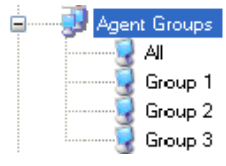
Temporary action scripts are detailed in this section according to a chronological order:

- The administrator applies a temporary action to an agent group.
- The user sends a temporary action request to the administrator.
- The administrator manages the temporary action requests sent by the user.
- The user displays the temporary actions in progress.
- The user stops a temporary action in progress.

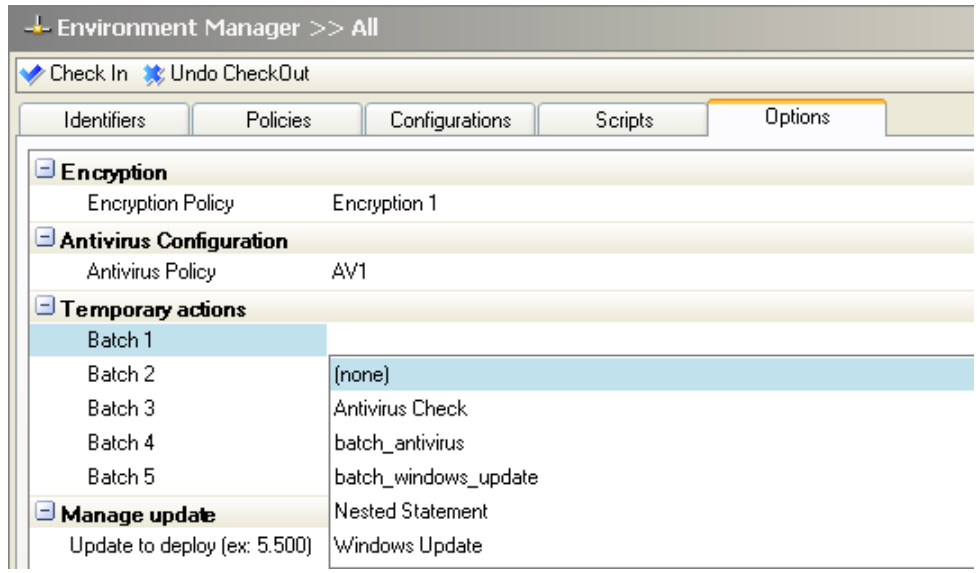
ADMINISTRATOR APPLYING A TEMPORARY ACTION TO AN AGENT GROUP

To directly apply a temporary action to an agent group, the administrator follows the steps below:

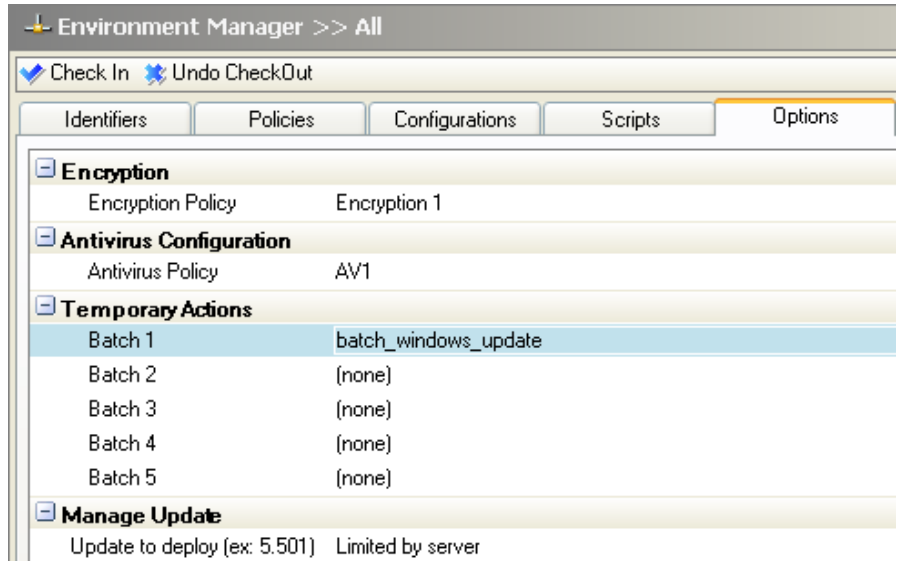
1. In the Environment Manager, click the **Agent Group** to be associated with a temporary action.



2. Click the **Options** tab.
   A list of numbered batches without parameters is displayed by default.



3. Click any batch field to display the ... button.
   A list of scripts becomes accessible to the administrator.
4. To use an existing batch script as a temporary action, select the batch from the dropdown menu.
   The batch will be associated with the edited agent group.



The scripts used for temporary actions are created in the **Script Editor**. For more information, see "Batch scripts", page 416.

USER SENDING A TEMPORARY ACTION REQUEST TO THE ADMINISTRATOR

Reminder

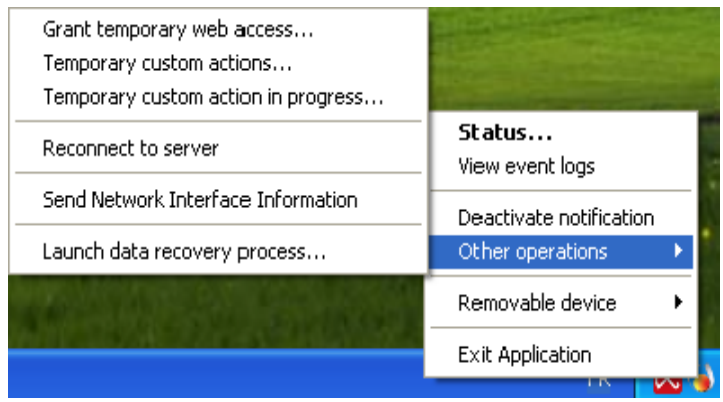
Before applying any temporary action, the user should request the right to apply any particular action from the administrator. This is a temporary action request.

The administrator is in charge of selecting the temporary action type and its duration. The temporary action selected by the administrator from the SkyRecon management console is activated for the time period specified.

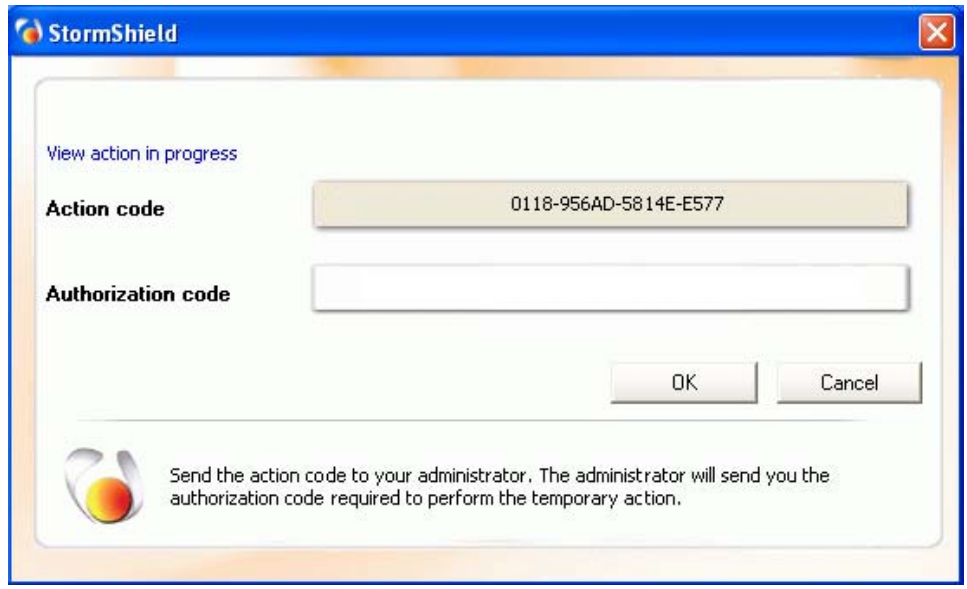
Procedure

To send a temporary action request, the user must follow the steps below:

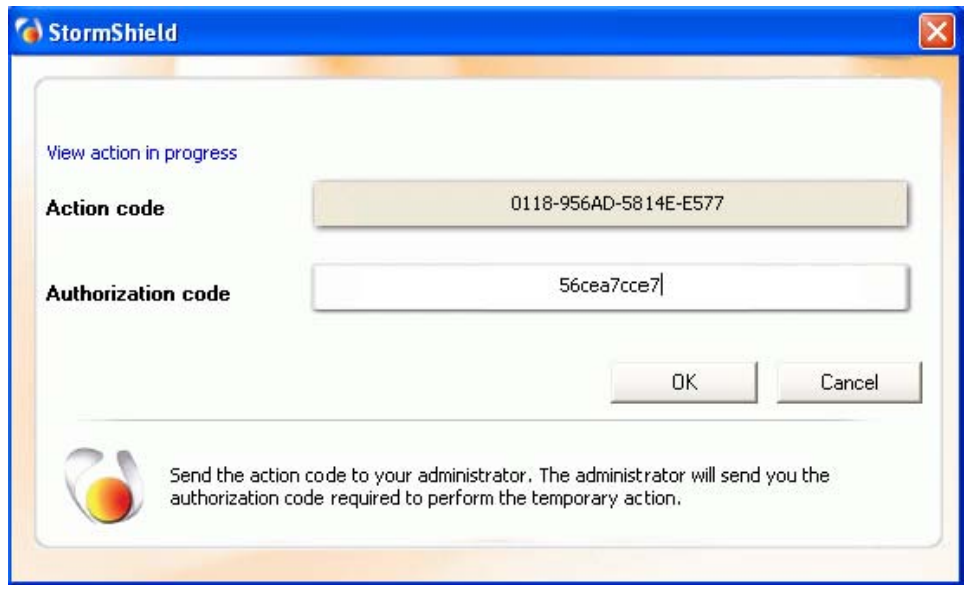
1. Right-click the StormShield Monitor icon and click **Other operations** > **Temporary custom actions**.



2. Send the **Action code** that is displayed to the administrator.
In return, the administrator will provide you with an **Authorization code**.



3. In the **Authorization code** field, enter the code provided by the administrator.



4. Click **OK**.

The temporary action selected by the administrator from his console is activated as specified on the timeline in the **Generate Challenge** window.

If the administrator selects **Disable Protections**, the user will have to wait for at least 30 seconds to allow the agent protection process to be stopped. In the other cases, the action is immediately effective.

5. To check that the temporary action is in progress:
   - Right-click the StormShield Monitor icon .
   - Select **Status** or **View event logs**.

   Example of **Status** window for a Disable Protections temporary action (stand-by mode):

ADMINISTRATOR MANAGING THE TEMPORARY ACTION REQUESTS SENT BY THE USER (CHALLENGES)

Reminder

Stage 1: The user sends a temporary action request. The administrator receives the action code (agent key) assigned to this user.

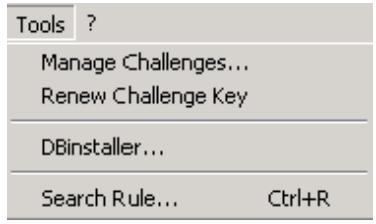
Stage 2: The administrator generates the authorization code assigned to the temporary action.

Stage 3: The user enters the authorization code which initiates the temporary action on his workstation.

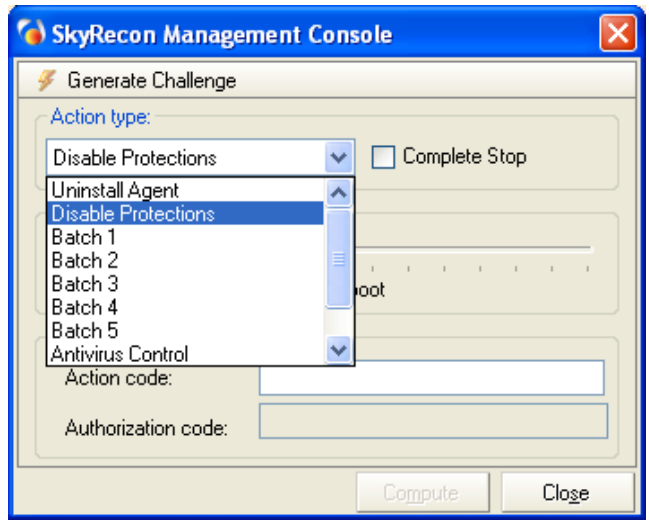
Procedure

To answer the user's request for a temporary action, the administrator follows the steps below:

1. On the SkyRecon management console, select **Tools > Manage Challenges**.



2. Define the following parameters:



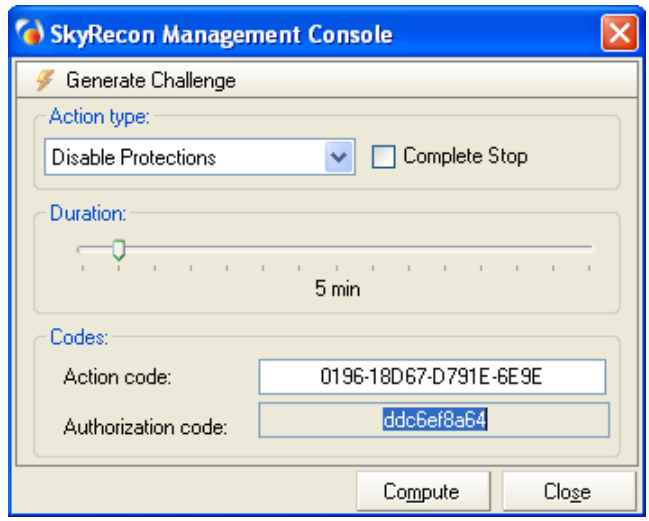
- **Action type** using to display the list of temporary actions.

  If you check the **Complete Stop** box opposite Disable Protections, the agent will stop completely and will not switch to Activated - Stand-by mode.

  Therefore, no log will be sent and no policy will be applied.

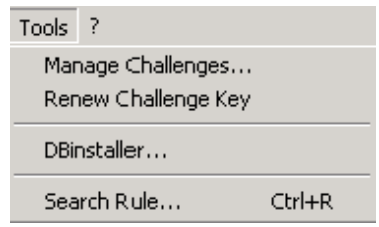
- **Duration** of the temporary action by sliding the cursor along the timeline.
- Enter the **Action code** sent by the user.

3. Click **Compute** to obtain the Authorization code.



4. Send this code to the user.

If the Administrator wants to renew the challenge code key, just click **Tools > Renew Challenge Key**.



USER DISPLAYING THE TEMPORARY ACTIONS IN PROGRESS

The user can consult the temporary actions in progress on his workstation by clicking **Other operations** > **Temporary custom action in progress**.

The information displayed on the temporary actions in progress are the following:

- **Start time**:

  The time when the temporary action was applied to the agent.

- **End time**:

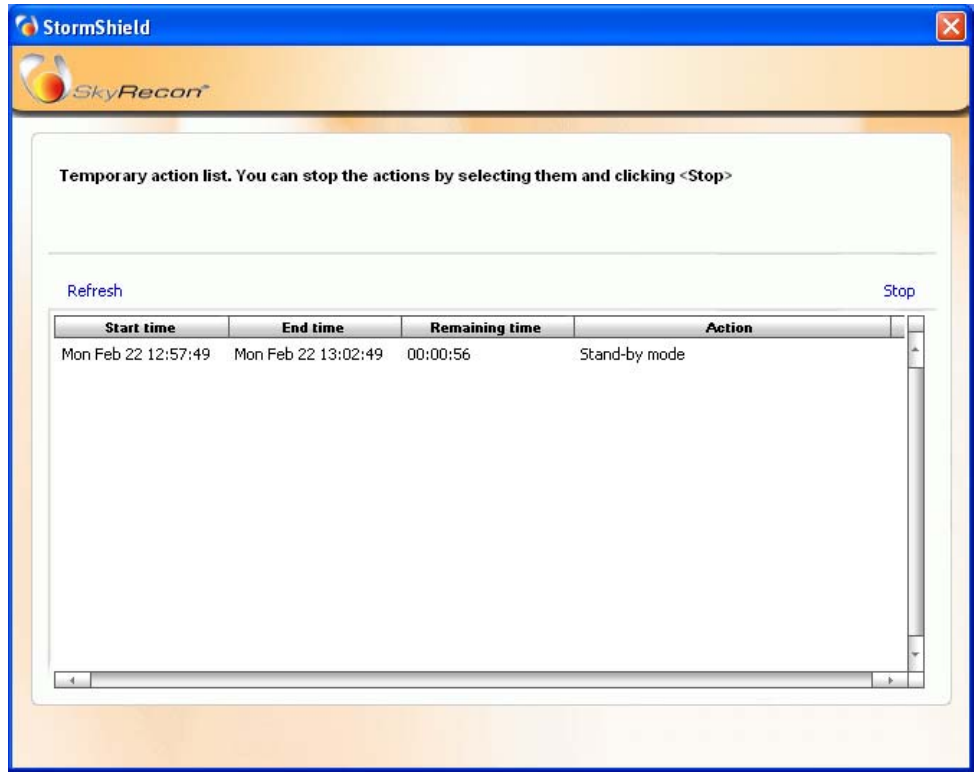
  The time when the temporary action stops.

- **Remaining time**:

  The time left before the temporary action stops.

- **Action**:

  Type of temporary action applied to the agent.

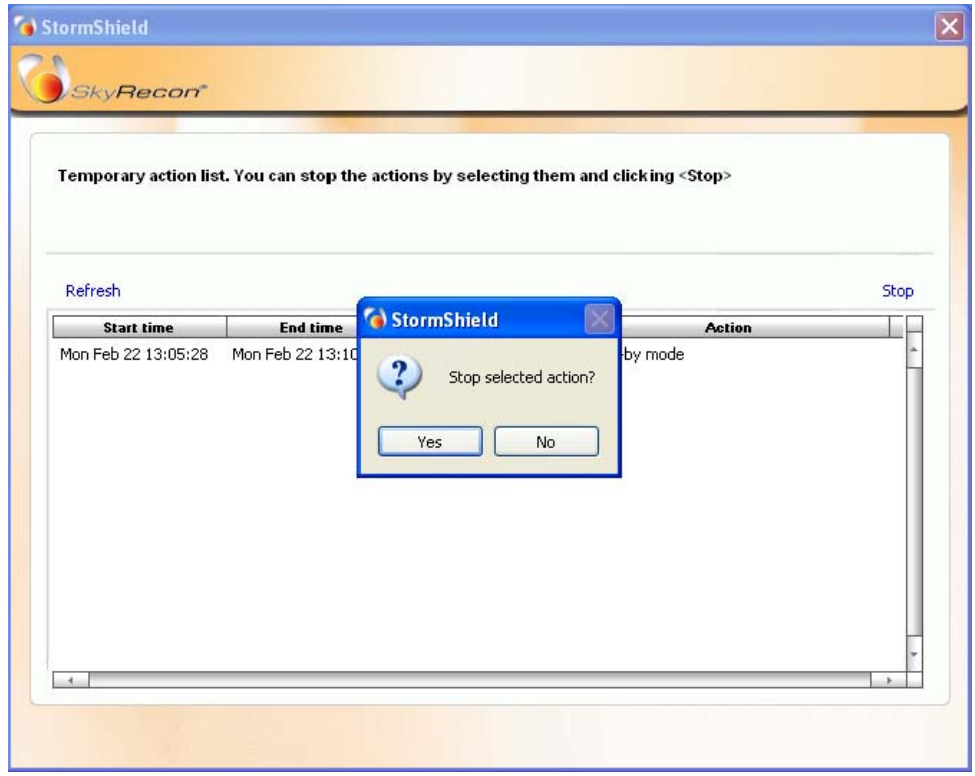


USER STOPPING A TEMPORARY ACTION IN PROGRESS

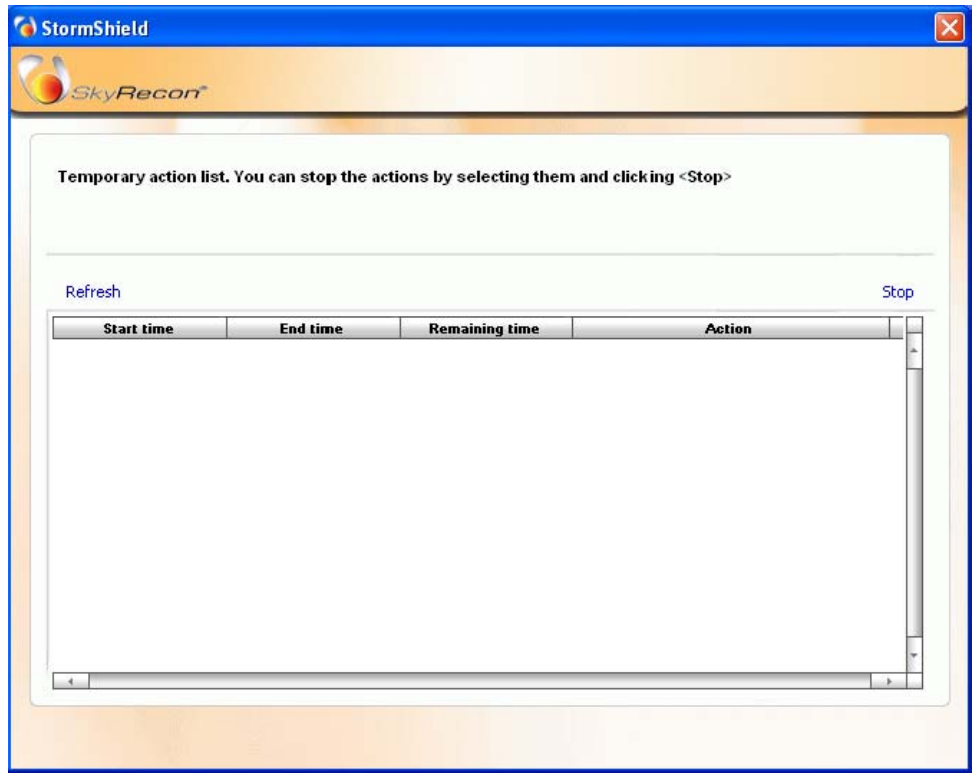
To stop the temporary action in progress on the agent computer, the user follows the steps below:

1. In the system tray:
   - Right-click the StormShield Monitor icon .
   - Select **Other operations > Temporary custom action in progress**.

   The list of temporary actions in progress is displayed.
2. Select the temporary action to be stopped.
3. Click **Stop** and **Yes**.



4. The resulting window appears.



UPLOADING FILES FROM THE MASTER SERVER

OVERVIEW

The Administrator can use the SkyRecon management console in order to:

- Upload a file from the master server.
- Distribute this file to agents.
- Distribute this file to slave servers.

For example, the administrator can upload and distribute a Script file to be applied to the agents.

It should be noted that only one file can be uploaded and deployed at a time.

Its characteristics are the following:

- The maximum size of the file to be uploaded must not exceed 1 MB.
- The uploaded file will be automatically renamed `upload_file.srn` by StormShield.
- The file deployed on the agents will be copied in: `[StormShield Agent install dir]\batch]`.
- The file deployed on the servers will be copied in: `[StormShield Server install dir\batch]`.

The extension of the `upload_file.srn` file implies that the applications:

- Whose checkbox in the **Files** column in **Trusted Rules** is not checked will be denied access to this protected file.
- Which are not launched by a StormShield batch will be denied access to this file.

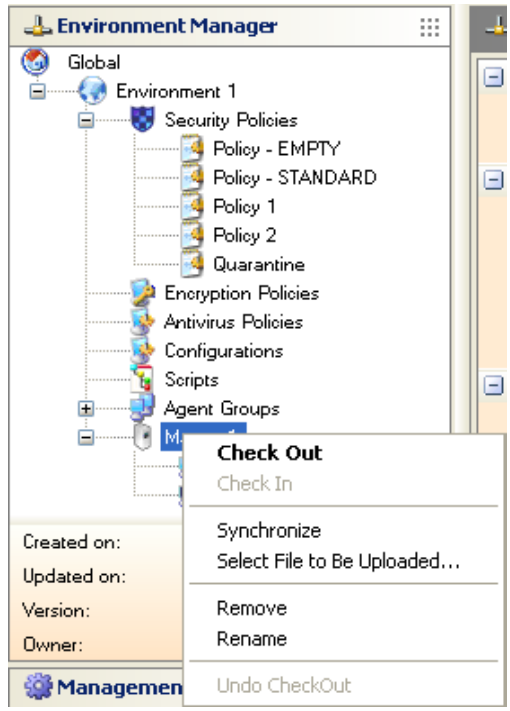
UPLOADING A FILE FROM THE MASTER SERVER TO THE AGENTS

Procedure

To upload a file from the master server to the agents, the administrator follows the steps below:

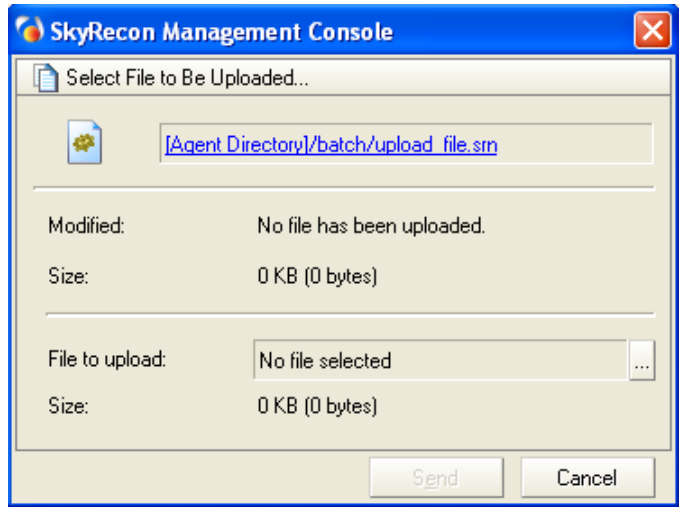
1. In the Environment Manager, right-click [**Master server**].

   The following dropdown menu is displayed:



2. From the dropdown menu, select **Manage file to upload**.

   The following window is displayed:



3. Click the Browse button ... next to the **File to upload** field.
   The Windows Explorer window is displayed.
4. Select the file to be uploaded.
   If a file has been previously uploaded, a window will notify the administrator.

   If you try to upload the same unmodified file, upload will be refused.

5. Click **Send**.
   - The file is distributed to the agents.
   - Slave servers will be synchronized.
   - The file will be renamed `upload_file.srn`.
   - The file deployed on the agents will be copied in:
     [`StormShield Agent install dir]\batch`].
   - The file deployed on the servers will be copied in:
     [`StormShield Server install dir\batch`].

Example

The Administrator can deploy a script on agents to make a distinction between workstations and laptops. This script will test the presence of batteries.

This script is not supplied with StormShield.

The script is written as follows:

- If a battery is detected, the script will return **TRUE** to the agent by sending value "1".
  This value is returned by the **vbscript** function "Wscript.quit(1)".
- Otherwise, the script will return **FALSE** to the agent by sending value "0".
  This value is returned by the **vbscript** function "Wscript.quit(0)".

To use this script in a test or a batch, the administrator will use the **Run** function and enter the following information:

```
Cscript.exe /E:Vbscript "c:\program files\SkyRecon\StormShield Agent\
Batch\upload_file.srn"
```

`/E:Vbscript` is used to indicate the file format (`upload_file.srn`) if its extension is not `.VBS`.

The administrator must not use the **Wscript** interpreter.

If the Vbs script allows the use of arguments, the administrator will use the **Run** function and declare arguments as shown below:

```
Cscript.exe /E:Vbscript "c:\program files\SkyRecon\StormShield Agent\
Batch\upload_file.srn" Argument1
```

or

```
Cscript.exe /E:Vbscript "c:\program files\SkyRecon\StormShield Agent\
Batch\upload_file.srn" Argument1 Argument2
```

Chapter 13

DATA ENCRYPTION

ABOUT THIS CHAPTER

This chapter describes how to use the **Data Encryption** feature to increase data security on the hard disk and when sending data over the Internet.

It includes the following:

- Overview:
  - Purpose.
  - Characteristics.
  - Supported system, hardware and software.

- Encryption types:
  - File Encryption.
  - Full Disk Encryption.

- Creating an encryption policy:
  - Graphical interface.
  - Procedure.

- File Encryption features :
  - Multi-user security.
  - Data erasure security.
  - File encryption options.
  - Password creation and user logon.
  - Synchronization.
  - Synchronization with multiple users.

- Encryption parameters:
  - General Settings.
  - File Encryption Parameters.
  - Full Disk Encryption Parameters.

- Applying an encryption policy to an agent group.

- Recovery of the following:
  - Password recovery when using File Encryption.
  - Data recovery from encrypted files (decryption).
  - Password recovery when using Full Disk Encryption.
  - Full-disk encryption data recovery via CD.

- Uninstalling StormShield agents:
  - Decryption before uninstallation.
  - Changing a User Account on a machine.

OVERVIEW

PURPOSE

Data Encryption provides an extra layer of data protection via encoding and password usage.

Your data can be:

- Either stored on the hard disk.
- Or sent to users both inside and outside of your company's network.

By password-protecting the encrypted data on your hard disks, sensitive data is protected in case of computer theft (**example**: laptops stolen during business trips).

Data Encryption also protects sensitive company data sent by users over the Internet. This feature will generate a password that the receiver will need to open your files.
The receiver does not need to have StormShield installed.

For more information, see "Authentication type", page 462.

CHARACTERISTICS

Advanced encryption standards

The StormShield Encryption feature is based on the **Advanced Encryption Standard** (AES). This is a symmetric encryption system which offers the choice of a **128, 192** or **256**-bit key length for encryption.

It has been approved by the U.S. Government for use with both their non-classified and classified documents.

StormShield's Data Encryption has obtained the **Federal Information Processing Standard** (*FIPS*) **140-2** certification.

Two **CBC** (Cipher Block Chaining) modes are available in **Data Encryption**.

For more information, see "Block-cipher mode of operation", page 475.

Invisibility

Once the administrator has configured the encryption options, the computer begins the synchronization process. The agent's computer data is automatically encrypted by **file** or by **disk** (depending on the encryption policy applied).

Data Encryption consists of File Encryption **and** Full Disk Encryption.

File encryption does not exclude the use of full disk encryption. Both options can be simultaneously enabled.

After the deployment of the encryption policy, StormShield users will not notice the encryption process in progress while working on their computer.

Nevertheless, some cases exist where a progress bar is visible during the encryption process (also called synchronization):

- Change of encryption policy.
- File transfer from unencrypted to encrypted zones.
- Recovery.

To prevent the display of encryption indicators, the administrator can enable **Stealth mode** under **File Encryption Parameters**.

The lock  indicating that encryption has been applied to a file will not be displayed on encrypted files.

If the stealth mode is enabled, the administrator needs to set authentication mode to **Windows**.

SUPPORTED SYSTEM, HARDWARE AND SOFTWARE

The **supported operating systems** are the following:

- Windows XP SP3 32bits.
- Windows Vista SP2 32bits.
- Windows 7 32bits.

The **unsupported hardware and software** are the following:

- Software RAID and dynamic disks.
- Partition management and disk cloning tools.
- Hard disks with sector size other than 512 bytes.
- Extended partitions are not supported by Full Disk Encryption. Only disks containing master partitions can be encrypted.
- Multiboot (several operating systems on the same partition or on two separate partitions) is not supported by Full Disk Encryption.
- Boot loaders other than Microsoft Windows boot loader are not supported by Full Disk Encryption.

Data Encryption is used to encrypt hard drives. It does not encrypt removable devices such as USB keys.
This feature cannot be used to encrypt removable devices such as USB keys.

On the other hand, to encrypt removable devices, you can use the **Removable Device Encryption** feature in StormShield.
For more information, see "Removable device encryption", page 355.

Before using the Data Encryption feature, you must save all your data.

If the encrypted hard disk includes one or several defective sectors, encryption will be interrupted and all data already encrypted will be decrypted again.

It is recommended to perform a deep scandisk and repair defective sectors before applying Full Disk Encryption.

Just after applying a Full Disk Encryption policy, downgraded performance can be observed when opening a session after startup.

This is absolutely normal due to the fact that encryption starts very early before the opening screen is actually displayed.

Furthermore, the agent has to connect to StormShield server in order to deploy Full Disk Encryption.

Full Disk Encryption or decryption cannot be interrupted once started.

ENCRYPTION TYPES

There are two types of encryption in StormShield:

- File encryption.
- Full disk encryption.

FILE ENCRYPTION

File Encryption characteristics are the following:

- Only file content is encrypted.
- The file list is defined by the Administrator.
- The system and programs remain unencrypted.

The **advantages** of File Encryption are the following:

- Each file is usually encrypted with a separate encryption key.
- Individual management of encrypted files.
- The Administrator can modify which files to encrypt.
- When a workstation is in multi-user mode, each user has a unique password for authentication.

The **disadvantages** of File Encryption are the following:

- The Administrator may forget to select important data that need to be encrypted.
- Users may save data in unencrypted folders.
- Less performance than Full Disk Encryption.

FULL DISK ENCRYPTION

Full Disk Encryption is used to encrypt everything on a specific disk partition.

When defining or typing the encryption password, follow these guidelines:

- do not use the Caps Lock key (use Shift).
- do not use the numeric keypad (use the numbers at the top of the keypad).

The **advantages** of Full Disk Encryption are the following:

- Everything is encrypted even computer configuration.

  This is a major advantage when the administrator forgets to encrypt some files.

  This becomes even more important when the administrator wants to encrypt sensitive configuration files or data which are directly stored by software into program directories.

- Full Disk Encryption deployment is easier than File Encryption deployment.

The **disadvantages** of Full Disk Encryption are the following:

- There is only one encryption password shared by all users of the computer.
- Full Disk Encryption deployment may take longer than File Encryption deployment depending on disk size.
- Only the hard disk on which the system has been installed is encrypted. If you want to encrypt documents present on another hard disk, you have to use both Full Disk Encryption and File Encryption (under General Settings > Protection mode).

  Only File Encryption will be applied to the second hard disk.

CREATING AN ENCRYPTION POLICY

GRAPHICAL INTERFACE

Encryption policies are located in the **Environment Manager** panel.

As for other policies, you can create encryption policies:

- On a global basis, that is encryption policies applicable to any environment.
- On a local basis, that is encryption policies dedicated to a single environment.

PROCEDURE

To create an encryption policy, follow the steps below:

1. In the Encryption Policy Editor, right-click in the **Encryption** column.

2. Select **Add** from the drop-down menu or click directly the Add icon in the toolbar.
3. Enter a name for the policy and click **OK**.

4. Specify the encryption parameters.

   For more information, see:

   - "File Encryption Parameters", page 462.
   - "Full Disk Encryption Parameters", page 474.

5. Apply the encryption policy to an agent group.

   For more information, see "Applying an encryption policy to an agent group", page 480.

6. Send the configuration to the server.

When you apply a new encryption policy to an agent group, the policy will not take effect until next reboot of the agent computer.

FILE ENCRYPTION FEATURES

MULTI-USER SECURITY

StormShield uses two types of encryption keys: a computer key and a user key.

Each computer has only one computer key but multiple user keys. This enables users to share computers and still maintain privacy and data confidentiality.

Computer encryption key

Folders and files which are encrypted with the computer encryption key can be opened by any authorized user.

User encryption key

After applying an encryption policy, folders and files which are encrypted with a user encryption key can only be opened by the first user who created or accessed the file/folder.

For more information, see "Computer encryption key", page 469 and "User encryption key", page 470.

DATA ERASURE SECURITY

Providing secure file erasure implies overwriting deleted files to prevent data recovery (especially by unauthorized users). This is highly important when a laptop has been stolen or left unattended.

You can select the number of overwrites to perform for data erasure.

Professionals can retrieve information from almost any magnetic data carrier, even damaged ones.
To delete a file permanently, the secure data erasure process performs several random data overwrites where the deleted file was stored.
Secure data erasure uses shredding methods to delete files permanently.
Shredding is currently the only method which is valid to obliterate securely data on your disk.

It makes it almost impossible to retrieve data via magnetic remanence.

FILE ENCRYPTION OPTIONS

There are two file encryption options:

- Encrypt files by their extension.
- Encrypt folders.

The administrator can encrypt files by their extension or using a wildcard *****.

Here are some examples of wildcard use:

- c:*
- *\crypt*
- c:*.txt
- c:\fichier.txt
- |userprofile|*

You can also exempt files and/or folders from encryption.

For more information, see "Encrypted zones", page 467 and "Unencrypted zones", page 472.

PASSWORD CREATION AND USER LOGON

Password creation

The first time the user logs onto the computer after the encryption policy is applied, he is prompted to create an authentication password or a PIN code depending on the type of authentication selected (Windows, Secondary or Smart-Card).

This authentication password becomes the encryption password to access protected data on the workstation.

If a user is in the process of creating a new password and the Agent loses its connection to the server before the password is confirmed, the following error message is displayed:

```
You are not connected to the server
```

If you apply a **file encryption** policy just after installing the StormShield agent, a popup window prompts the user to create his password.
An error message is displayed if the agent computer was not rebooted before creating the user password.

Reboot the computer in order to fix the problem and create the user password.

Create password prompt

The same password window is displayed to new users and users who already have passwords.

This is because a user may already have an existing encryption password on another computer.

Another situation may be that an encryption password already exists for the user and the StormShield agent has been uninstalled and re-installed on his computer.

If the user already has an encryption password, this password should be entered in both the **New password** and **Confirm password** fields.

Connection

If a user tries to log on with an incorrect password, an error message is displayed.

After five unsuccessful logon attempts, the user will be blocked from logging on for 30 seconds.
If the first logon attempt after the 30-second wait fails, the user will automatically be blocked from logging on for another 30 seconds.

SYNCHRONIZATION

A synchronization with the hard disk is performed when a user logs on for the first time after an encryption policy has been applied.

Next time this user logs in, synchronization will occur only if the list of encrypted zones is modified.

Synchronization occurs when a user moves a folder or several files from an unencrypted zone to an encrypted zone.

Desynchronization occurs when a user moves a folder or several files from an encrypted zone to an unencrypted zone.

If an unauthenticated user created files in an encrypted zone, the files will remain unencrypted until the user makes an encryption authentication or performs a manual synchronization of the encrypted zone.

To authenticate, the user must right-click the StormShield Monitor icon and select **Authentication > Access to Protected Data**.

The first time the user logs in, he will fill in the following fields:

Unencrypted files will be encrypted on next authenticated access or when performing a manual synchronization of the encrypted zone using **Resynchronize encryption policy**.

Desynchronization

During desynchronization, the hard disk is restored to its original state and all files are decrypted.

Desynchronization occurs when:

- A folder is removed from the list of encrypted zones.
- The StormShield agent is updated when upgrading from versions 4.5, 4.6, 4.7 to version 4.8.
  For more information, see "Synchronization after upgrading", page 454.
- The encryption key type associated with a zone is modified.
- The StormShield agent is uninstalled and **Decrypt data at uninstallation** is enabled. Only files encrypted with a computer key are unencrypted. Files encrypted with a user key must be decrypted manually.

When an encryption policy is modified, encrypted folders which no longer feature in the encrypted zone list are desynchronized whereas the folders which are defined in the new encryption policy are synchronized.

Synchronization after upgrading

The first time a user logs in after upgrading StormShield, a desynchronization process is launched.

All files are then decrypted before the new encryption policy is applied. The synchronization process proceeds as usual.

Desynchronization occurs when upgrading from version 4.5, 4.6 or 4.7 to version 4.8.

For agents, it is necessary to first upgrade from versions 4.5, 4.6 and 4.7 to version 4.8 before upgrading to a higher version.

Under Environment Manager > [Master server] > Encryption, make sure that:

- The **Start date of allow uninstall**,
- The **End date of allow uninstall**,

in the Environment Manager panel cover the appropriate time period, otherwise desynchronization will not occur.

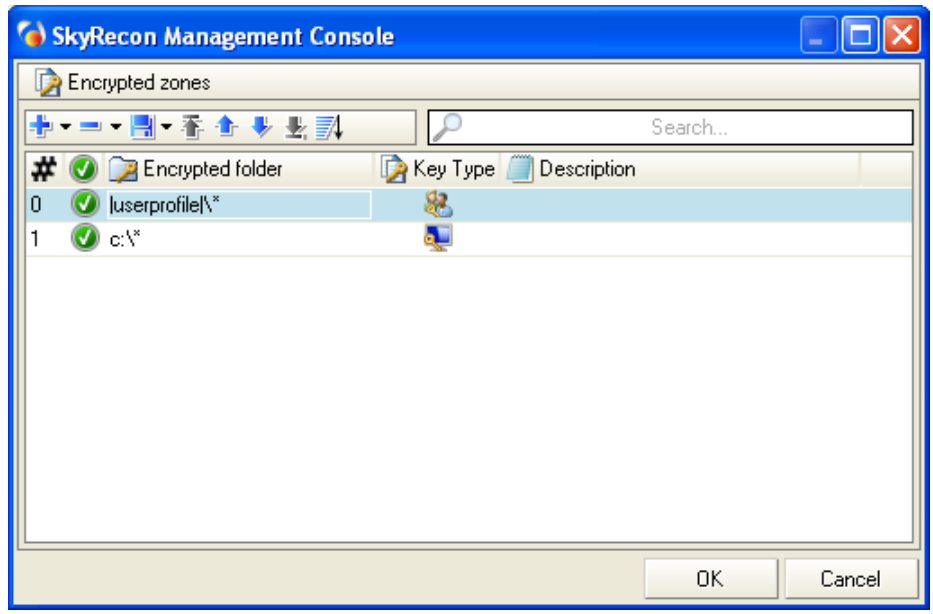
SYNCHRONIZATION WITH MULTIPLE USERS

If a computer has multiple users, encrypted files are resynchronized whenever a new user logs on for the first time.

Encrypted files are resynchronized with the encryption key type associated with each new user.

To illustrate this, consider the following example. Two users share the same computer. Each user has a specific user profile.

To display the window below, go to **Encryption Policies > File Encryption Parameters > Encrypted zones**.



The encryption policy is defined as follows:

- The user encryption key is applied to folder `|userprofile|\*`
- The computer encryption key is applied to `C:\*`

The encrypted zone with the most generic path should always appear **last** in the encrypted zone list so that the more specific rules are applied **first**.

Unencrypted zone rules have priority over other encryption rules.

First synchronization

For example, Craig is the first user to log on. His user profile is:

```
userprofile = c:\Documents and Settings\craig
```

The synchronization process encrypts:

- With Craig's **user key** all files stored in:

  `c:\Documents and Settings\craig`

- With the **computer key** all files stored on drive `C:\` except:
  - The folders defined in the Unencrypted zones option (if any).
  - `c:\Documents and Settings\craig`
  - See Appendix "Files Exempted from Encryption", page 697.

Subsequent synchronizations

A new user, Lucy, logs on. Her user profile is:

```
userprofile = c:\Documents and Settings\lucy
```

A new synchronization process is now launched.

The files stored in `c:\Documents and Settings\lucy` were previously encrypted with the computer key on first synchronization.

This new synchronization process will remove the computer key and re-encrypt the files with Lucy's user key.

Even if some users allow other users to access their files with ACL on the New Technology File System (NTFS), access to files encrypted with user keys will be denied to the latter.

ENCRYPTION PARAMETERS

GENERAL SETTINGS

General Settings enable you to set a number of commands and options such as:

- Protection mode.
- Authorize creation of encrypted archives.
- Authorize secure erasing of files.
- Number of secure erase cycles.
- Erase swap file when machine is stopped.
- Minimum characters required for second authentication password.
- Mandatory password strength.
- Encryption key size.
- Enforce encryption policy.
- Password change enforcement.

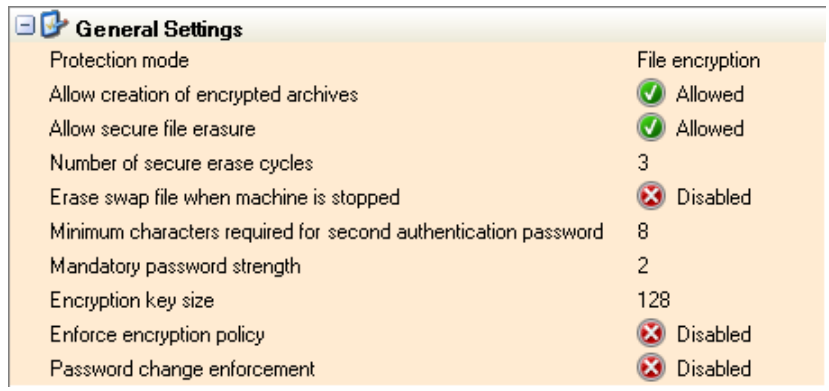


Fig. 13.1: Encryption: General Settings

Protection mode

The protection mode can be set to:

- File encryption.
- Full disk encryption.
- Full disk encryption and file encryption.

File encryption

If the protection mode is set to File encryption:

- **Full Disk Encryption Parameters** are disabled.
- The **Skip System Partition** option (below File Encryption Parameters) is disabled.

Full disk encryption

If the protection mode is set to Full disk encryption, **File Encryption Parameters** are disabled.

Full disk encryption and file encryption

If the protection mode is set to Full disk encryption and file encryption, all other commands and options are enabled and can be modified.

The administrator **cannot** change directly the protection mode from File encryption to Full disk encryption.
The user must first unencrypt all encrypted files.
This can be achieved by using:

- Either a recovery process.
- Or a file encryption policy without encrypted data or zones which would force desynchronization.

Allow creation of encrypted archives

This option allows StormShield Agent users to create their own encrypted files which they can safely send by email to other users, inside or outside the company network, without the risk of their contents being read in transit over the internet.

In the Encryption Policy Editor, when **Authorize creation of encrypted archives** is set to **Allowed**, the Agent user can right-click on the file/folder to display the Encryption options in the pop-up menu.

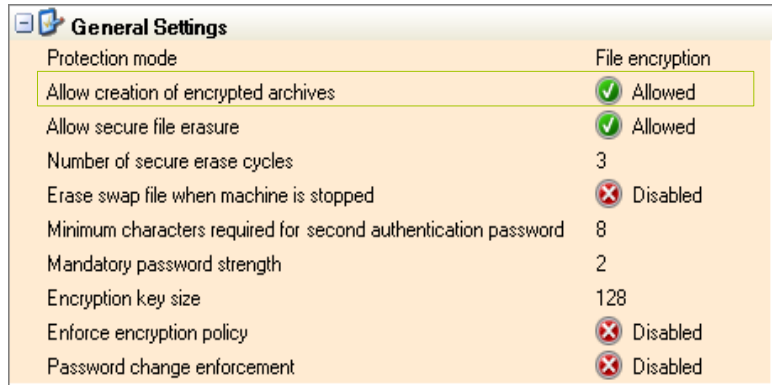


Fig. 13.2: Authorize creation of encrypted archives

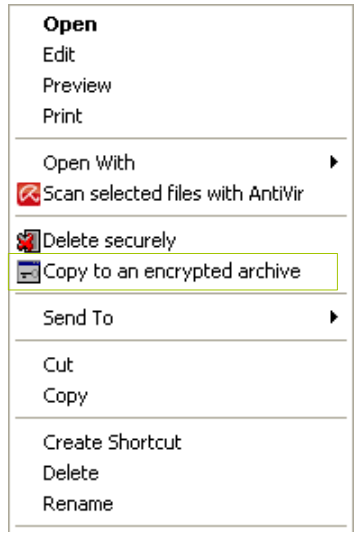


Fig. 13.3: StormShield Agent menu used to encrypt a file/folder (workstation)

For more information on encrypted files and archives, see "SURT", page 509.

Allow secure file erasure

When this option is enabled, StormShield Agent users can erase their files securely.

Files are overwritten the number of times specified in **Number of secure erase cycles** in General Settings.

When this option is disabled, it is no longer displayed in the menu. The user cannot select the **Delete securely** option.

Number of secure erase cycles

This option indicates the number of erase cycles to be performed to delete securely files and folders.

The files marked deleted are overwritten the number of times specified in **Number of secure erase cycles** in General Settings.

By default, the value is **3**.

You can set the number of cycles higher but it will increase the time it takes to erase files/folders, which can a problem with bulky files/ folders.

Erase swap file when machine is stopped

This option ensures that the swap file is completely erased whenever the computer is stopped.

Minimum characters required for second authentication password

This is the minimum number of characters that the user requires to create the password for protected data encryption and decryption.

By default, the value is **8**.

This option can be modified only when the authentication type is set to **Secondary**.

Mandatory password strength

The administrator can define the minimum strength a password should have. The password strength ranges from 1 to 5 (5 being the maximum level).

When the user defines his password, StormShield performs a real-time evaluation of the strength of the password which has just been keyed in. If the strength is lower than that defined by the administrator, the password is rejected.

Password strength evaluation is based on an entropy coefficient of the characters used. The following formula is used:

```
Coefficient = (log base 2 (range of the characters used) *
(password size)
```

A malus is then applied to the entropy coefficient if any repetition is detected in the password entered.

When using Full disk encryption, the number of password entry attempts on computer startup is limited to 10.

When exceeding 10 attempts, it is necessary to start the computer again.

Encryption key size

The administrator can set the encryption key size to:

- 128 bits.
- 192 bits.
- 256 bits.

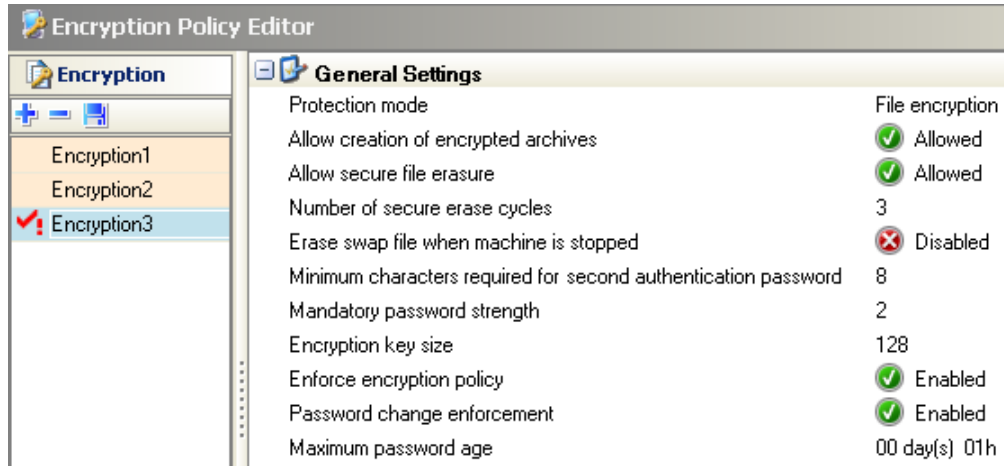
Enforce encryption policy

The option is set by default to **Disabled**. If the administrator enables this option, it will prevent the user from closing the password prompt window when opening the session.

Enforce password policy

The option is set by default to **Disabled**. If the administrator enables this option, it will recommend the user to change his password. If the user does not change his password, the old password will remain valid.

When this option is enabled, the **Maximum password age** field is displayed.



FILE ENCRYPTION PARAMETERS

File Encryption Parameters enable you to control the following parameters:

- Authentication type.
- Cryptographic Service Providers (CSP).
- Authorized to stop synchronization.
- Authentication after unlock session.
- Skip system partition (already encrypted at disk level).
- Force user authentication.
- Stealth mode.
- Encrypted zones.
- Encrypted file types.
- Unencrypted zones.

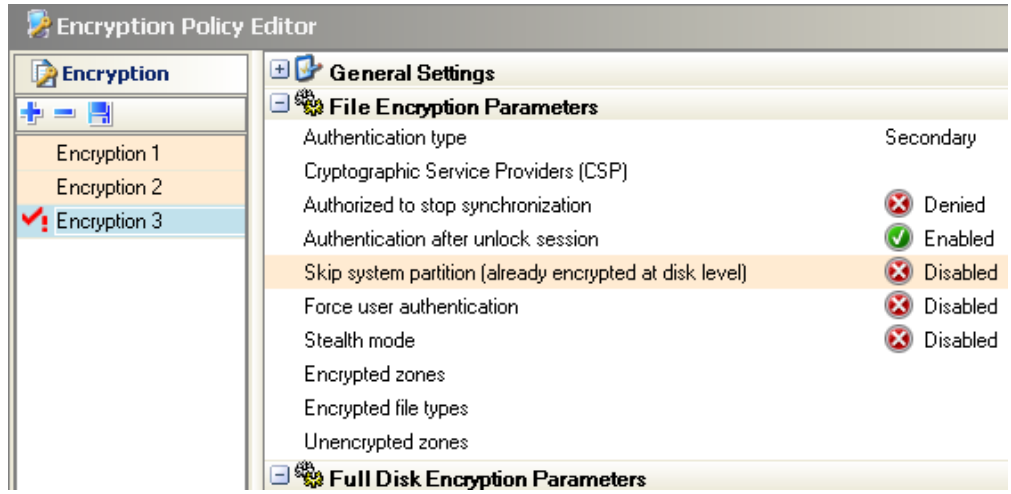


Fig. 13.4: File Encryption Parameters

Authentication type

An authentication type is defined for each encryption policy. Different authentication types can be applied to different agent groups.

There is only one authentication type per encryption policy.

After agent deployment, authentication types cannot be modified. Modifications must be performed manually by the administrator for each user.

For more information, see "Change authentication type", page 487.

The three authentication types are the following:

- Windows.
- Secondary.
- Smart-Card.

Fig. 13.5: File Encryption Parameters: Authentication type

Windows authentication type

This authentication type is based on Windows authentication. It is not as secure as Secondary or Smart-Card authentications.

The user can easily access encrypted files using this authentication type by simply logging into Windows using his Windows login ID and password.

Secondary authentication type

When starting for the first time the computer after an encryption policy has been applied, the user is prompted to create a secondary authentication password.

In addition to entering the Windows login password during startup, the user must also enter another password to access encrypted data stored on the hard disk.

Fig. 13.6: Secondary authentication password

It is highly recommended to create a secondary authentication password.

Smart-Card authentication type

The smart-card and the card reader must be connected to the computer in order to access encrypted data in the system.

After Windows startup, the user is prompted to enter a password to open encrypted files stored on the hard disk.

Usually, the password used for this authentication type is the PIN code supplied by the Smart-Card service provider.

Cryptographic Service Providers (CSP)

Cryptographic Service Providers are the Smart-Card manufacturers. The smart-cards provided by the CSP include a software that must be installed on the Agent's computer to allow use of Smart-Card authentication.

For user-friendly purposes, it is recommended to install the CSP on the computer where the SkyRecon Management Console has been installed to configure smart-card administrative tasks (**example**: change user smart-cards by simply choosing from the drop-down menu of the CSP parameter in the Encryption Policy Editor).

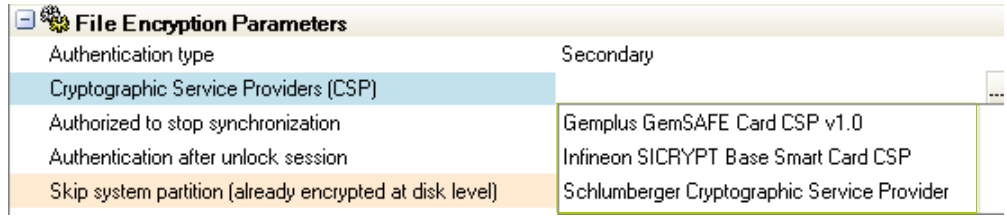


Fig. 13.7: Cryptographic Service Providers (CSP)

If the CSP is not installed on the StormShield server but on the Agent's computer, the administrator must enter the accurate name of the CSP by double-clicking on the field on the right.

This option can be set only when the authentication type is Smart-Card.
The names of the CSP installed are to be found in the registry under:
`HKLM\Software\Microsoft\Cryptography\Defaults\Provider`

The CSP name string must be exactly the same on the console and on the client workstations.

The three folders below are added by default to the files/folders exempted from encryption:

- `|userprofile|\application data\microsoft\crypto\*`
- `|userprofile|\application data\microsoft\systemcertificates\*`
- `|userprofile|\application data\microsoft\protect\*`

Depending on the CSP used, these folders can include cache data for smart-card certificates which must be readable by the system.

Authorized to stop synchronization

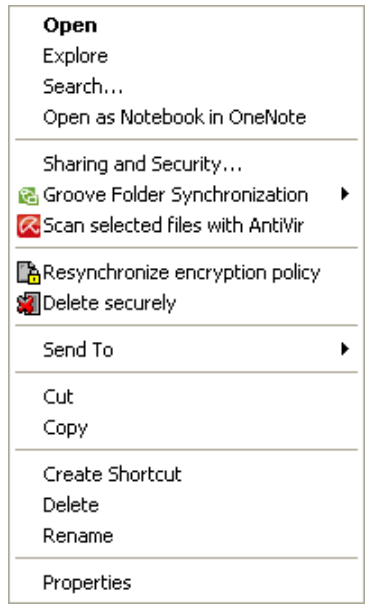
If data is updated in:

- Encrypted zones,
- Encrypted file types,
- Unencrypted zones,

then synchronization will be relaunched.

By default, this parameter is set to **Denied.** When set to **Allowed**, the user can stop the synchronization process.

To start resynchronization manually, use the right-click options on the folder to be resynchronized on the Agent's computer.



Authentication after unlock session

When this option is set to **Enabled**, it prevents flushing the encryption keys when the user session is locked.

It is useful for software which could crash when accessing encrypted files, while the user session is locked.

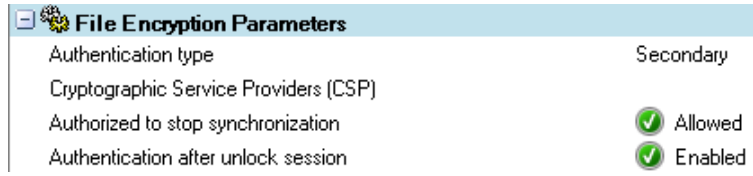


Fig. 13.8: Authentication after unlock session

On the other hand, if you want to **disable** this option, think about it twice. Indeed, there are some serious drawbacks to this action. For example, a hacker could steal the user encryption keys contained in the `hiberfil.sys` file by using the hibernate function in the operating system.

If a hacker breaks the session lock, encrypted files will be accessible without authentication (since encryption keys have not been flushed).

Skip system partition (already encrypted at disk level)

This option is enabled only when **Protection mode** is set to Full disk encryption and file encryption.

If the option is set to **Enabled**, the path `|systemdrive|` will be encrypted by Full disk encryption but will not be protected by File encryption.

If the option is set to **Disabled**, the path `|systemdrive|` will be protected by Full disk encryption.
If the path is also included in **Encrypted zones**, then it will be encrypted twice: by File encryption and by Full disk encryption.

Unencrypted zone rules have priority over other encryption rules.

Force user authentication

When this option is set to **Enabled**, the user is prompted to authenticate when opening a session so as to prevent him from creating unencrypted files.

Stealth mode

When this option is set to **Enabled**, file encryption is applied to the workstations but their users will not notice the encryption process in progress.

The agent will not display the following elements on the user's workstation:

- Right-click file encryption window.
- Encryption progress bar.
- Right-click menu (**Copy to an encrypted archive**).
- The lock icon  on encrypted files.

If the stealth mode is enabled, the administrator needs to set authentication mode to **Windows**.

Encrypted zones

This option is used to encrypt all the files in a folder. The administrator has to define the folders where the users will store their files in security.

The Administrator has to inform the users where they can store their files in security.

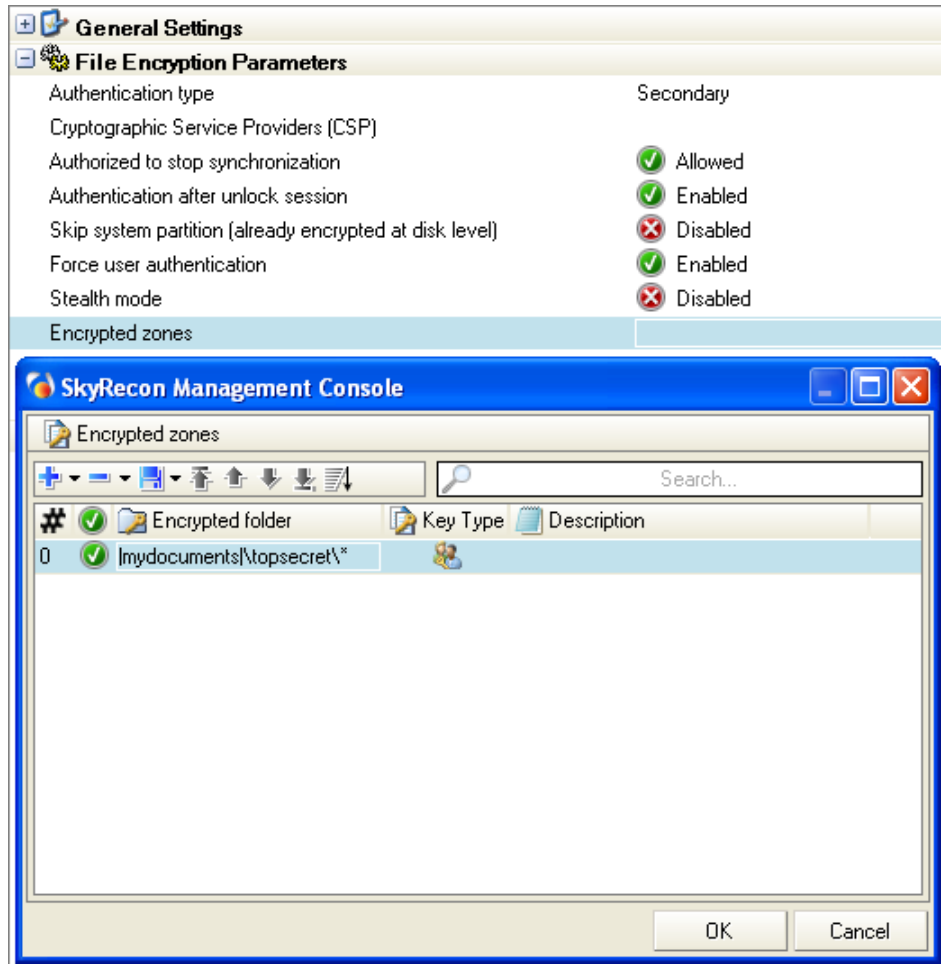


Fig. 13.9: Encrypted zones

The encrypted zone with the most generic path should always appear **last** in the list of **Encrypted zones** so that the more specific rules are applied **first**.

Unencrypted zone rules have priority over other encryption rules.

Environment variables

Environment variables make it easier to configure encrypted zones.

For example, you can enter `|userprofile|` to specify all individual user folders, rather than enter each individual folder one at a time.

Supported environment variables are the following:

- |username|
- |systemroot|
- |systemdrive|
- |programfiles|
- |userprofile|
- |mydocuments|

Environment variables, in particular |username| and |userprofile|, are dynamic. They change with each user session.

Let us consider the following situation:

- user1 logs on.
  The zone to be encrypted which is defined by the policy is:
  c:\documents and settings\user1
  (the environment variable is replaced by its value).
- user2 logs on after user1 on the same computer.
  The zone to be encrypted which is defined by the policy is:
  c:\documents and settings\user2
  and synchronization is launched.

If user2 is allowed to access **c:\documents and settings\user1** (provided that file system permissions are granted and files are encrypted with a computer key), decryption will take place.
To prevent this, the administrator must define a user key for these types of folders.

For more information on key types, see "Encrypted file types", page 470.

For more information, see "Environment variables", page 341.

Encryption key types

There are two encryption key types:

- The computer encryption key.
- The user encryption key.

Computer encryption key

The computer encryption key  is available to any user who has an encryption password for that particular computer.

This means that encrypted data is protected from theft and access by unauthorized users.

Each computer has only one computer key. The computer key is changed on every StormShield Agent installation so that each computer has a unique computer encryption key.

User encryption key

The user encryption key  is unique to the user.

This means that if a file is encrypted by user "A", only user "A" can access the file.

When the user logs on for the first time with a password, StormShield creates a unique user key. The user key is a combination of the computer key and the user key with the user password.

Here are three typical situations:

- **Files encrypted by one key**

  A file can be encrypted by only one key: a unique user key **or** the computer key.

- **User access to computer key**

  Each user is able to access the computer key with his own password. Actually, the user password is used both for computer and user encryption keys. This is invisible to the user.

- **File access denied**

  Access to encrypted files is denied when:

  - The file has been encrypted with the user key of another user.
  - No password authentication has been entered.
  - There are several user sessions on a computer under Windows Vista.
  - The StormShield agent is stopped.
  - The administrator has disabled the encryption policy whereas files are still encrypted.

Encrypted file types

This option is used to specify which files are to be encrypted based on their extensions.

Example: In order to encrypt and password protect Word documents, text files and Excel files, you could enter: `.doc; .txt; .rtf; .xls`.

Encrypted file types must be associated with a computer key or a user key.

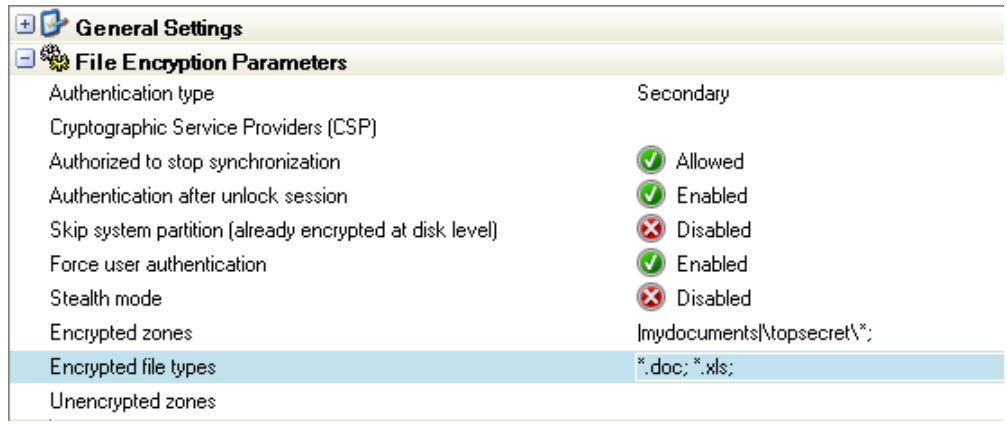
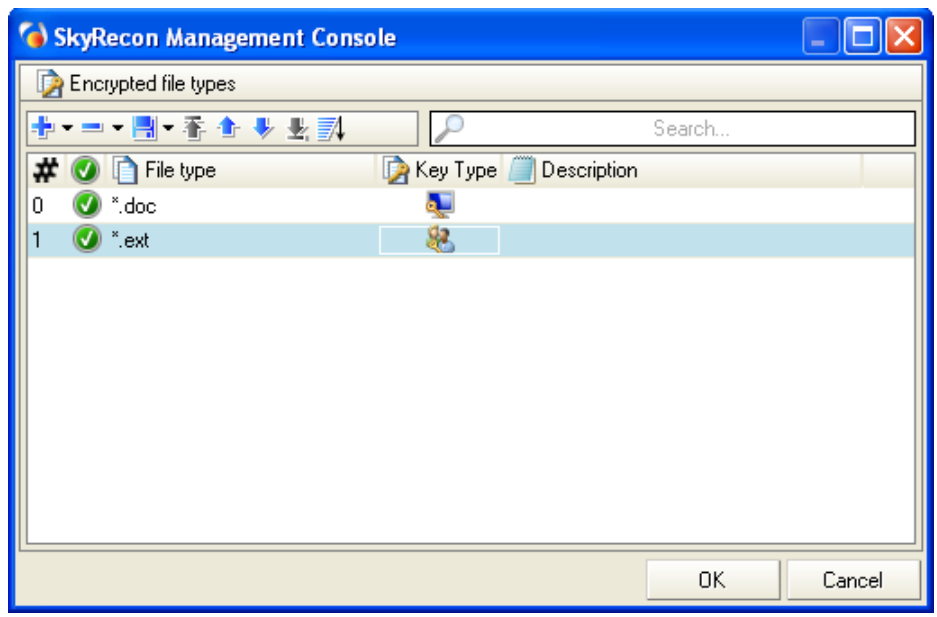


Fig. 13.10: Encrypted file types

Encrypted file types must be associated with a computer key or a user key.



Unencrypted zones

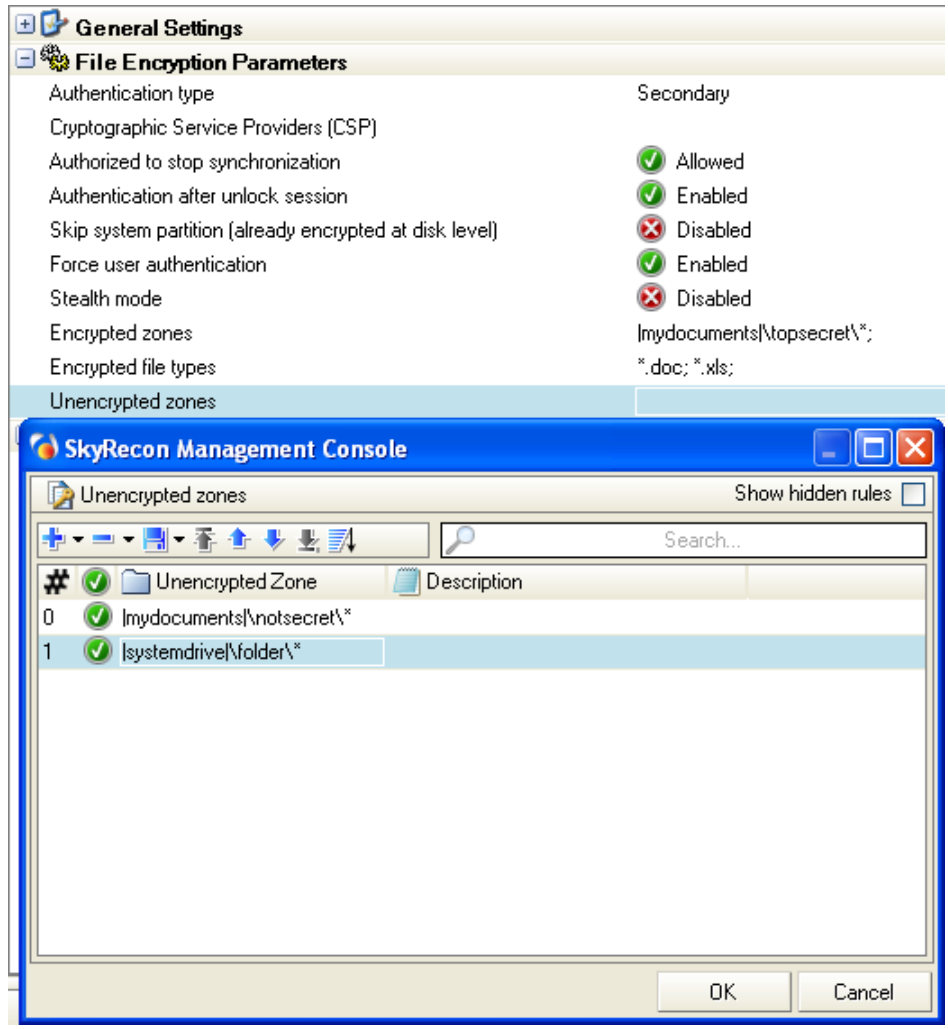


Fig. 13.11: Unencrypted zones

Unencrypted files

For each unencrypted zone, enter the pathname and folder name so that the files within that folder will not be encrypted.

If you check the **Show hidden rules** box in the pop-up window, you will display a sample of predefined rules.

Unencryptable files

Important applications that are initialized during computer start-up are not encrypted, namely:

- Windows Operating System files.
- System Volume Information.
- StormShield.

For more information, see Appendix "Files Exempted from Encryption", page 697.

The following must also be exempted from encryption:

- **Any system file loaded during Windows startup.**
  Since files can be decrypted only after the user logs on, all files used during the boot-up sequence by services, drivers or the operating system must not be encrypted. This includes the desktop manager file currently selected.
- **Roaming profiles.**
  Access to encrypted files is denied until after encryption password authentication. Since Windows synchronization occurs before authentication, the roaming profile would still be encrypted and Windows synchronization would fail.

FULL DISK ENCRYPTION PARAMETERS

Full Disk Encryption Parameters enable you to control full disk encryption protection by modifying the settings in:

- Partition encryption.
- Block-cipher mode of operation.
- Secure shredding before encryption.
- Number of secure erase cycles.
- Allow automatic restart.
- Single Sign-On (SSO).
- One-time recovery password.
- Use guest account.

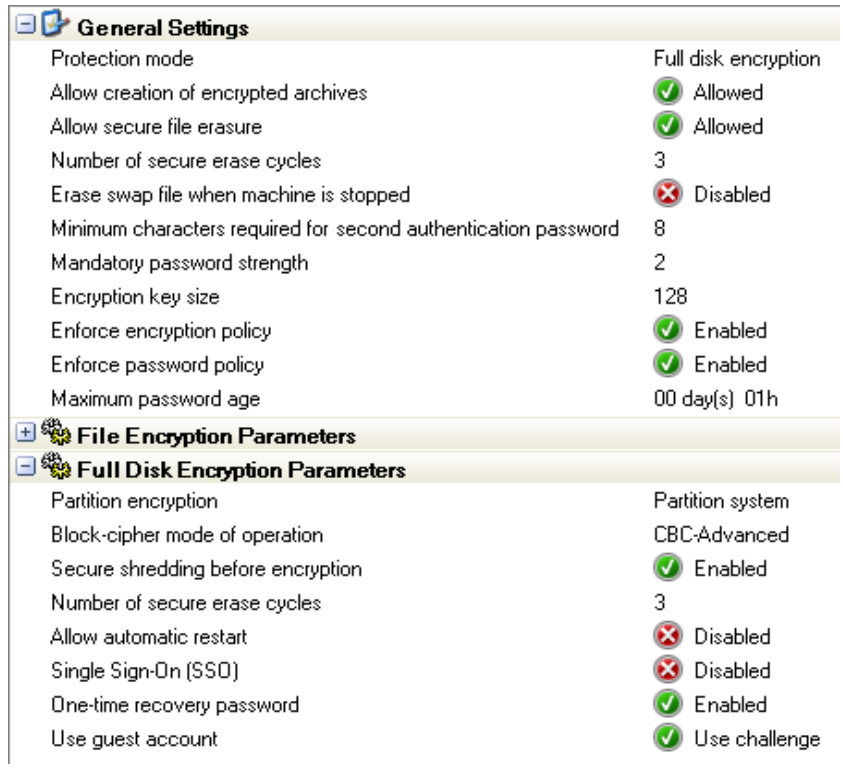


Fig. 13.12: Full Disk Encryption Parameters

Partition encryption

This option includes the following:

- **System partition**

  Only the system partition where the operating system of the computer is installed is encrypted.

- **All partitions**

  All the partitions on the hard disk on which StormShield is installed are encrypted. Only master partitions are supported.

Block-cipher mode of operation

This option runs on blocks with a fixed length of 128 bits.

Since messages may be of any length and encrypting the same plaintext by the same key usually generates the same output, various operating modes have been created.

These operating modes permit block ciphering to ensure confidentiality for messages whatever their length.

This option can be set to:

- **CBC (Cipher Block Chaining)**

  CBC is the most frequently used mode. Its main drawback is that encryption is sequential (the encrypted output of previous block is transmitted to next block) with no capability for parallel processing. Therefore the message must be stretched to a multiple of the cipher block size.

  StormShield uses CBC with 128-bit blocks for each 512-bit sector of the disk.

- **CBC Advanced**

  Same as CBC mode except for including certain algorithmic rules such as complexity levels. For each encrypted block, an Advanced Encryption Standard (AES) key is dynamically generated to prevent cryptanalysis.

Secure shredding before encryption

When this option is enabled, the disk is securely erased before the encryption process.

Number of secure erase cycles

This option is the number of erase cycles performed to ensure a complete erasure. The blocks on the disk are overwritten by the number of times set, with random data before encryption.

The more the number of erase cycles, the longer the synchronization.

Allow automatic restart

Console

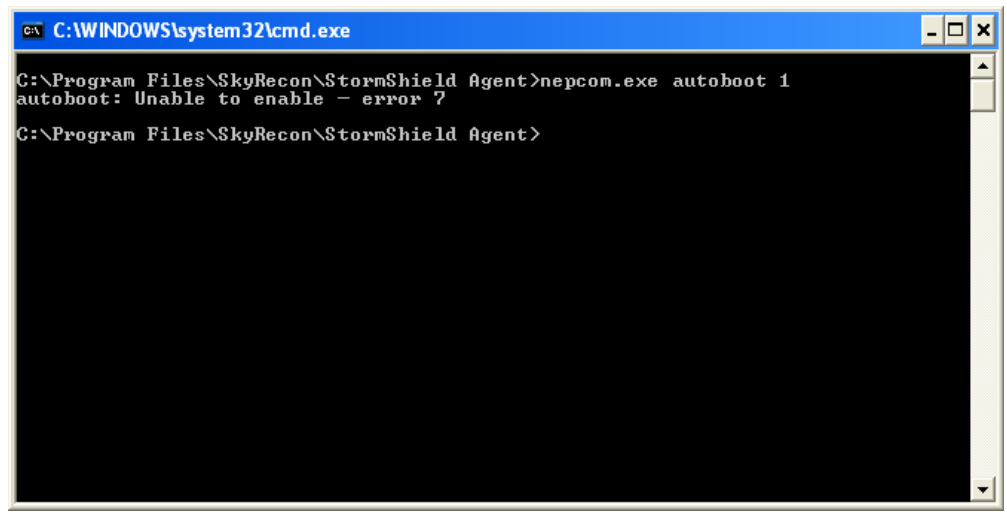
This option allows automatic restart for remote maintenance without using encryption passwords.
After disabling StormShield's bootloader, the administrator will reboot manually or via a script.
See Table "Built-in action definitions", page 410, line "Enables/Disables automatic restart (without compulsory password entry) for full disk encryption.", page 412.

Agent

On the StormShield Agent, the administrator may allow a predefined number of automatic restarts via `nepcom.exe`.

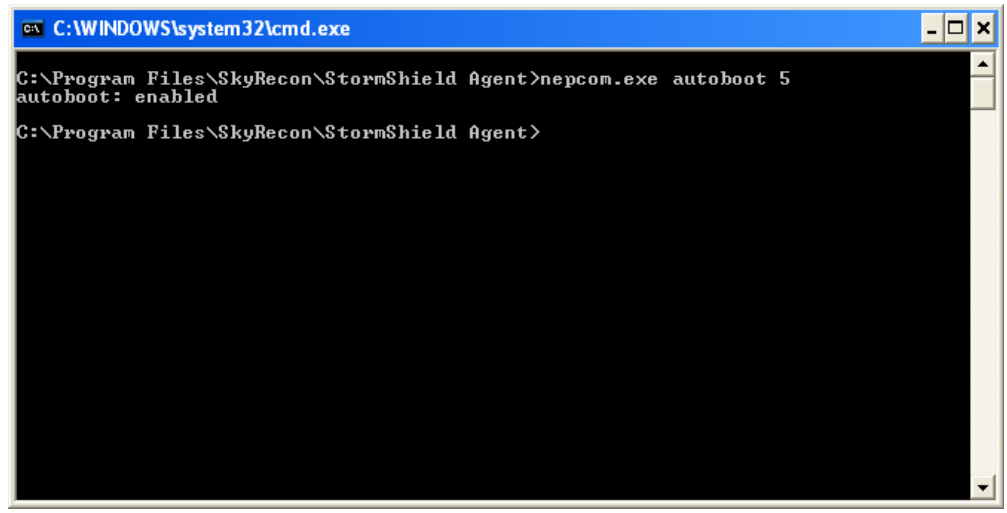
Prerequisites

To allow automatic restarts on the StormShield Agent, you should enable **Allow automatic restart** on the console.
Otherwise, you will not be able to use `nepcom.exe` and the "`Unable to enable`" message will be displayed.



Procedure

To allow automatic restarts on the StormShield Agent, follow the steps below:

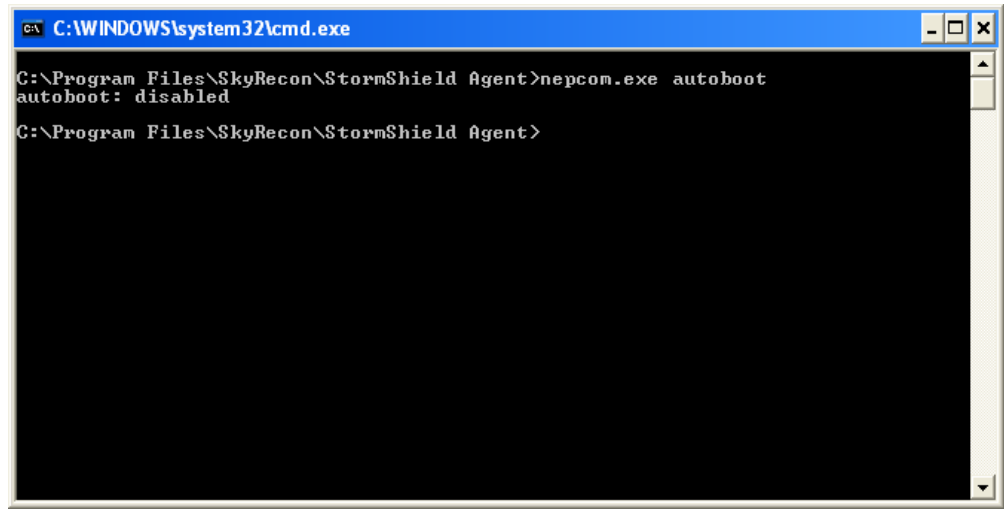


1. Open a command prompt window.
2. Go to the StormShield Agent directory.
3. Enter the following command:

   `nepcom.exe autoboot [number of automatic restarts allowed]`

   To check that the command has been enabled, the "`enabled`" message is displayed.

To disallow automatic restarts on the StormShield Agent, follow the steps below:



1. Open a command prompt window.
2. Go to the StormShield Agent directory.

3. Enter the following command:

   `nepcom.exe autoboot`

   To check that the command has been enabled, the "`disabled`" message is displayed.

Single Sign-On (SSO)

This option is used to combine two authentifications (Encryption+Windows) for the main user.

When the user authenticates himself/herself for the first time with his/her login and Windows password via StormShield's authentication service, user authentication information will be encrypted with the encryption key and stored on the agent.

From now on, the user will **no longer** need to enter his/her login **or** Windows password as the agent has decrypted and sent this information to StormShield's authentication service. The service will at present fill in automatically Windows account authentication details.

If the user changes his Windows password, he will follow the steps below:

- The user will proceed as usual under Windows in order to change his password.
- He/She will reboot his machine.
- He/She will enter his new Windows password when opening a new session so that StormShield will encrypt and store at agent level his new user password.

If the user directly clicks **OK** (or enter his old password), the authentification process will be blocked. The window will indicate to the user that he must enter his new Windows password.

On next session, the user will no longer need to enter his/her login or Windows password.

One-time recovery password

When the user authenticates with his recovery password, this option generates a new recovery password on next login.

Use guest account

This option is enabled by default. It is designed to create a temporary guest account. The guest account makes it possible to authenticate on the workstation without using the main user account.

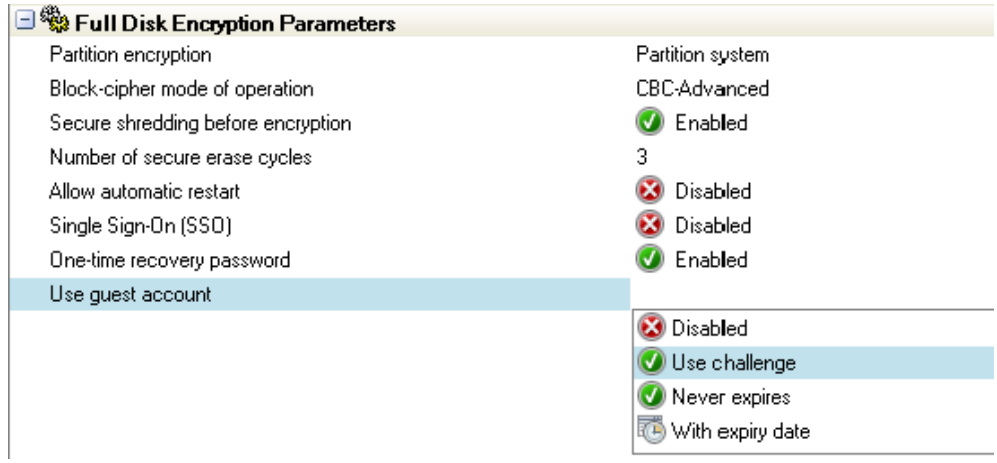
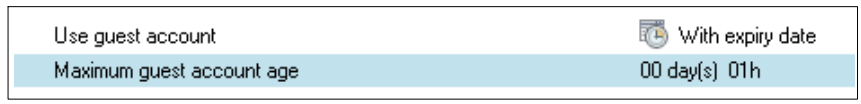


Fig. 13.13: Use guest account

Available options are the following:

- Disabled.
- Use challenge.
- Never expires.
- With expiry date.
  In this case, the administrator has to set the **Maximum guest account age**.



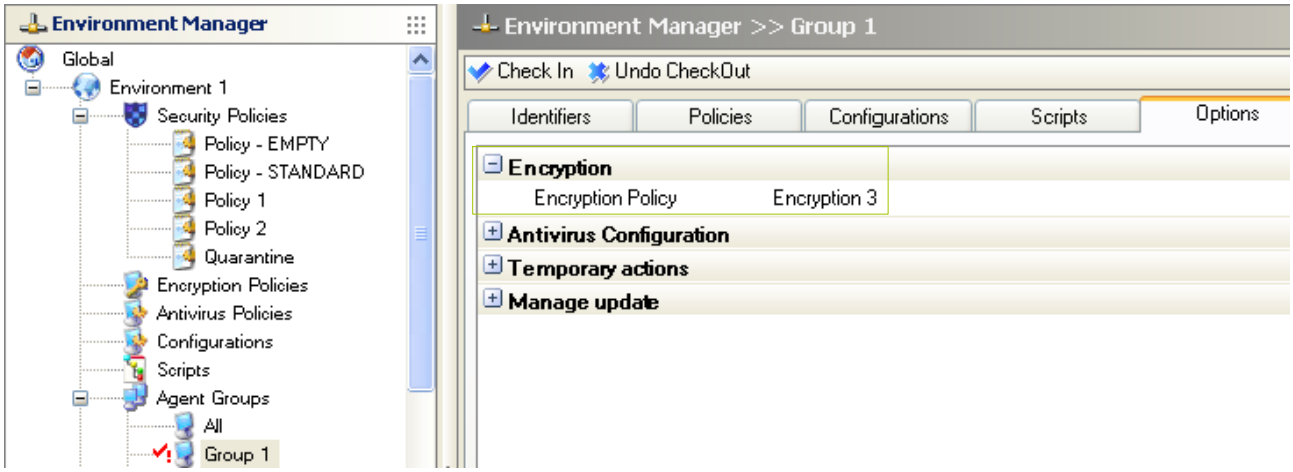
For more information on challenges, see "Temporary action scripts", page 427.

APPLYING AN ENCRYPTION POLICY TO AN AGENT GROUP

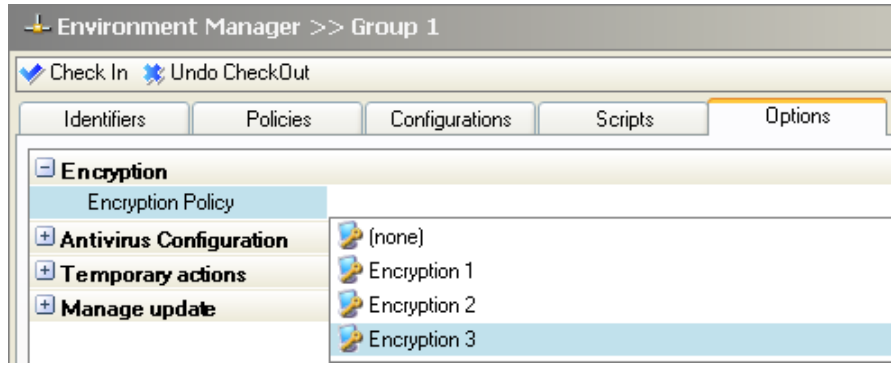
Encryption policies are applied to agent groups.

To apply an encryption policy to an agent group, follow the steps below:

1. Click **Agent Groups** in the Environment Manager panel.
2. Edit the appropriate agent group to know or modify its encryption policy.
3. Click the **Options** tab to display the encryption policy applied to the agent group.



4. To modify the encryption policy, click in the field column opposite **Encryption Policy** and then click the Browse button ....
   The drop-down list of existing encryption policies is displayed.



5. Select the encryption policy to be applied to the agent group.
6. Validate your modifications.
7. Synchronize.

RECOVERY

PASSWORD RECOVERY WHEN USING FILE ENCRYPTION

Agent side

Overview

When the user creates a password, a **backup password** is automatically generated.

To replace a lost password, the user may contact the administrator. The administrator locates the backup password and sends it to the user.

Once the backup password is located, the administrator can copy, paste and send it by email to the user. The user can paste it directly into the password field.

The backup password works in the same way as the regular password.

To help the administrator locate the user's backup password by his user ID instead of his User Name, the user can proceed as described further on in "Get IDs", page 481.

If Active Directory is not used, users working on different workstations can have the same **User Name** (example: administrator account), but **not** the same **User ID**.
To locate a user by his user ID, ask the user to email it to the administrator.

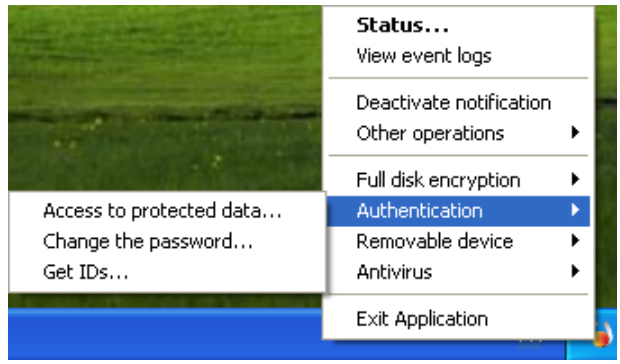
The **Domain** column only contains computer names.

Get IDs

To obtain his user ID from the StormShield Agent computer, the user must perform the steps below:

1. Right-click the StormShield Monitor icon  .

2. Select **Authentication > Get IDs**.



3. The user ID is displayed.
Copy the **User ID** number and email it to the administrator.

The user should change his backup password as soon as possible in order to use it as old password.

4. Paste the backup password sent by the administrator in the **Old password** field. Enter and confirm your new password.

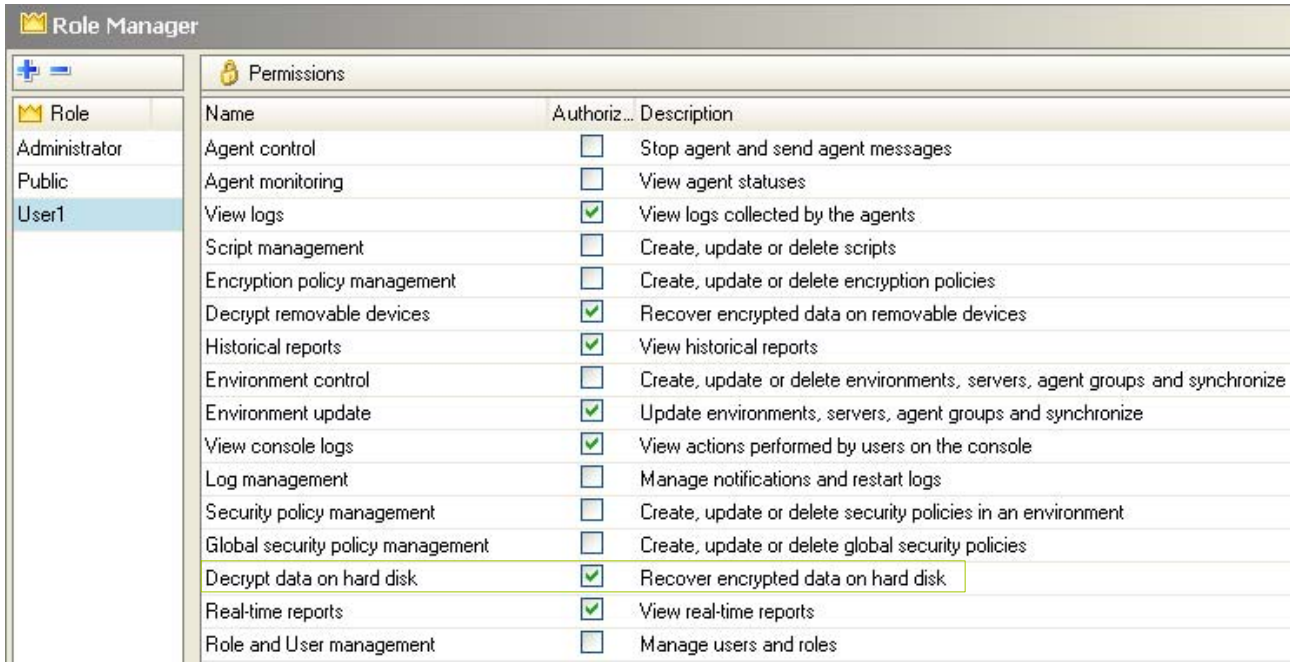
If the user creates a new password on one computer and goes to another computer using the same account, the user must enter the new password and not the backup password.

Administrator side

Prerequisites

In order that the administrator can search for backup passwords, **Role Manager > Permissions > Decrypt data on hard disk** must be set to **Authorized**.

The Role Manager is used to create the roles assigned to the SkyRecon console management users.

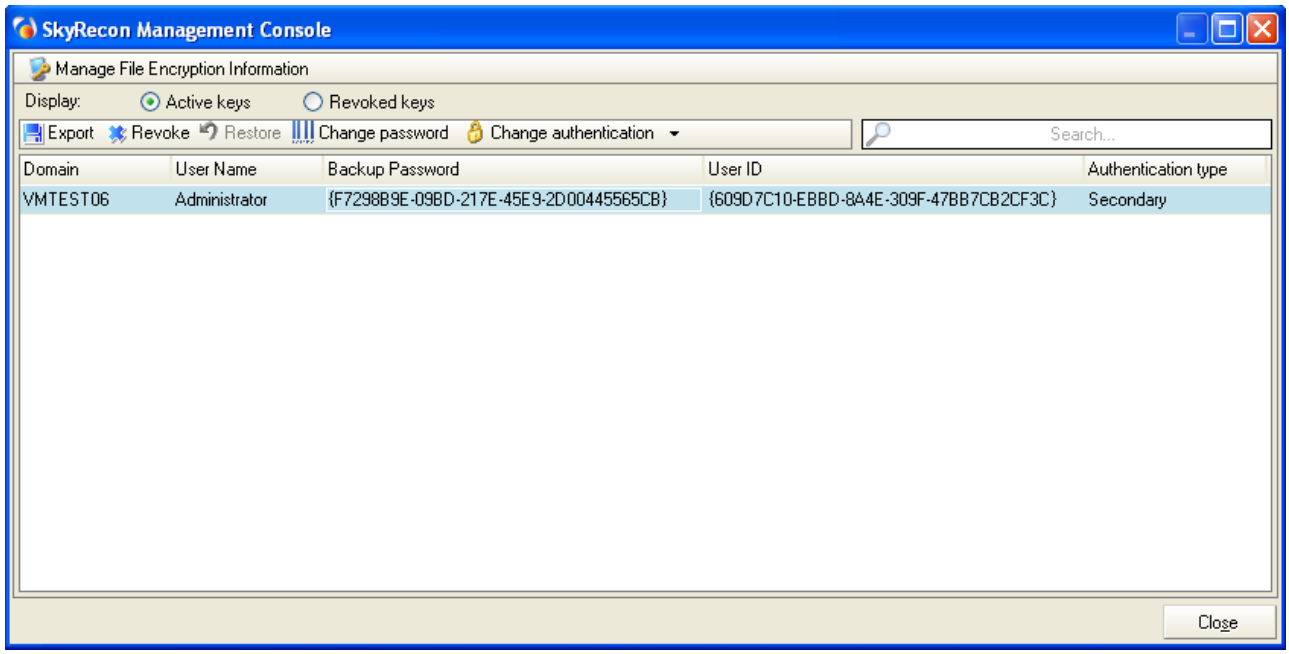


Backup password recovery

To recover the backup password, the administrator must perform the steps below:

1. Select **Encryption > Manage File Encryption Information**.

2. Enter the password for the console certificate.
   The **Manage File Encryption Information** window is displayed.



If you receive an error message, the console has not been correctly configured.

Check that console certificate paths are correct.

3. Locate the **User Name** in the list of **Active Keys**.
   For long lists, you can use the **Search** field to locate the user name quickly.
4. Send the **Backup Password** to the user.

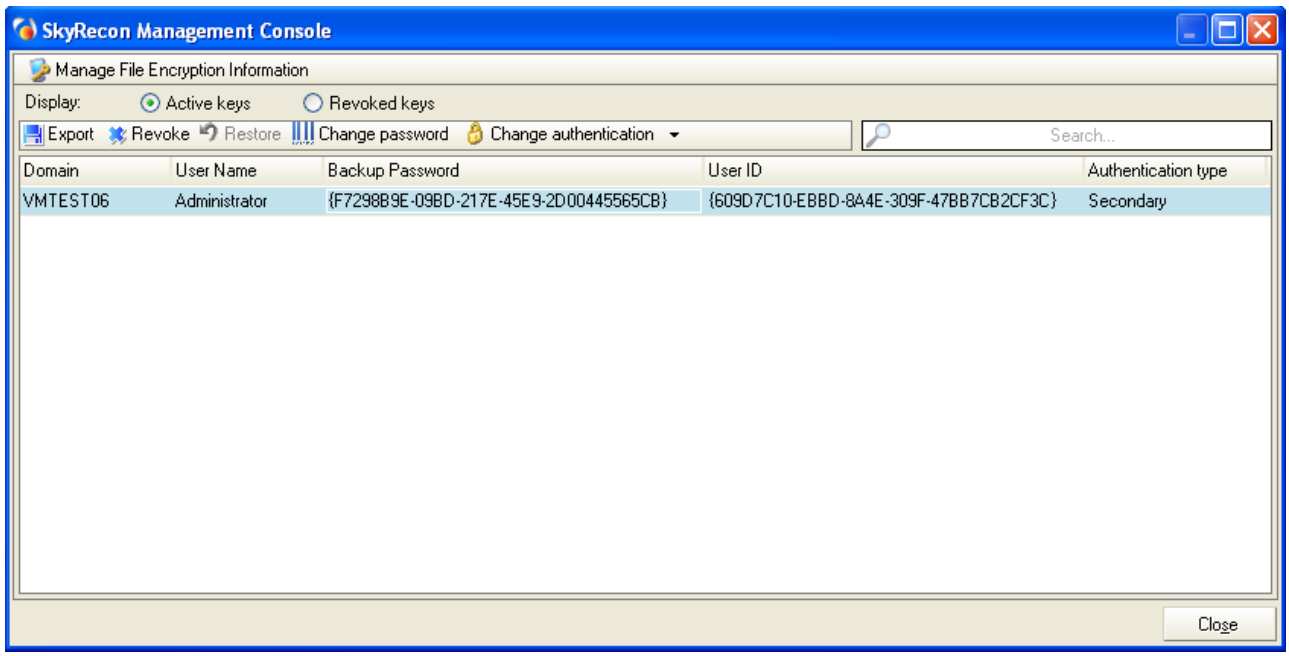
Change secondary authentication password

To change the secondary password used for encryption by the user, the administrator must follow the steps below:

1. Select **Change Password** under **Encryption > Manage File Encryption Information**.

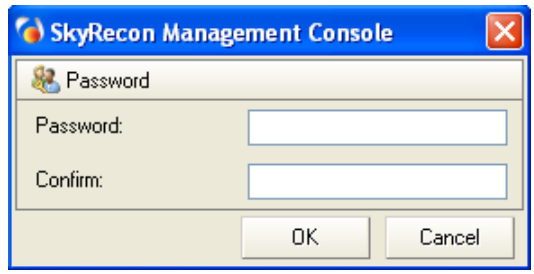
2. Enter the password for the console certificate.

   The **Manage File Encryption Information** window is displayed.



3. Select **Change Password**.

4. Enter and confirm the new password.



5. Click **OK**.

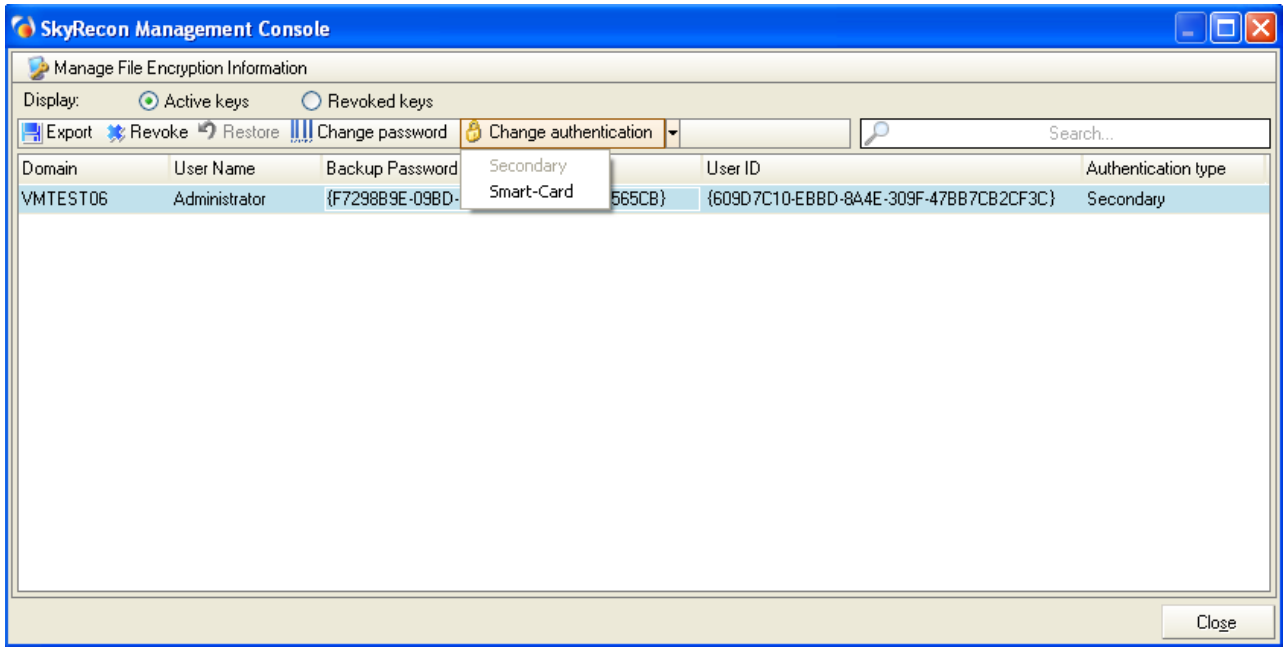
To activate the new password, the user must first log off from the system and then log in.
For the encryption process to take effect, the user must enter the new secondary authentication password after Windows startup.

The StormShield agent must be connected.

Change authentication type

To change the authentication type of the agent, the administrator must follow the steps below:

1. Click on the user name to highlight it.
2. Click **Change authentication** and select the authentication type from the drop-down menu.



The encryption policy assigned to the agent must be configured so as to have the same authentication type as the one defined for the user.

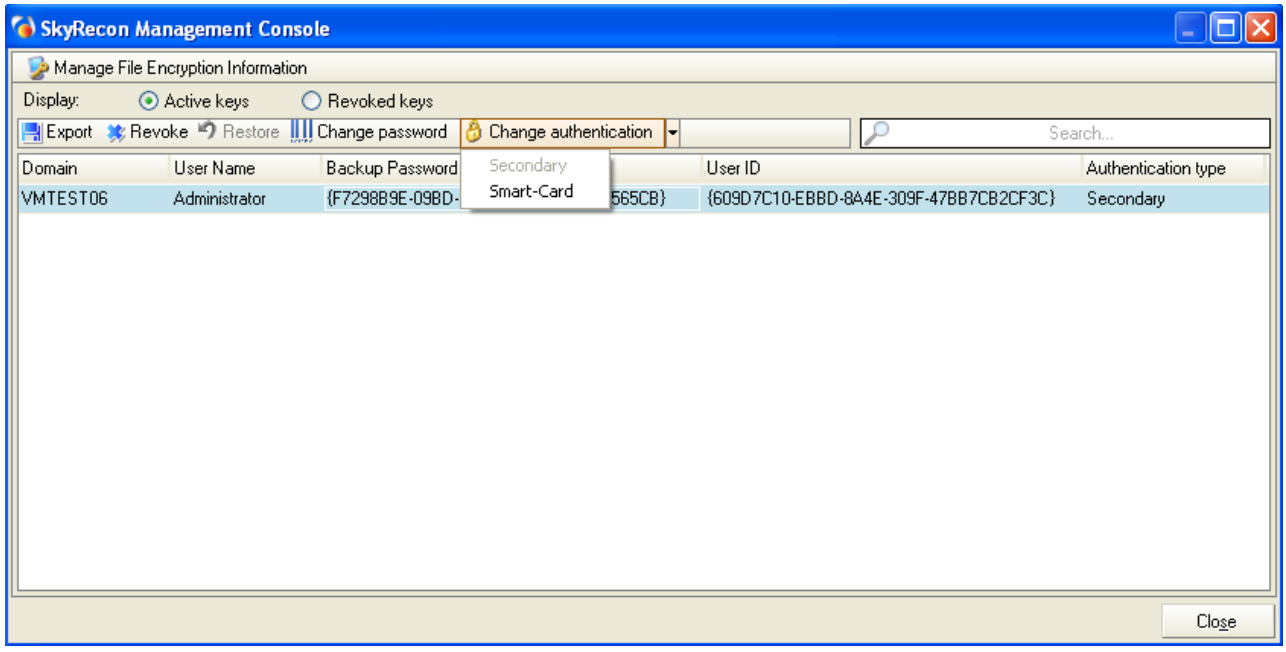
3. Enter required information.
4. Validate your modifications.
5. Synchronize.

After the StormShield agent reconnects to the server and receives new information, the user must log off and log on again to apply the new authentication type.

Change to Smart-Card authentication

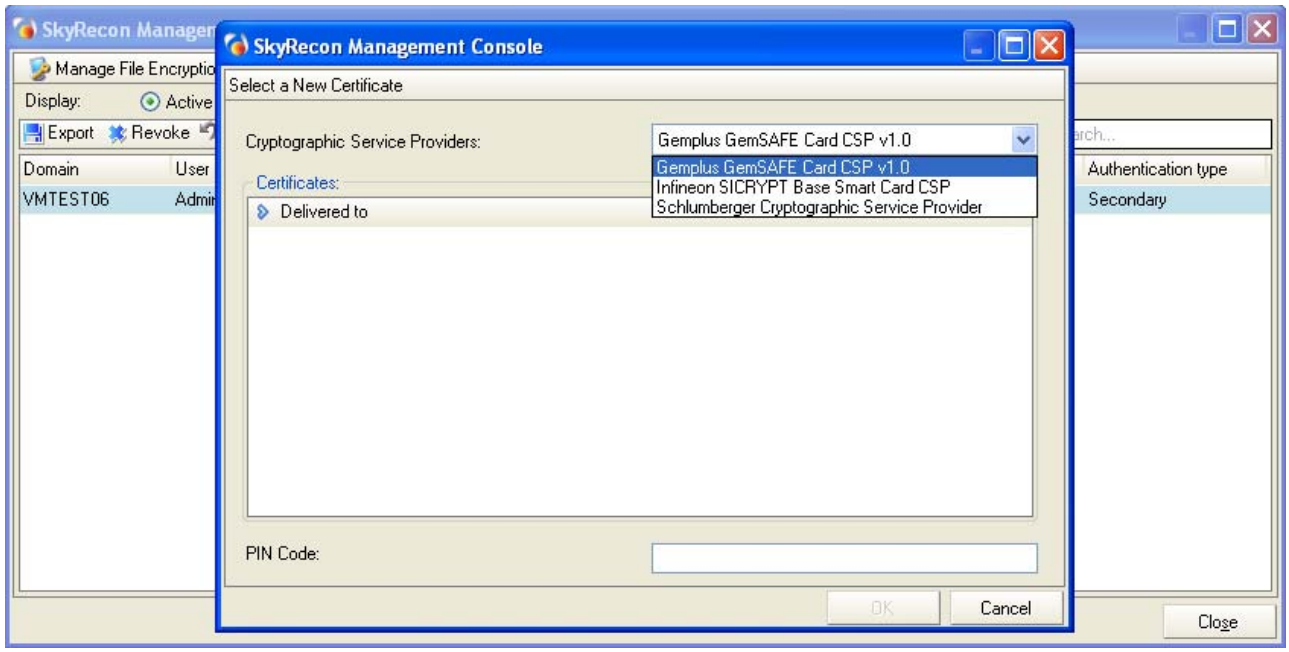
To change to Smart-Card authentication, the administrator must follow the steps below:

1. Click on the user name to highlight it.
2. Click **Change authentication** and select the **Smart-Card** type from the drop-down menu.



3. Specify the following settings:
   - Select the CSP.
   - Select the certificate.

- Enter the PIN code.



4. Click **OK**.
5. Synchronize.

After the StormShield agent reconnects to the server and receives new information, the user must log off and log on again to apply the new authentication type.

Upon login, StormShield prompts the user to insert the smart-card and enter the PIN code (provided by the CSP).

Revoking and restoring user keys

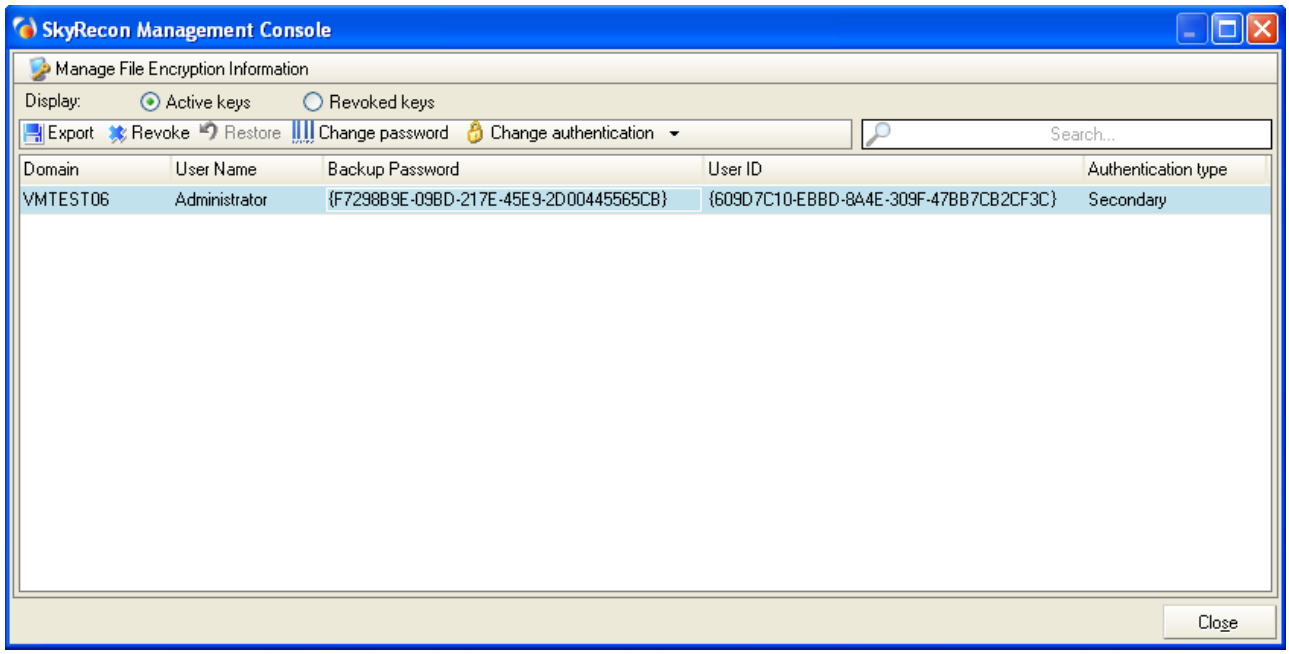
There are two types of user keys in **Manage File Encryption Information**:

- **Active keys**
  They are the keys belonging to active users who can authenticate themselves.
- **Revoked keys**
  They are the keys belonging to revoked users. The administrator can reactivate revoked keys.

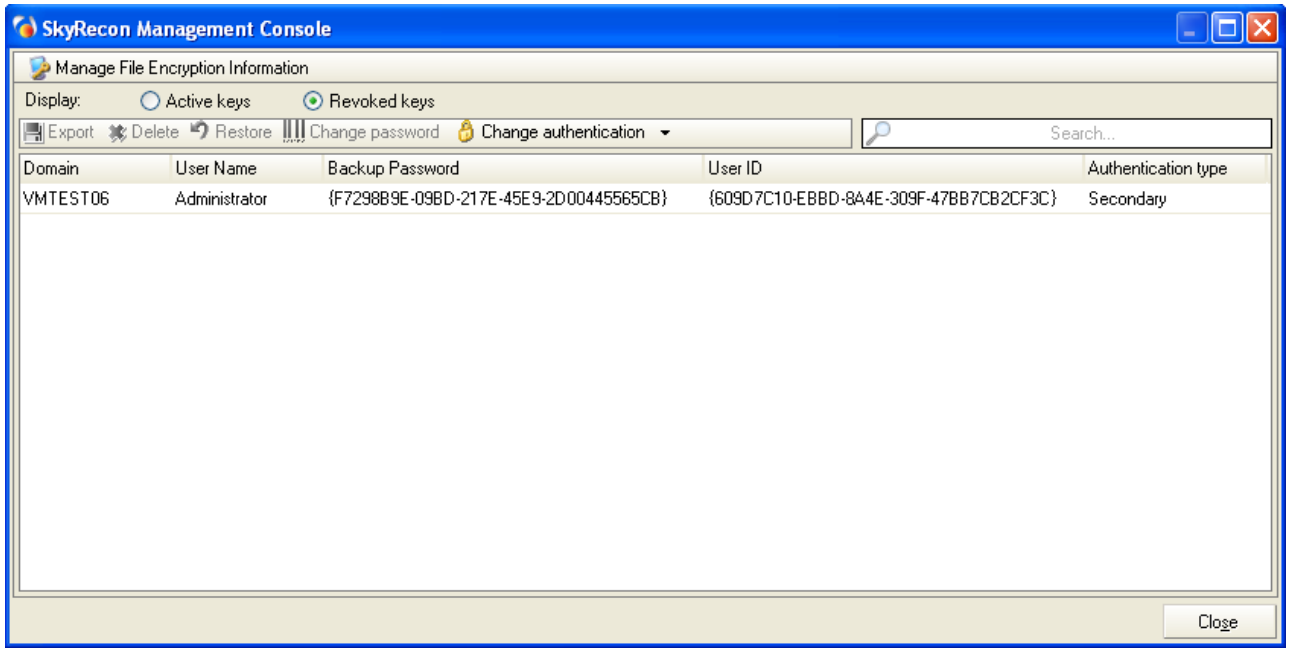
A user with a revoked key will not be able to access encrypted files. Authentication will be rejected.

To revoke or restore user keys, the administrator must follow the steps below:

1. Search for a user using the Search field and click **Revoke**.



2. The user is removed from the list of Active keys. On the other hand, his name will appear on the list of Revoked keys.
   To check this out, click the **Revoked keys** radio button.



3. Several actions are available from the toolbar:
   - **Export** the user key as a `[RecoveryKey].srk` file.
   - **Delete** the user key.
   - **Restore** the user key (Revoked key > Active key).
   - **Change** user **password**.
   - **Change** user **authentication**.

DATA RECOVERY FROM ENCRYPTED FILES (DECRYPTION)

The administrator may need to decrypt some or all of the data on a hard disk.

Examples:

- When a user leaves the company.
- When data is to recovered from a damaged hard disk.

Recovery key rings

If the administrator needs to decrypt more than one hard disk, he can create a recovery key ring.

The recovery key ring is a file that can be copied onto a USB key and which can be used to manually decrypt each computer in turn.

To create a recovery key ring, see "Decrypting data manually", page 491.

In Step 3 in the manual data decryption procedure, the administrator selects the user names that he wants to include in the recovery key ring.
He can then rename the file (if necessary), and export it to a USB key.

The recovery key ring includes all the keys of the computers used by selected users.

Decrypting data manually

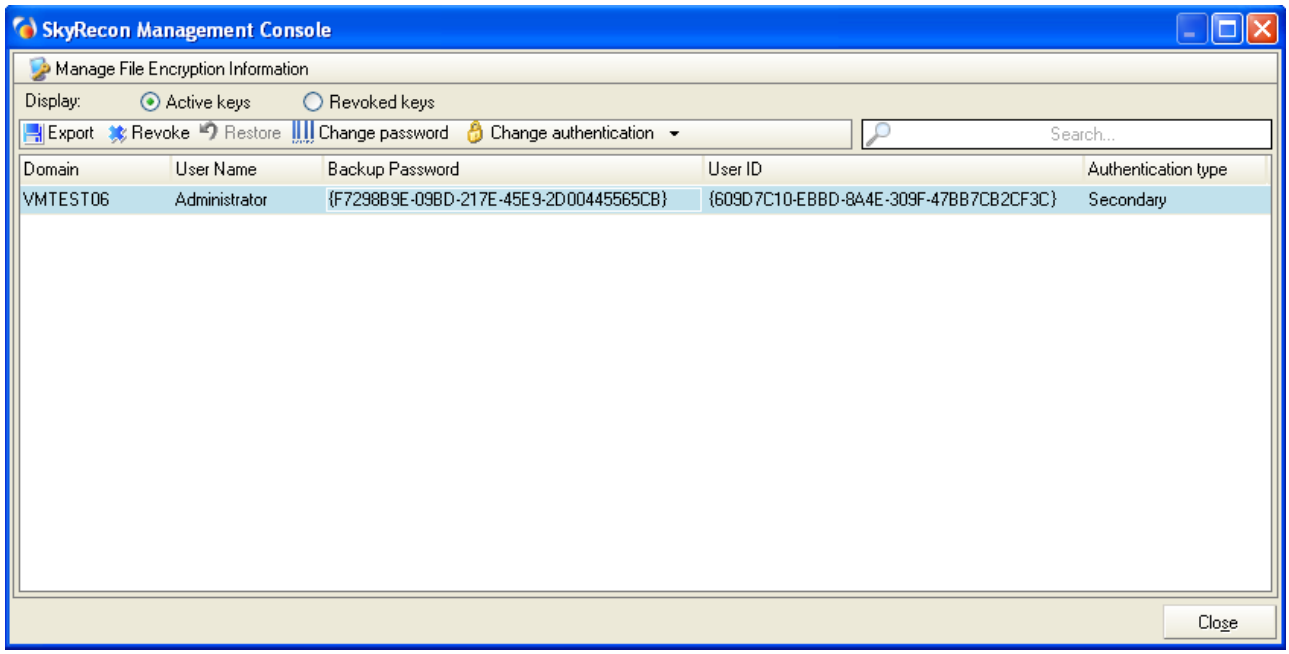
Administrator side

To decrypt data manually, the administrator must follow the steps below:

1. Select **Encryption > Manage File Encryption Information**.

2. Enter the password for console certificate.

   The **Manage File Encryption Information** window is displayed.



If you receive an error message, the console has not been correctly configured.

3. Locate the user name in the list.

   For long lists, you can use the **Search** field to locate the user name quickly.

   You can select multiple user names to create a key ring.

   For more information, see "Recovery key rings", page 491.

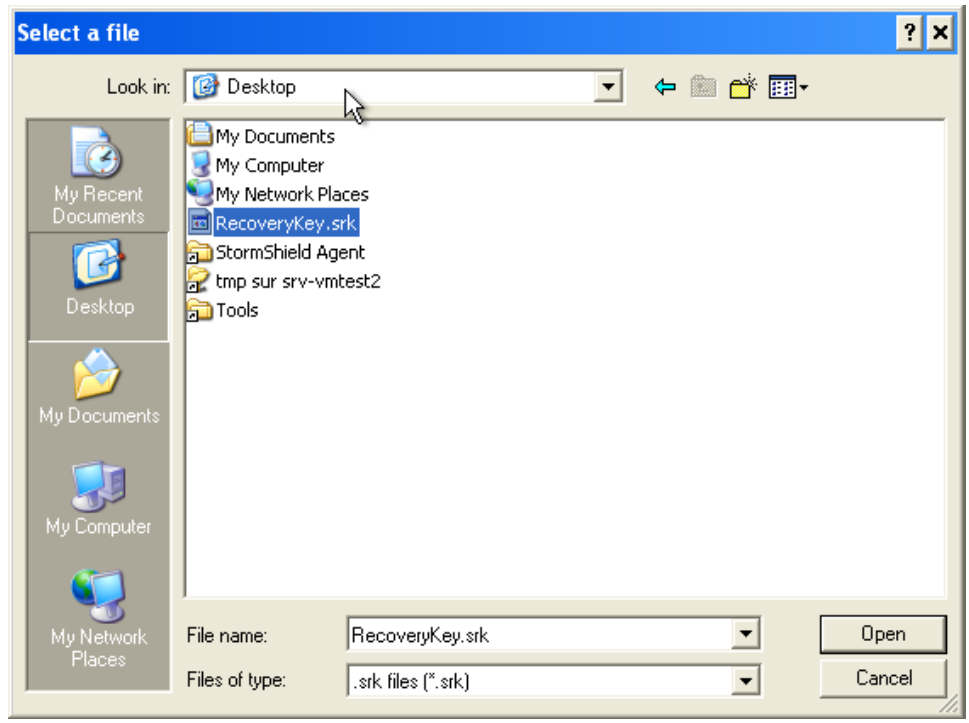
If Active Directory is not used, users working on different workstations can have the same **User Name** (example: administrator account), but **not** the same **User ID**.
To locate a user by his user ID, ask the user to email it to the administrator.

For more information, see "Get IDs", page 481.

4. After selecting the User Names (or User IDs), click **Export**.
5. Select the path and file name.

   The file is saved as a `[RecoveryKey].srk` file which contains the keys used for file recovery.

   SRK files can be exported from the console and used on the StormShield Agent.



   For more information on file recovery rules, see "Decrypting data manually", page 491.

   The SRK file can be saved onto a USB key or another server.

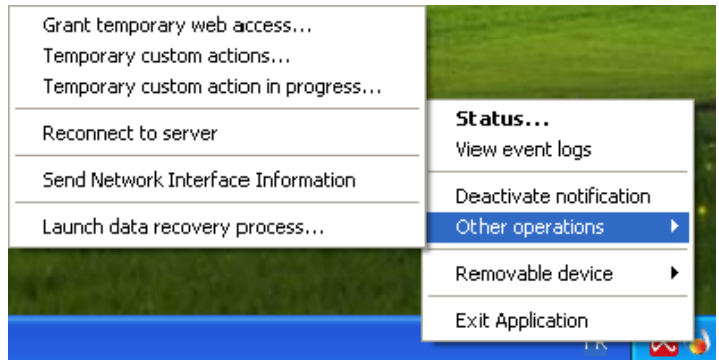
   It is highly recommended that the **SRK** file be stored in a secure location whose access should be reserved for authorized personnel (administrators).

Agent side

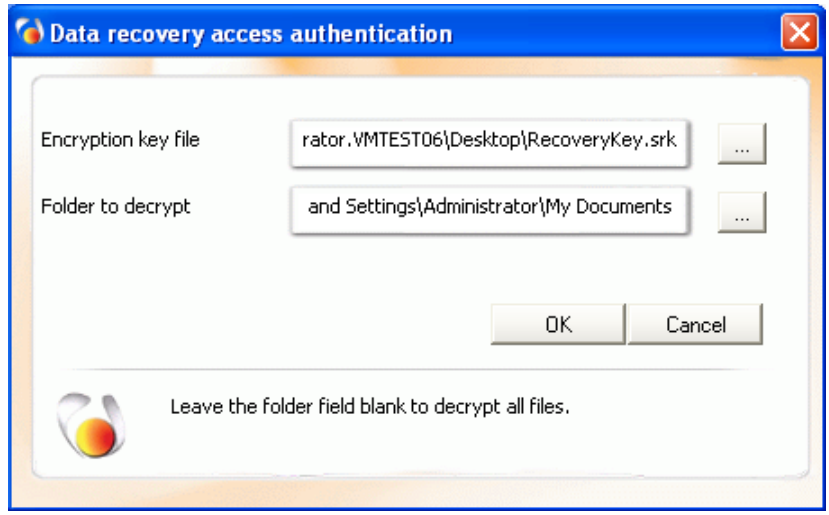
To decrypt data manually, the user must follow the steps below:

1. Right-click the StormShield Monitor icon .

2. Select **Other operations > Launch data recovery process**.



3. In the **Encryption key file** field, enter the path and filename of the recovery key or click directly the Browse button ....



Use the **Folder to decrypt** field if you need to decrypt one folder at a time (example: if you perform data recovery on a hard disk other than your computer HD).

4. Restart the computer.

The decryption process begins when the computer restarts.

If the encryption policy was not removed beforehand, the encryption policy is applied once again when the agent restarts in order to re-encrypt files.
The user can go on working during the recovery process. Decryption continues even when the computer is locked.

If you repeat Step 1 to launch the data recovery process before the agent has restarted, you will be asked if you want to cancel data recovery **or** perform another data recovery process.

Automatic decryption

To achieve a successful automatic decryption process:

1. The StormShield agent must be able to connect to the StormShield server.
2. In the Configuration Editor under Agent configuration, **Allow stop agent** must be set to **On**.
3. In the Environment Manager under Master server > Encryption:
   - **Decrypt data at uninstallation** must be set **On**.
   - The uninstall date must fall between **Start date of allow uninstall** and **End date of allow uninstall**.

Only files encrypted with the computer key can be recovered during automatic decryption.
For files encrypted with a user key, the administrator must perform one of the following:

- Perform a manual recovery.
- Reinstall the StormShield agent.
- Transfer the files encrypted with a user key into a folder encrypted with a computer key.
- Use SURT to decrypt files after uninstalling StormShield if the user does not wish to install the StormShield agent again.

If the **Decrypt data at uninstallation** parameter is enabled in the encryption policy, the decryption process begins automatically when the user runs the `Srend.exe` file to uninstall the StormShield agent.

During automatic decryption, it is not necessary to restart the computer if no user has logged in previously (**example**: when uninstalling with Active Directory GPO).

However, if the user is currently logged in or has logged in previously (with no reboot), then the computer must be restarted. The user will be prompted to restart the computer.

PASSWORD RECOVERY WHEN USING FULL DISK ENCRYPTION

Recovery procedure

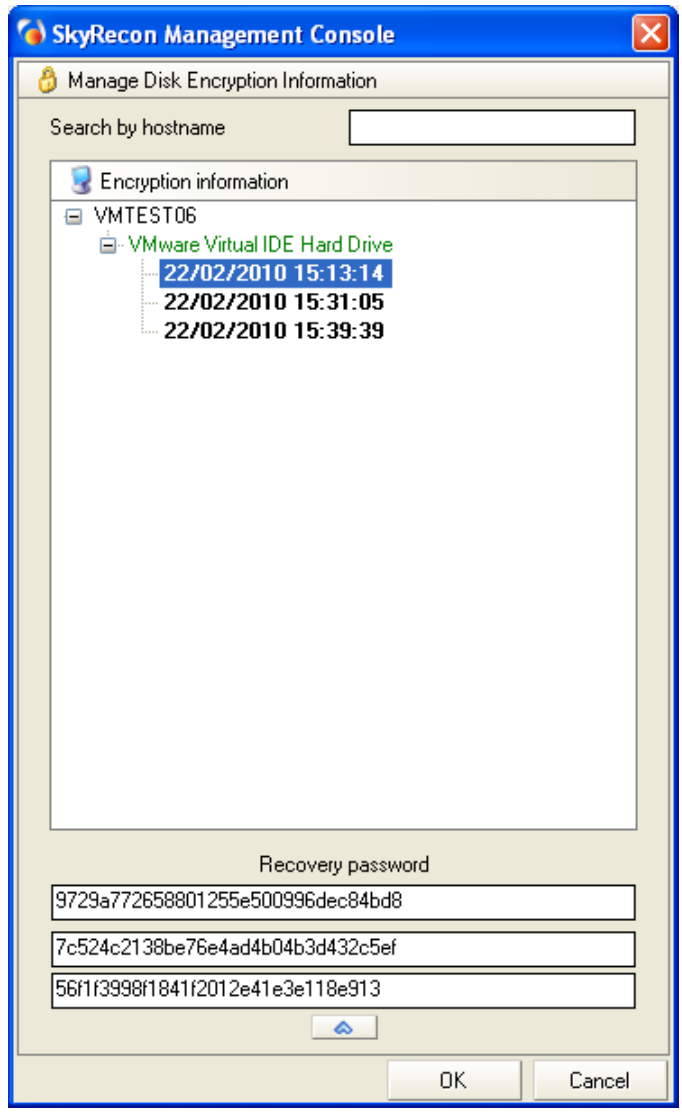
To access the recovery password when using Full disk encryption, the administrator must follow the steps below:

1. Go to **Encryption > Manage Encryption Disk Information**.

2. Enter the password for the console certificate.

3. The encrypted disks of the agent are detected automatically and listed in a tree structure in the window.

   To locate a disk or an encrypted system, use the hostname search bar.



4. Click the date under the disk name. The recovery password is displayed in the **Recovery password** field.

   This key is sent to the agent by email or telephone in order to recover encrypted disk data.

   If several dates are associated with a given disk, it is recommended to use the recovery password located under the most recent date.

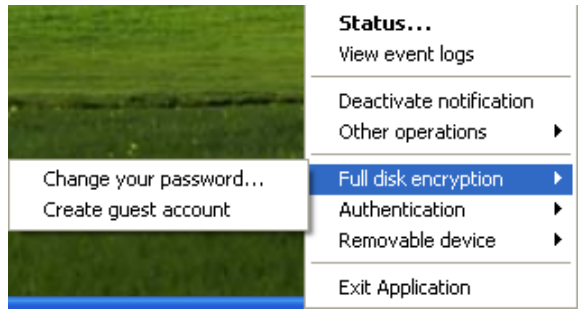
   The former recovery dates are kept in the list for reference should a problem arise.

If the administrator has enabled **One-time recovery password** in the encryption policy (full-disk encryption parameters), and if the user cannot connect to the StormShield server, his recovery password will not be automatically updated.
The administrator will send the user a previous password that will remain valid until next connection to the server.

Password change

Password change via the StormShield agent

1. On the agent computer:
   - Right-click the StormShield Monitor icon .
   - Select **Full disk encryption > Change your password**.



2. In the window, enter the **Old password**.
   If you do not remember your old password, enter the recovery password that was sent by your administrator.
   If you check the **Use recovery password** box. The recovery password will be displayed in clear text.

   If you do not check the Use recovery password box, the recovery password will be automatically converted into QWERTY mode.

Paste the recovery password sent by the administrator into the Old password field.

3. Enter and confirm the new password.
4. Click **OK**.

If the user remembers the old password, he can enter the old user password instead of the recovery password.

Password change upon startup

If you do not remember your user password, you can start the computer using the recovery password (Admin).

To do so, follow the steps below:

1. Press **F2** (admin).
2. Enter the recovery password in the prompt window.
3. Press **Enter**.

FULL-DISK ENCRYPTION DATA RECOVERY VIA CD

The administrator performs a full-disk encryption data recovery via CD if the encrypted disk did not launch properly.

Recovery is mainly used for disk decryption and when the machine cannot be started under normal conditions. Examples: lost password or system crash even when booting in Safe Mode.

The CD-ROM will enable users to:

- Decrypt data on the hard disk.
- Change passwords.
- Decrypt and remove boot loader.

Create a CD for data recovery

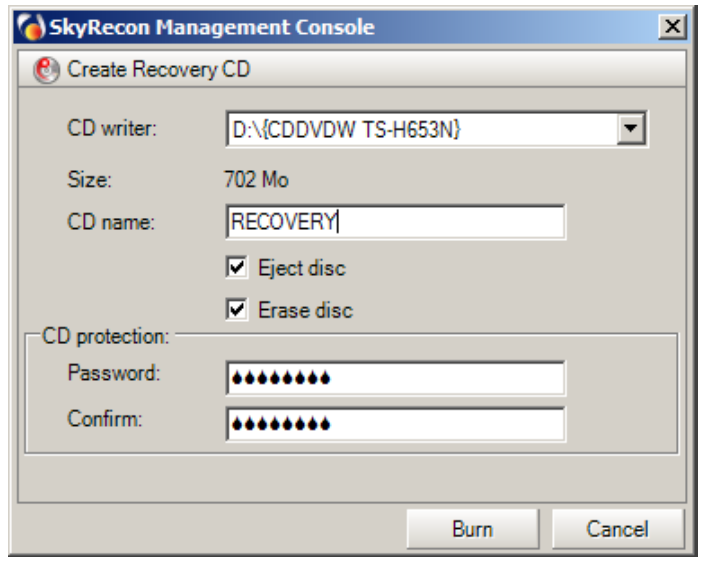
On the SkyRecon Management Console, the administrator can create a CD-ROM in order to:

- Launch a disk recovery on an agent computer.
- Decrypt all encrypted data.

To recover the encrypted disk by CD, the administrator must follow the steps below:

1. Go to **Encryption > Create Recovery CD**.

2. Specify the following settings:



- Select the CD writer.
- Rename the recovery CD.
  - Check the **Eject disc** box to boot out the CD after burning.
  - Check the **Erase disc** box to reformat the CD before writing. This works if your CD is rewritable.
- Enter and confirm a **Password** to protect the CD.

  It is necessary to define a password for CD protection. Indeed, the CD can be used to recover all the data stored on the agent computers that have encrypted disks.

The CD can be used to access all company data. Unauthorized persons might have access to this CD and use it to steal company information. It is therefore essential that extreme security measures are taken and applied to the CD.

3. Click **Burn** to start the writing process.

Repair your machine (via CD)

It is recommended to decrypt files using the SkyRecon Recovery Tool if encryption fails.

The encryption process may fail due to a damaged block.

To repair a machine, the user must follow the steps below:

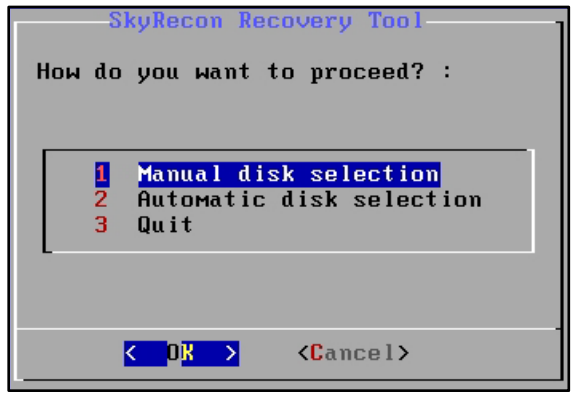
1. Insert the burned CD.

StormShield provides all the tools required for recovery.

2. On startup, enter CD password.

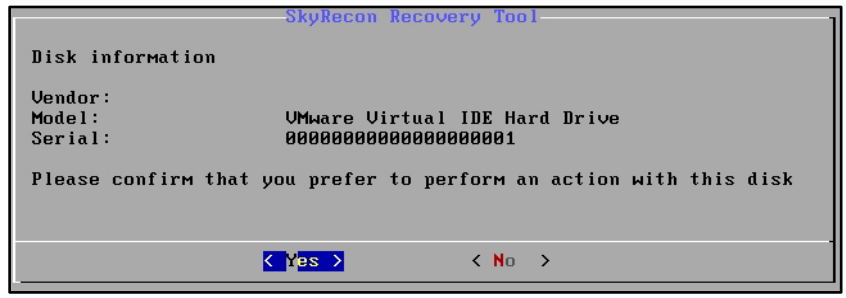
3. Select **Repair your machine**.

4. Select the appropriate process type and click **OK**.
   - If you choose **Automatic disk selection**, please proceed to Step 7.

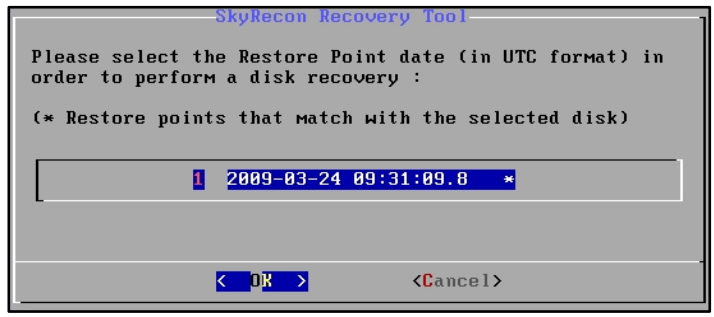


   - If you choose **Manual disk selection**, select the appropriate encrypted disks which are detected by the system.

5. The hard disk information window is displayed.
   Select **Yes** to proceed.



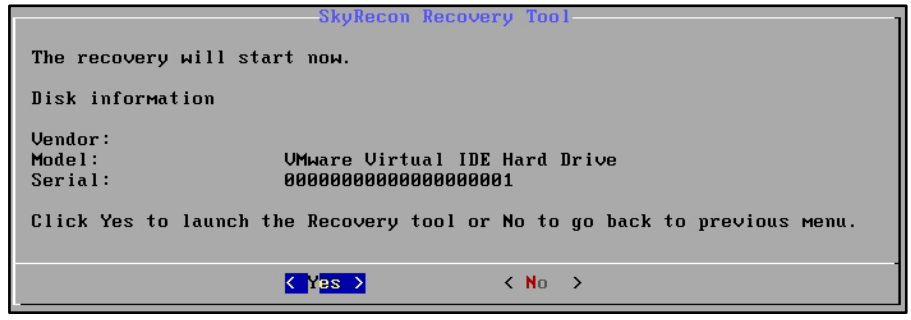
6. Select the Restore point date to perform disk recovery.



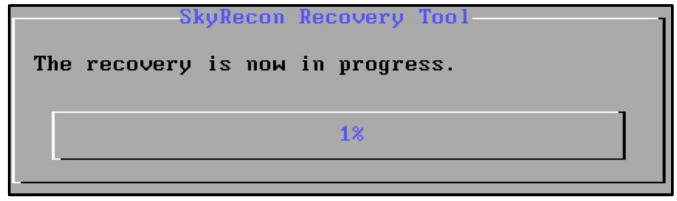
The **Restore Point** includes all the keys required to recover system data.

The date and time stamps allow you to use older keys as backups, should a problem arise with the most recent restore point date.

7. If you choose **Automatic disk selection**, you will be prompted to start the recovery immediately.
   Select **Yes** to proceed.



8. The recovery process starts.



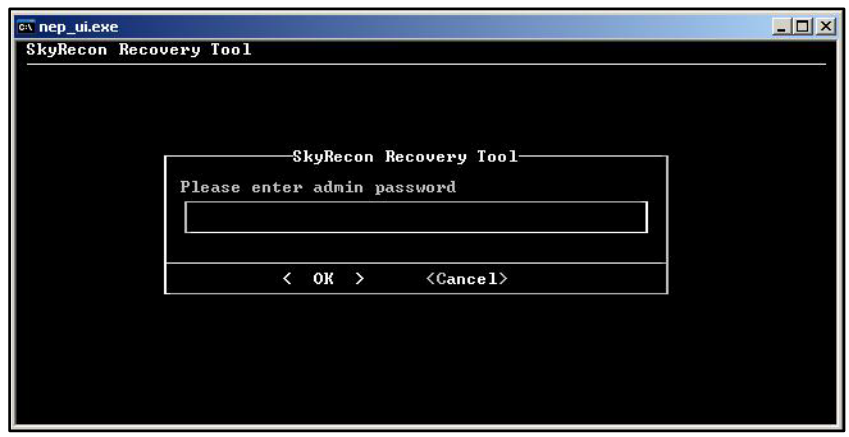
Recovery in Windows mode

The user can perform this type of recovery only on extra hard disks which do not run in the system.

Example:
If the user has no CD-ROM drive at his disposal, he can remove his hard disk from his computer and put it inside another computer which includes a CD-ROM drive to perform the recovery process.

To perform a recovery in Windows mode, the user must follow the steps blow:

1. Insert the recovery CD.
   Select **OK** to proceed.

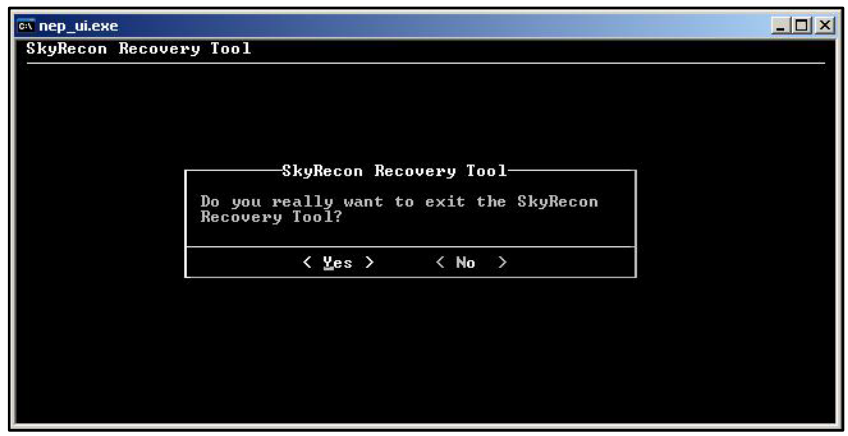


2. Enter the password.
   Select **OK** to proceed.

3. Select **Repair your machine**.
   Select **Continue** to proceed.

4. Select the appropriate process type.
   Select **OK** to proceed.

5. Once the recovery process is completed, exit the wizard.
   Select **Yes** to proceed.



Change password

If the user forgets the encryption password, StormShield offers an option to guide the user through the password change process.
This process applies to recovery via CD and in Windows mode.

To change the encryption password, the user must follow the steps below:

1. Select **Change your user password**.
2. Enter the new encryption password.
3. Confirm the new encryption password.

The user is notified if password change is successful.

UNINSTALLING STORMSHIELD AGENTS

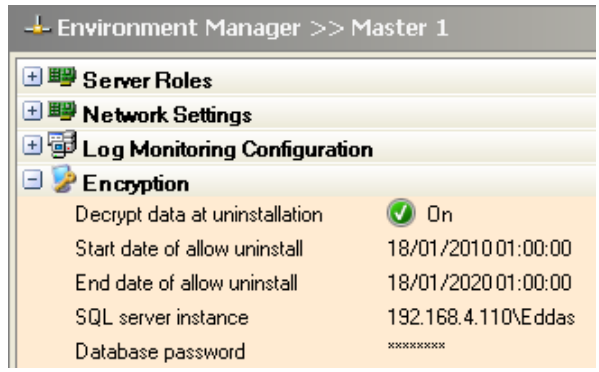
DECRYPTION BEFORE UNINSTALLATION

When agents are uninstalled, StormShield must decrypt the folders and files stored on the agent's hard disk, so that the users can access their data after software removal.

Multiple agents can be uninstalled at the same time using Group Policy Objects (GPO), without any need for user intervention.

However, in order to use GPOs in the Environment Manager panel, parameters must be configured as follows:

- The agent must be connected to the server.
- The **Decrypt data at uninstallation** option must be set to **On**.



- The **Start date of allow uninstall** and **End date of allow uninstall** must be specified.

  During this period, agents can request the server encryption key which enables StormShield to decrypt the hard disk without the need for user authentication.

Only files encrypted with the **computer key** are recovered during automatic decryption.
To recover files encrypted with a **user key**, the administrator must perform one of the following actions:

- Perform a manual recovery.
- Reinstall the StormShield agent.
- Transfer the files encrypted with a user key into a folder encrypted with a computer key.
- Use SURT to decrypt files after uninstalling StormShield if the user does not wish to install the StormShield agent again.

If the automatic decryption process is launched and the recovery procedure fails, the StormShield agent will be uninstalled anyway. It is then necessary to decrypt files manually.

CHANGING A USER ACCOUNT ON A MACHINE

After changing a user account on a machine, check that the **Start date of allow uninstall** and the **End date of allow uninstall** cover the time period when the user first logs on.

This is to ensure that:

- The agent will be able to request the server encryption key.
- The user will be able to access encryption features.

To maintain encryption security, keep the allow uninstall period to a minimum.

Chapter 14

SURT

ABOUT THIS CHAPTER

This chapter describes how to use SURT and its graphical interface.

It includes the following:

- Overview.
- Encrypting a file.
- Decrypting an encrypted file:
  - Procedure.
  - Progress bar.
- Reference menu:
  - Graphical interface.
  - Options.
- Removable device encryption and SURT:
  - Removable device group settings.
  - SURT settings.
- Recovering data encrypted via the Data Encryption feature:
  - Prerequisites.
  - Procedure.

OVERVIEW

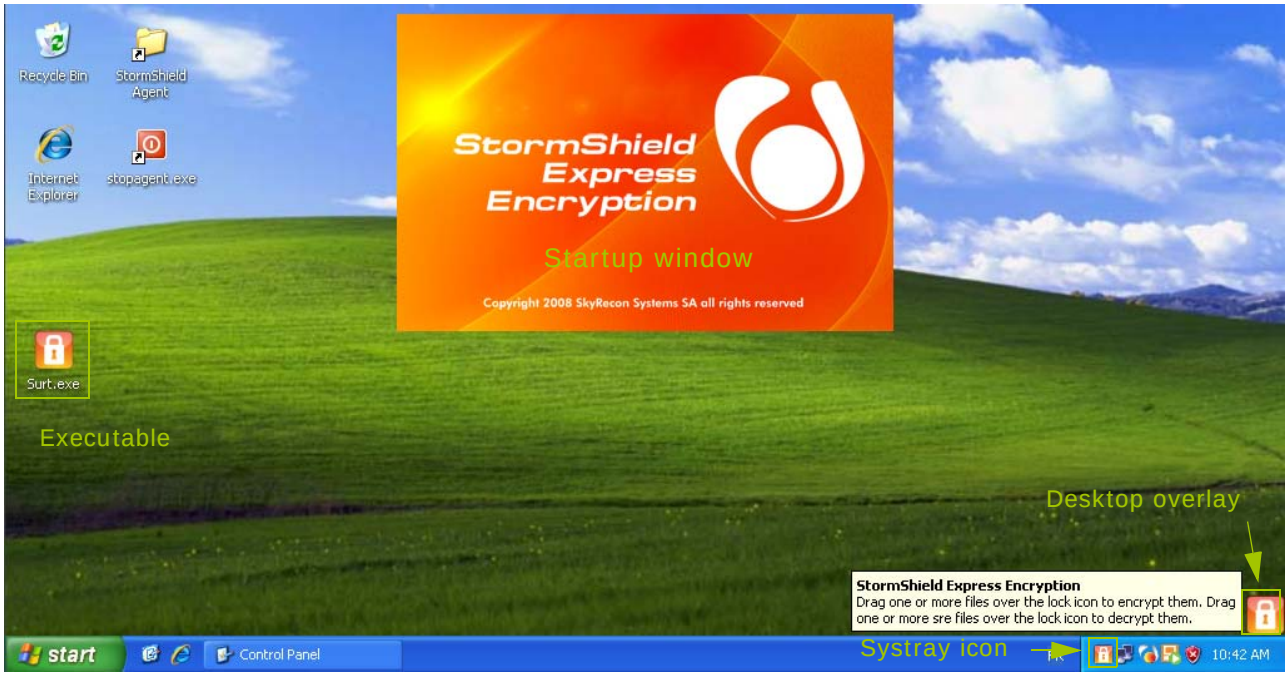
A user who does not have StormShield installed on his computer may download free of charge StormShield's SURT encryption tool from SkyRecon Systems' website "http://www.skyrecon.com/Downloads".

SURT (also called **StormShield Express Encryption**) is a portable software that can be used without having to install it on your computer.

SURT is associated with the file extension `.sre`. Therefore, when you copy it from another location to your computer, it will be displayed as `Surt.exe`.

If you double-click SURT, the following window will be displayed including the icons below:

- Icon in the system tray: .
- Desktop overlay: .
- Executable icon: Surt.exe.



ENCRYPTING A FILE

PROCEDURE

To encrypt a file, follow the steps below:

1. Double-click the `surt.exe` icon on your desktop or in the location in which you copied SURT.

   A startup screen will be displayed and another  icon will appear on the lower right corner of your Windows desktop.

2. Drag the desired file to the icon  .
3. Specify the encryption settings:
   - Password to access the encrypted archive.
   - Confirm the password.
   - Encrypted archive name.
   - Archive destination:
     - Within the same folder.
     - On my desktop.
     - In my documents.
     - Browse for a location.

      The **Generate an encrypted archive** box is checked by default.

4. You may write directly the encrypted archive onto the CD-ROM.

   To do so, check the **Write to a CD/DVD** box and specify the following settings:
   - Recorder name.
   - Media name.
   - Other options:
     - Erase CD/DVD.
     - Eject CD/DVD after burning.
     - Add StormShield Express Encryption to the media.

5. Click **OK**.

6. If you have checked the **Write to a CD/DVD** box, the burning process starts immediately.

7. When the burning process is completed, a new window is displayed. Click **OK**.

DECRYPTING AN ENCRYPTED FILE

PROCEDURE

To decrypt a file, the user must follow the steps below:

1. Drag and drop the file to be decrypted on the desktop overlay  .
   The window below is displayed.

2. Enter the password of the encrypted file.
3. Specify the decrypted file path.
4. Click **OK**.

If you want to overwrite an already existing file in the same location, click **Yes**.

The following message is displayed to apply overwrite to all files.

PROGRESS BAR

The progress bar is displayed during file encryption only when:

- The user drags and drops more than one file at a time.
- The file that the user is encrypting is bulky.

Fig. 14.1: StormShield Express Encryption: Progress bar

REFERENCE MENU

GRAPHICAL INTERFACE

The StormShield Express Encryption reference menu is displayed when the user right-clicks the system tray icon .

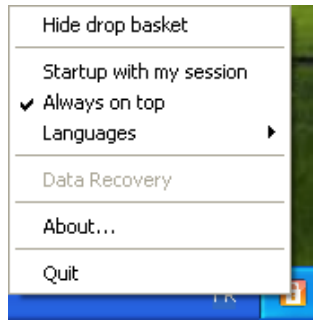


Fig. 14.2: StormShield Express Encryption: Reference menu

OPTIONS

The reference menu options are the following:

- **Hide/Show drop basket**:

  If Hide drop basket is enabled, the icon is displayed only in the system tray.

  If Show drop basket is enabled, the icon is displayed on the desktop.

- **Startup with my session**:

  This option automatically starts SURT during Windows login.

- **Always on top**:

  This option keeps the icon on top of all running applications.

- **Languages**:

  This option sets the language used for SURT (French, English, Spanish or Portuguese).

- **Data recovery**:

  This option recovers the encrypted files created with the Data Encryption feature on the SkyRecon management console.

  To recover encrypted files created with the Data Encryption feature on the SkyRecon management console, the user must start his computer in **SAFE** mode.
  If the user wishes to be in NORMAL mode, the StormShield agent must be uninstalled.

  For more information, see "Recovering data encrypted via the Data Encryption feature", page 519.

- **About**:

  This option shows the software version and copyright information.

- **Quit**:

  This option exits the application.

REMOVABLE DEVICE ENCRYPTION AND SURT

REMOVABLE DEVICE GROUP SETTINGS

On the SkyRecon management console, SURT is set to **Allowed** or **Denied** in the Security Policy Editor, under the **Removable devices** category.

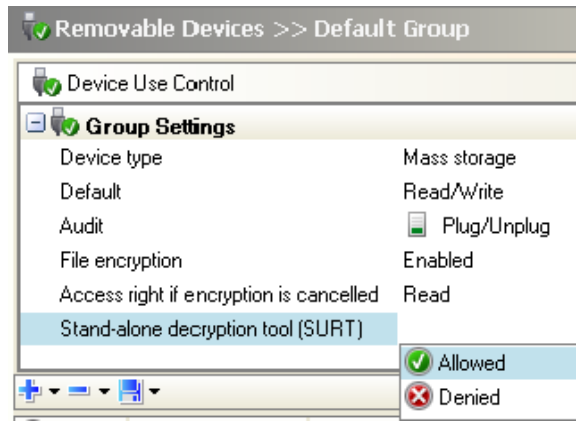


Fig. 14.3: SURT settings on the SkyRecon management console

SURT SETTINGS

SURT settings are the following:

- **Allowed:**

  When set to Allowed, the user can encrypt and decrypt data on removable devices.

  The executable file `SURT.exe` will be automatically copied onto the USB key. This way, any attempt to replace this `SURT.exe` by a hacked SURT file will be countered as a new version of `SURT.exe` will overwrite the hacked file.

- **Denied**:

  When set to Denied, the user cannot use SURT to encrypt or decrypt data on removable devices.

RECOVERING DATA ENCRYPTED VIA THE DATA ENCRYPTION FEATURE

PREREQUISITES

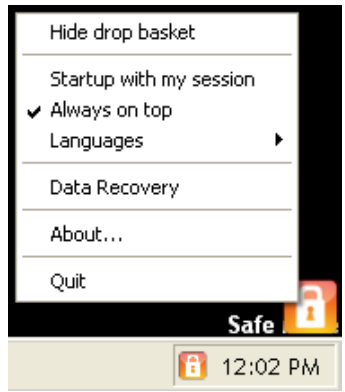
To recover encrypted files created via the Data Encryption feature on the SkyRecon management console, the user has to start his workstation in **SAFE** mode.

If the user wishes to be in NORMAL mode, the StormShield agent must be uninstalled.

PROCEDURE

To recover data encrypted via the Data Encryption feature, follow the steps below:

1. Right-click the icon and select **Data Recovery**.



2. The window below is displayed.

Specify the settings using the Browse button ... .

- The name and path of the folder to decrypt.
- The path of the recovery key file sent by the administrator.

3. Click **OK**.
   Folder decryption starts.
4. After decryption, a window prompts the user that the process is completed.

5. Reboot in NORMAL mode.

Chapter 15

ANTIVIRUS

ABOUT THIS CHAPTER

This chapter presents the AntiVirus Protection (AVP) option used by StormShield.

It includes the following:

- Overview of the antivirus.
- Antivirus integration:
  - StormShield server.
  - StormShield agent.
- Creating an antivirus policy:
  - General Settings.
  - Real-Time Protection Parameters.
  - Web Protection Parameters.
  - Mail Protection Parameters.
  - Scanner Parameters.
  - Password Parameters.
- Assigning an antivirus policy to an agent group:
  - Overview.
  - Procedure.
- Antivirus user interface:
  - Symbology.
  - Menu.
  - Administering quarantine.
  - Stopping the antivirus temporarily.

OVERVIEW

The Antivirus option is **not** embedded during the installation of StormShield on your computer.

It has to be integrated both into the Server and Agent sides of StormShield.

Moreover, a valid StormShield license has to be applied to your environment on the SkyRecon management console.

If this is not the case, please update your StormShield license before updating the antivirus license.

For more information, see:

- "AVP option", page 51.
- "Licenses", page 51.

ANTIVIRUS INTEGRATION

You will have to integrate your antivirus option at two levels:

- StormShield server.
- StormShield agent.

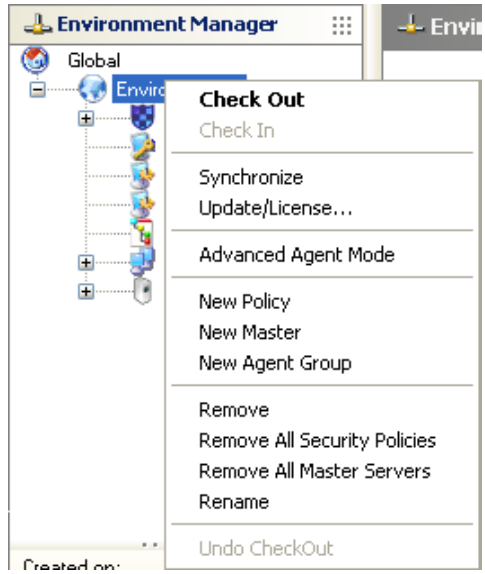
STORMSHIELD SERVER

To integrate the antivirus module, the administrator follows the steps below:

1. Check that the StormShield license is up to date.

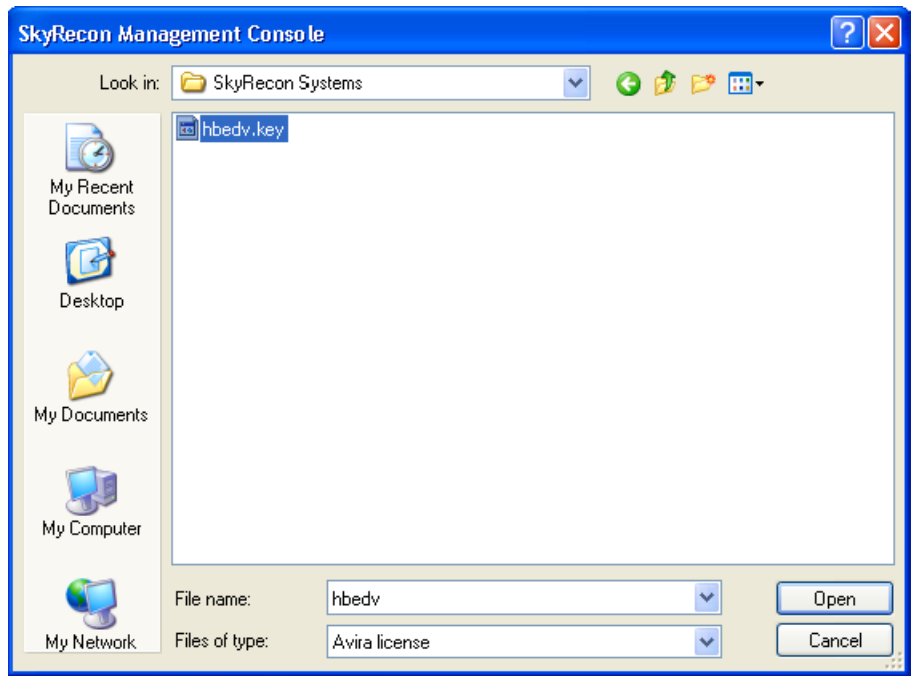
   To do so, right-click your environment and select **Update / License**.

   For more information, see "Licenses", page 51.

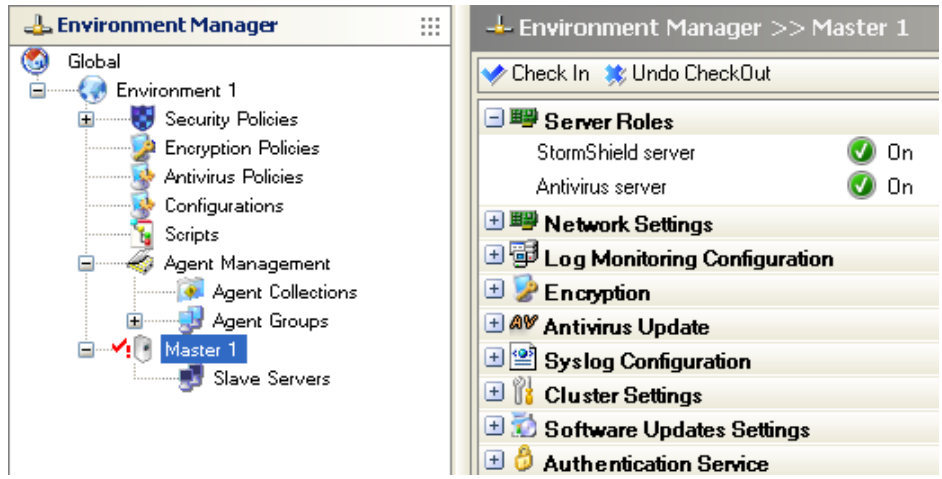


The window below is displayed.
Example: 20 StormShield licenses including the AVP option.

2. To update the StormShield license (if necessary), click **Update**.
3. To update your Antivirus license, click **Avira license**.
4. Select the Avira license and click **Open**.



5. After updating the StormShield and Avira licenses, configure the master server.

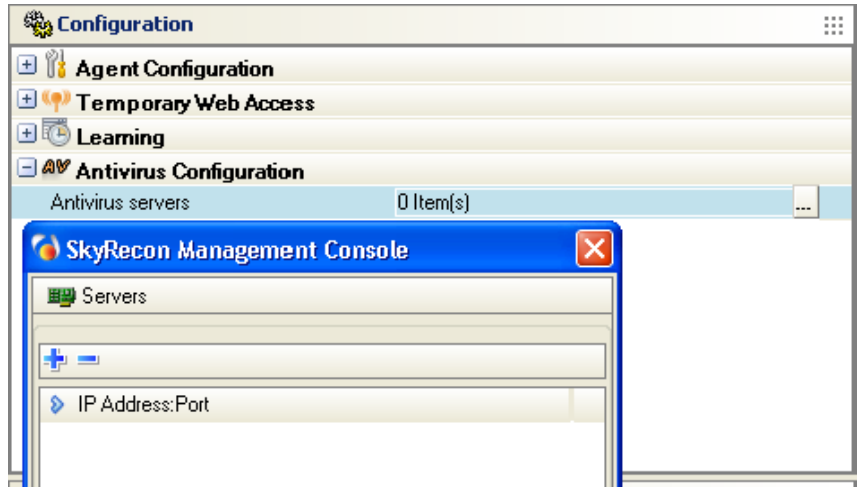


- For first-time users, follow the steps below to enable the antivirus server:
  - Click the [**Master server**] in the Environment Manager.
  - Go to **Server Roles**.
  - Set **Antivirus server** to **On**.
- If this is not the case, go directly to Step 6.

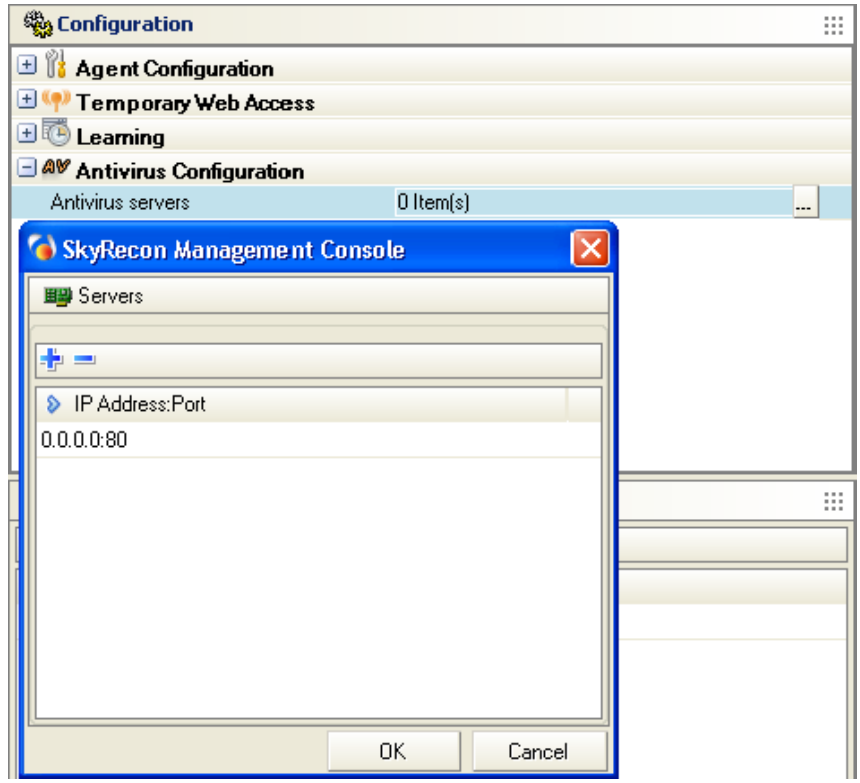
6. Configure the antivirus server.

   The antivirus may have one **or** several servers. Now, you have to select the IP address and the port assigned to the antivirus server(s).

   - If you enable for the first time the antivirus server, follow the steps below in the Environment Manager:
     - Click **Configurations**.
     - Edit the appropriate configuration.
     - Expand **Antivirus Configuration** in the Configuration panel.
     - Click **Antivirus servers** using the Browse button ... to display the **Servers** window below:

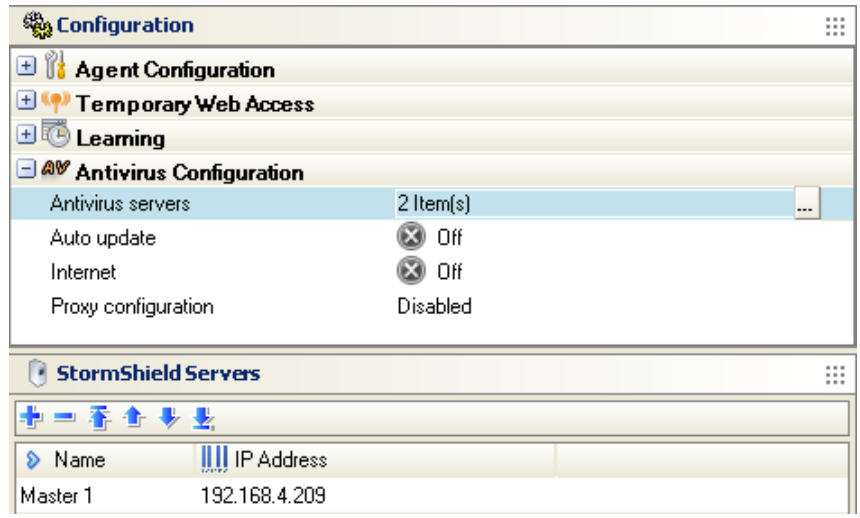


- Click + to add the IP address of an antivirus server.
- Replace `0.0.0.0:80` by the IP address and port allocated to each antivirus server.



- Click − to remove an antivirus server from the list.
- Click **OK** when you have finished.

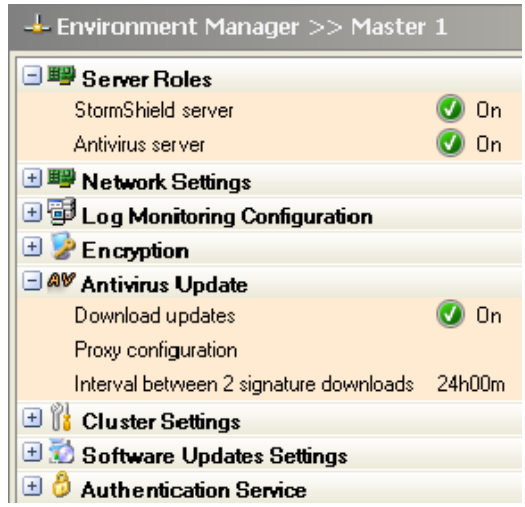
The window below is displayed which indicates that two antivirus servers have been added.



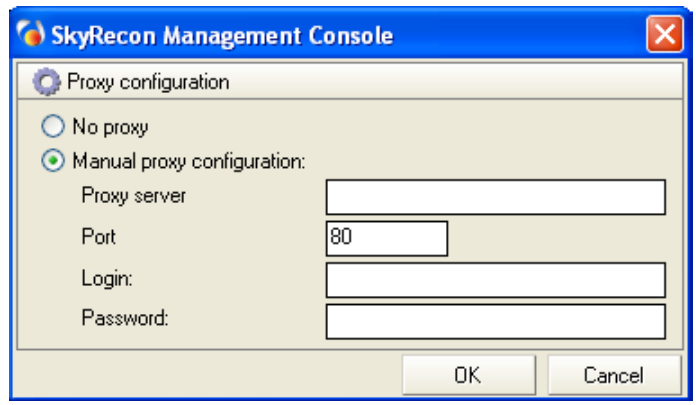
The administrator must specify the port dedicated to each server. This port is the same as the one used for the Apache web server.

- If this is not the case, go directly to Step 7.

7. Get the latest signature from the antivirus repository. To do so, follow the steps below:



- Click the [**Master server**] in the Environment Manager.
- Expand the **Antivirus Update** area.
- Click **Interval between 2 signature downloads** and modify the update interval.
- If necessary, configure the HTTP **proxy** so that the server can connect to the antivirus update servers.



8. Validate your modifications.
9. **Synchronize** by right-clicking your [master server] or in the environment area.

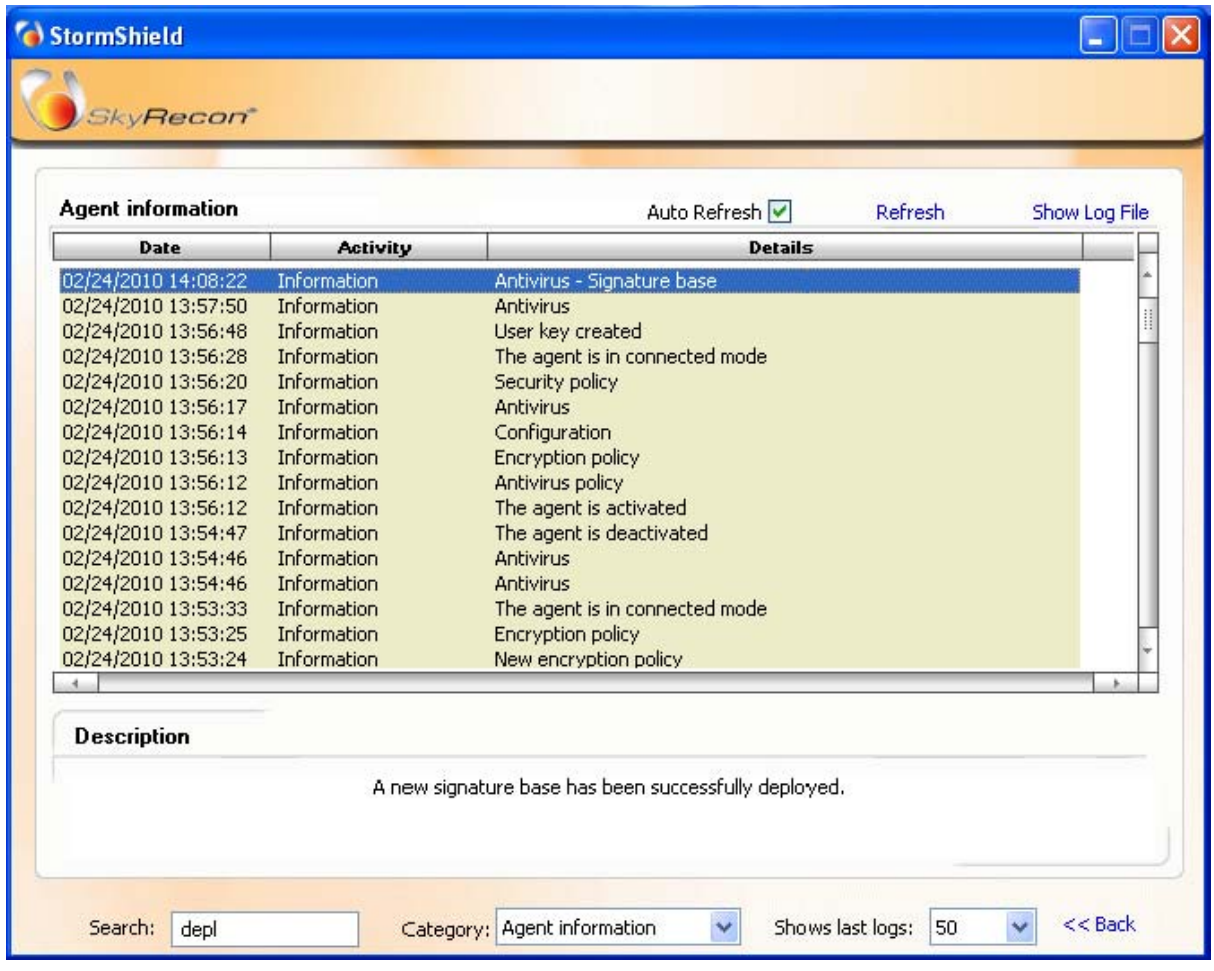
   The server will download the latest signature database from the Avira servers.

STORMSHIELD AGENT

After installing your StormShield agent, a connection to the antivirus server is established to download the latest signature database.

To achieve this connection, the time interval to download signatures should be configured in the **Antivirus Policy Editor**.

To check that the antivirus protection and signature database have been deployed successfully, click **View event logs** on the StormShield agent.



The antivirus protection supports English and French.

By default, the antivirus installer chooses the default language of your computer's operating system. If the default language of your operating system is not supported, you are prompted to install the antivirus using English as the default language.

CREATING AN ANTIVIRUS POLICY

The administrator can create a new antivirus policy to be applied to an agent group.

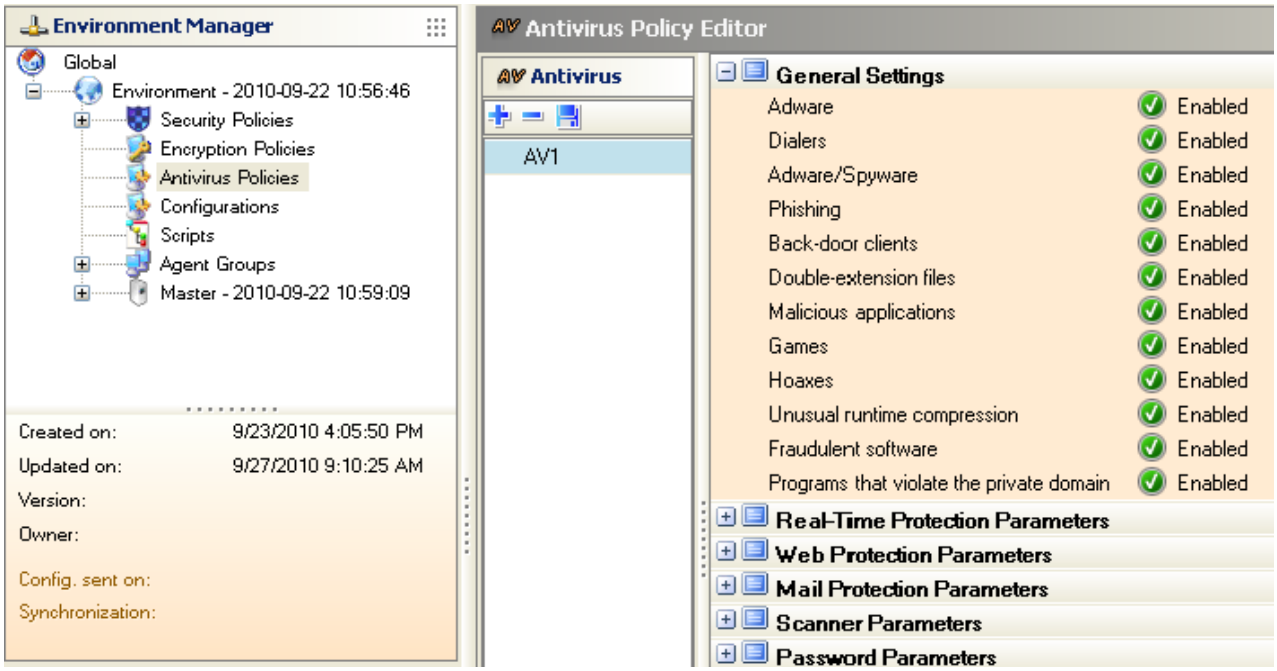


Fig. 15.1: Antivirus Policy Editor

GENERAL SETTINGS

This menu allows you to configure the general settings of the antivirus protection.

General Settings include the following options:

- **Adware**:

  Blocks advertising spyware on the user's workstation.

- **Dialers**:

  Blocks malicious dialers that create a connection to premium-rate telephone numbers and result in extra charges for the user.

- **Adware/Spyware**:

  Blocks advertising spyware and spyware that gather information without the user's knowledge.

- **Phishing**:

  Blocks phishing attempts to acquire sensitive information (identity theft) about the user.

- **Back-door clients**:

  Blocks back doors which allow hackers to perform remote actions on the user's workstation.

- **Double-extension files**:

  Blocks the installation of software with a hidden extension on the user's workstation.

- **Malicious applications**:

  Blocks malicious applications.

- **Games**:

  Blocks access to games.

- **Hoaxes**:

  Blocks hoaxes.

- **Unusual runtime compression**:

  Blocks software whose structure has been modified for malicious purposes and whose compression technique is highly suspect.

- **Fraudulent software**:

  Blocks malicious software (which charge extra fees, install no function or suspect components).

- **Programs that violate the private domain**:

  Blocks programs that violate users' privacy.

REAL-TIME PROTECTION PARAMETERS

Real-Time Protection scans any copied or modified file on the user workstation. It detects viruses and malicious programs.

Real-Time Protection is called Guard in Avira's antivirus.

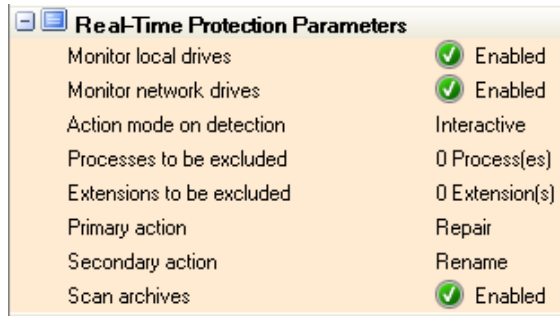


Fig. 15.2: Antivirus: Real-Time Protection Parameters

- **Monitor local drives**:

  Monitors local drives and checks for viruses and unwanted programs.

- **Monitor network drives**:

  Monitors network drives and checks for viruses and unwanted programs.

- **Action mode on detection**:

  Applies predefined actions when viruses or unwanted programs are detected.

  Two modes are available:

  - **Interactive:**

    This mode displays a popup on the user's workstation when real-time protection detects viruses or unwanted programs.

    The user decides what action to take depending on the administrator's settings.

    For more information, see "Primary action:", page 536.

  - **Automatic**:

    When this mode is enabled, real-time protection automatically applies the actions defined by the administrator.

- **Processes to be excluded**:

  Excludes from the analysis the processes selected by the administrator.

  You can add up to 128 processes to the list.

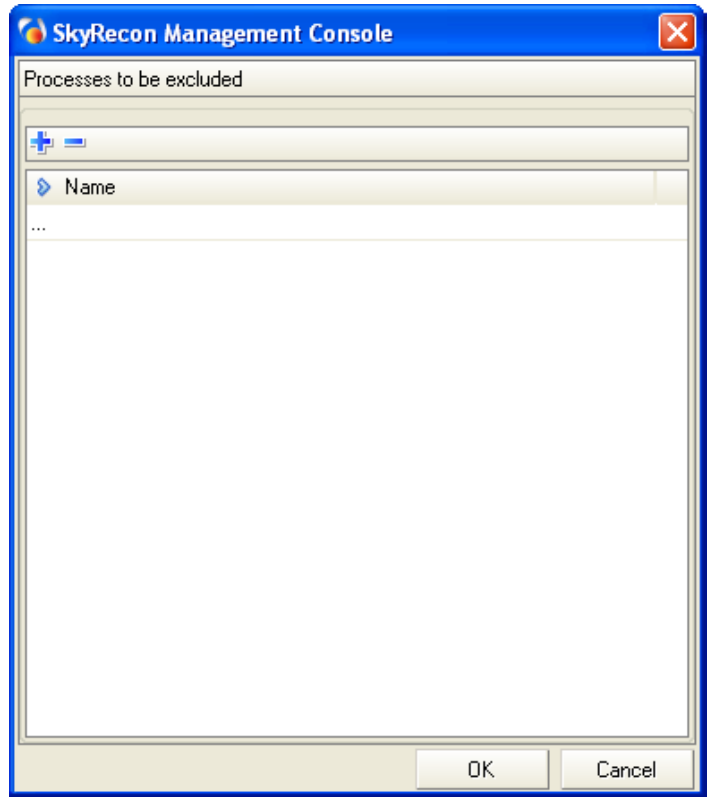
  Entries on the list must not exceed 6,000 characters in total.

  The path and filename of the process must not exceed 250 characters.

  Windows Explorer and operating systems are systematically scanned. Even if you add them to the list, they will be scanned by the real-time protection.

  To exclude processes from the analysis, follow the steps below:

  - Click the browse button ... in the **Real-time Protection Parameters** panel.
  - Add in the **Processes to be excluded** window the appropriate processes.



  To add a process to the list displayed:

  - Click +.
  - Enter the process name in the field.
  - Click **OK** when you have finished.

  To remove a process:

  - Select the process name from the list.
  - Click −.
  - Click **OK** when you have finished.

- **Files to be excluded**:

  Excludes from the analysis the files selected by the administrator.

  Entries on the list must not exceed 6,000 characters in total.

  For each drive, you can add up to 20 exceptions (starting with the drive letter followed by the complete path).

  Example:
  `C:\Program Files\Application\Name.log`

  You can add up to 64 exceptions (without specifying the complete path).

  Examples:
  `*.log`

  Only use **`*`** and **`?`** wildcards in filenames and extensions.

  Use a backlash \ at the end of directory names, otherwise the directory will be regarded as a file.

  The list is processed from top to bottom.

  If you add a directory to the list, all its subdirectories will be automatically excluded from the analysis.

  The longer the list, the longer the analysis. To prevent slow processing, keep the list as short as possible.

  To add short DOS filenames (~) to the list, observe DOS naming rules (DOS 8.3) when adding filenames to the list.

  To add directories and files on connected network drives, specify the UNC path that you use to connect to the network drive.

  Example:
  `\\<Computer name>\<Enable>\-OR-\\<IP address>\<Enable>\`

  Do not use a backlash **** at the end of a filename which includes wildcards. Otherwise, the entry will not be valid and will not be regarded as an exception.

  Example:
  `C:\Program Files\Application\applic*.exe`**`\`**

  Regarding connected network drives, do not use the letter assigned to the drive. Directories and folders will be scanned anyway by the real-time protection.
  If the UNC path in the list differs from the UNC path used to connect to the network drive (IP address, computer name), directories and files will be scanned anyway by the real-time protection.
  To check UNC paths, refer to the logs sent to the server.

  Regarding dynamic drives mounted as a directory on another drive, use the operating system alias for the integrated drive:

  Example:
  `\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVOlume1\`

  If you use, for instance, the mount point **`C:\DynDrive`**, the dynamic drive will be scanned anyway. To check the operating system alias, refer to the logs sent to the server.

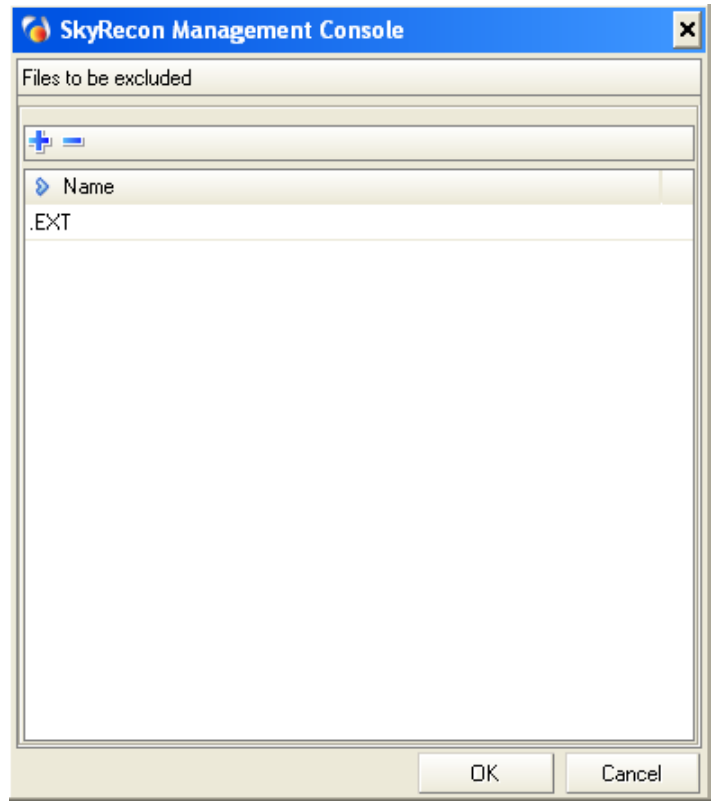
The path used by the real-time protection when scanning for infected files is indicated in the logs. Always use these paths in the list.

Examples:

```
C:
C:\
C:\*.*
C:\*
*.exe
*.xl?
*.*
C:\Program Files\Application\application.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\applic*
C:\Program Files\Application\applic?????.e*
C:\Program Files\
C:\Program Files\Application\*.mdb
\\Computer name\Enable\
\\1.0.0.0\Enable\application.exe
```

To exclude extensions from the analysis, follow the steps below:

- Click the browser button ... in the **Real-Time Protection Parameters** panel.
- Add in the **Extensions to be excluded** window the appropriate extensions.



To add an extension to the list displayed:

- Click .
- Enter the extension name in the field.
- Click **OK** when you have finished.

To remove an extension:

- Select the extension name (Example: `.doc`) from the list.
- Click .
- Click **OK** when you have finished.

- **Primary action**:

  Defines the first action to be performed in case a virus or an unwanted program is detected.

  Available options are the following:

  - **Repair**:

    Tries to repair the infected file.

  - **Rename**:

    Renames the infected file. Direct access to this file is no longer possible (by double-click). This file can be repaired later and renamed to its original name.

  - **Move to quarantine**:

    Moves to quarantine the infected file.

  - **Delete**:

    Deletes the infected file.

  - **Ignore**:

    Allows the user to access the infected file. No action is applied.

  - **Overwrite and delete**:

    Overwrites the infected file with a default pattern and then deletes it. This file cannot be restored.

  - **Block**:

    Blocks access to the infected file.

- **Secondary action**:

  Defines the second action to be performed in case an infected file is detected.

  The **Secondary action** can be configured only if the **Primary action** is set to **Repair**.

Available options to configure the secondary action are the following:

- **Rename**.
- **Move to quarantine**.
- **Delete**.
- **Ignore**.
- **Overwrite and delete**.
- **Block**.

For more information, see "Primary action:", page 536.

- **Scan archives**:

  Scans compressed files on the user's workstation. After scanning, the antivirus decompresses compressed files and scans them again.

WEB PROTECTION PARAMETERS

Web Protection checks in real time for viruses and malicious software which may infect the user's workstation when downloading web pages.

Web Protection is called WebGuard in Avira's antivirus.

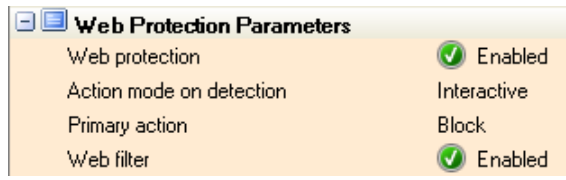


Fig. 15.3: Antivirus: Web Protection Parameters

- **Web protection**:

  Enables/Disables Web protection when an infected file has been detected.

- **Action mode on detection**:

  Applies predefined actions when viruses or unwanted programs are detected.

  Two modes are available:

  - **Interactive:**

    This mode displays a popup on the user's workstation when Web protection detects an infected file.

    The user decides what action to take depending on the administrator's settings.

- **Automatic**:

  When this mode is enabled, Web protection automatically applies the actions defined by the administrator.

- **Primary action**:

  Defines the first action to be performed in case an infected file is detected.

  Available options are the following:

  - **Block**:

    Denies access to the websites considered as malicious, and blocks file and data downloads to the user's web browser.

    A popup is displayed on the user's workstation.

  - **Move to quarantine**:

    Moves to quarantine the websites, as well as the files and data downloaded from these websites.

    Files can be recovered via the quarantine manager.

  - **Ignore**:

    Websites, files and data considered as malicious are downloaded to the user's web browser.

- **Web filter**:

  Filters URLs using an internal database which is updated daily. This database is designed to block the download of URLs based on their content.

MAIL PROTECTION PARAMETERS

Mail Protection scans in real time incoming emails that may infect the user's workstation, and possibly outgoing emails.

POP3 and IMAP protocols are supported. The protection monitors ports.

MailGuard is the interface between your computer and the email server from which your email program (email client) downloads emails. MailGuard is connected as a so-called proxy between the email program and the email server. All incoming emails are routed through this proxy, scanned for viruses and unwanted programs and forwarded to your email program. Depending on the configuration, the program processes the affected emails automatically or asks the user for a certain action.

Mail Protection is called MailGuard in Avira's antivirus.

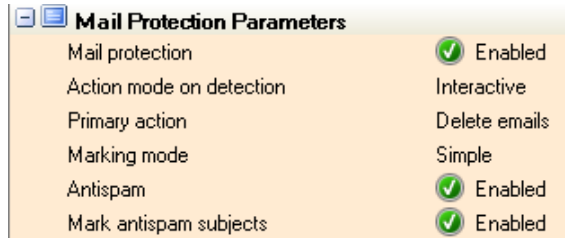


Fig. 15.4: Antivirus: Mail Protection Parameters

- **Mail protection**:

  Enables/Disables Mail protection on the user's workstation.

- **Action mode on detection**:

  Applies predefined actions when viruses or unwanted programs are detected.

  Two modes are available:

  - **Interactive:**

    This mode displays a popup on the user's workstation when Mail protection detects an infected email.

    The user decides what action to take depending on the administrator's settings.

  - **Automatic**:

    When this mode is enabled, Mail protection automatically applies the actions defined by the administrator.

- **Primary action**:

  Defines the action performed in case an infected email is detected.

  Available options are the following:

  - **Delete emails**:

    Deletes the infected email. The email body and its attachments are replaced by default text which is defined by the administrator.

  - **Move emails to quarantine** :

    Moves to quarantine the infected email and its attachments. The email is then deleted. The email body and its attachments are replaced by default text which is defined by the administrator.

  - **Ignore emails and delete attachments**:

    Allows the user to receive infected emails but replaces their attachments by default text.

  - **Ignore emails and move attachments to quarantine**:

    Allows the user to receive infected emails and moves to quarantine their attachments.

    Replaces attachments by default text which is defined by the administrator.

- **Ignore emails and attachments**:

  Allows the user to receive infected emails and attachments.

- **Antispam**:

  Enables spam protection.

- **Mark antispam subjects**:

  When enabled, a note is added to the original subject line when a spam email is detected.

- **Marking mode**:

  Two marking modes are available:

  - **Simple**:

    If a spam or phishing email is detected, **[SPAM]** or **[Phishing]** is added to the mail subject.

    This is the default setting.

  - **Detailed**:

    The subject line in a spam or phishing email is prefixed with **[***SPAM***]** or **[***Phishing***]** to draw the user's attention.

SCANNER PARAMETERS

The Scanner scans on demand the user's workstation.

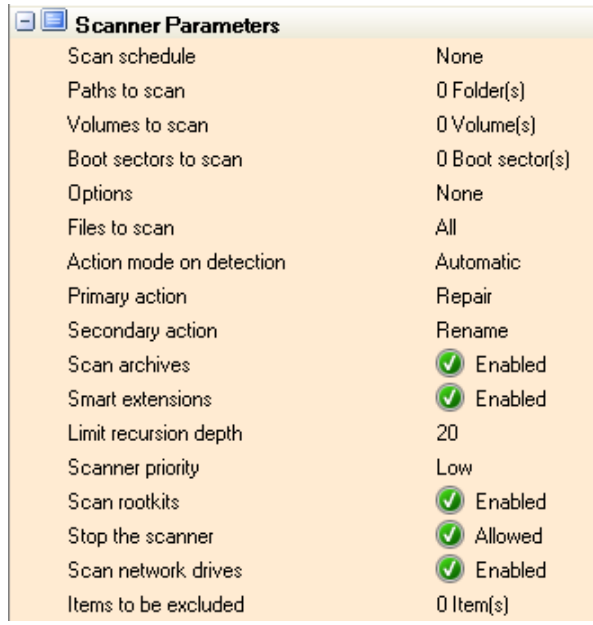


Fig. 15.5: Antivirus: Scanner Parameters

The Scanner can be configured with the following options:

- **Scan schedule**:

  Defines the frequency, time and date for starting the scan (if you have enabled the option) depending on the administrator's settings:

- Monthly.
- Weekly.
- Daily.

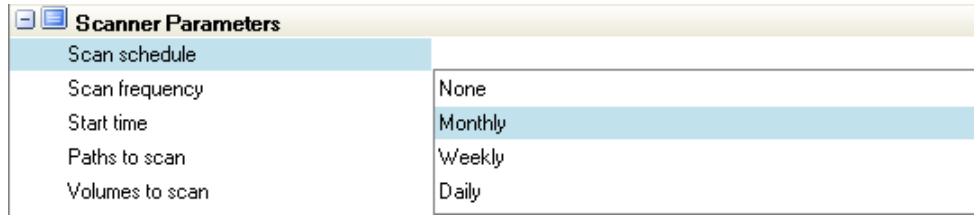


Fig. 15.6: Antivirus: Scanner Parameters: Scan schedule

The options displayed depend on the scan schedule selected by the administrator (**Example**: Weekly).

- **Paths to scan**:

  Defines the paths to be scanned.

- **Volumes to scan**:

  Defines the volumes to be scanned.

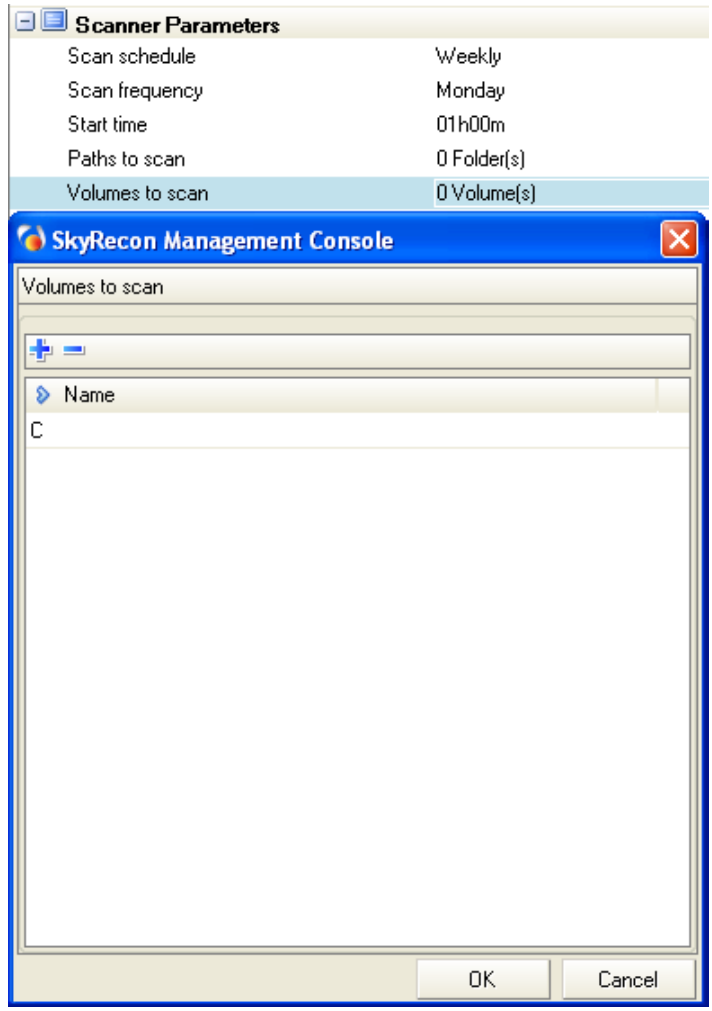


Fig. 15.7: Antivirus: Scanner Parameters: Volumes to scan

To add a volume to the list:

- Click the browser button ....
- Click +.
- Enter the letter-code identifier assigned to the volume.
- Click **OK**.

To remove a volume from the list:

- Click the browser button ... .
- Select the volume to be removed.
- Click − .
- Click **OK**.

- **Boot sectors to scan**:

  Defines the boot sectors to be scanned.

- **Options**:

  Defines the options to apply when scanning the user's workstation.

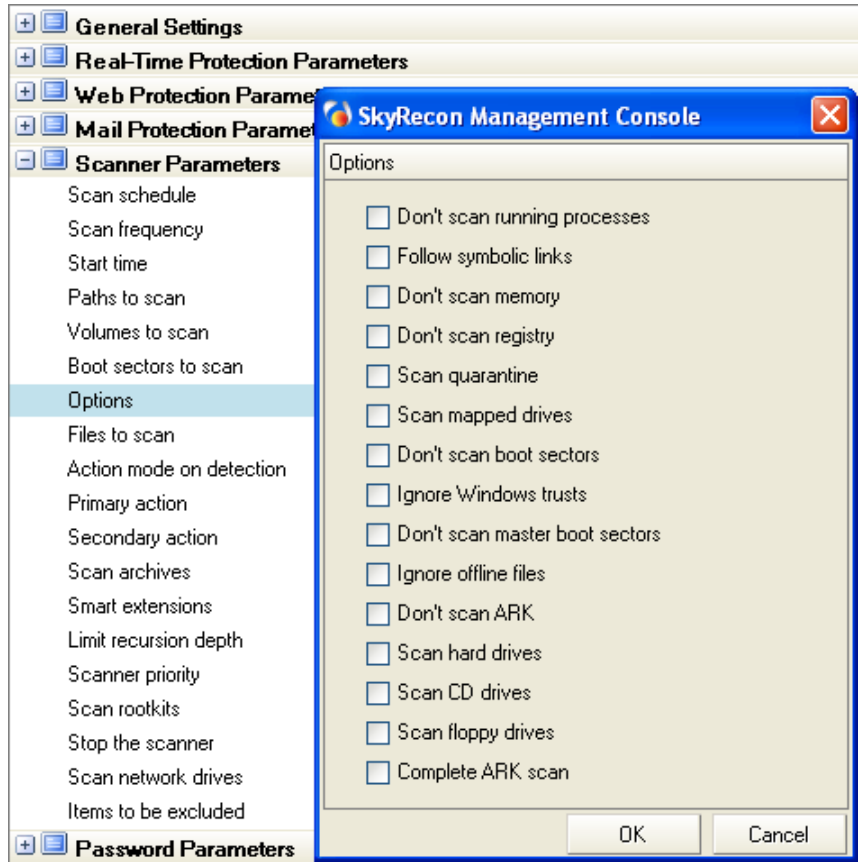


Fig. 15.8: Antivirus: Scanner Parameters: Options

The scanner options are the following:

- **Don't scan running processes**.
- **Follow symbolic links**:

  The scanner follows and scans the symbolic links to files, and scans the linked files for viruses and malware.

Follow symbolic links is incompatible with Windows 2000.

- **Don't scan memory.**
- **Don't scan registry**.
- **Scan quarantine**.
- **Scan mapped drives**.
- **Don't scan boot sectors**.
- **Ignore Windows trusts**.
- **Don't scan master boot sectors**:
  The scanner scans Master Boot Records on the system hard disks.
- **Ignore offline files**.

  Offline files are files which have been moved physically via a *Hierarchical Storage Management system* from the hard disk to another media (example: optical disk).

- **Don't scan ARK**.

  ARK stands for *Avira Rootkit Library*.

- **Scan hard drives**.
- **Scan CD drives**.
- **Scan floppy drives**.
- **Complete ARK scan**.

- **Files to scan**:
  Two options are available:
  - **All**:
    Scans all files on the user's workstation (regardless of file extension or content).
  - **Use smart extensions**:
    Scans only the files that are automatically selected by Avira. Scanning is based on file extension and content.

- **Action mode on detection**:

  Applies predefined actions when an infected file is detected.

  Two modes are available:

  - **Interactive**:

    When scanning is complete, a list of infected files (if any) is displayed in a dialog box on the user's workstation.

    The user decides what action to take depending on the administrator's settings.

  - **Automatic**:

    When this mode is enabled, the scanner automatically applies the actions defined by the administrator.

- **Primary action**:

  Defines the first action to be performed in case an infected file is detected.

  Available options are the following:

  - **Repair**:

    Tries to repair the infected file.

  - **Rename**:

    Renames the infected file. Direct access to this file is no longer possible (by double-click). This file can be repaired later and renamed to its original name.

  - **Move to quarantine**:

    Moves to quarantine the infected file.

  - **Delete**:

    Deletes the infected file.

  - **Ignore**:

    Allows the user to access the infected file. No action is applied.

  - **Overwrite and delete**:

    Overwrites the infected file with a default pattern and then deletes it. This file cannot be restored.

- **Secondary action**:

  Defines the second action to be performed in case an infected file is detected.

  The **Secondary action** can be configured only if the **Primary action** is set to **Repair**.

Available options to configure the secondary action are the following:

- **Rename**.
- **Move to quarantine**.
- **Delete**.
- **Ignore**.
- **Overwrite and delete**.

For more information, see "Primary action:", page 536.

- **Scan archives**:

  Scans compressed files on the user's workstation.

- **Use smart extensions**:

  Scans only the files that are automatically selected by Avira. Scanning is based on file extension and content.

- **Limit recursion depth**:

  Controls the scan depth applied to archives.

  The archives nested into the main archives will be scanned depending on the depth selected by the administrator.

  Authorized values range from 1 to 99. The default value is 1. The recommended value is 20.

- **Scanner priority**:

  Defines the scanner priority levels.

  This option is useful when several processes are running on the user's workstation.

  The administrator's selection will impact scanning speed.

  Available options are the following:

  - **Low**:

    Scanner resources are managed by the operating system. The Scanner runs in the background if other processes are running on the user's workstation. If no other process is running, the Scanner will be allocated most processor time.

    This is the scanner priority level by default.

  - **Normal**:

    The Scanner runs in normal conditions. The operating system distributes evenly the processor time among all running processes.

  - **High**:

    The Scanner runs at maximum speed.

    Other running processes are considerably slowed down.

- **Scan rootkits**:

  Scans Windows system directory to check for rootkits.

- **Stop the scanner**:

  The user can stop at any time the scanning in progress on his workstation.

- **Scan network drives**:

  Disabling this option may prove useful when network drives are protected by another antivirus or another version of the antivirus.

- **Items to be excluded**.

PASSWORD PARAMETERS

The administrator can password-protect antivirus settings.

Fig. 15.9: Antivirus: Password Parameters

Two parameters are available:

- **Password**:

  The password can include a maximum of 20 alphanumeric characters. For security reasons, characters are replaced by asterisks.

- **Password-protected areas**:

  The administrator defines the areas to be password-protected.

  The user will have to enter this password to access protected areas.

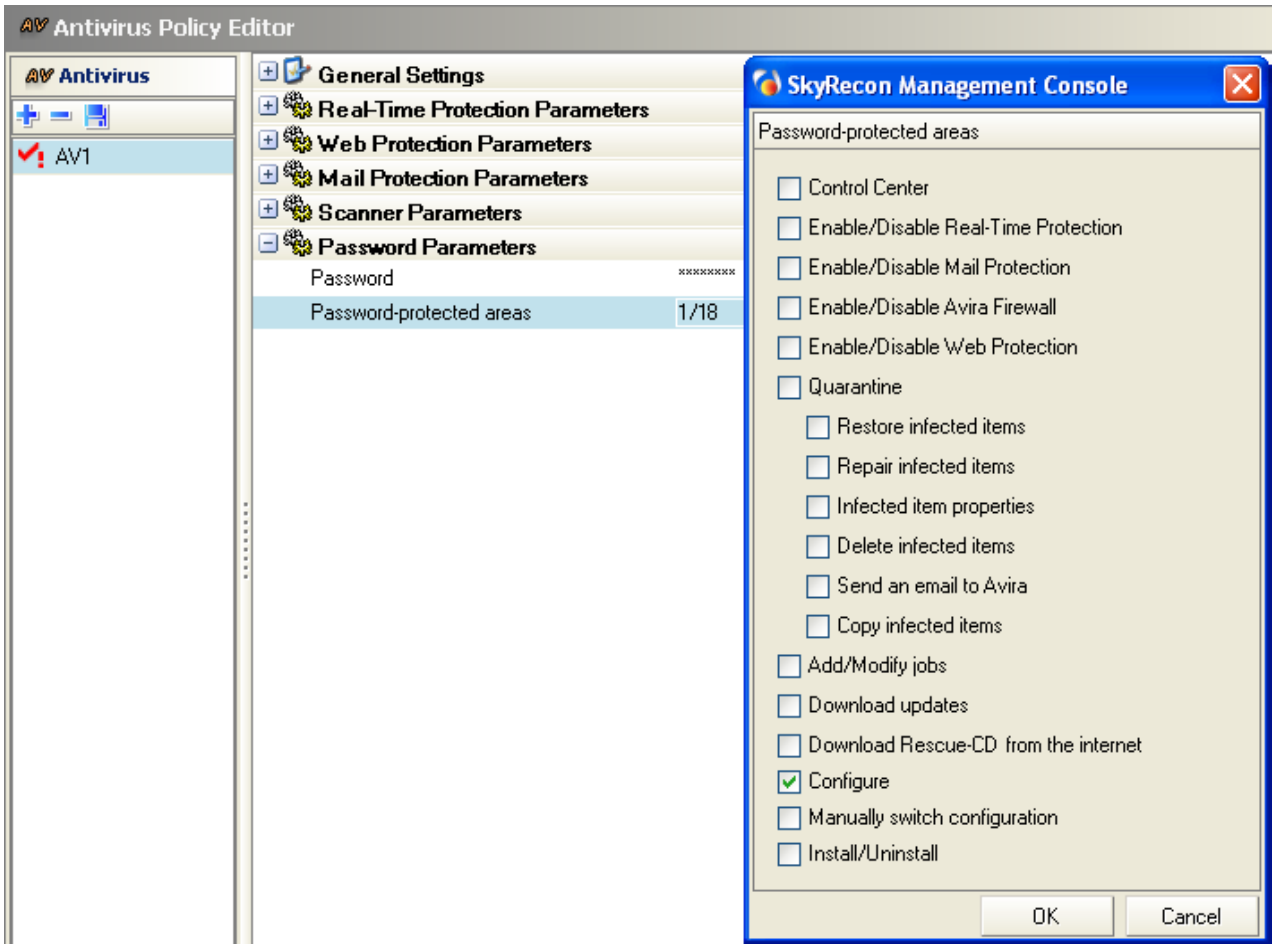


Fig. 15.10: Antivirus: Password Parameters: Password-protected areas

The administrator can enable/disable the password protection applied to the following areas:

- **Control Center**:

  Password required to start the Control Center.

- **Enable/Disable Real-Time Protection**:

  Password required to enable/disable Real-time protection.

- **Enable/Disable Mail Protection**:

  Password required to enable/disable Mail protection.

- **Enable/Disable Avira Firewall**:

  Password required to enable/disable Avira's firewall.

- **Enable/Disable Web Protection**:
  Password required to enable/disable Web protection.

- **Quarantine**:
  If the administrator checks the **Quarantine** box, all areas in the quarantine manager are checked by default:

  - **Restore infected items**:
    Password required to restore an infected item.
  - **Repair infected items**:
    Password required to repair an infected item.
  - **Infected item properties**:
    Password required to display the properties of an infected item.
  - **Delete infected items**:
    Password required to delete an infected item.
  - **Send emails to Avira**:
    Password required to send an email to Avira.
  - **Copy infected items**:
    Password required to copy an infected item.

- **Add/Modify jobs**:
  Password required to add or modify jobs in the Scheduler.

- **Download updates**:
  Password required to update the antivirus.

- **Download Rescue-CD from the internet**:
  Password required to download the antivirus rescue CD.

- **Configure**:
  Password required to configure the antivirus.

- **Manually switch configuration**:
  Password required to modify the antivirus configuration profile.

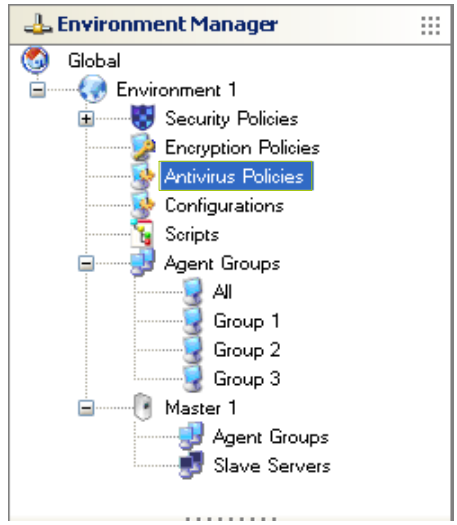
- **Install/Uninstall**:
  Password required to install or uninstall the antivirus.

ASSIGNING AN ANTIVIRUS POLICY TO AN AGENT GROUP

OVERVIEW

Antivirus Policies can be configured at two levels:

- Environment level:
  - General Settings.
  - Real-Time Protection Parameters.
  - Web Protection Parameters.
  - Mail Protection Parameters.
  - Scanner Parameters.
  - Password Parameters.
- Agent level in the **Options** tab under Encryption > Encryption Policies.



PROCEDURE

When assigning an antivirus policy to an agent group, follow the steps below:

1. Click to select the agent group (example: Group1).
2. Edit the agent group to access the **Options** tab.
3. Click the Browse button ... to select the antivirus policy to be assigned to the group under **Antivirus configuration** (example: AV1).
4. Click **Validate**.

5. Click **Synchronize** in the Environment Manager to apply your modifications to the agent group.

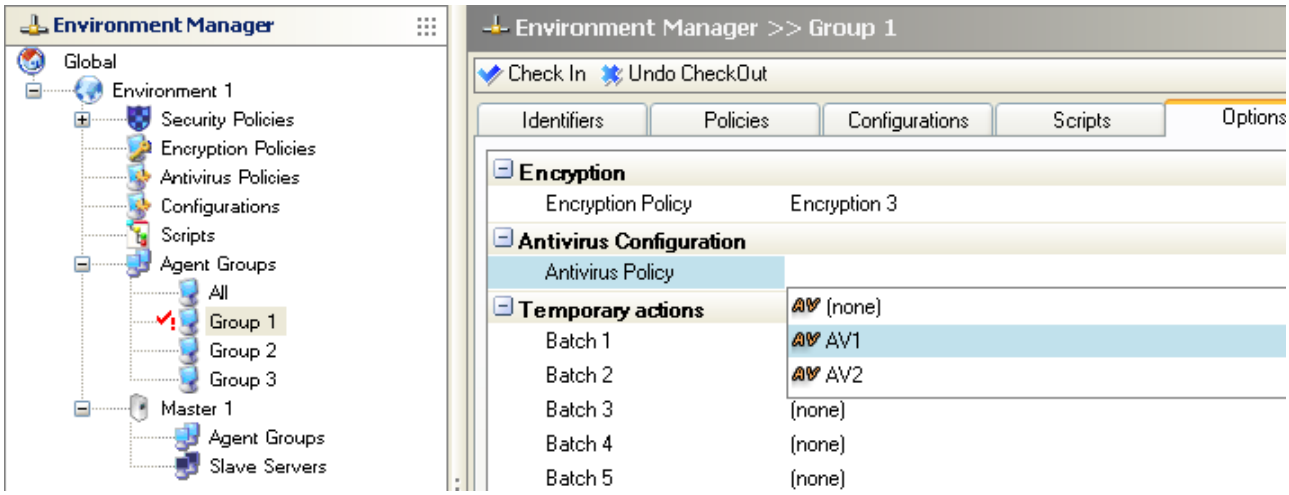


Fig. 15.11: Agent group: Antivirus Configuration

ANTIVIRUS USER INTERFACE

SYMBOLOGY

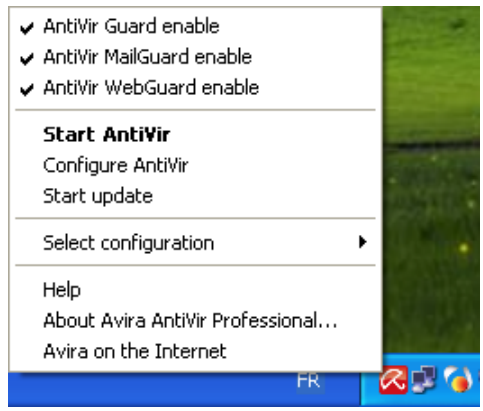
The antivirus protection is represented by the icon in the system tray on the agent computer.

Hovering the icon displays the product name (antivirus protection).

MENU

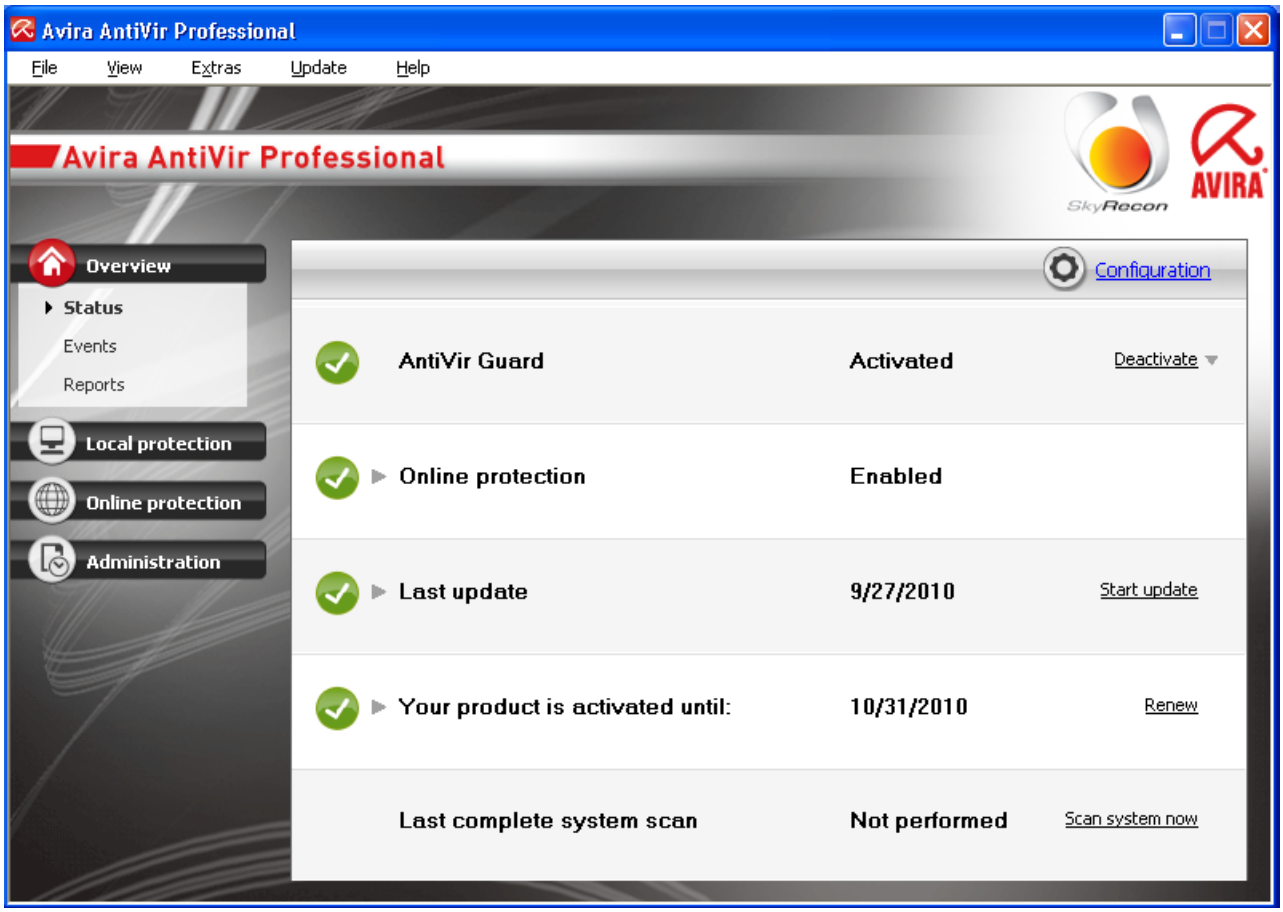
To select an action from the antivirus menu, follow the steps below:

1. When right-clicking the icon , the following menu is displayed depending on the settings enabled by the administrator:



2. Select the action to be applied.

3. If you select **Start AntiVir**, the following window is displayed.
   You can select any action available, depending on the administrator's settings.



4. Wait until the process is completed.

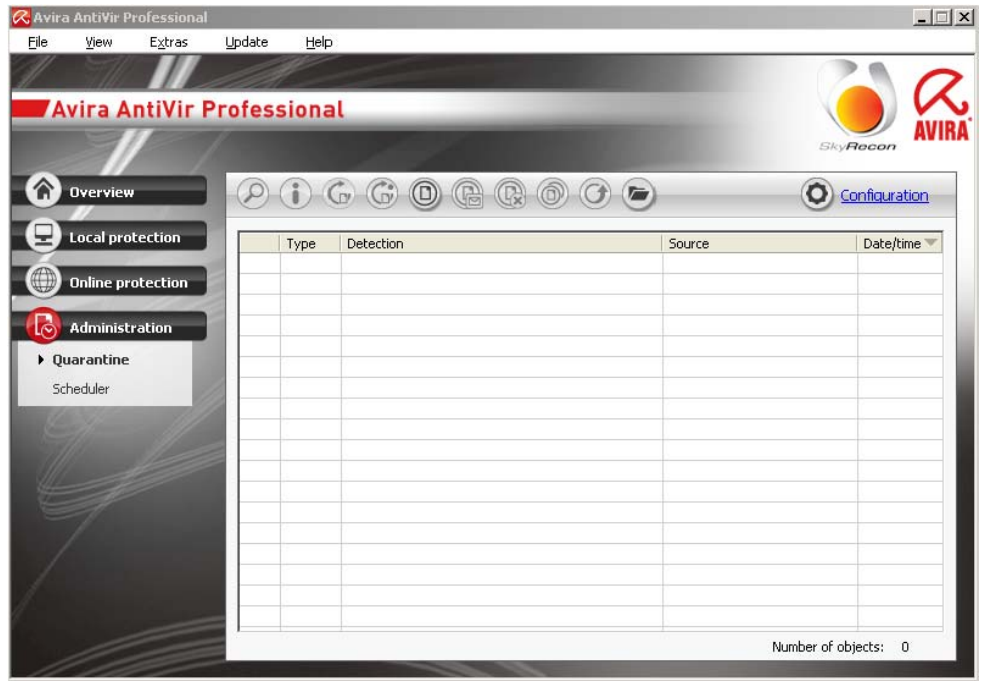
ADMINISTERING QUARANTINE

To display the quarantined file list, the user must follow the steps below:

1. Right-click the StormShield Monitor icon in the system tray.

2. Select from the menu **View** > **Administration** > **Quarantine**.

   Any operations performed on the quarantined files (new scan, quarantined file removal, repair, etc.) are performed in the Avira console.



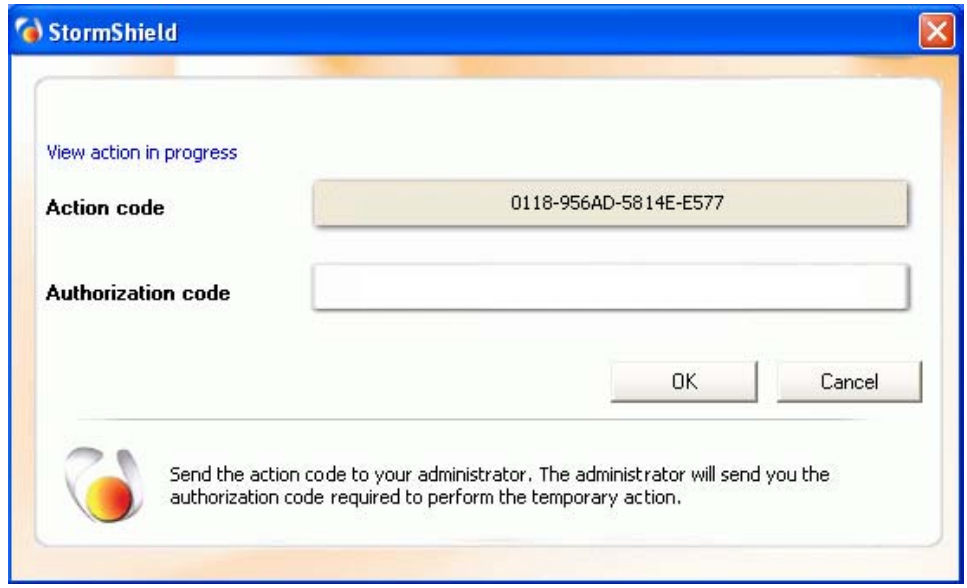
STOPPING THE ANTIVIRUS TEMPORARILY

To suspend the antivirus protection, the user must follow the steps below:

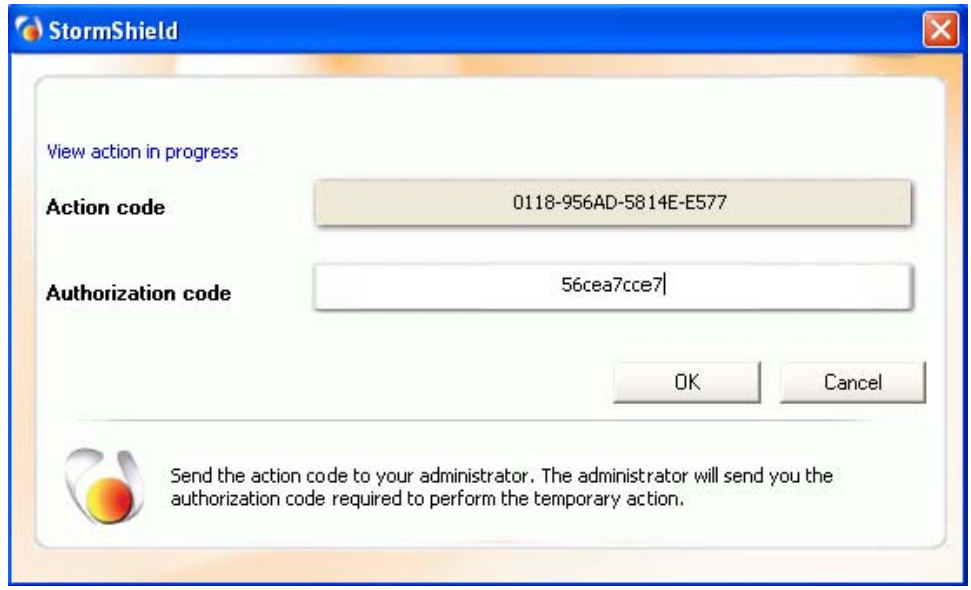
1. Right-click the StormShield Monitor icon in the system tray.
2. Select **Other operations > Temporary custom actions**.

   For more information, see "User sending a temporary action request to the administrator", page 429.

3. Send your **Action code** to the administrator.
The administrator will send you the **Authorization code** displayed on his console.



4. Enter the authorization code in the **Authorization code** field.



5. Click **Validate** to start the temporary action on your workstation.

The antivirus icon becomes .

Chapter 16

STORMSHIELD REPORTING

ABOUT THIS CHAPTER

This chapter describes the reports available in StormShield and how to access them.

This chapter includes the following:

- Report management:
  - Two-level management:
    - Reporting level.
    - Role Manager level.
  - Report path.
- Report description:
  - Categories.
  - Types.
- Graphical interface:
  - Menu bar.
  - Display settings:
    - Options.
    - Filters.

- Real-Time reports:
  - Servers and Agents.
  - Workstation Integrity.
  - System Security.
  - Removable Devices.
  - Antivirus.

- Historical reports:
  - Servers and Agents.
  - Removable Devices.
  - Workstation Integrity

REPORT MANAGEMENT

StormShield reports are managed at two levels on the SkyRecon management console:

- **Reporting** level.
- **Role Manager** level.

Both levels are accessible from the Management and Monitoring Tools panel.

TWO-LEVEL MANAGEMENT

Reporting level

To generate and view reports, the administrator clicks **Reporting** in Management and Monitoring Tools on the SkyRecon management console.

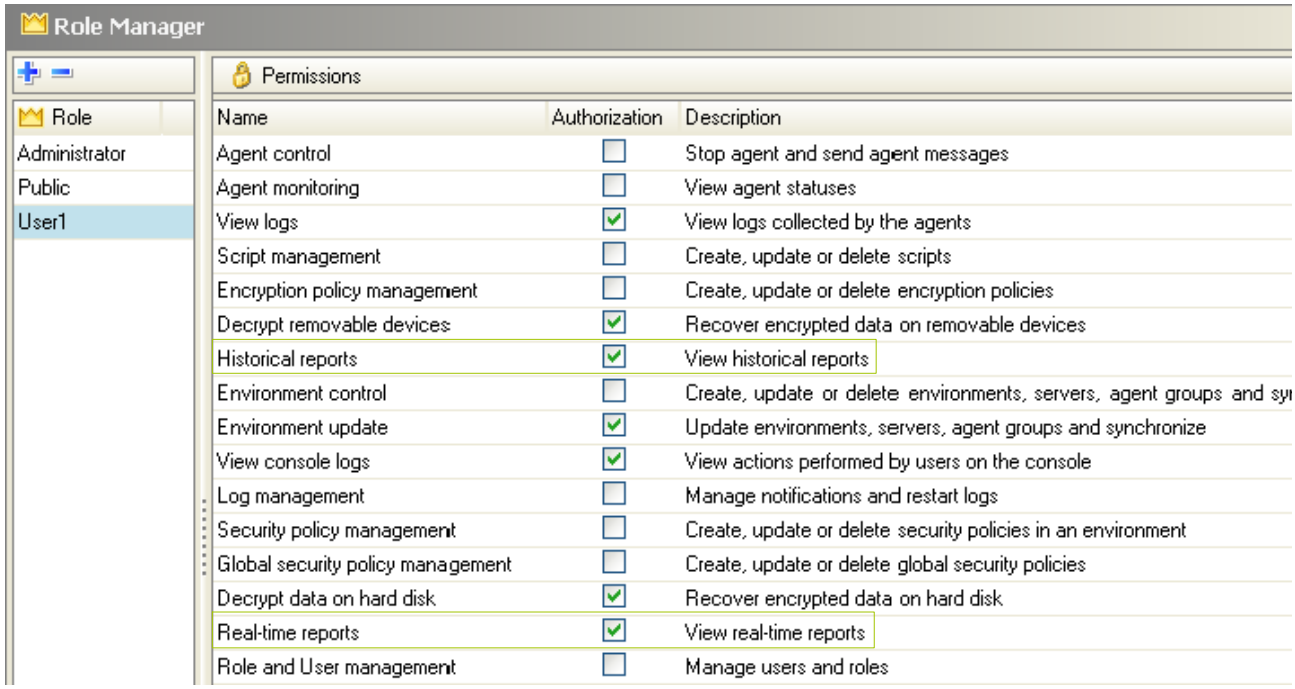
Role Manager level

To generate and view reports, the console user must have appropriate permissions.

Permissions are given to the console user by the administrator via the **Role Manager** in Management and Monitoring Tools.

The administrator determines who has access rights to reports by checking the appropriate boxes in the **Role manager**.

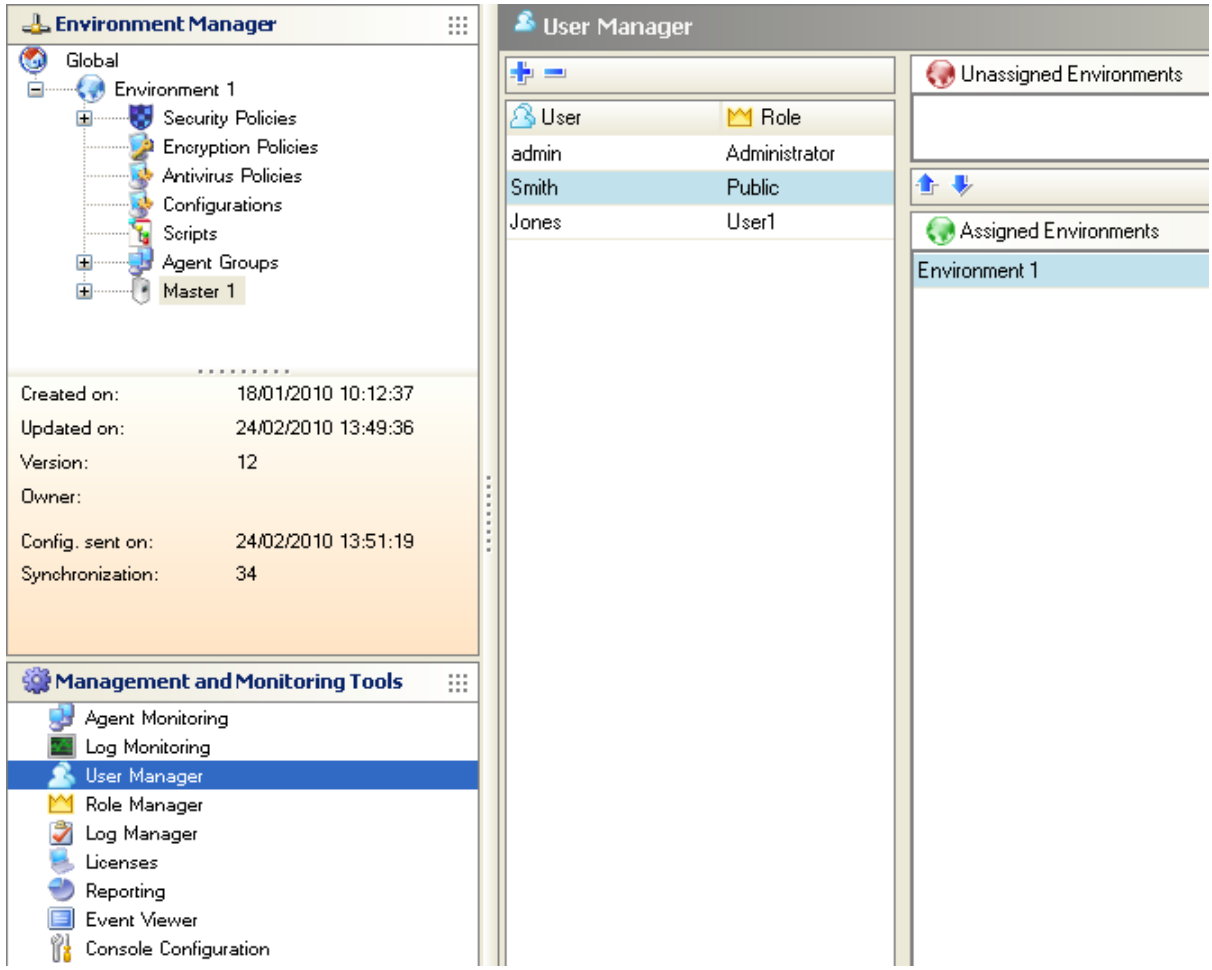
Example: **User1** is allowed to view historical reports and real-time reports checked boxes).



Administrator and **Public** roles are created by default. They cannot be modified.

For more information, see "Role Manager", page 189.

Roles are assigned to console users via the **User Manager** in Management and Monitoring Tools.



For more information, see "User Manager", page 187.

REPORT PATH

The path followed by the information used to generate reports is described below:

1. Reports are based on the logs sent by the agents to the StormShield server.
2. The server sends these logs to the StormShield SQL database.
3. The database stores these logs.

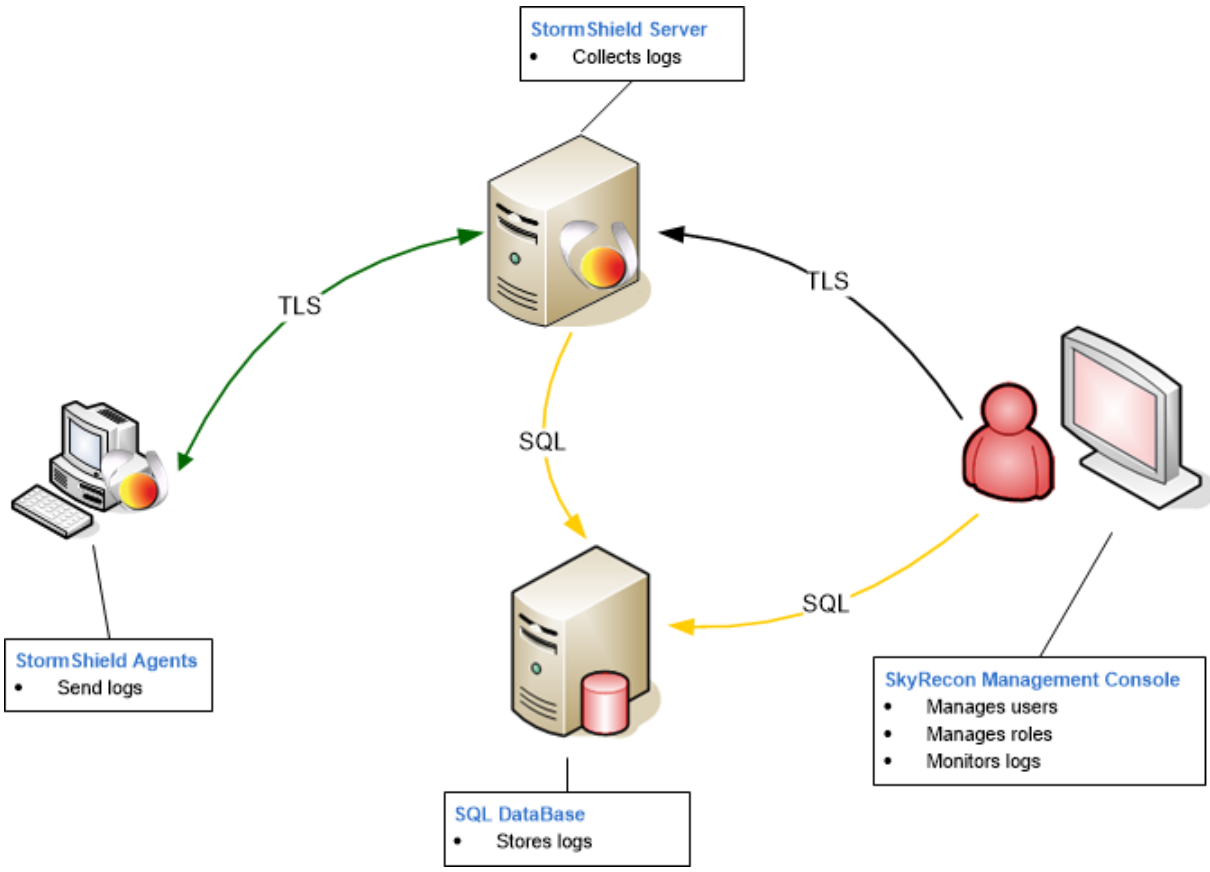


Fig. 16.1: StormShield report management

REPORT DESCRIPTION

CATEGORIES

There are five StormShield report categories:

- **Server and Agents**.
- **Workstation Integrity**.
- **System Security**.
- **Removable Devices**.
- **Antivirus**.

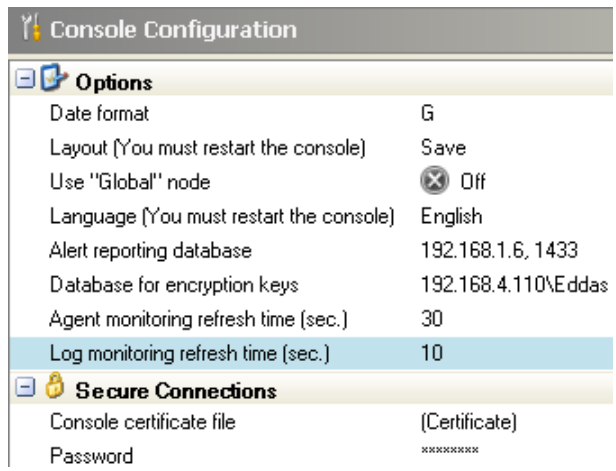
TYPES

Categories are divided into two report types:

- **Real-Time reports**.
- **Historical reports**.

The Real-Time type provides the latest information.

This information is automatically updated depending on the number of seconds set in **Log monitoring refresh time (sec.)** under **Console Configuration**.



You can also force reports to update by clicking **Update Report**.

GRAPHICAL INTERFACE

MENU BAR

The menu bar is displayed as follows:

Fig. 16.1 : Reporting: Menu bar

The menu bar contains the following actions:

- **Reports** :

  This action is used to select the category of report to be generated.
- **Save Report**:

  This action is used to save reports to the location specified, in the `.png` or `.csv` format.
- **Update Report**:

  This action is used to update reports.

DISPLAY SETTINGS

Options

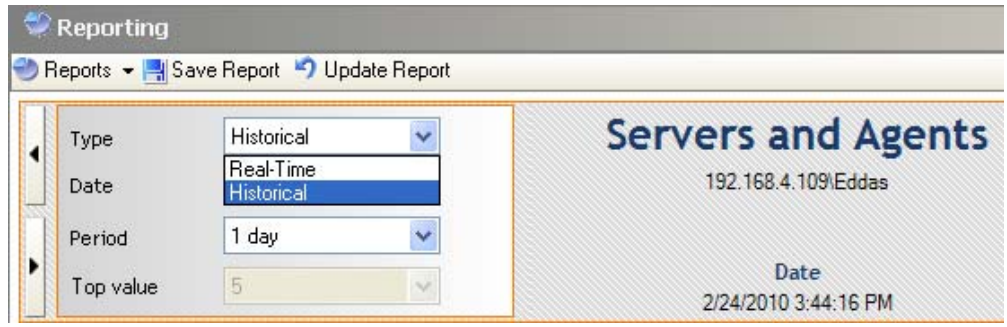
Depending on the category selected, the report can include the following options:

- Type.
- Date.
- Period.
- Top value.

Unavailable options are greyed out.

Type

This option is used to select the **Historical** or **Real-Time** report type.

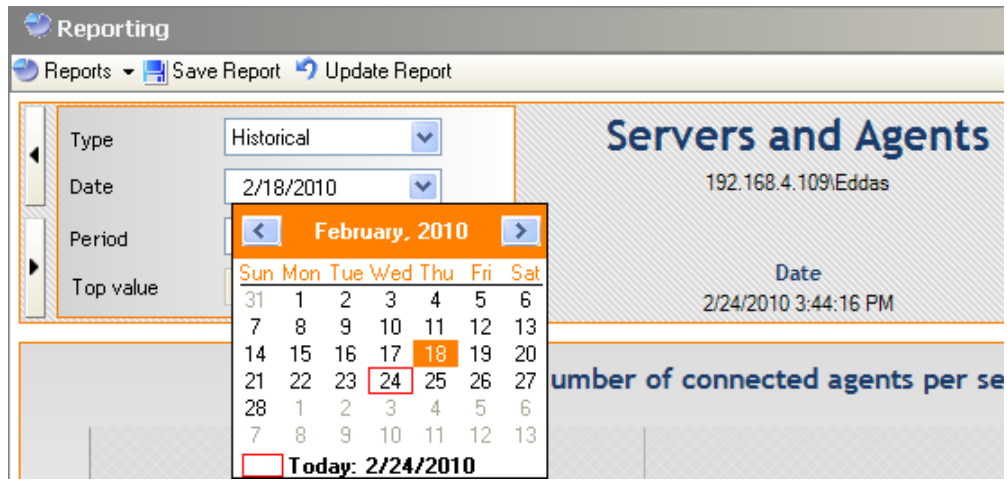


If you select **Real-Time**, the information displayed is the latest.

If you select **Historical**, the information displayed covers the time interval specified by the administrator.

Date

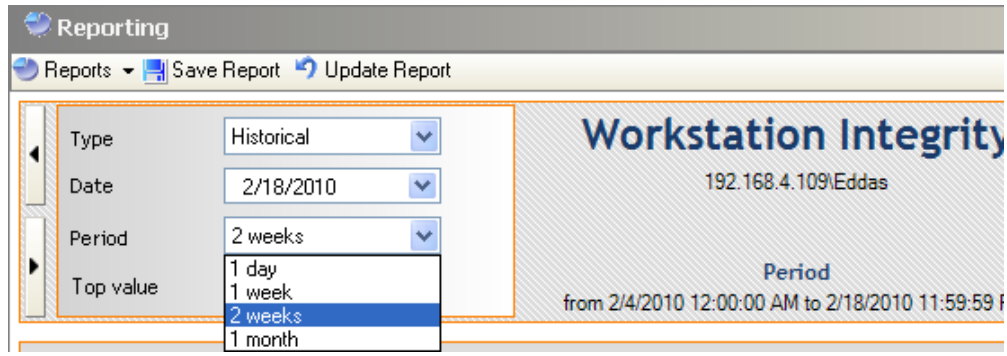
This option is used to select the start date to generate a **historical** report.
The current date is selected by default.



Period

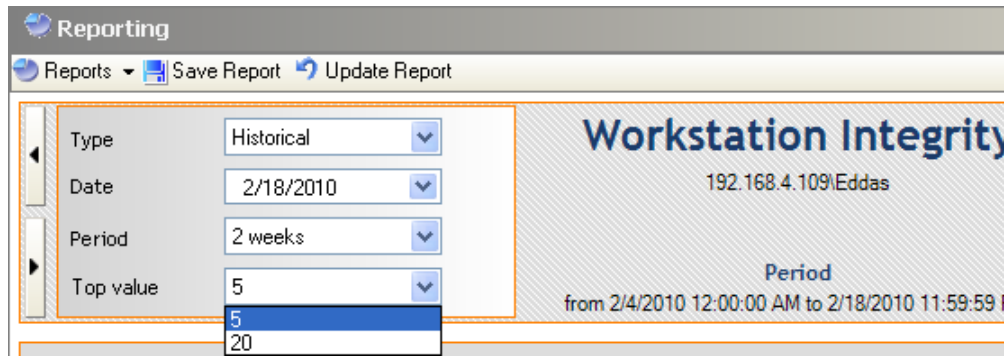
This option is used to define the time interval required to generate a **historical** report:

- 1 day.
- 1 week.
- 2 weeks.
- 1 month.



Top value

This option is used to select the top value (5 or 20) required to generate a report.

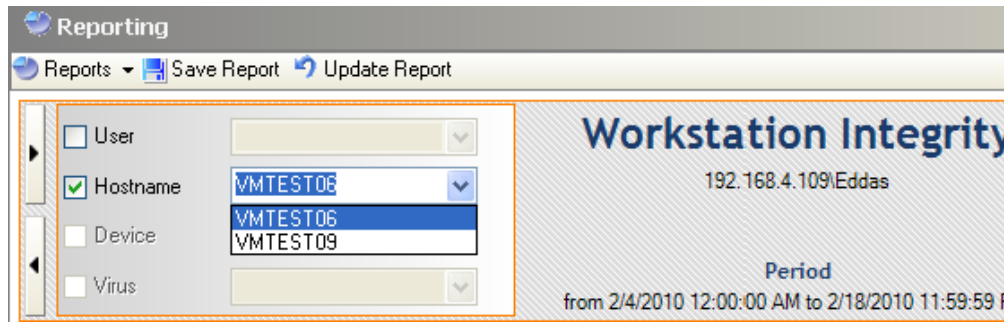


Filters

Depending on the category selected, the report can be generated by applying the following filters:

- User.
- Hostname.
- Device.
- Virus.

Unavailable filters are greyed out.

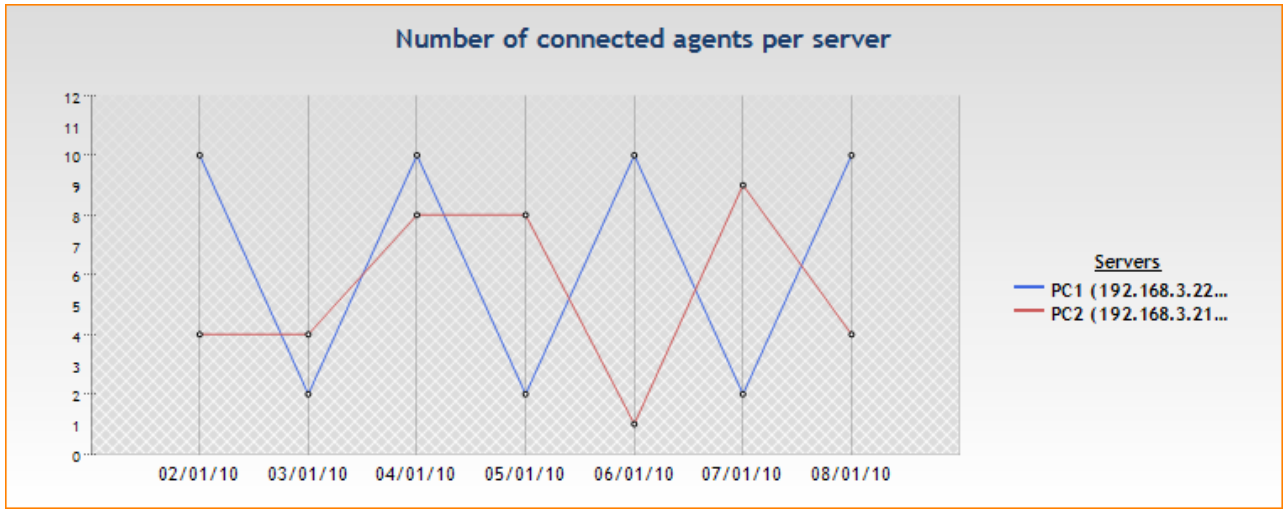


REAL-TIME REPORTS

SERVERS AND AGENTS

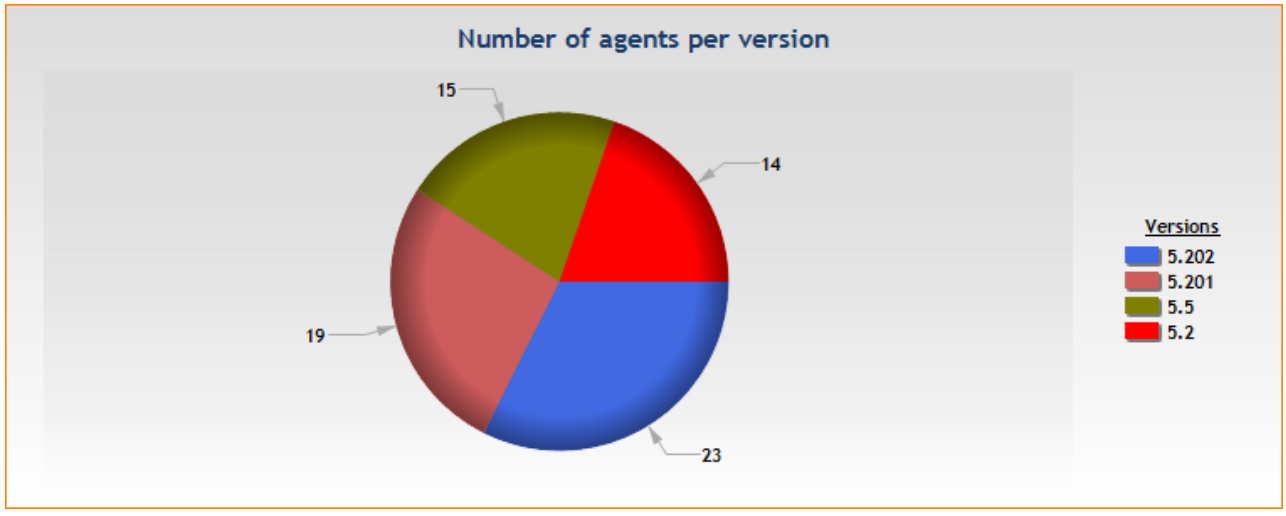
The Servers and Agents report provides information on the StormShield servers:

- **Number of connected agents per server:**



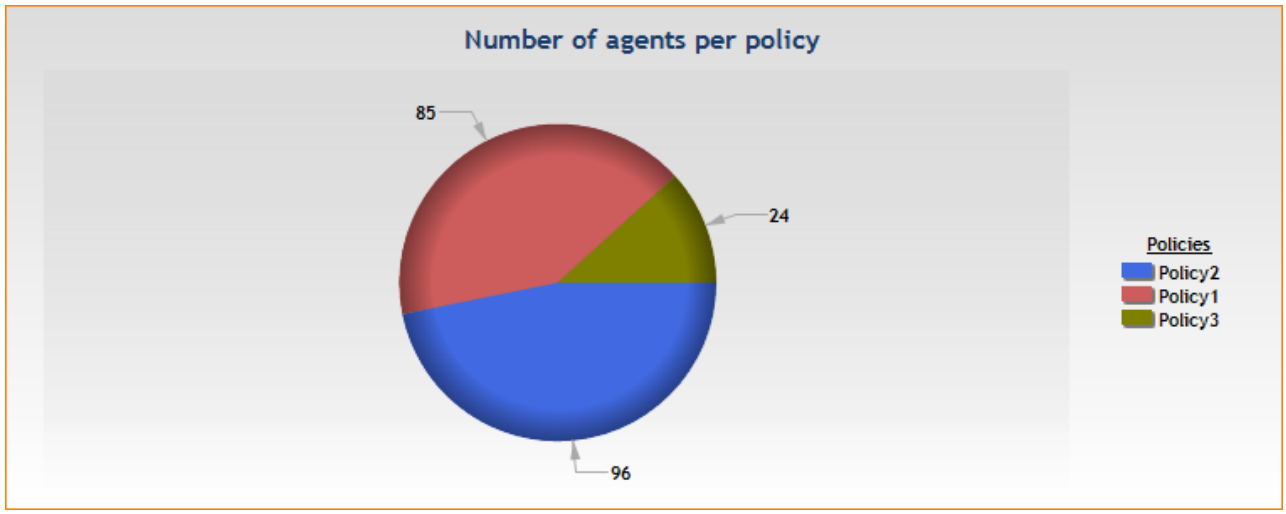
- **Number of agents per version:**

  It displays all the StormShield versions in use and the number of agents per version.



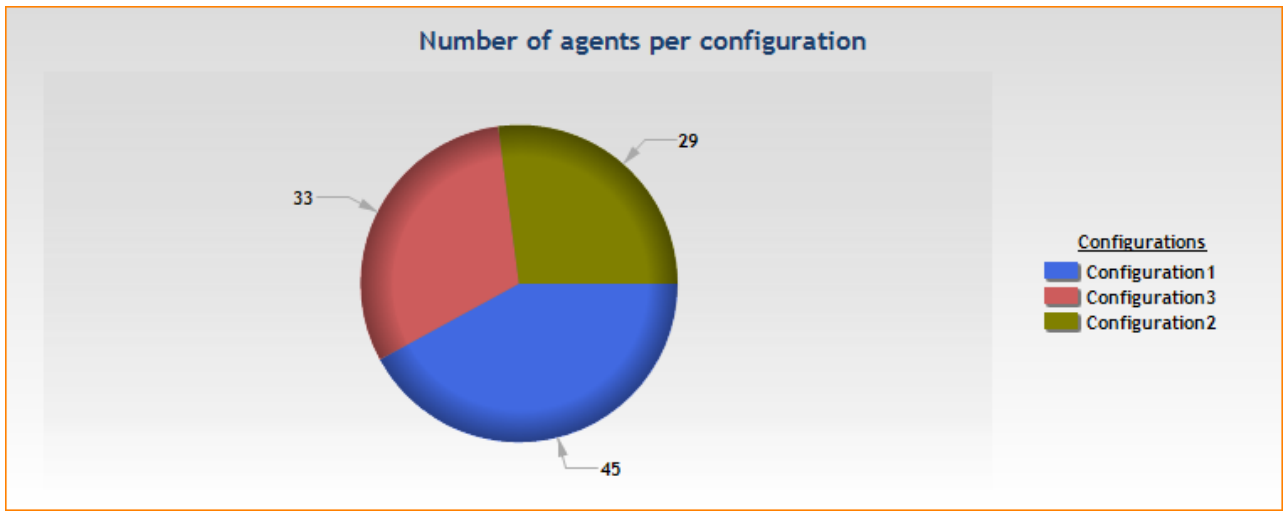
- **Number of agents per policy:**

  It displays the policies by name, and the number of agents which use this policy.



- **Number of agents per configuration:**

  It displays the configurations by name, and the number of agents which use this configuration.

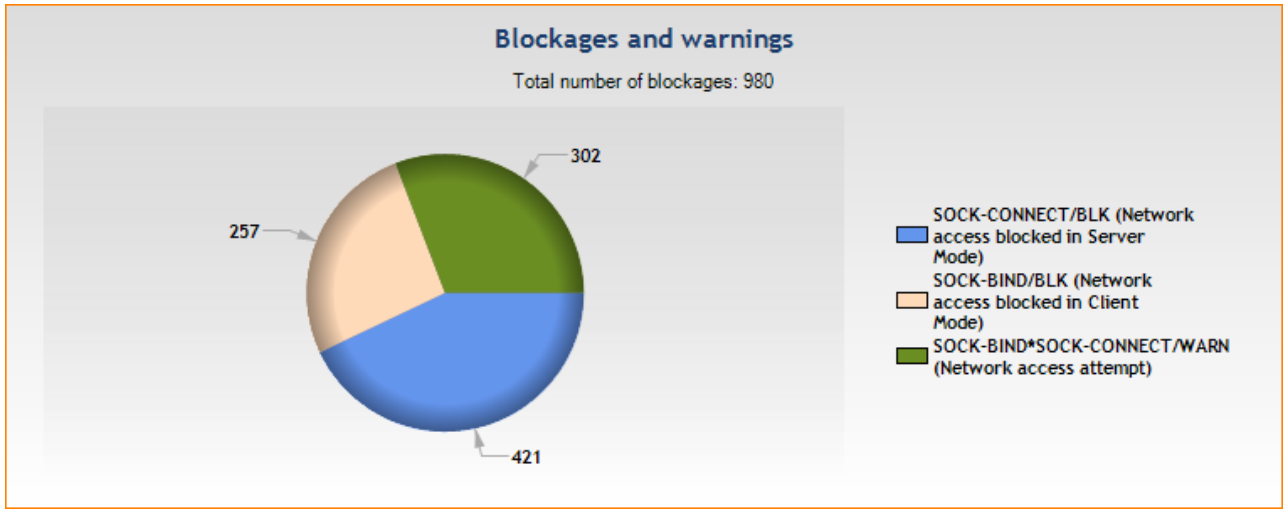


The captions displayed on the right of the graphs are **interactive**. Graphs change when hovering the caption items with your mouse.

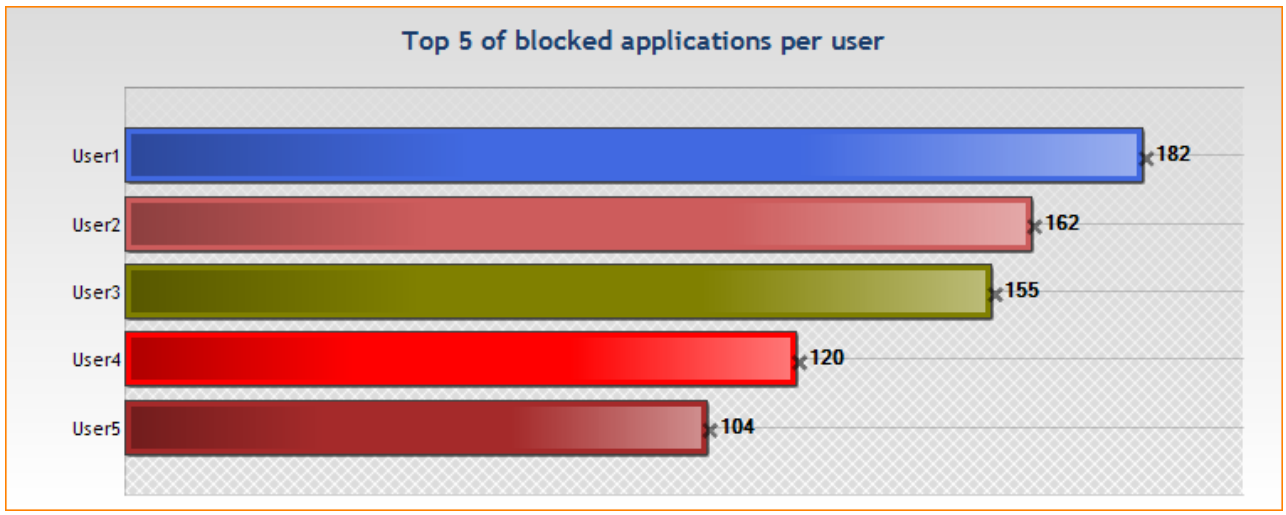
WORKSTATION INTEGRITY

The Workstation Integrity report provides the following information:

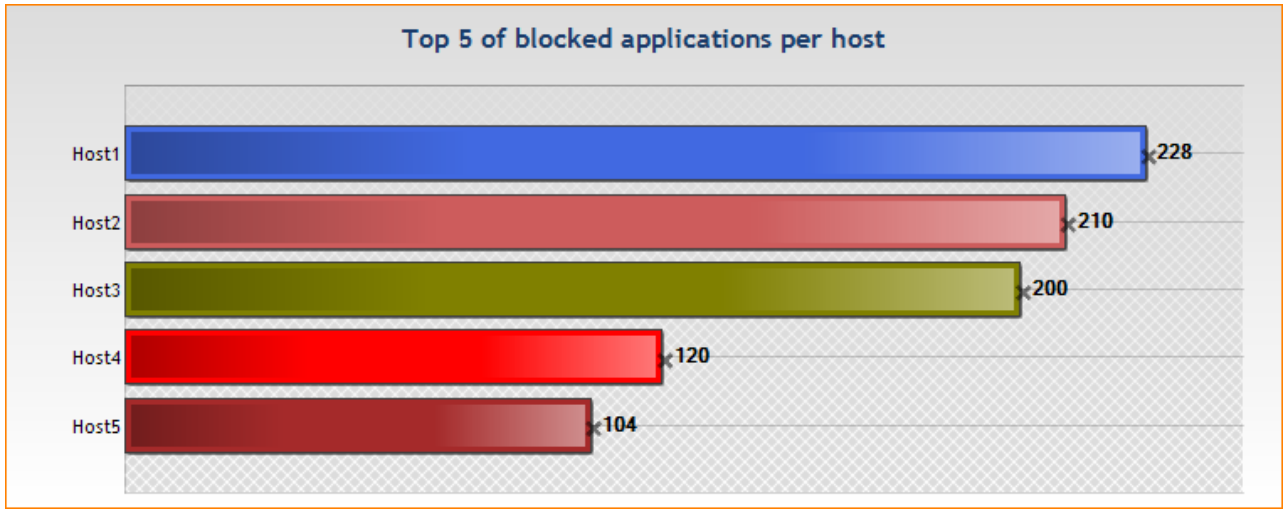
- **Blockages and warnings:**



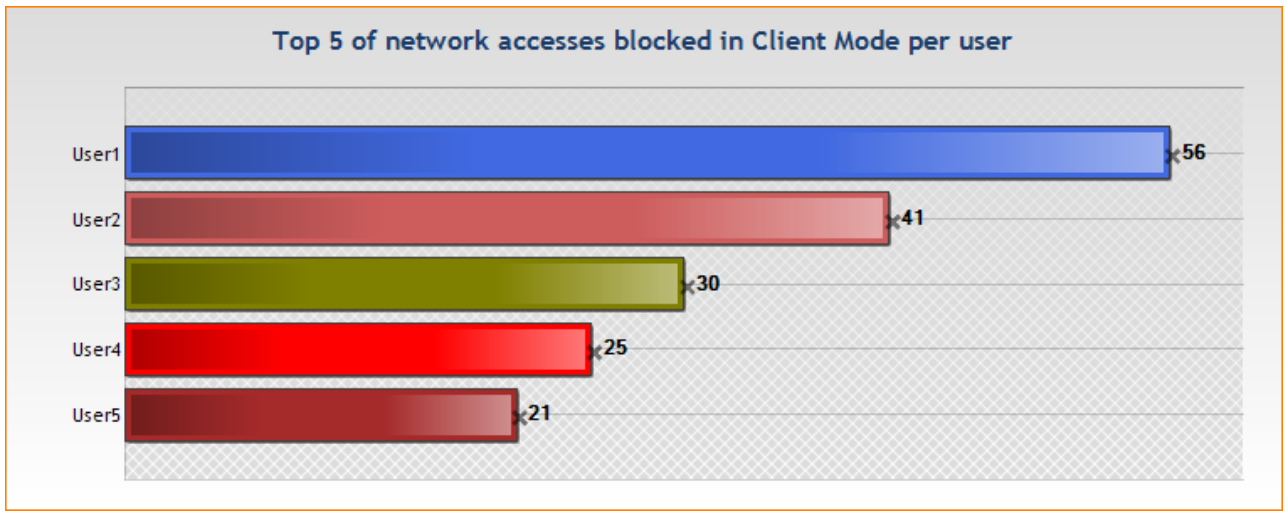
- **Top [5] of blocked applications per user:**



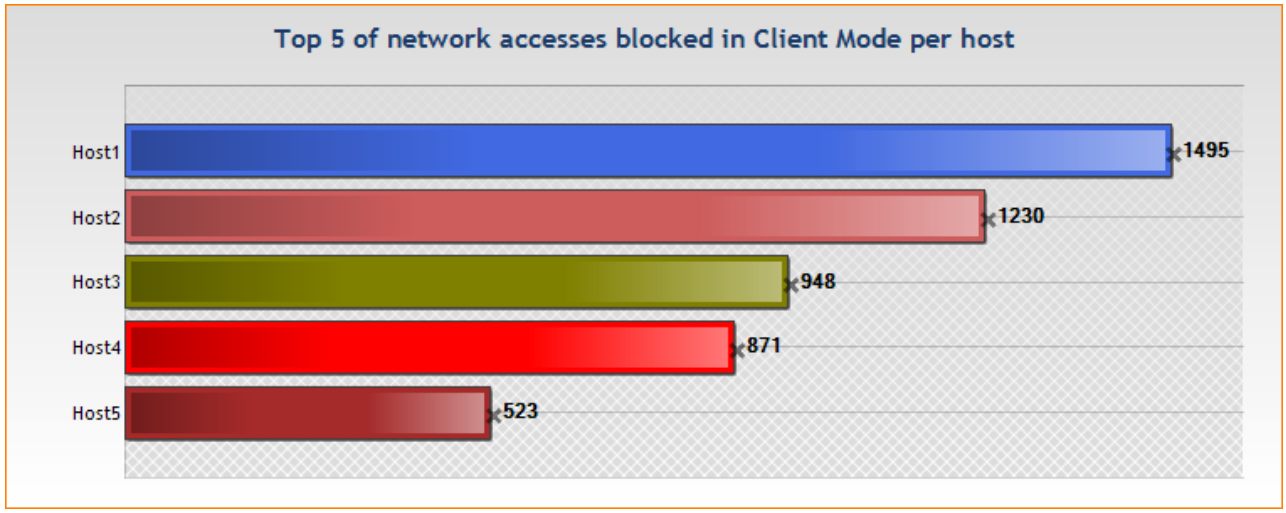
- **Top [5] of blocked applications per host:**



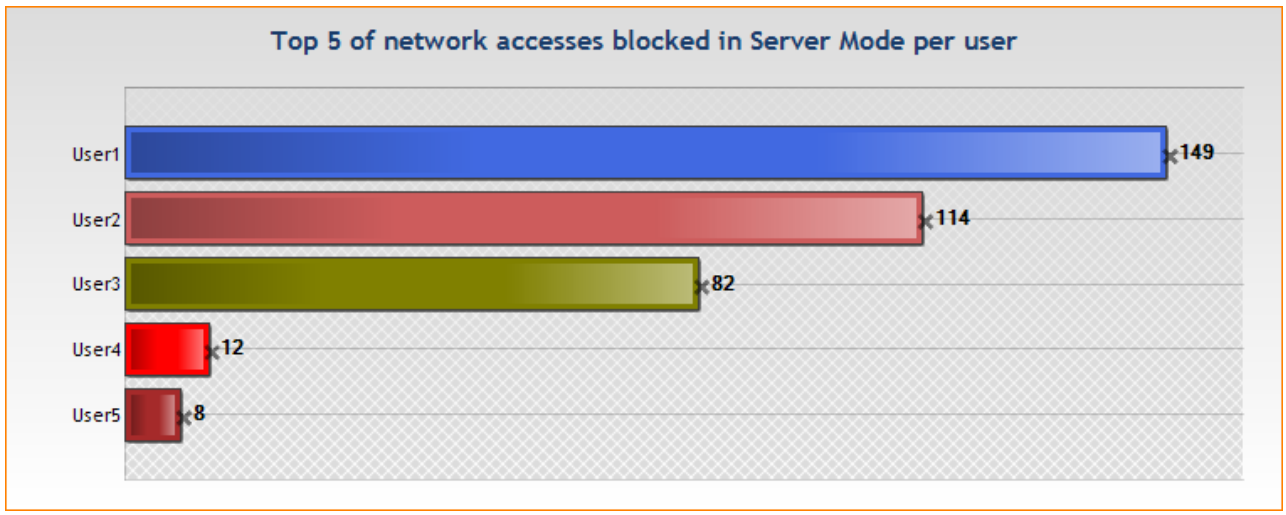
- **Top [5] of network accesses blocked in Client Mode per user:**



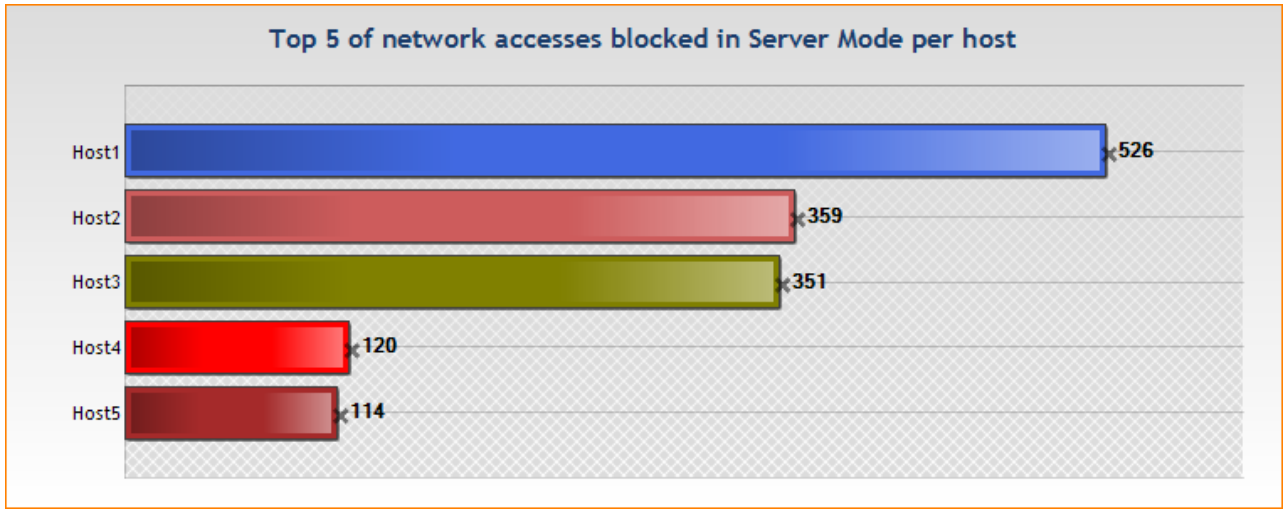
- **Top [5] of network accesses blocked in Client Mode per host:**



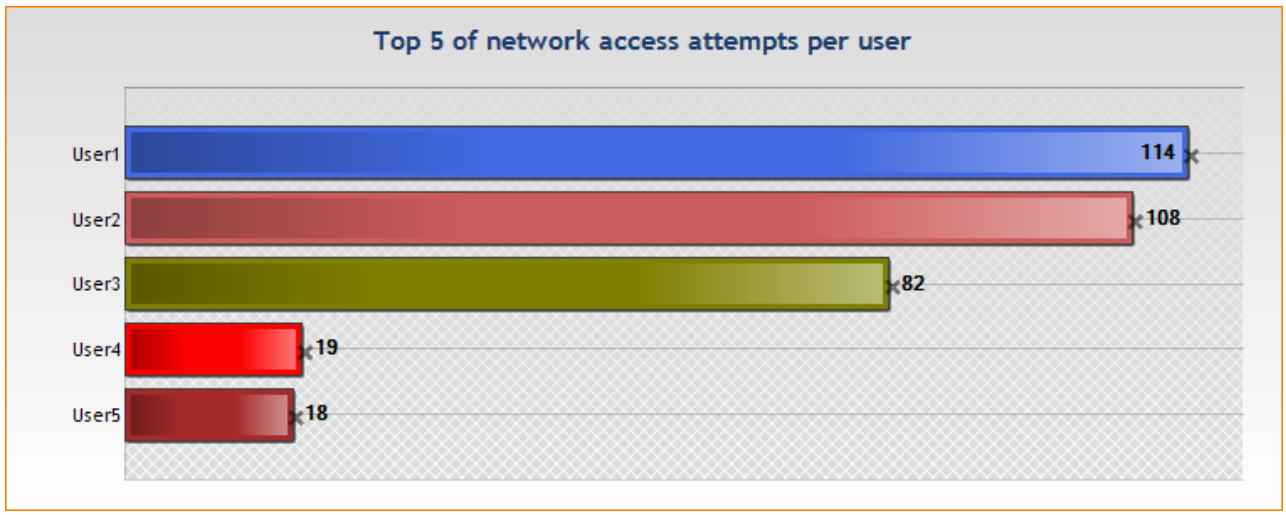
- **Top [5] of network accesses blocked in Server Mode per user:**



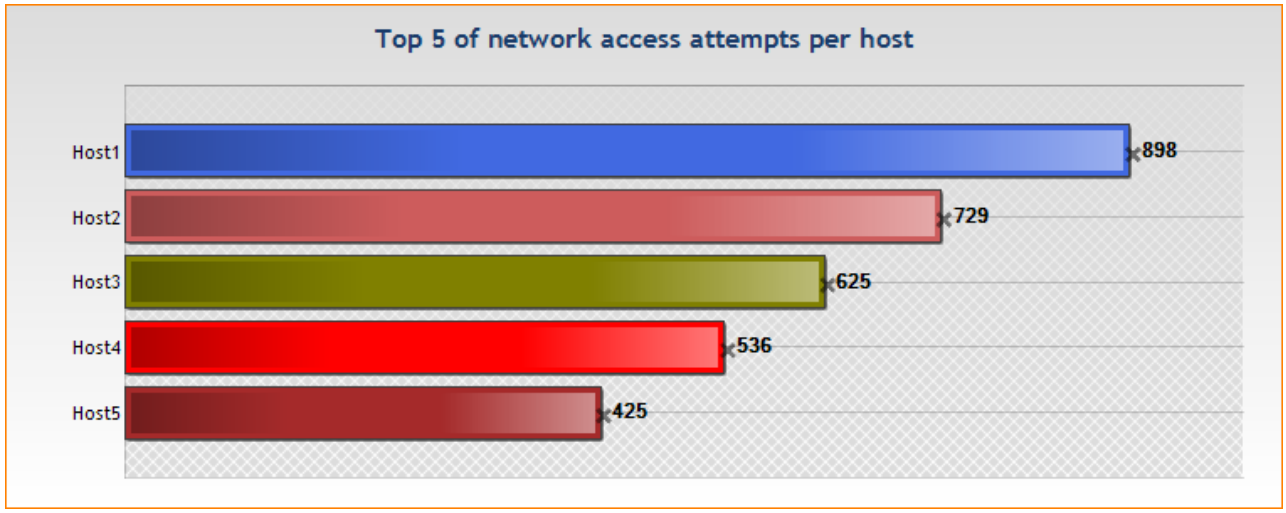
- **Top [5] of network accesses blocked in Server Mode per host:**



- **Top [5] of network access attempts per user:**



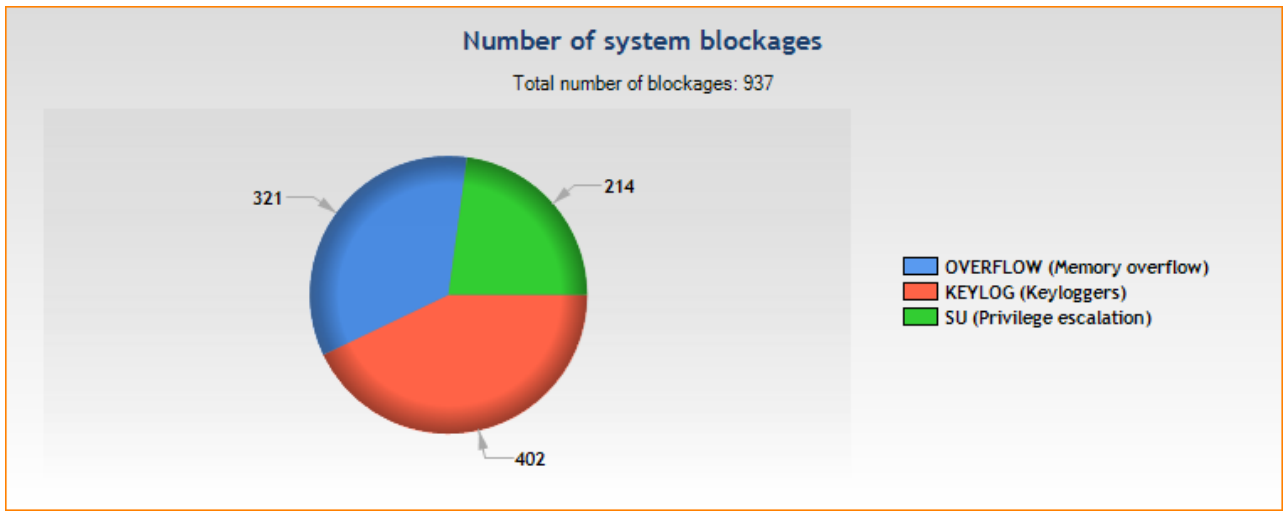
- **Top [5] of network access attempts per host:**



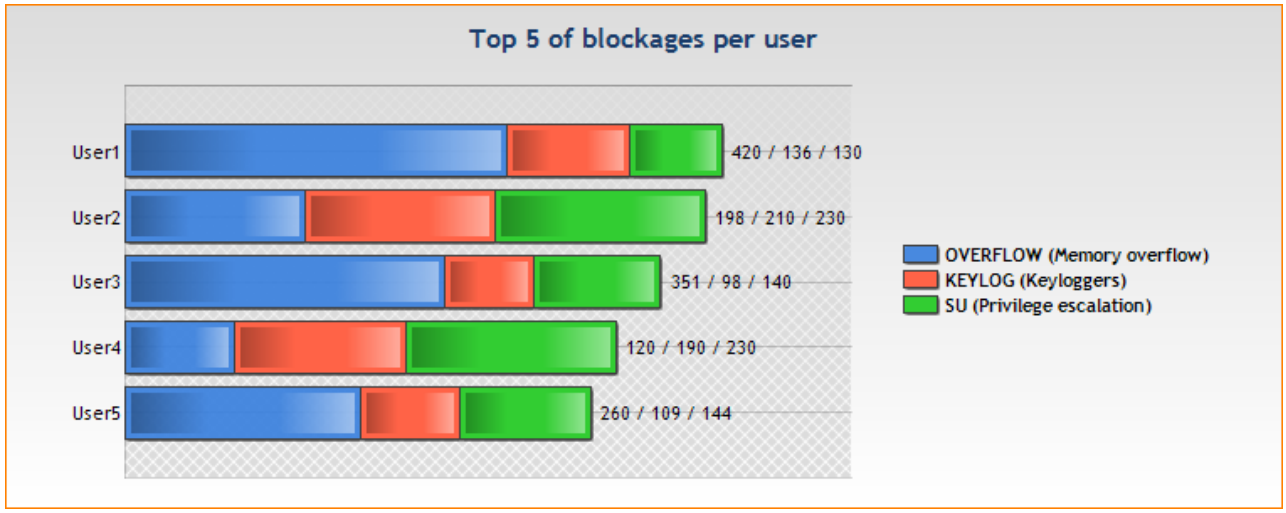
SYSTEM SECURITY

The System Security report provides the following information:

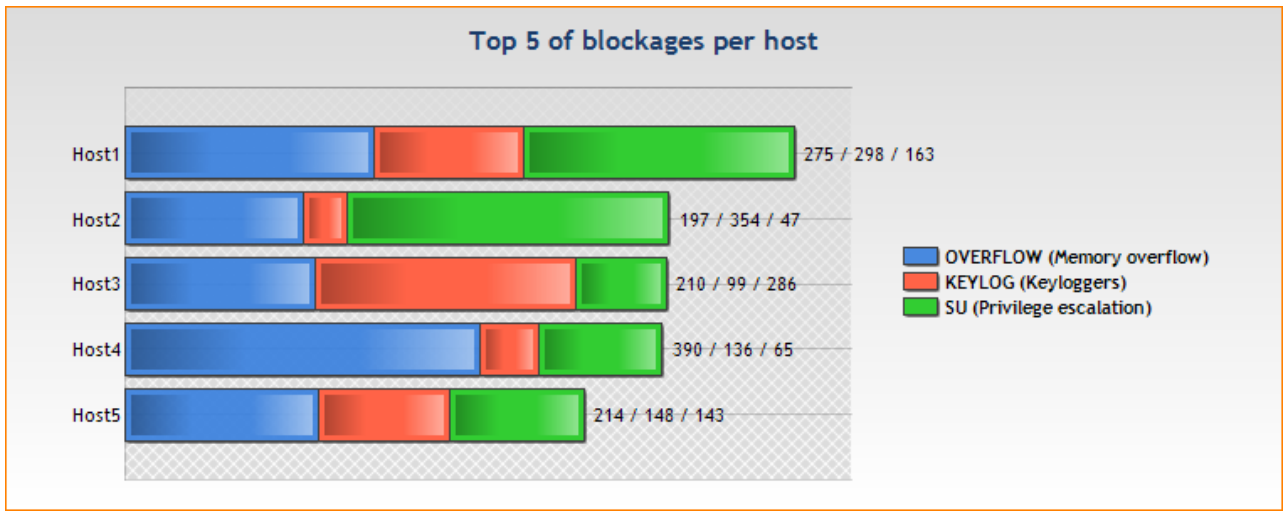
- **Number of system blockages:**



- **Top [5] of blockages per user:**



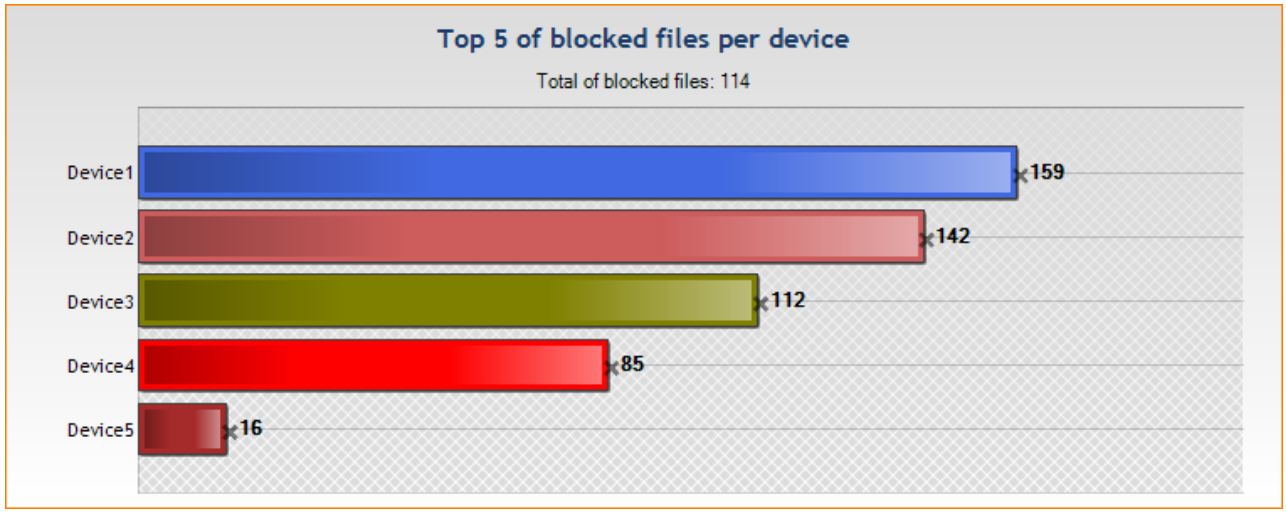
- **Top [5] of blockages per host:**



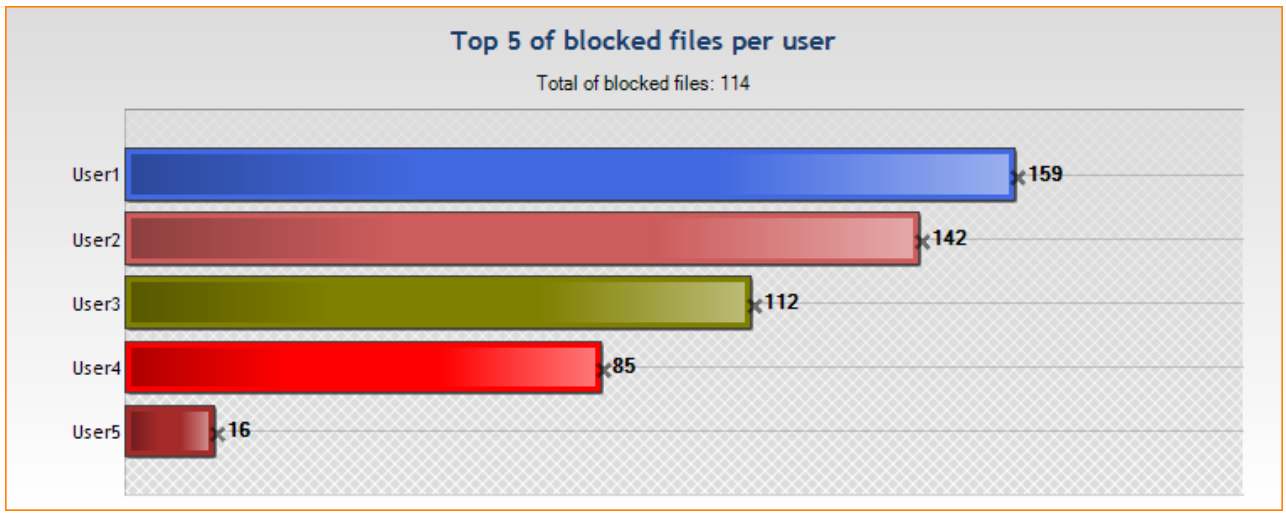
REMOVABLE DEVICES

The Removable Devices report provides the following information:

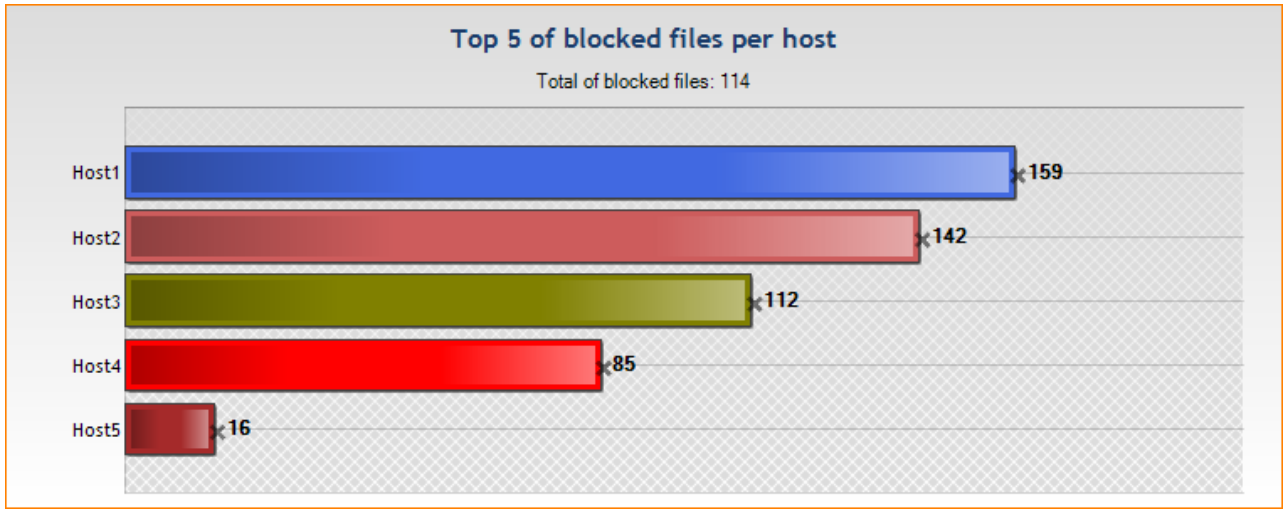
- **Top [5] of blocked files per device:**



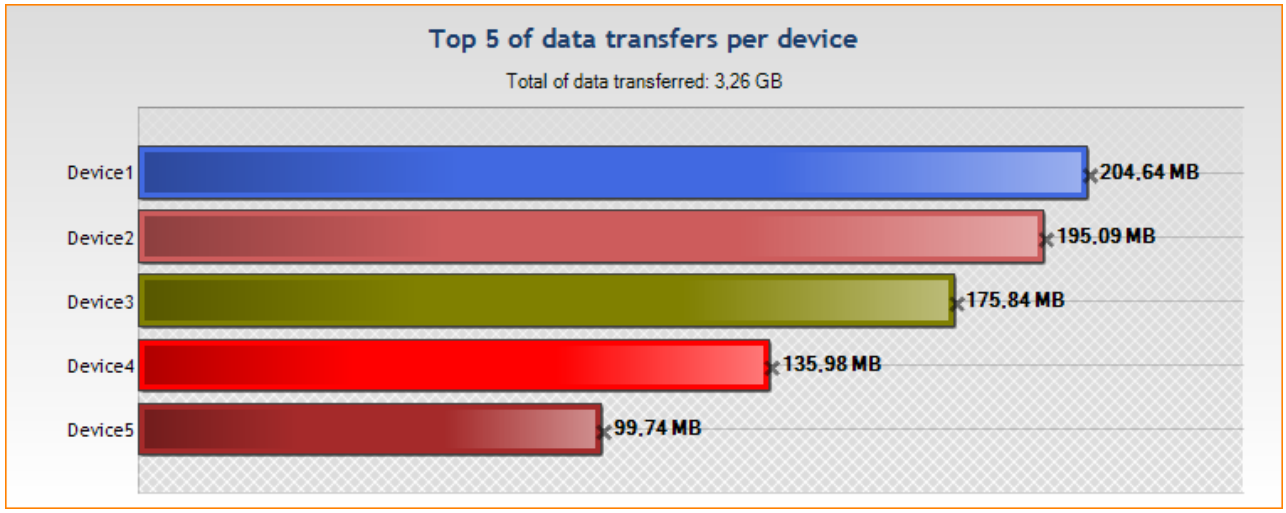
- **Top [5] of blocked files per user:**



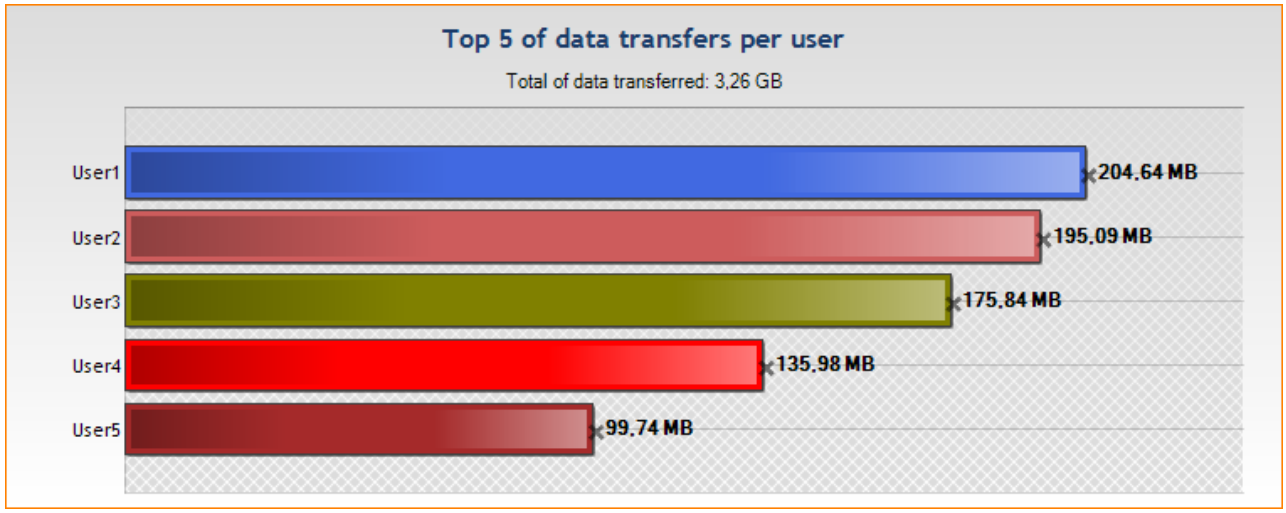
- **Top [5] of blocked files per host:**



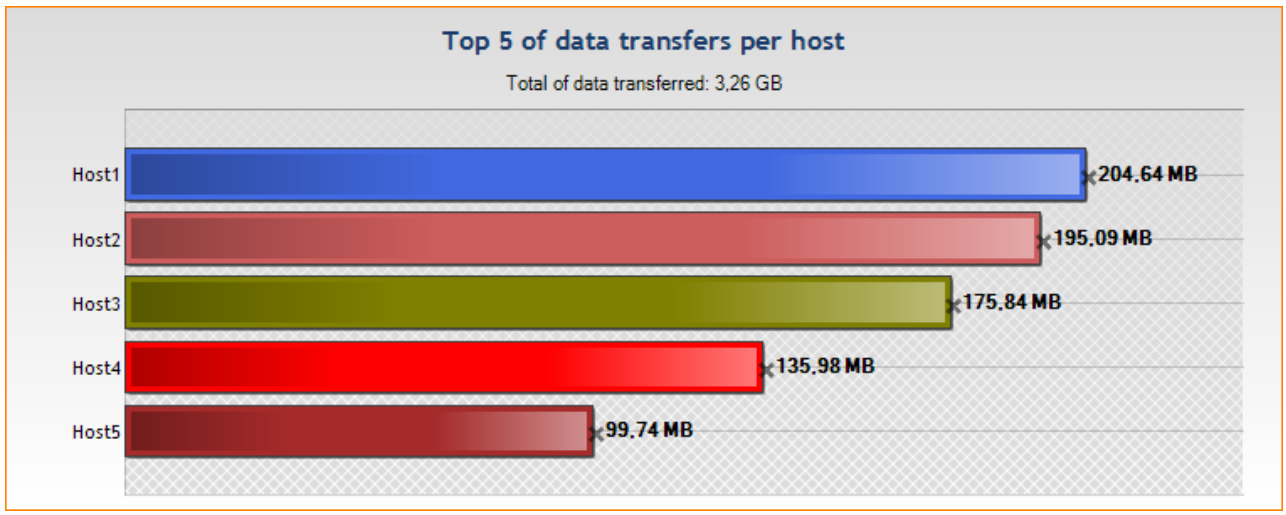
- **Top [5] of data transfers per device:**



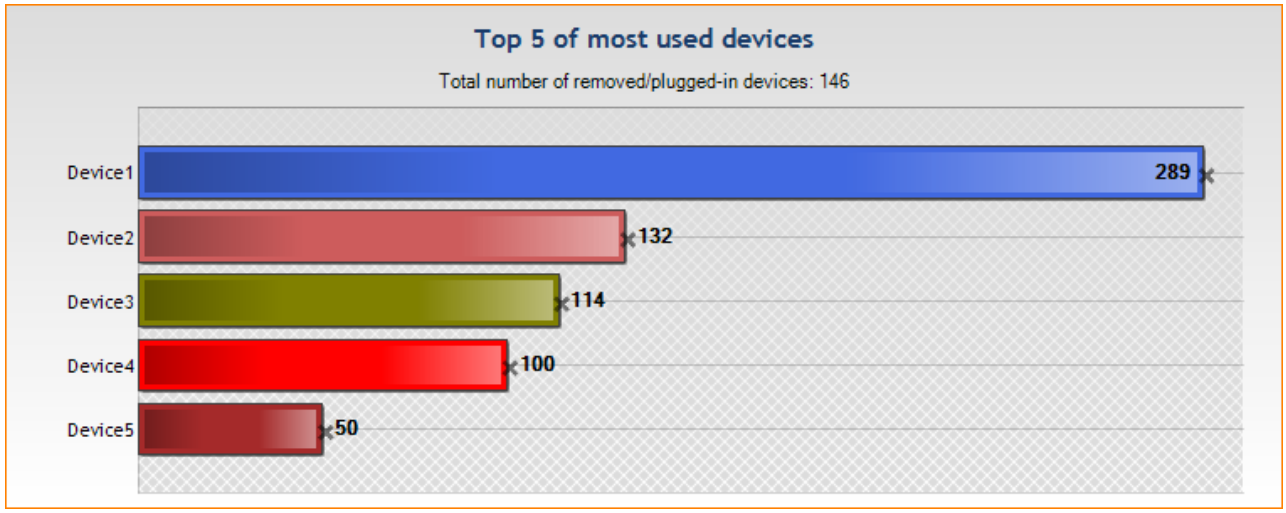
- **Top [5] of data transfers per user:**



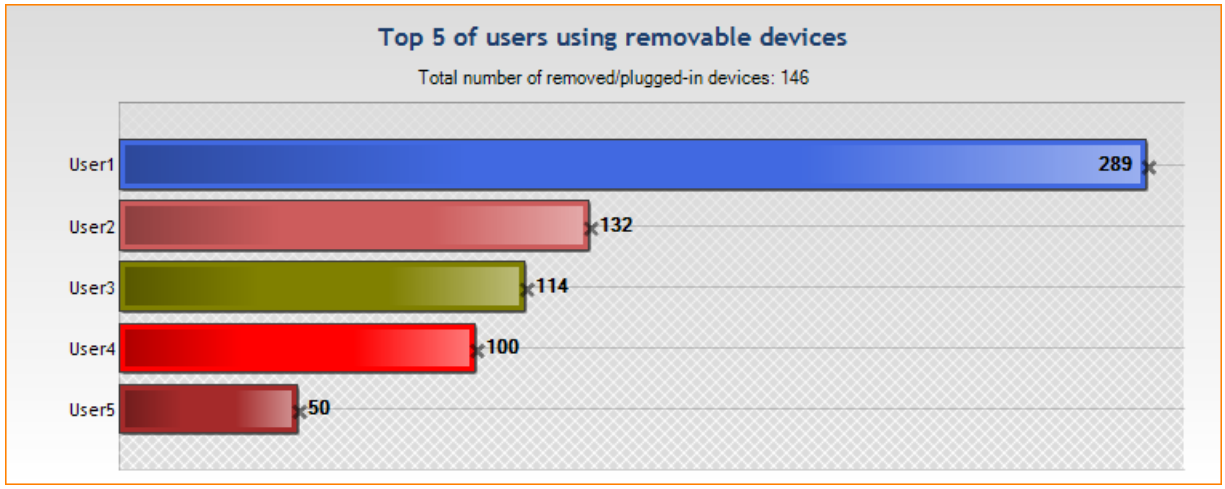
- **Top [5] of data transfers per host:**



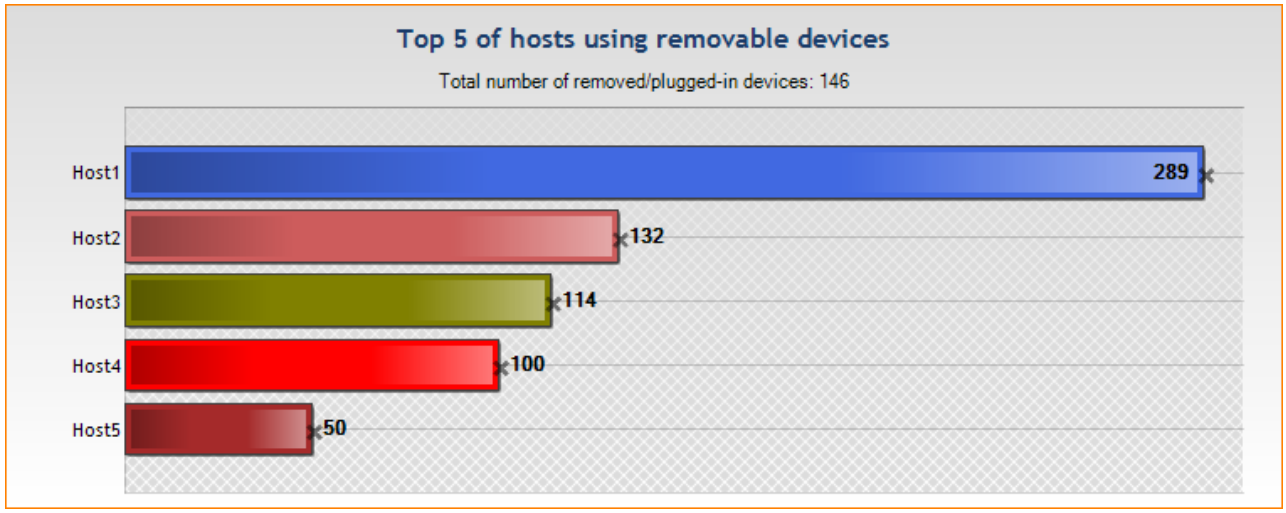
- **Top [5] of most used devices:**



- **Top [5] of users using removable devices:**



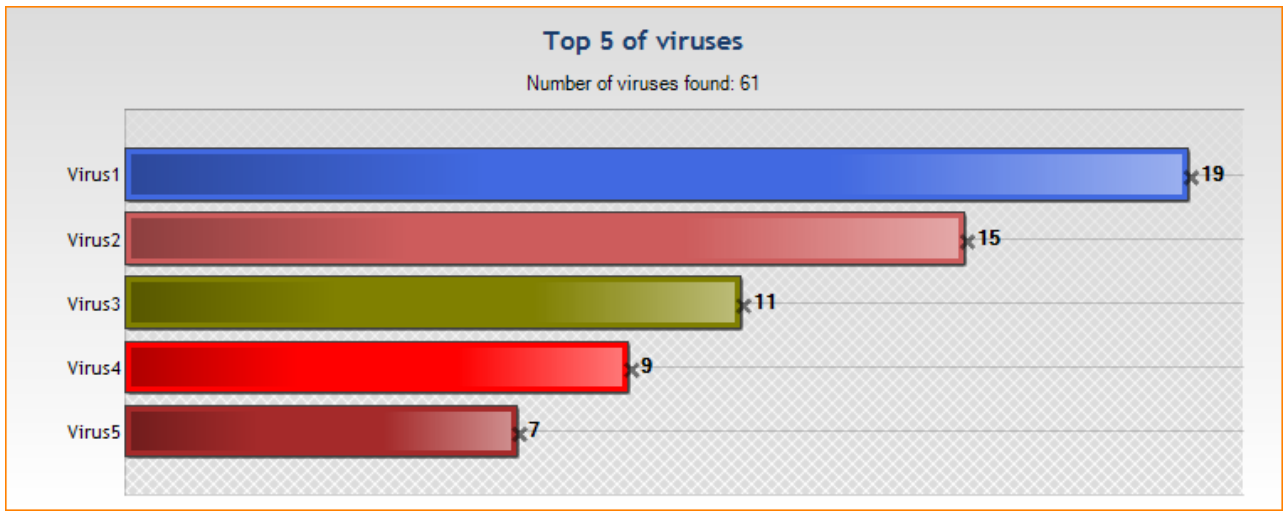
- **Top [5] of hosts using removable devices:**



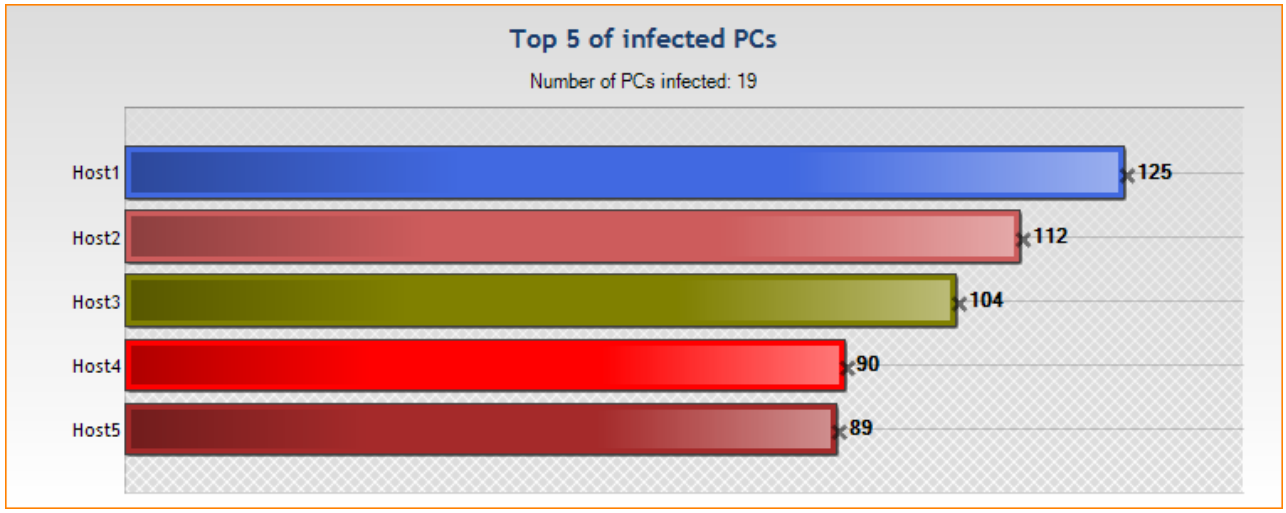
ANTIVIRUS

The Antivirus report provides the following information:

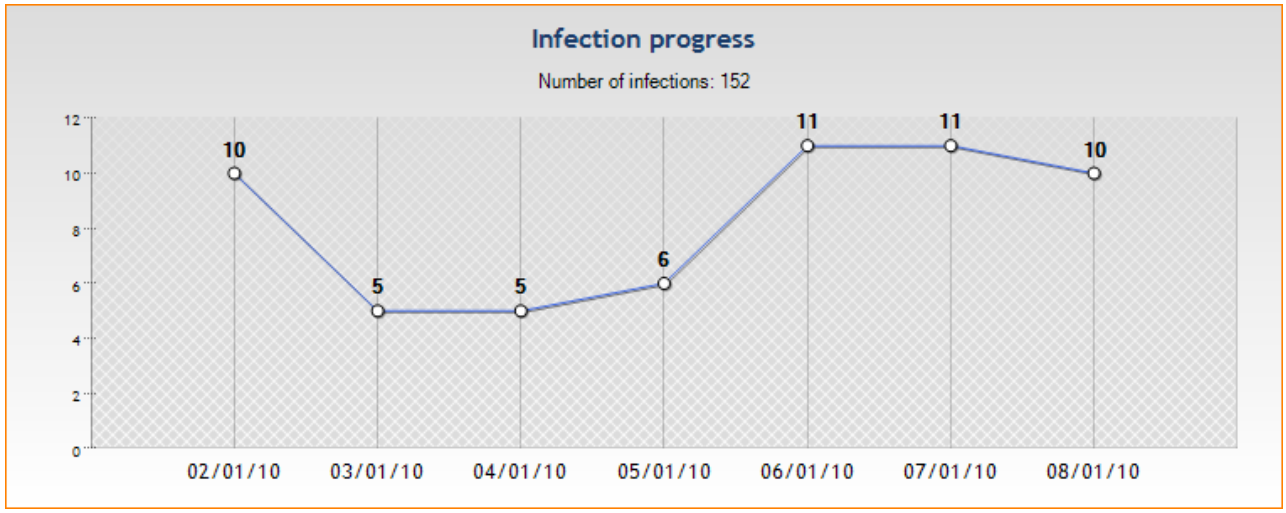
- **Top [5] of viruses:**



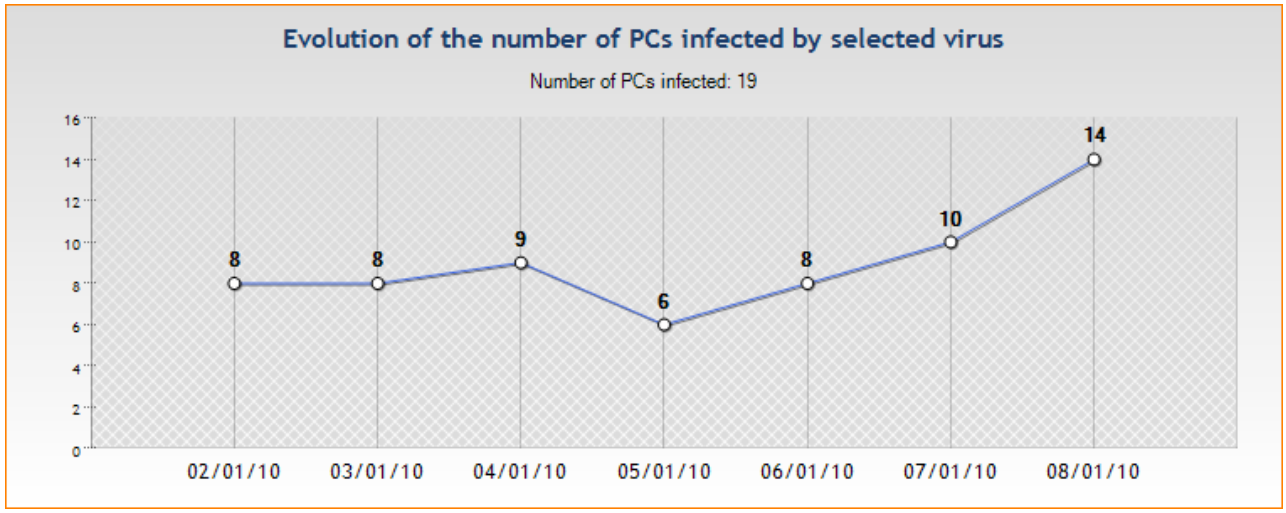
- **Top [5] of infected PCs:**



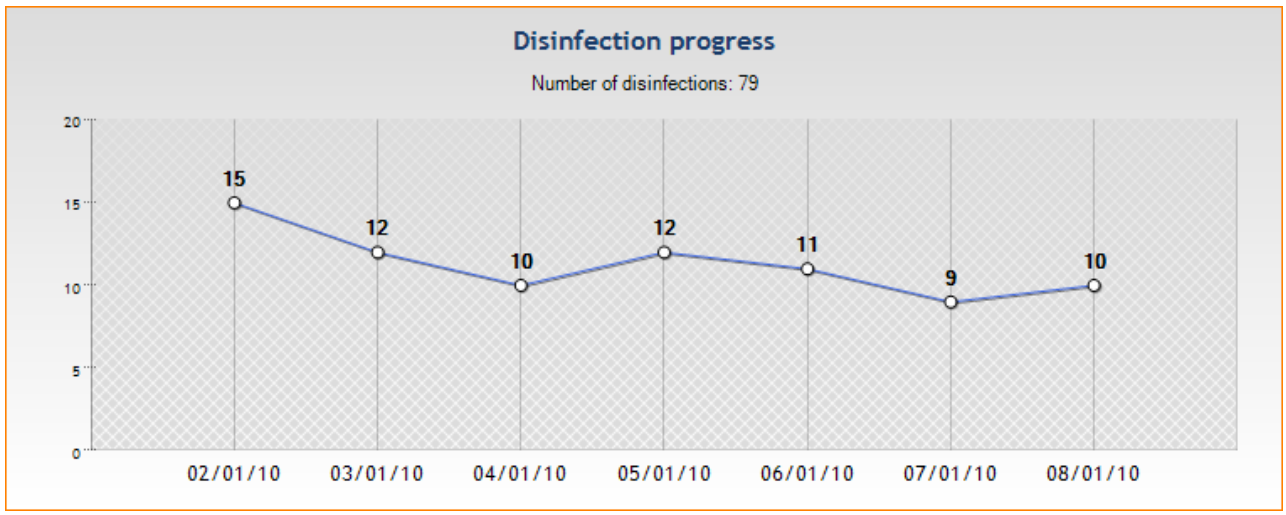
- **Infection progress:**



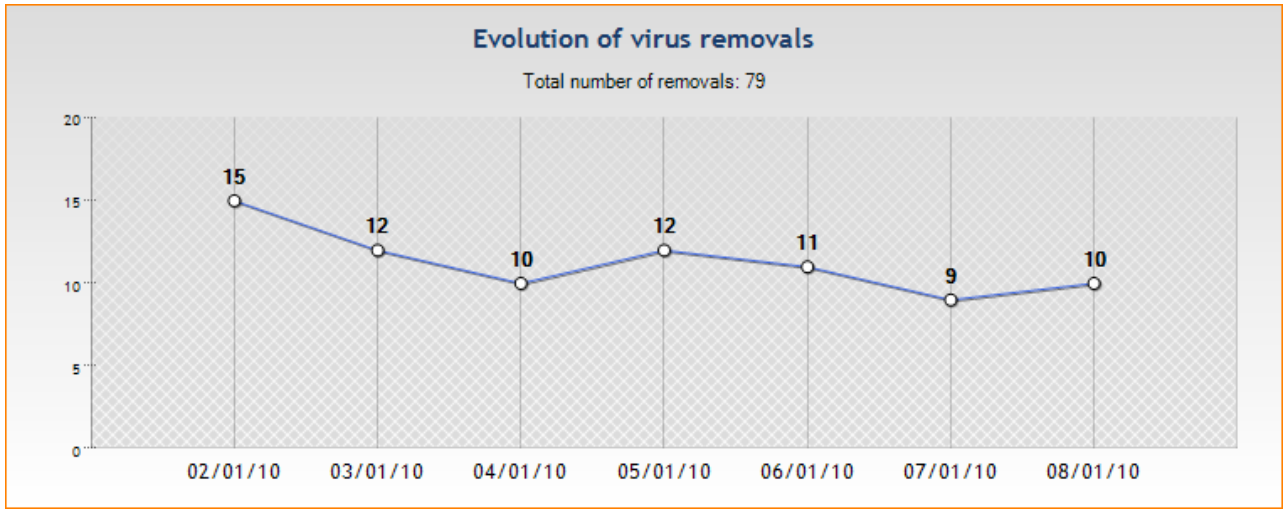
- **Evolution of the number of PCs infected by selected virus:**



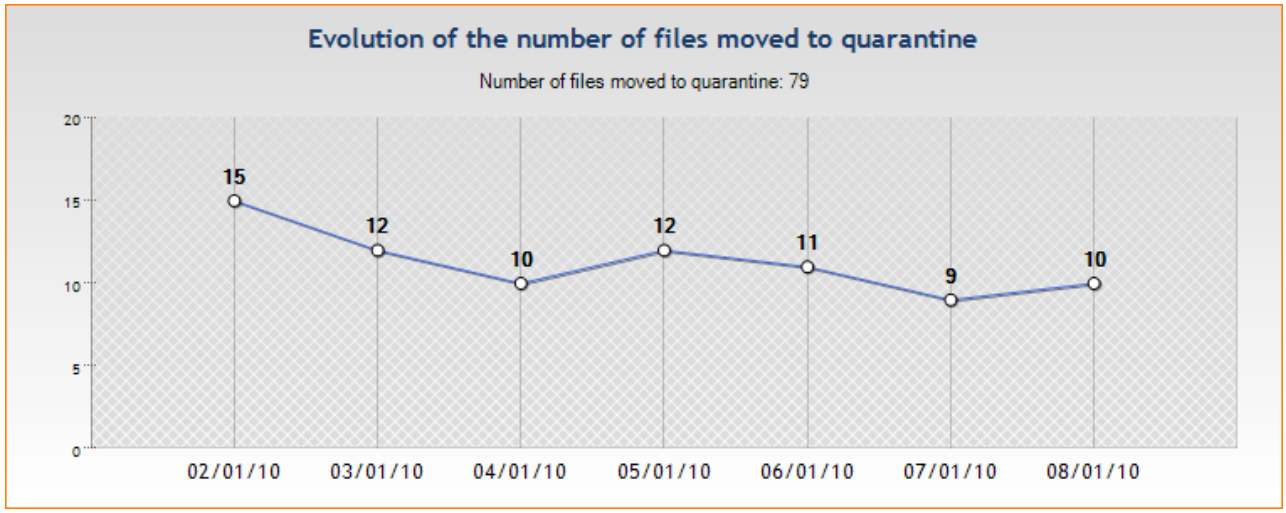
- **Disinfection progress:**



- **Evolution of virus removals:**



- **Evolution of the number of files moved to quarantine:**



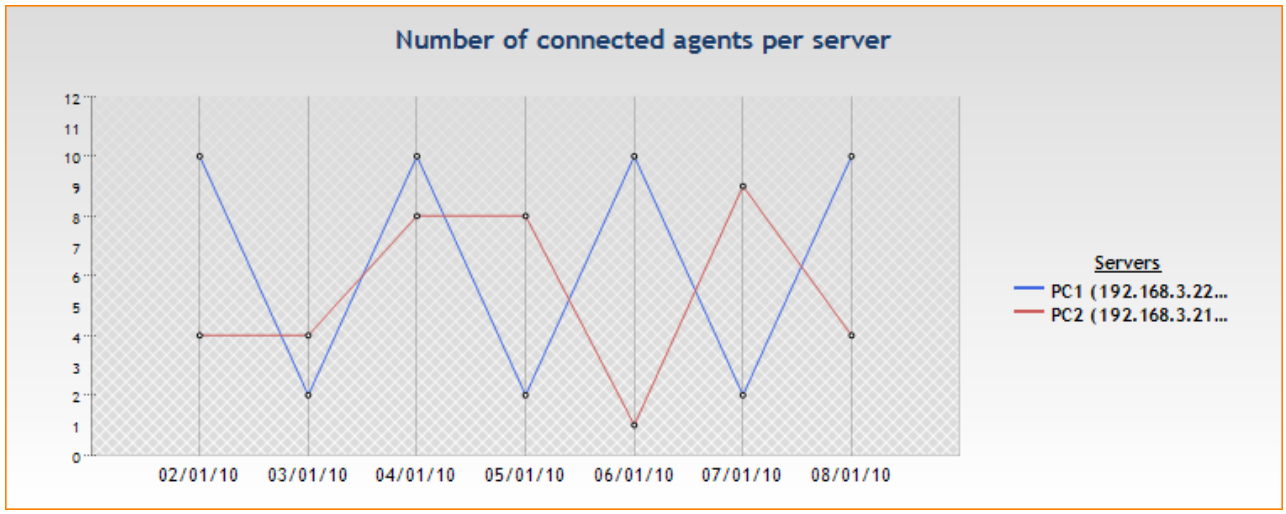
HISTORICAL REPORTS

SERVERS AND AGENTS

The Servers and Agents report provides the following information on the StormShield servers:

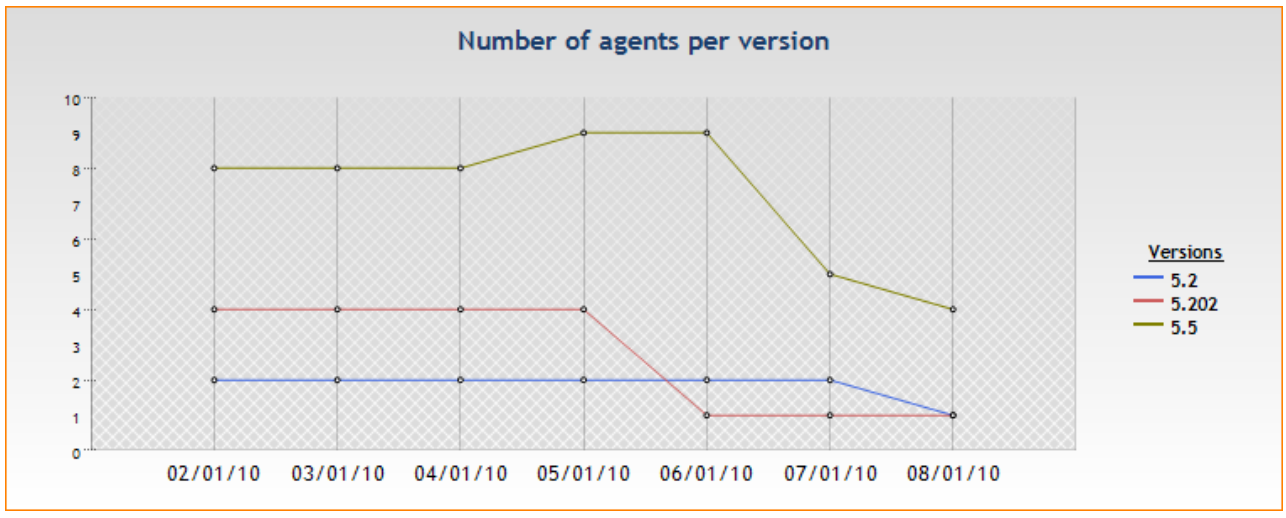
- **Number of connected agents per server:**

  It displays the number of connected agents per server over the period selected.



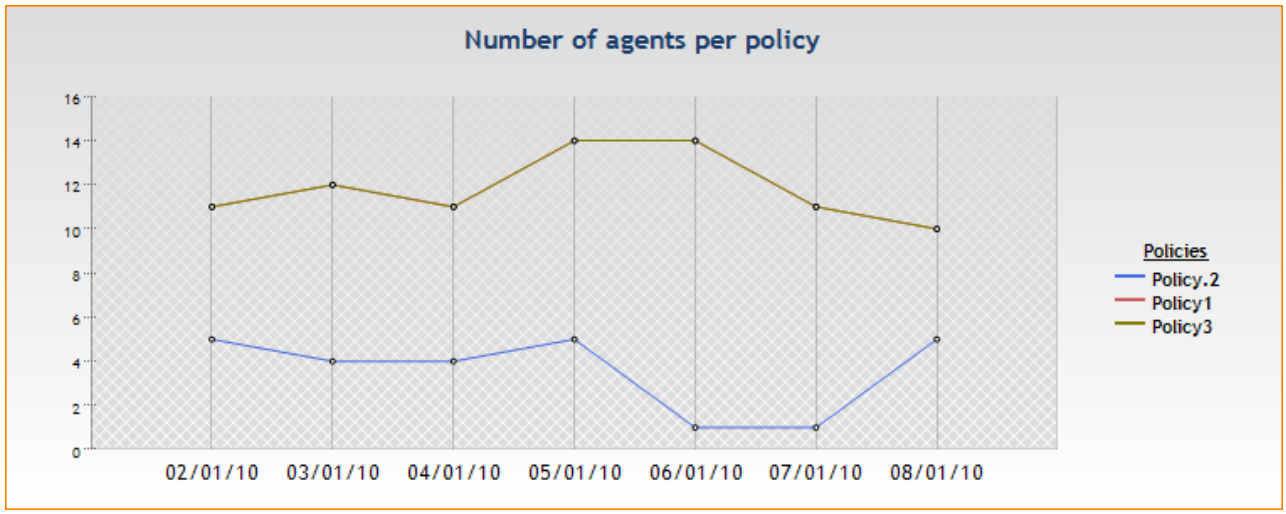
- **Number of agents per version:**

  It displays all the StormShield versions in use and the number of agents per version over the period selected.



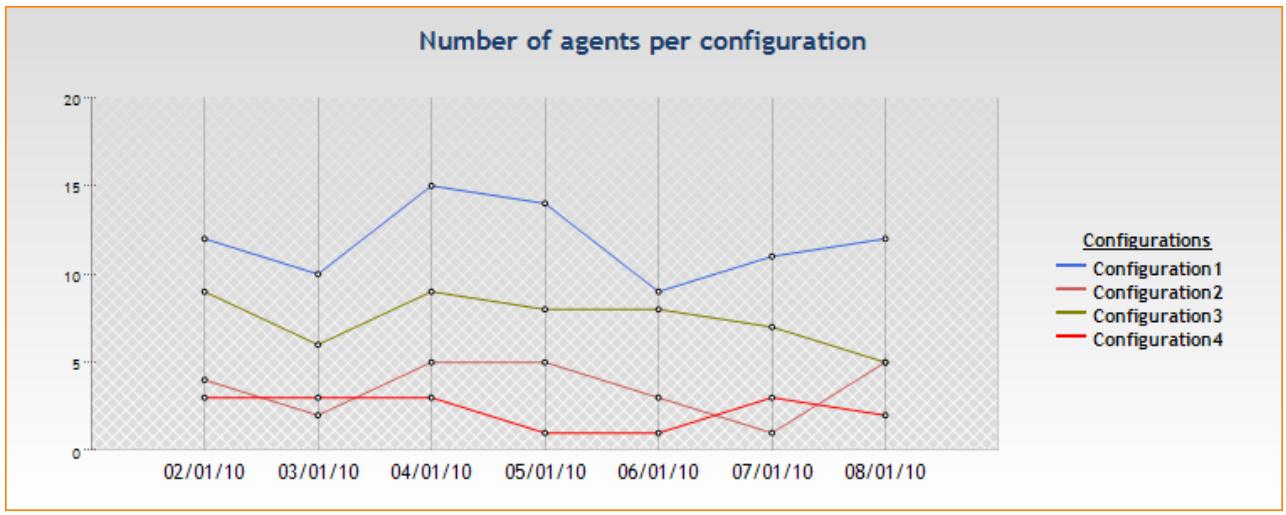
- **Number of agents per policy:**

  It displays the policies by name, and the number of agents which use this policy over the period selected.



- **Number of agents per configuration :**

  It displays the configurations by name, and the number of agents which use this configuration over the period selected.



The following reports are in Excel format:

- **Agents status:**

  It displays the last connection date, the last user and each agent version.

- **StormShield configuration modifications:**

  It displays all the modifications performed in the configuration with the involved administrators' names and policies.

- **Stopped agents:**

  It displays the list of all agents stopped during a particular period.

- **Agents configuration:**

  It displays the date and the version of the configuration used by each agent.

- **Agents policies:**

  It displays the date and the version of the policies used by each agent.

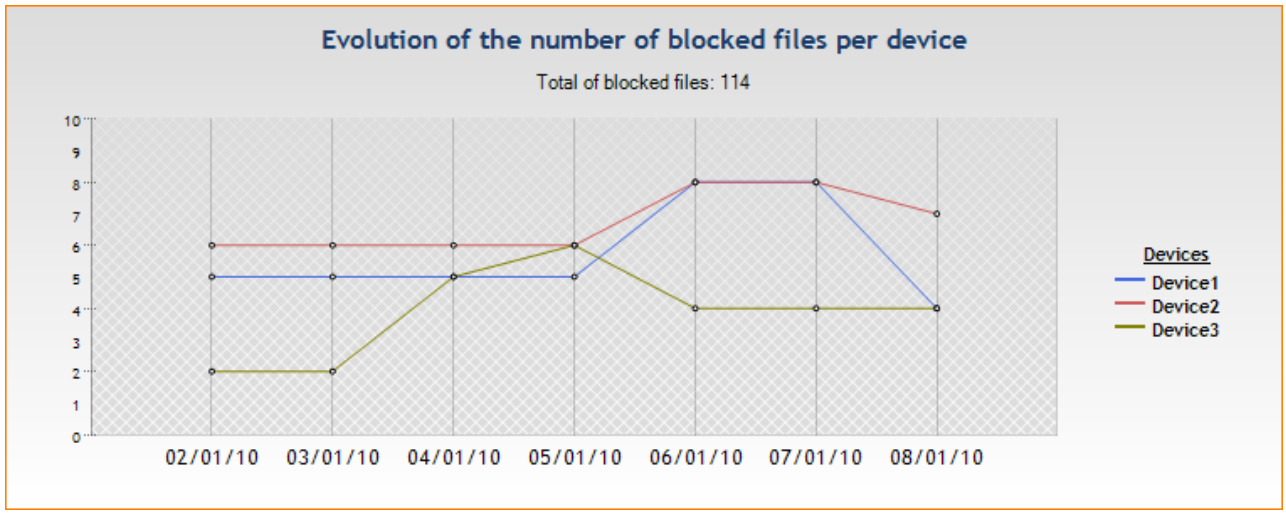
- **Agents groups policies:**

  It displays the policies available for each agents group.

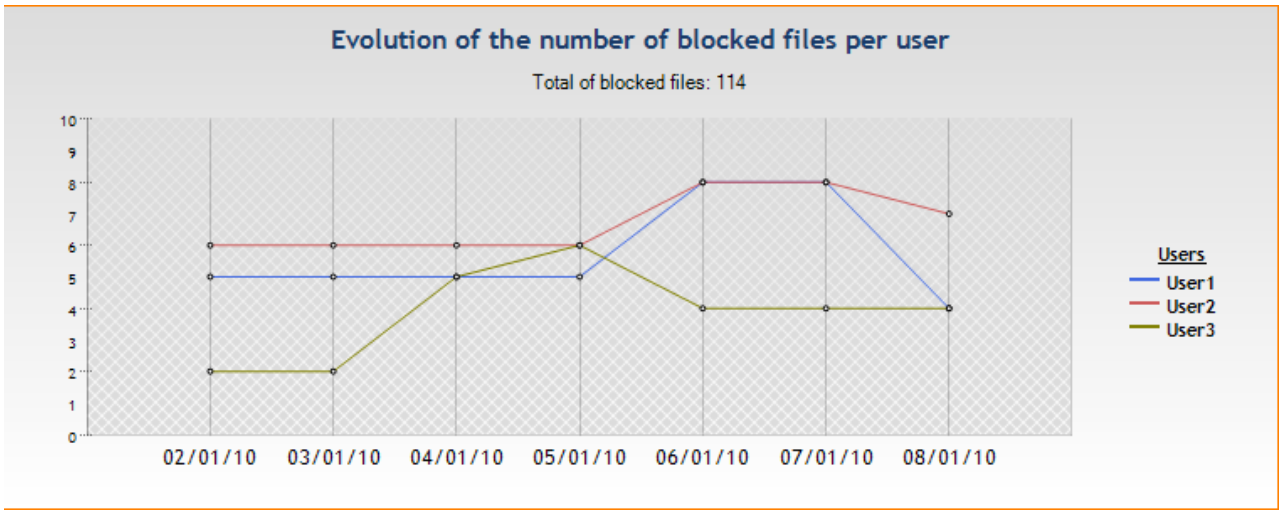
REMOVABLE DEVICES

The Removable Devices report provides the following information:

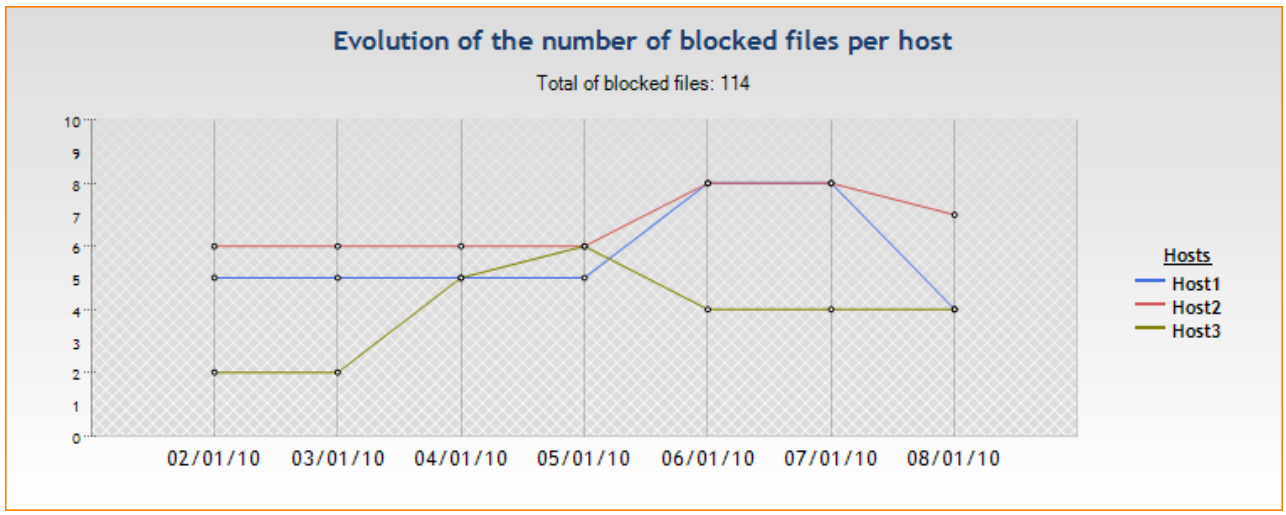
- **Evolution of the number of blocked files per device:**



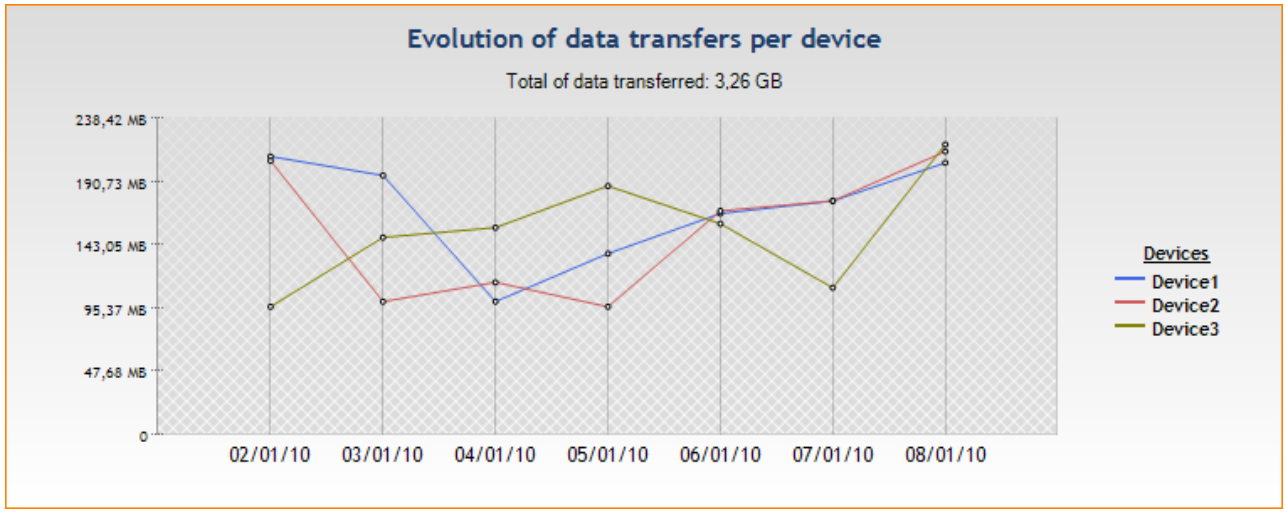
- **Evolution of the number of blocked files per user:**



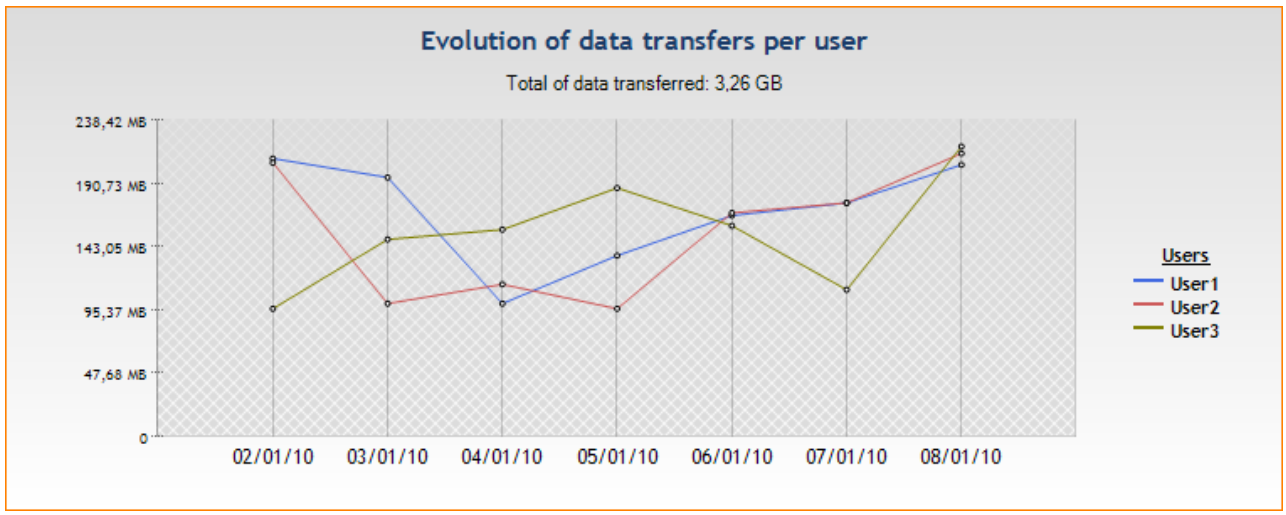
- **Evolution of the number of blocked files per host:**



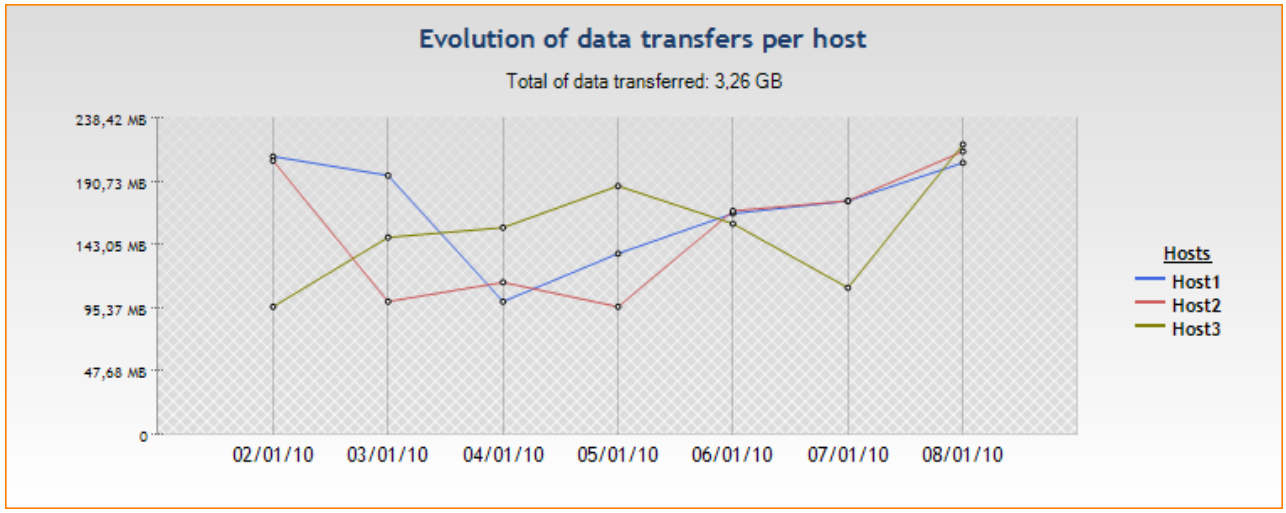
- **Evolution of data transfers per device:**



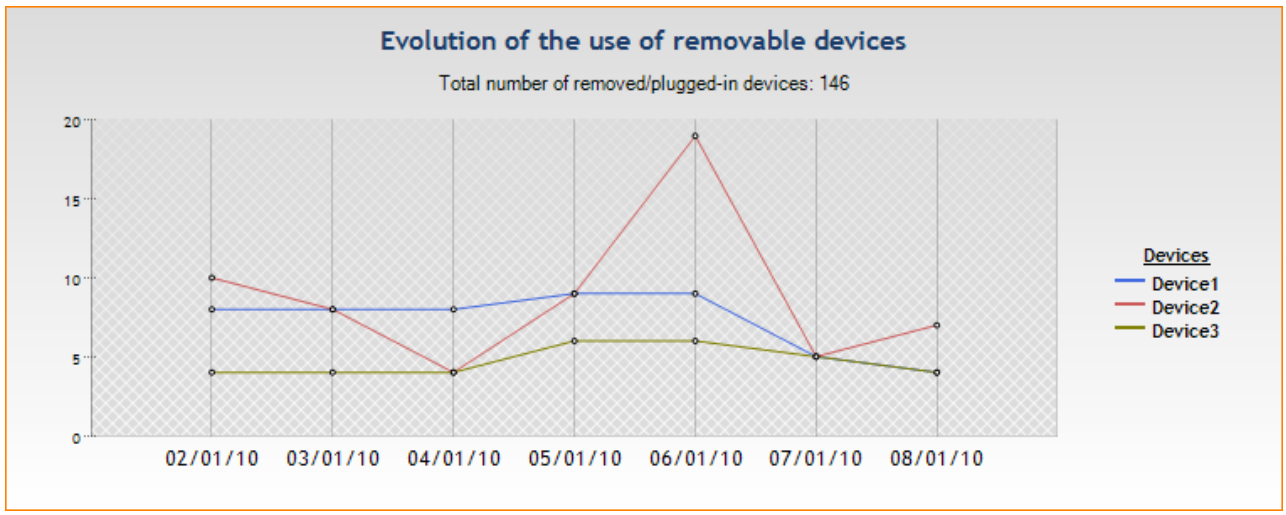
- **Evolution of data transfers per user:**



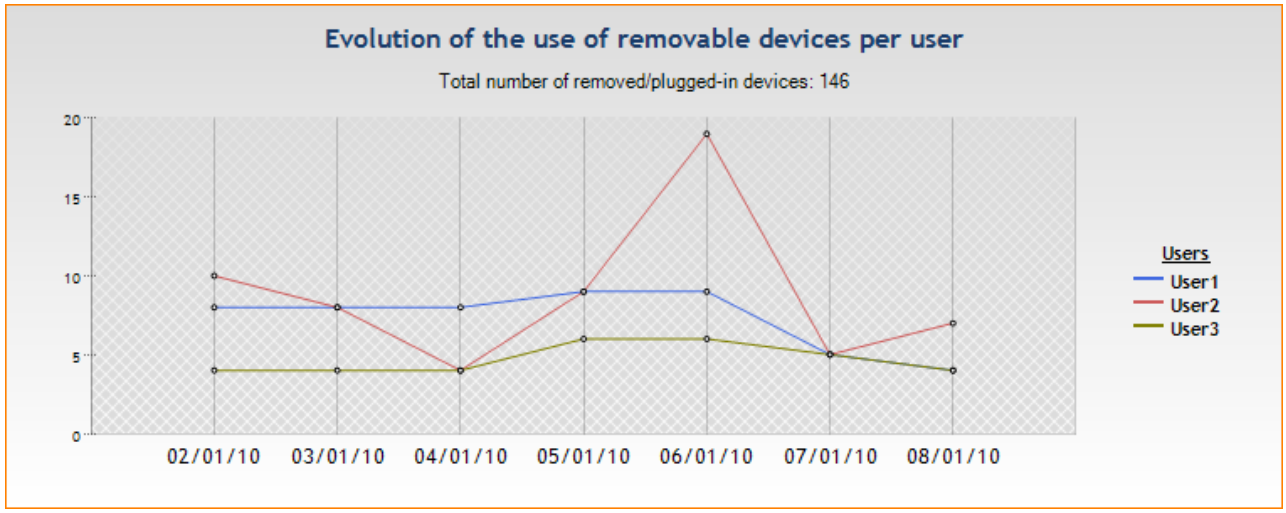
- **Evolution of data transfers per host:**



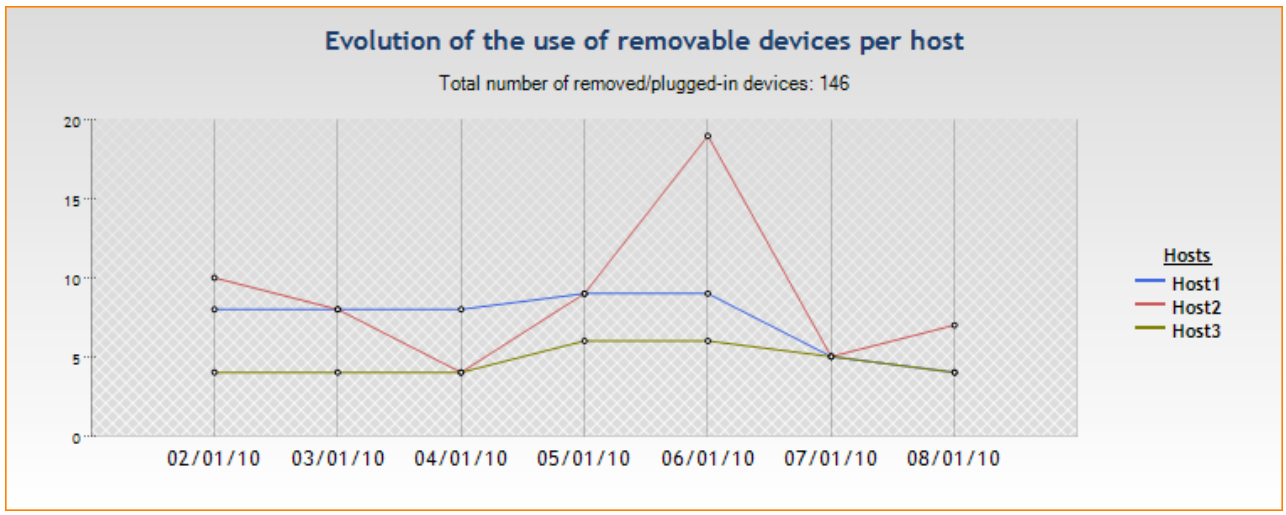
- **Evolution of the use of removable devices:**



- **Evolution of the use of removable devices per user:**



- **Evolution of the use of removable devices per host:**



WORKSTATION INTEGRITY

The Workstation Integrity reports provide the following information in the Excel format:

- **Policies violations by user and agent:**

  It displays the number of violations of each type for each user and each agent.

- **Blocked files:**

  It displays the files names, the agent and the access date.

- **Access by devices:**

  It displays the files copied from a USB key for each user and each agent.

Chapitre 17

ACTIVITY MONITORING

ABOUT THIS CHAPTER

This chapter describes the tools used to control, monitor and record activity on workstations. It explains how to access this information.

It includes the following:

- Overview Overview.
- Agent Monitoring :
  - Graphical interface :
    - Display options.
    - Details.
    - Filters.
  - Presence/absence of the agent on a workstation.
- Log Monitoring :
  - Overview.
  - Graphical interface :
    - "Logs" area.
    - "Information" area.
    - "Filters" area.
- Log Manager :
  - Overview.
  - Graphical interface :
    - Log types.
    - Display options.
    - Messages.

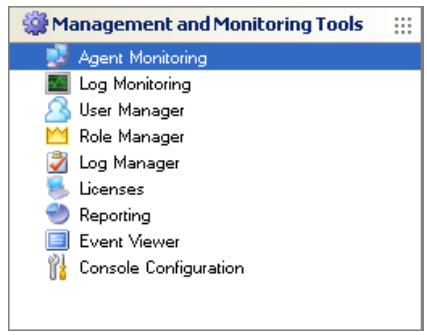
- Exporting logs to an external system (SMTP or Syslog) :
  - Overview.
  - Exporting logs via SMTP.
  - Exporting logs via syslog.

- Event Viewer :
  - Overview.
  - Graphical interface :
    - Menu bar.
    - Columns.
    - Expand/Collapse.
    - Details.

OVERVIEW

StormShield is used to control, monitor and record activity on workstations via the following features located in the **Management and Monitoring Tools** panel:

- Agent Monitoring.
- Log Monitoring.
- Log Manager.
- Event Viewer.



If you are using StormShield for the first time, it is unlikely that any event captured by the StormShield agents has been recorded in the reporting database.

In this case, the functions covered in this chapter will of course be available but without any data.

AGENT MONITORING

GRAPHICAL INTERFACE

Display options

Agent Monitoring display options in the menu bar are the following:

- **Real-Time:**

  Continuous display of monitoring information which is updated as the information is refreshed.

  By default, monitoring information is automatically updated according to the **Agent monitoring refresh time** (sec.) set in Console Configuration in the Management and Monitoring Tools.

- **Review:**

  Display of monitoring information without automatic update.

  Click **Refresh** when you want to update information.

- **Refresh:**

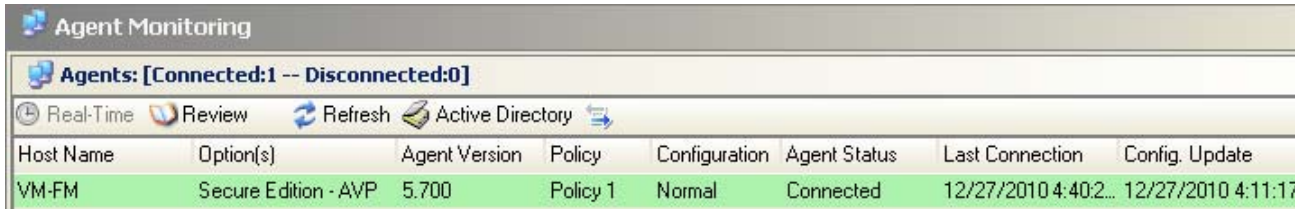
  Forces a refresh of monitoring information (displayed in real-time mode or review).

- **Active Directory:**

  Used to determine which machines do not have the StormShield agent software installed.

- **or :**

  Used to display basic or detailed information on the agents. The number of columns displayed depends on your selection.



Details

In the Agent Monitoring area, each line displays the following information on the agent selected:

- **Host Name**.
- **OS**.
- **IP Address**.
- **Net Mask:**

  Sub-network mask.
- **Option(s):**

  StormShield package and option (if any).
- **AD Name:**

  Full hostname in the Active Directory domain.
- **Agent Version:**

  Version number of the StormShield agent.
- **Config. Status :**

  The configuration status can be valid or invalid:
  - **Valid** indicates that the configuration is up-to-date.
  - **Invalid** indicates that the administrator has sent a new configuration but that the latter has not yet been received by the agent.
- **Policies:**

  Name of the applied policy.
- **Configuration:**

  Name of the applied configuration.
- **Agent Status:**
  - Connected.
  - Disconnected.
  - Warning.
  - StandBy.
  - Unknown.

- **Recommendation:**

  Status of a variable (used in Test scripts and Action scripts) which can be used by TNC clients (Trusted Network Connect) such as Odyssey Access Clients on Juniper Networks (R).

  Available options are:

  - Allow,
  - Isolate,
  - No access,
  - No recommendation.

  No recommendation is enabled by default and works only in Juniper server mode.

  Should a driver be missing (heimdall, loki, thor), the value applied by default will be **No recommendation**. It will be impossible to modify this value until the next reboot of the agent. Besides, drivers will have to be installed properly.

- **First Connection:**

  The first time the agent and the server communicated with each other.

- **Last Connection:**

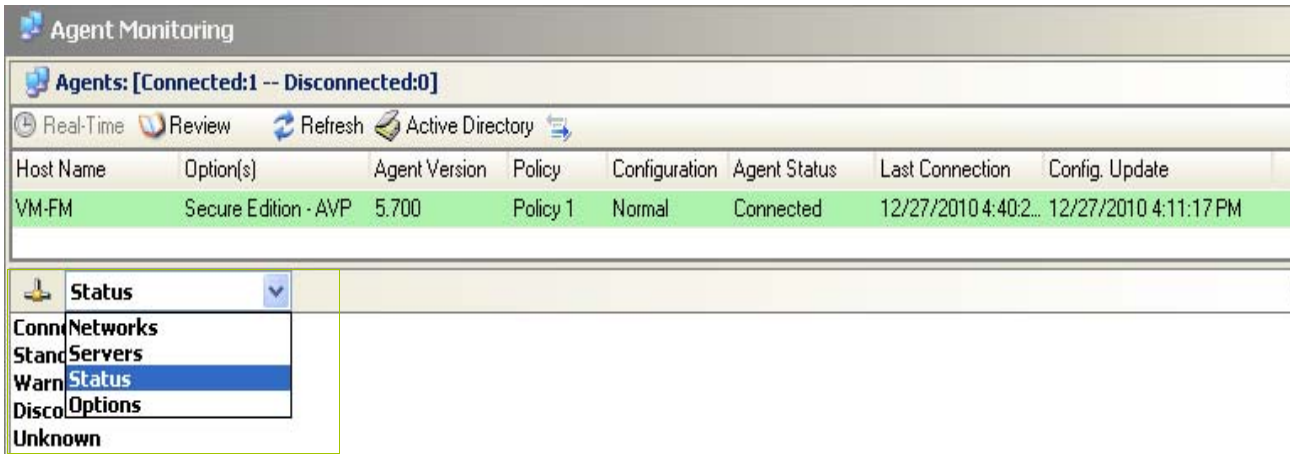
  The most recent time the agent and the server communicated with each other.

- **Config. Update : :**

  The date and time when the current configuration was received and applied.

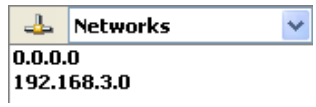
Filters

The administrator can filter agents using the following elements:



- **Status**:
  - Connected agents.
  - Agents in StandBy mode.
  - Agents in Warning mode.
  - Disconnected agents.
  - Agents with an unknown status.
- **Networks**.
- **Servers**.
- **Options**:
  - Professional Edition.
  - Secure Edition.
  - Professional Edition - AVP.
  - Secure Edition - AVP.

Example: If you select **Networks**, you can choose a specific network address. The log will display information only for the network selected.



Right-click menu

Merge

The administrator can merge machine identifiers to display only one entry concerning the monitoring of an agent. This is designed to update the number of licenses effectively used.

To do so, the administrator will right-click in the agent list to display the following options:

- **Selected**:

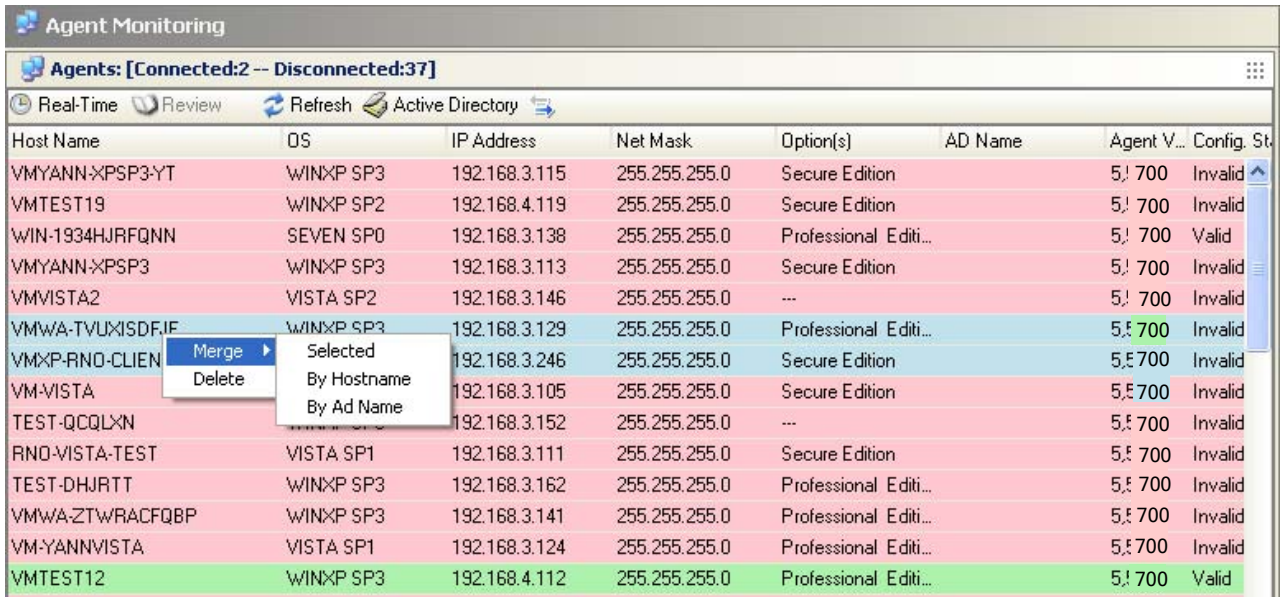
  The entries selected by the administrator will be merged. The administrator must select at least two entries to enable this option.

- **By hostname**:

  All the entries on the same machine will be merged. The fusion by hostname applies to the entire agent list.

- **By AD name**:

  All the entries having the same AD name will be merged. The fusion by AD name applies to the entire agent list.



Remove

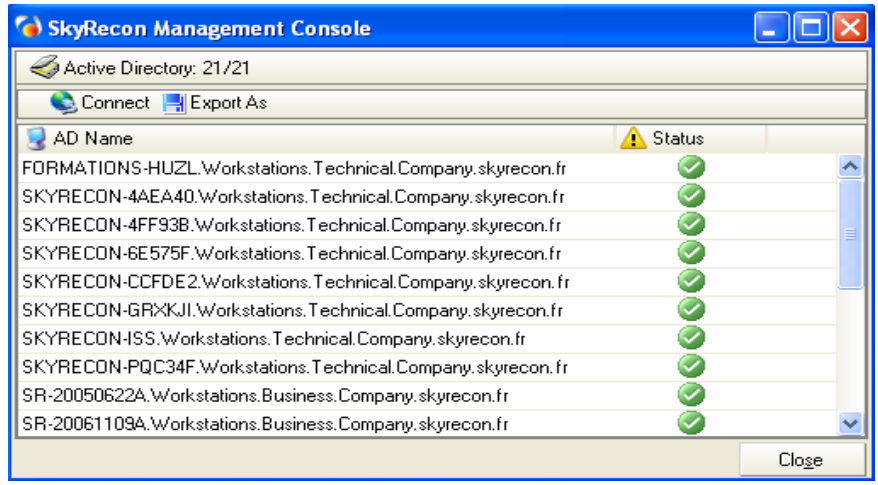
The administrator can delete the status history of an agent. If the agent is no longer present on a workstation, its license will become available for another workstation.

Alerts sent by the agent are retained.

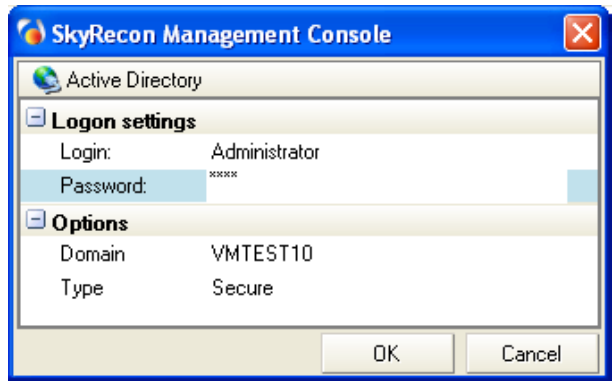
PRESENCE/ABSENCE OF THE AGENT ON A WORKSTATION

To check the presence or absence of the agent on workstations, follow the steps below:

1. In the Agent Monitoring window; click **Active Directory**. The AD list is displayed.



2. Click **Connect**.
3. Enter the following information:
   - Login.
   - Password.
   - Domain.
   - Type (of connection).



4. Click **OK**.
   A list of machines is displayed showing their respective status:
   - If the agent software has been installed, a ticked icon is displayed.
   - If the agent software has not been installed, a cross icon is displayed.

5. You can use **Export as** to save the information to a file in either of the following formats:
   - TXT (tabs used as separators).
   - CSV (commas used as separators).
   - XML.

LOG MONITORING

OVERVIEW

Log Monitoring records any suspicious activity on client workstations and servers and the corresponding reaction of the StormShield agent.

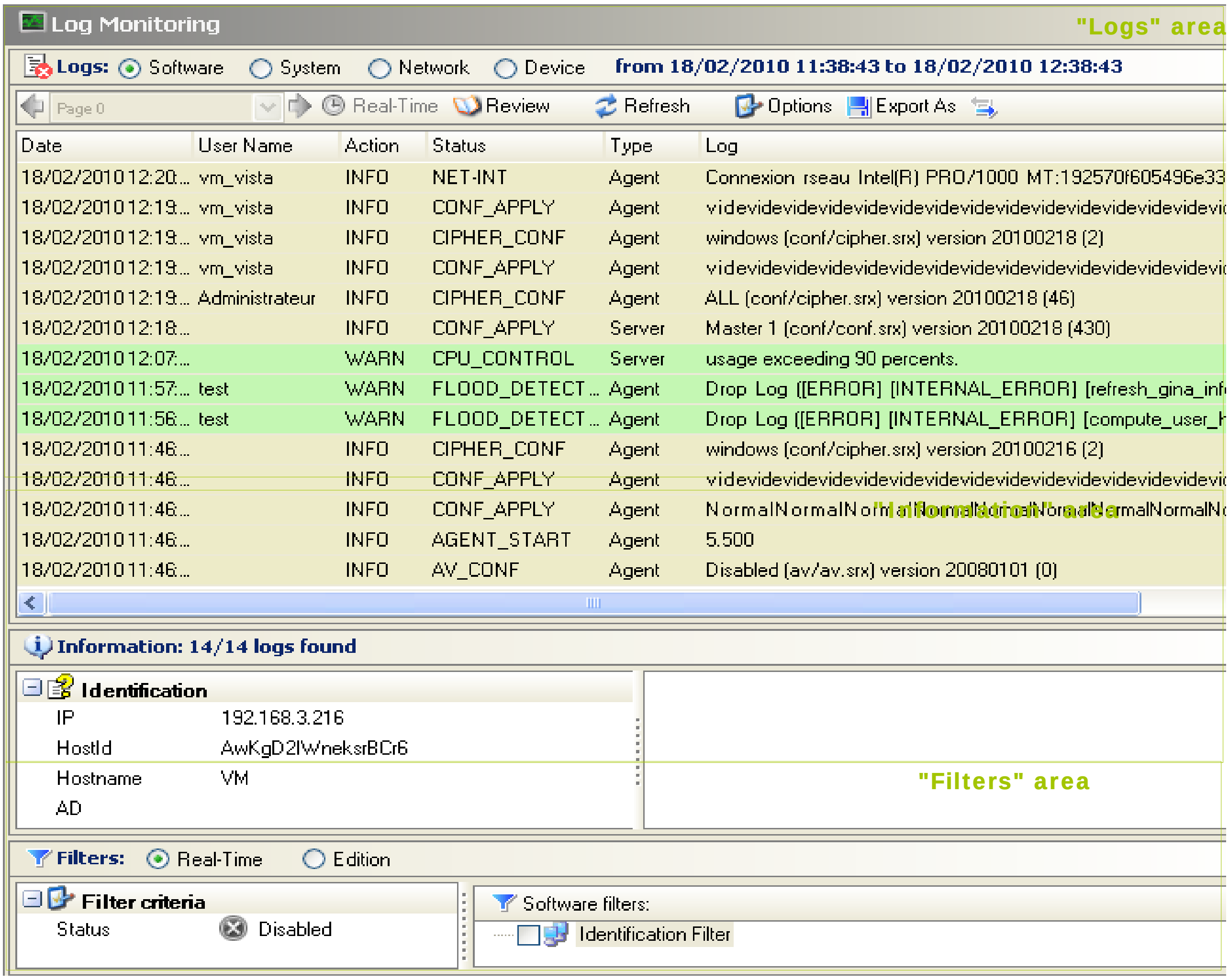
This data is consolidated in a database where it can be consulted via the SkyRecon console.

StormShield logs contain a record of all events triggered by the following:

- Software.
- System.
- Network.
- Device.

Activities that trigger an event are defined in the security policies.

GRAPHICAL INTERFACE



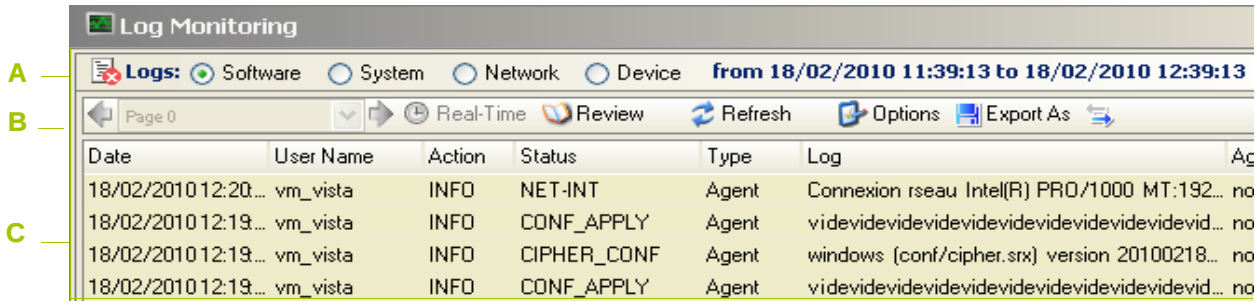
The **Log Monitoring** graphical interface includes three areas:

- Logs.
- Information.
- Filters.

"Logs" area

The **Logs** area is divided into three sub-areas:

- Log type (**A**).
- Display options (**B**).
- Details (**C**).



Log type sub-area

The Log type sub-area includes the following elements:

- Software.
- System.
- Network.
- Device.

Software logs

Purpose

A software log records the agent behavior whenever:

- The agent applies a configuration or a policy.
- The agent downloads a certificate or an update.
- There is a CPU overload on a server.
- The number of agents exceeds the maximum allowed by the license.
- Etc.

Logs are displayed on the SkyRecon console with filters applied. However, when you export a log to a file, the entire log is included (without any filter being applied).

"Software" log columns

In **Expand** mode (click ), the "Software" log columns are the following:

- **Date**.
- **User Name**:

  User identifier.
- **Action**:

  Logged action.

  Possible actions are: [BLK] for blockage, [INFO] for audit and [WARN] for warning mode.
- **Status**:

  Action status:

  Example: [ACTION-FAILED].
- **Type**:

  Possible statuses are: [AGENT] and [SERVER].
- **Mod. Name** :

  Module name.
- **Log**:

  Information message.
- **Agent mode**.

  Possible agent modes by default are NORMAL and WARNING.

In **Collapse** mode (click ), the Software log columns are the following:

- **Date**.
- **User Name**.
- **Action**.
- **Status**.
- **Type**.
- **Log**.
- **Agent mode**.

For more information, see "Software logs", page 641.

"System" logs

Purpose

The "System" logs contain information on system protection.

"System" log columns

In **Expand** mode (click), the "System" log columns are the following:

- **Date**.
- **User Name**:
  User identifier.
- **Action**:
  Logged action.
- **Status**:
  Action status:
- **Source**:
  Source program name.
- **Destination**:
  Destination program/file name.
- **Option**.
- **RID:**
  Unique Rule IDentifier.
- **Agent mode**:
  Possible agent modes by default are NORMAL and WARNING.

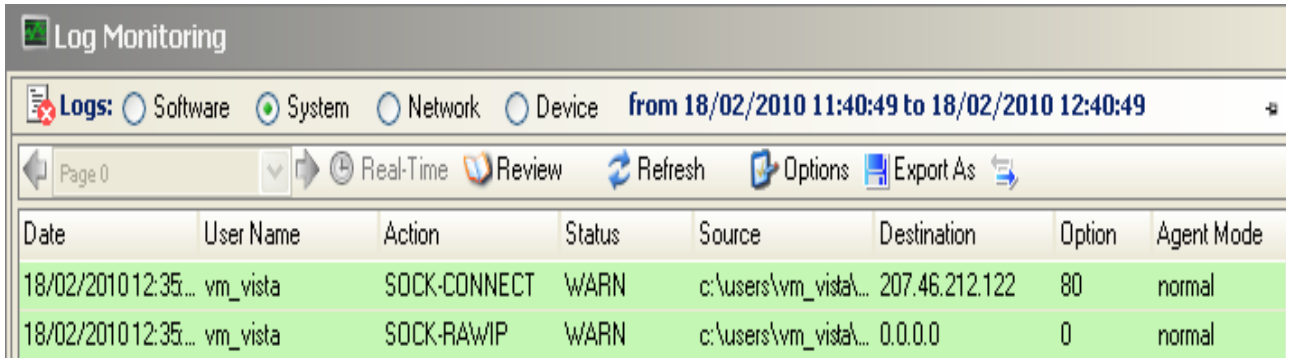
In **Collapse** mode (click), the "System" log columns are the following:

- **Date**.
- **User Name**.
- **Action**.
- **Status**.
- **Source**.
- **Destination**.
- **Option**.
- **Agent mode**.

For more information, see "System logs", page 648.

"System" log variables

For more information, see "System log variable details", page 650.



Network logs

Purpose

"Network" logs contain information on:

- Network Firewall (Category).
- Intrusion Detection System (General Settings > Network security control).

"Network" log columns

In **Expand** mode, the Network log columns are the following:

- **Date**.
- **User Name**:
  User identifier.
- **Action**:
  Logged action.
- **Status**:
  Action status:
- **Metadata**:
  Information on the logged event.
  Example: In case of flood, the field indicates how many times the event occurred. Otherwise, it displays the MAC address.

- **IP Address**:
  SSID (WiFi), IP fragment or IP address.
- **Src. Port** :
  Source port.
- **Dst. Port** :
  Destination port.
- **Proto1**. :
  Protocol over ethernet.
- **Proto2**. :
  Protocol over IP.
- **RID:**
  Unique Rule IDentifier.
- **Agent mode**:
  Possible agent modes by default are NORMAL and WARNING.

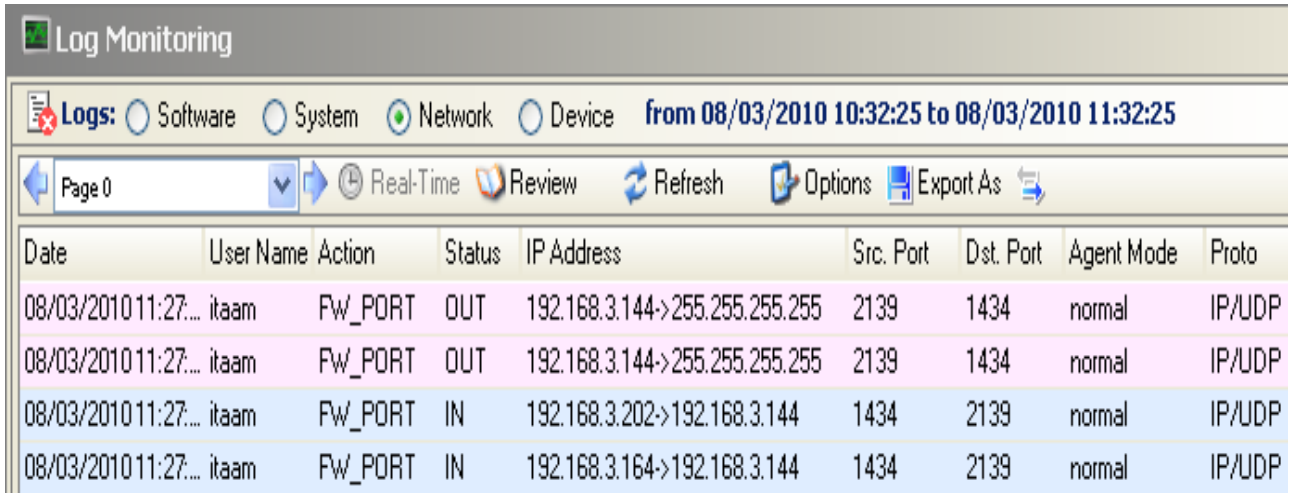
In **Collapse** mode, the "Network" log columns are the following:

- **Date**.
- **User Name**.
- **Action**.
- **Status**.
- **IP Address**.
- **Src. Port**
- **Dst. Port**
- **Agent mode**.
- **Proto**:
  [Protocol over ethernet]:[IP protocol].

For more information, see "Network logs", page 654.

"Network" log variables

For more information, see “Network log variables”, page 654



from 08/03/2010 10:32:25 to 08/03/2010 11:32:25

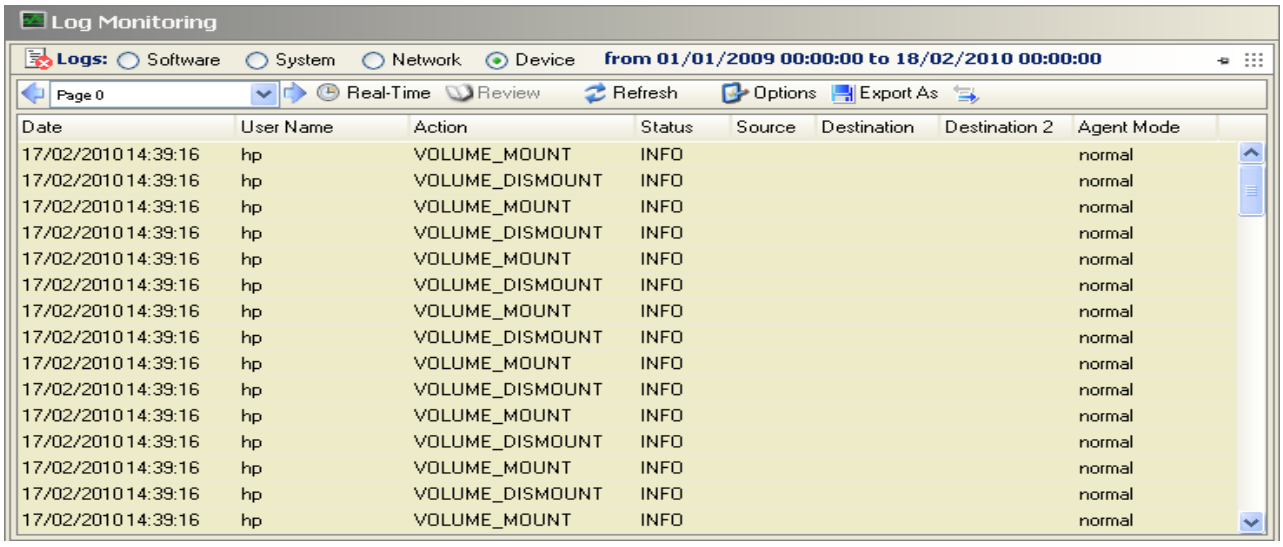
Date	User Name	Action	Status	IP Address	Src. Port	Dst. Port	Agent Mode	Proto
08/03/2010 11:27:...	itaam	FW_PORT	OUT	192.168.3.144->255.255.255.255	2139	1434	normal	IP/UDP
08/03/2010 11:27:...	itaam	FW_PORT	OUT	192.168.3.144->255.255.255.255	2139	1434	normal	IP/UDP
08/03/2010 11:27:...	itaam	FW_PORT	IN	192.168.3.202->192.168.3.144	1434	2139	normal	IP/UDP
08/03/2010 11:27:...	itaam	FW_PORT	IN	192.168.3.164->192.168.3.144	1434	2139	normal	IP/UDP

"Device" logs

Purpose

The "Device" logs contain information on:

- Removable devices (Category).
- Device control (General settings).
- WiFi encryption and authentication (General settings).



from 01/01/2009 00:00:00 to 18/02/2010 00:00:00

Date	User Name	Action	Status	Source	Destination	Destination 2	Agent Mode
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal

"Device" log columns

In **Expand** mode, the "Device" log columns are the following:

- **Date**.
- **User Name**:

  User identifier.
- **Action**:

  Logged action.
- **Status**:

  Action status:

  Possible statuses are: [BLK] for blockage, [INFO] for audit and [WARN] for warning mode.
- **Source**:

  Name of the network card (WiFi) or process (removable mass storage device).
- **Destination**:

  File name, path or MAC address (WiFi blocked).
- **Destination2**:

  File name after renaming (removable mass storage device) or SSID (WiFi).
- **Size**:

  Device size.
- **Type**:

  Device type.

  Possible statuses are: [FIREWIRE], [NETWORK], [PCMCIA], [USB], [NONE].
- **Class**:

  Device class identifier.

  Possible classes are: [BLUETOOTH], [CDROM], [DISK], [IRDA], [MODEM], [PARALLEL], [PCMCIA], [SERIAL], [WIFI].
- **RID:**

  Unique Rule IDentifier.
- **Agent mode**:

  Possible agent modes by default are NORMAL and WARNING.

In **Collapse** mode, the "Device" log columns are the following:

- **Date**.
- **User Name**.
- **Action**.
- **Status**.
- **Source**.
- **Destination**.
- **Destination2**.
- **Agent mode**.

For more information, see "Device logs", page 657.

"Device" log variables

For more information, see "Variables", page 658.

WiFi variables

For more information, see " WiFi variables", page 663.

Type variables

For more information, see "Type variables", page 664.

Class ID variables

For more information, see "Class ID variables", page 664.

Display options sub-area

The Display options sub-area includes the following:

- **Real-Time:**

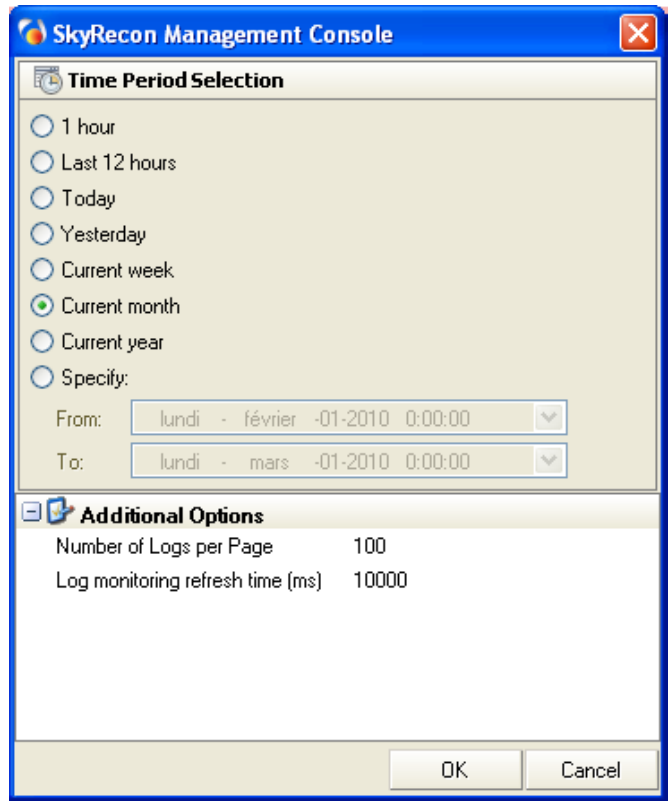
  Continuous display of monitoring information which is updated as the information is refreshed.

  By default, monitoring information is automatically updated every 30 seconds.
- **Review:**

  Display of alerts reported throughout a period defined by the administrator.
- **Refresh:**

  Forces a refresh of monitoring information.

- **Options**:



  - **Time Period Selection:**

    Specifies the period of time to be used to display data in Review mode.

  - **Additional Options:**

    Specifies the number of logs to be displayed per page and the log monitoring refresh time.

- **Export As:**

  Saves log information to a file.

  This feature enables the administrator to export the visible log (i.e. what is currently displayed on the SkyRecon console).

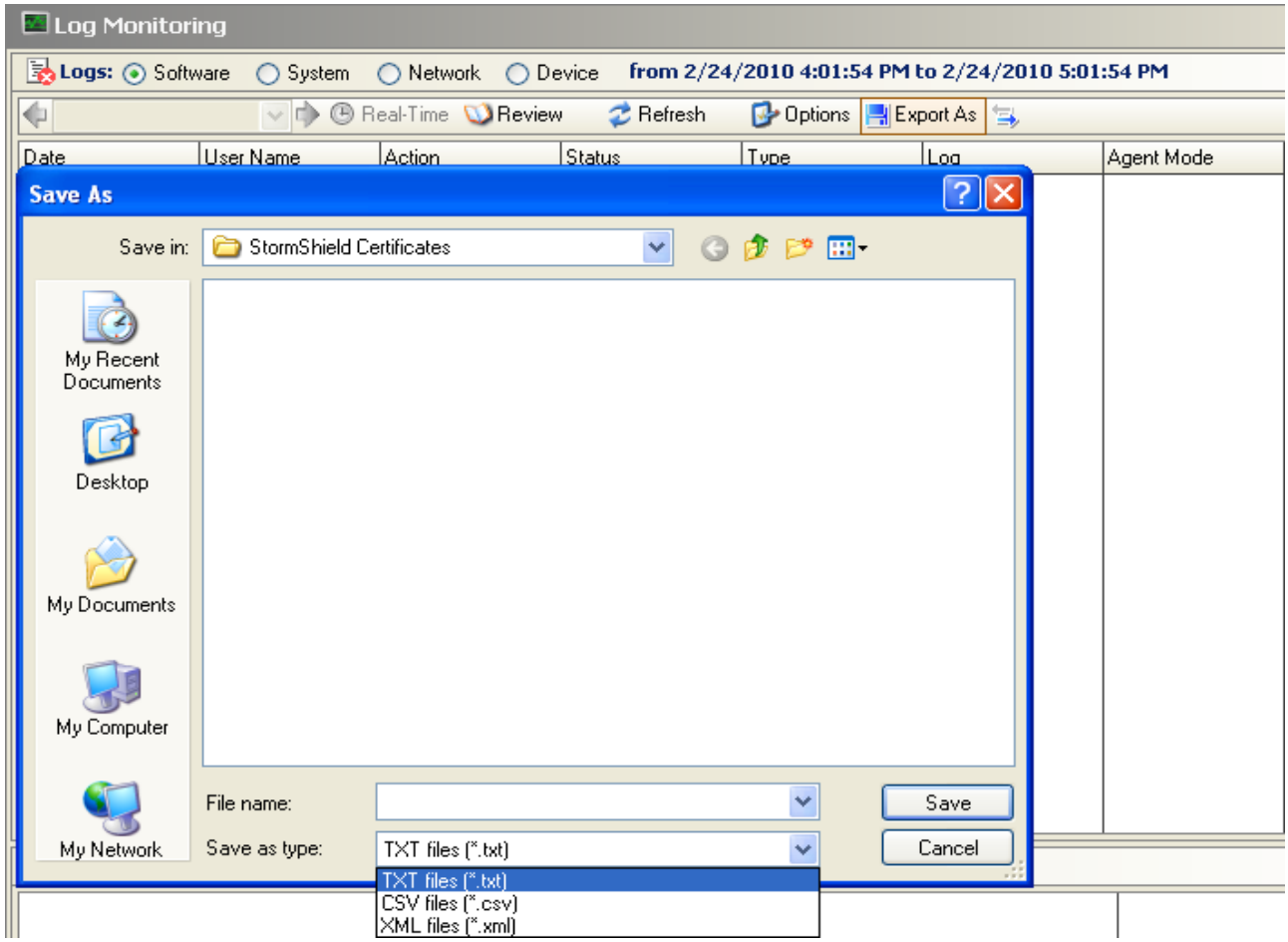
  The following file formats are supported by the **Export As** feature:

  - TXT (tabs used as separators).
  - CSV (commas used as separators).
  - XML.

  The information included in the exported file consists of the currently selected log (the log displayed) and identification information.

To export a log to a file, follow the steps below:

1. Select the logs that you want to export.
2. Click **Export as**.
3. From the drop-down list, select the file format that you want to use (example: `txt`).
4. Set the file path and enter the filename.
5. Click **Save**.



Details sub-area

The data provided by the Details sub-area (columns) depends on the type of log selected. This sub-area will systematically display the **Action** and **Status** columns.

Clicking the icon displays less information. Clicking the icon displays more information.

The Details sub-area display can be configured for later analysis.

For more information, see:

- “"Software" log columns”, page 606.
- “"System" log columns”, page 607.
- “"Network" log columns”, page 608.
- “"Device" log columns”, page 611.

"Information" area

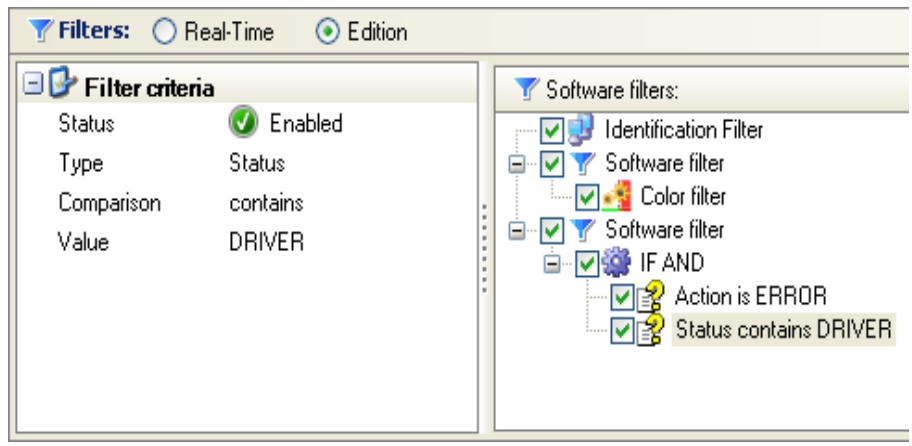
The Information area contains relevant information on the machine which generated the log:

- Its IP address.
- Its hostID (unique identifier created by StormShield for each agent).
- Its name.
- Its Active Directory name.

"Filters" area

The Filters area contains filter criteria for selective display.

For example, you can filter **Software** logs so that only ERROR actions having a DRIVER status will be displayed.



There are two options:

- **Real-Time**.

  Filtering is applied to the log display immediately after sending the request.

- **Edition**.

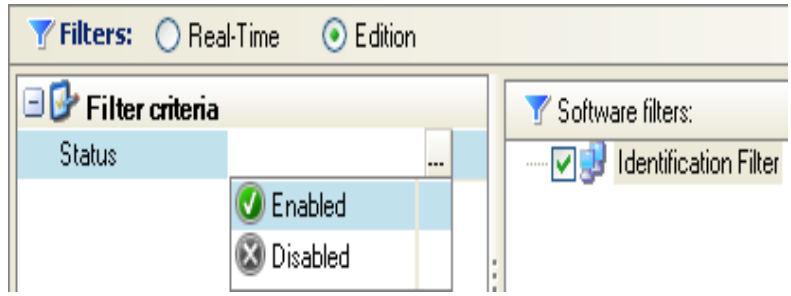
  Filtering is applied to the log display when the administrator clicks **Refresh**.

When creating or modifying filters, you can move items by a simple drag-and drop.

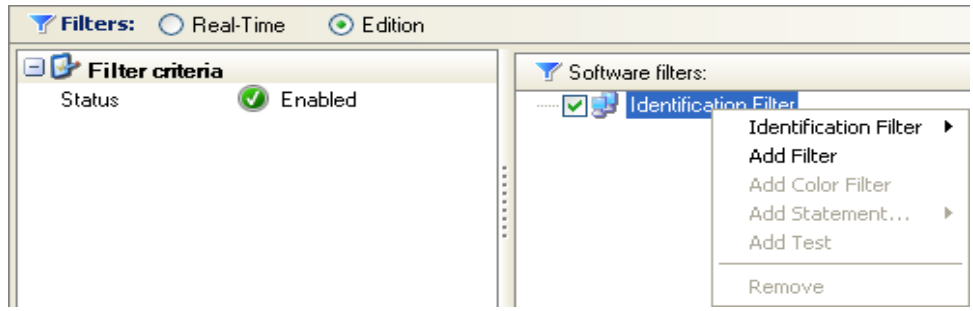
Adding Filters

To add a filter, follow the steps below:

1. Right-click the second column, opposite "Status" in Filter Criteria to enable the filter.

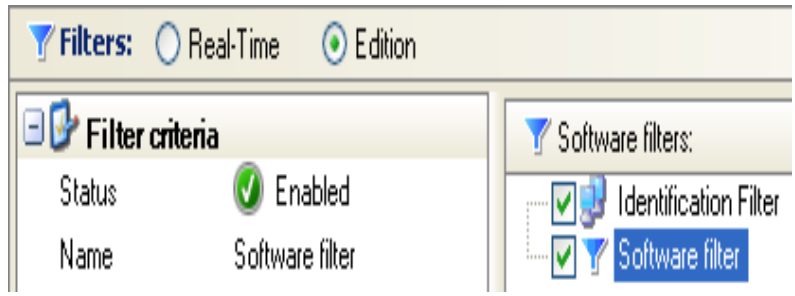


2. Right-click **Identification Filter** which is displayed by default in the filter window (on the right).
The following drop-down menu is displayed:



3. Click **Add Filter**.
The new filter is displayed in the tree structure.

A Software filter is displayed in this example because you are in the Software Logs section.

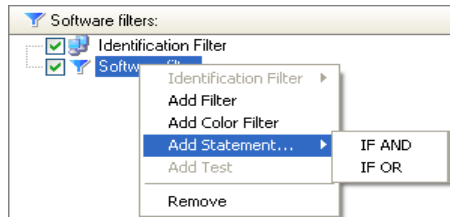


4. Define the settings of the filter that you have just added (example: Add Color Filter).
5. You can also add another Software filter.

Adding a statement

To add a statement to a filter, follow the steps below:

1. Right-click the appropriate filter.
   The following drop-down menu is displayed:

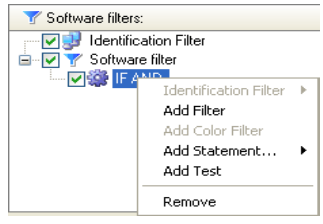


2. Click **Add Statement**.
3. Select the appropriate statement.

Adding a test

To add a test to a statement, follow the steps below:

1. Right-click the appropriate statement.
2. Select **Add Test**.
3. Define test settings.



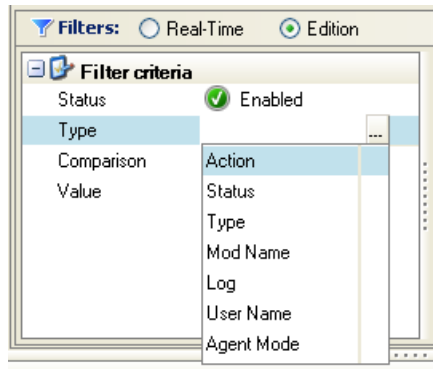
You can configure the test using the following fields:

- **Status**:

  Enables or disables the test (Enabled/Disabled).

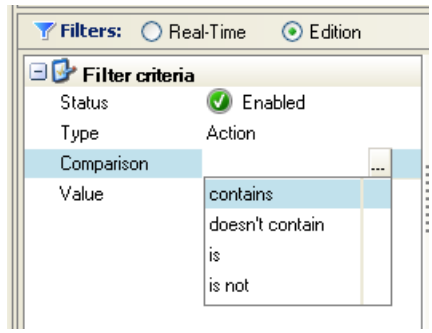
- **Type**:

  Defines which element is to be tested.



- **Comparison** :

  Defines the comparison values to be used in the test.



- **Value**:

  To be entered by the administrator.

If "contains" or "doesn't contain" is selected in the **Comparison** field, the search of the value is based on the SQL engine search and its syntax.

This syntax implies the following:

- _: stands for any character.
- %: stands for any character repeated 0 or n times.

To search for a metacharacter ("_" or "%" character) without interpreting it, the user must place it between square brackets.

The console encapsulates the search string into "%" characters when the user does not enter SQL metacharacters (example: file => %file%), which corresponds to the filter "contains".

If the user adds an "_" or "%" to the search string, the console no longer encapsulates the search string. The search is thus totally based on what the user has entered in the **Value** field.

The following table shows how the mode **Comparison** = "contains" works. The "Searched string" column is the value entered in the **Value** field. The "Interpreted string" column is the value sent to the SQL search engine. The "Match" column displays examples which would match the searched string. The " Do not match" column displays examples which would not match the searched string.

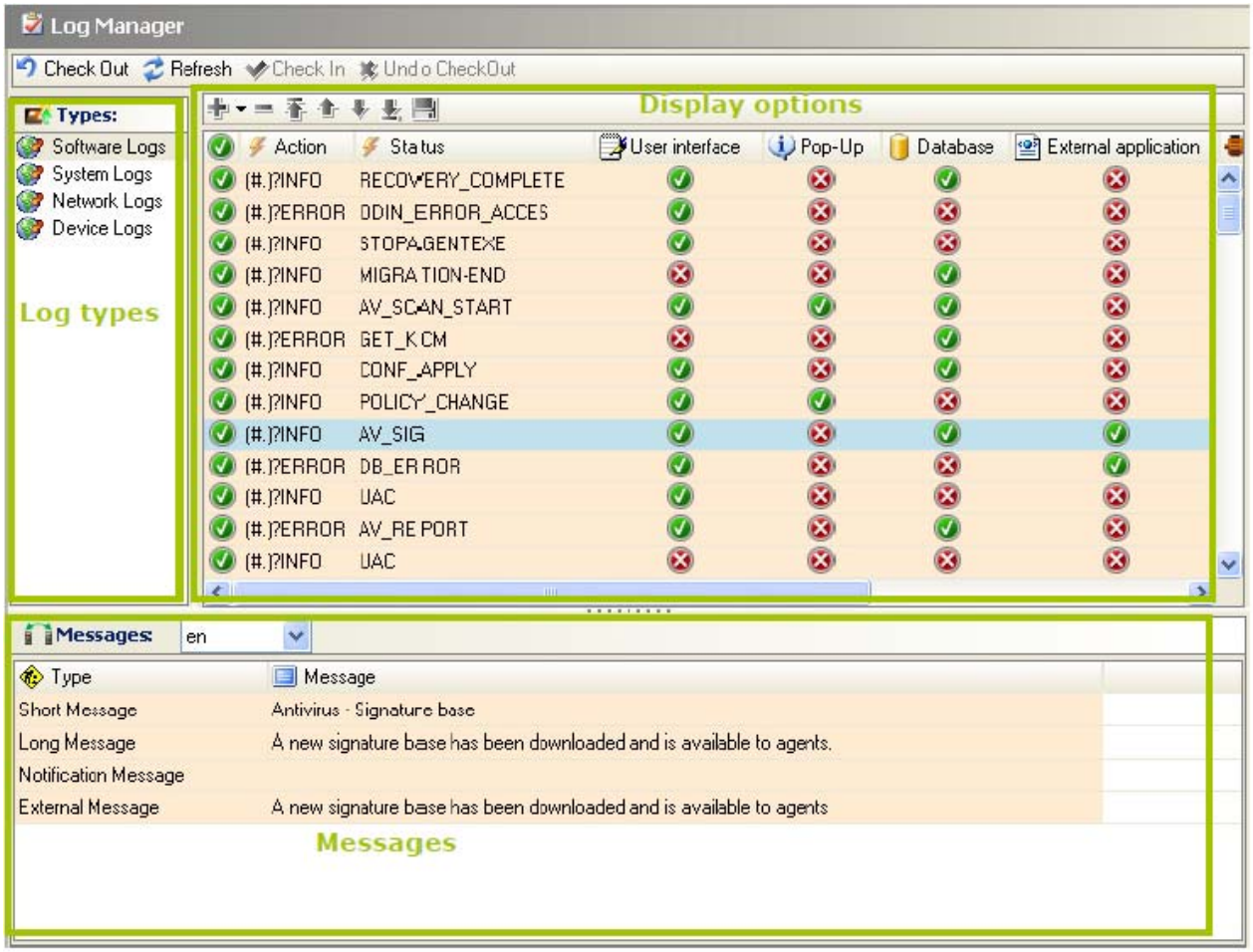
Searched string	Interpreted string	Description	Match	Do not match
FILE[_]	%FILE[_]%	All values containing "FILE_"	FILE_READ and FILE_	_READ and FILE
FIL_	FIL_	All values equal to "FIL" + one letter	FILE	FILE_READ, FILE_ and _READ
%[_]READ	%[_]READ	All values ending with "_READ"	FILE_READ and _READ	FILE_ and FILE
FILE[_]%	FILE[_]%	All values beginning with "FILE_"	FILE_ and FILE_READ	_READ and FILE

LOG MANAGER

OVERVIEW

The **Log Manager** is used to customize StormShield agent logs. It is designed to configure event reporting for:

- Software Logs.
- System Logs.
- Network Logs.
- Device Logs.



The events used to generate reports are triggered by certain actions and statuses.

The actions and statuses which trigger a log are defined in the security policies.

Example 1:

The **INFO** action with status:

- **AGENT_START**:

  Creates reports based on the agent version.

- **SERVER_VERSION**:

  Creates reports based on the server version and server name.

- **CONF_APPLY**:

  Creates reports based on the policy or configuration name.

Example 2:

The **WARN** action with status **FLOOD_DETECTED** is used to create flood reports (repeated log messages until saturation).

If the administrator filters any of these actions in the **Log Manager**, reports based on any of the following cannot be displayed:

- Version.
- Policy name.
- Configuration name.
- Server flood.

After **updating** StormShield, new log filters may be located after the "*" wild card. To use these new filters, for each log type you must:

- Go to Log Manager.
- Move the "*" wild card at the end of the list.
- Synchronize with the server.

GRAPHICAL INTERFACE

The graphical interface includes three sub-areas:

1. Log Types.
2. Display options.
3. Messages.

Log types

The log types which can be managed from the Log Manager are the following:

- Software.
- System.
- Network.
- Device.

Display options

Simply click in the appropriate column to parameterize the display of each log.

If you enable a parameter, the column will contain the icon .

If you disable a parameter, the column will contain the icon .

For more information, see "Enable logs", page 217.

All logs contain the **Action** and **Status** columns.

According to your configuration, logs can be consulted and stored in the following locations:

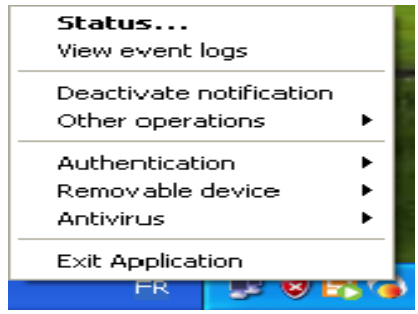
- User Interface.
- Pop-up.
- Database.
- External application.

You can add or delete logs coming from a StormShield agent in the Log Manager on the SkyRecon console.

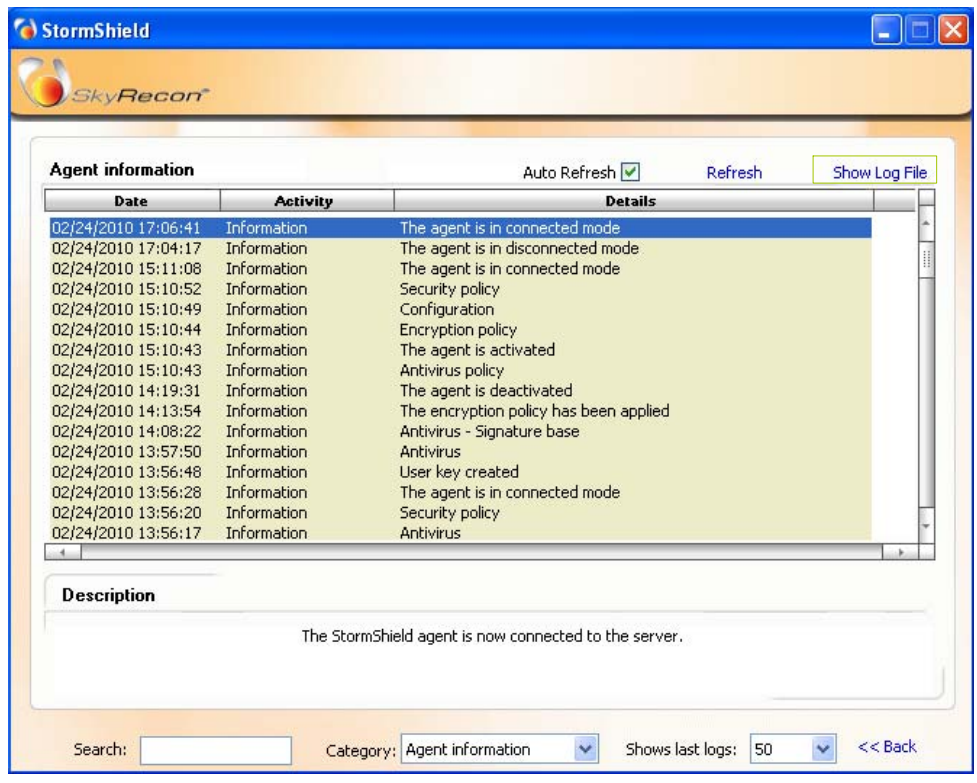
User interface

This is the System log file of the StormShield agent. To display this file on the agent computer, follow the steps below:

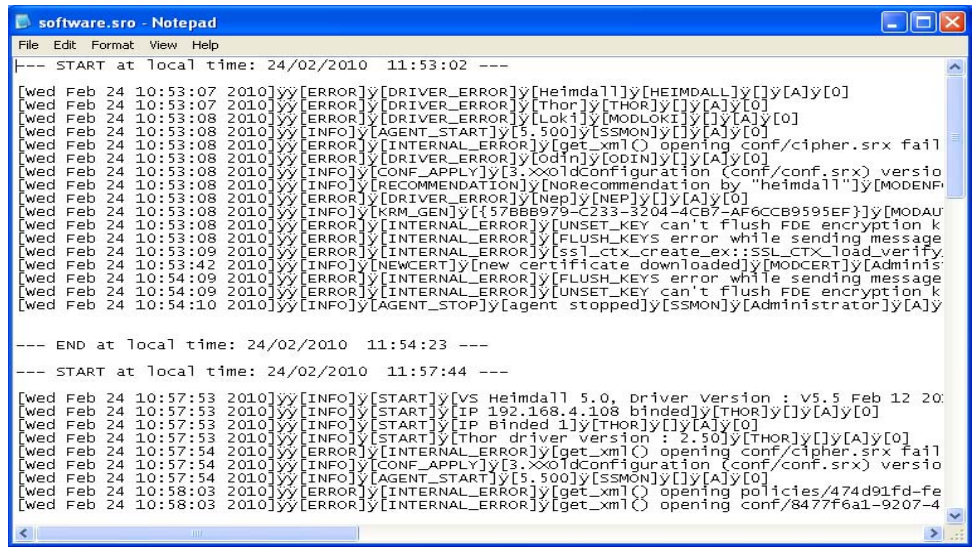
1. Click **View event logs**.



2. Click **Show Log File**.



The following window is displayed.



Pop-up

The log will be displayed in the notification window of the StormShield agent.

Database

The log will be recorded in the log database.

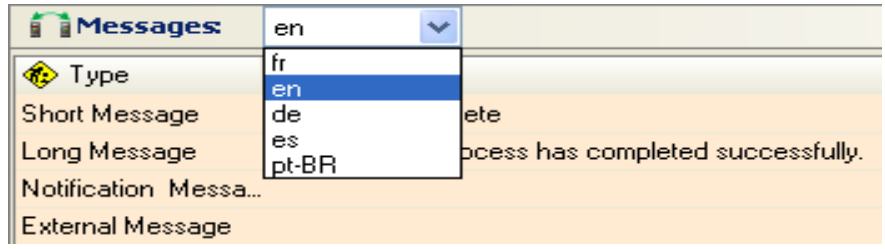
External application

The log will be sent to an external system (syslog or SMTP).

Messages

Language

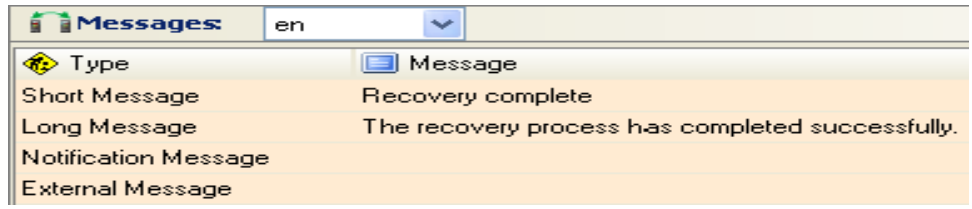
In the **Messages** window, you can choose the language used to display messages. The default language is English.



Message types

The Messages window includes four types of messages:

- Short Message.
- Long Message.
- Notification Message.
- External Message.

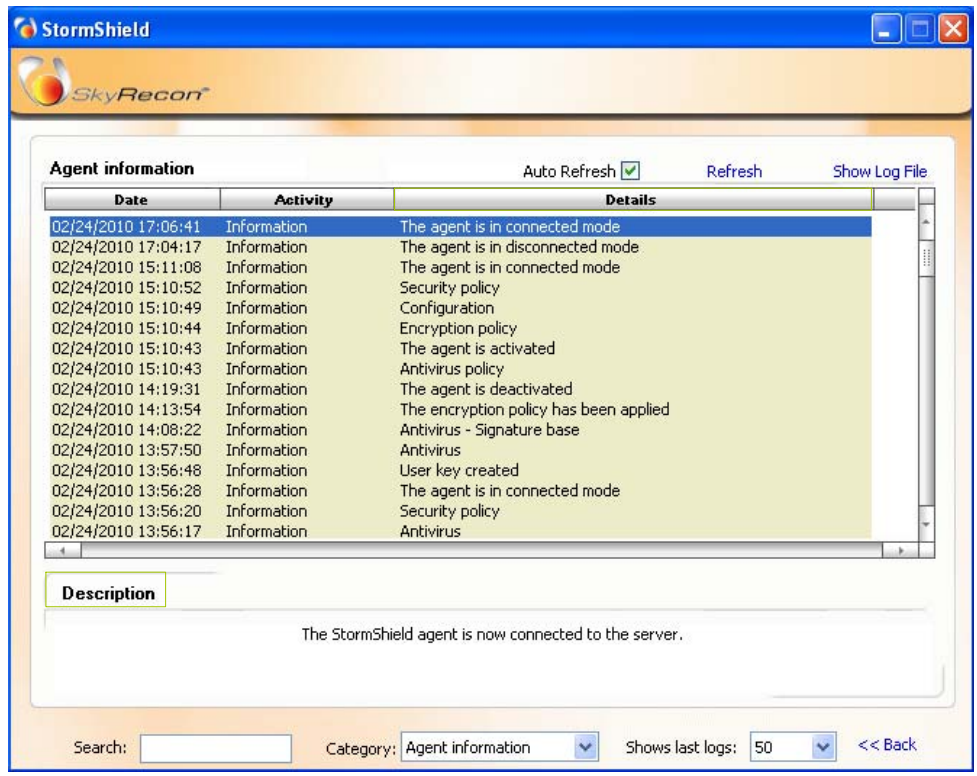


1. **Short Message**

   This is the message displayed in the **Details** column after selecting View event logs on the StormShield agent.

2. **Long Message**

   This is the message displayed in the **Description** column after selecting View event logs on the StormShield agent.



3. **Notification Message**

This is the message displayed in the notification pop-up of the StormShield agent.

4. **External Message**

   This is the message which will be sent to an external system (syslog or SMTP).

EXPORTING LOGS TO AN EXTERNAL SYSTEM (SMTP OR SYSLOG)

OVERVIEW

The administrator can use **Syslog** or **SMTP** (email) to send logs to an external server. He will have to configure external log transfer.

Log export is configured in the Environment Manager > [Master server] > **LogMonitoring Configuration**.

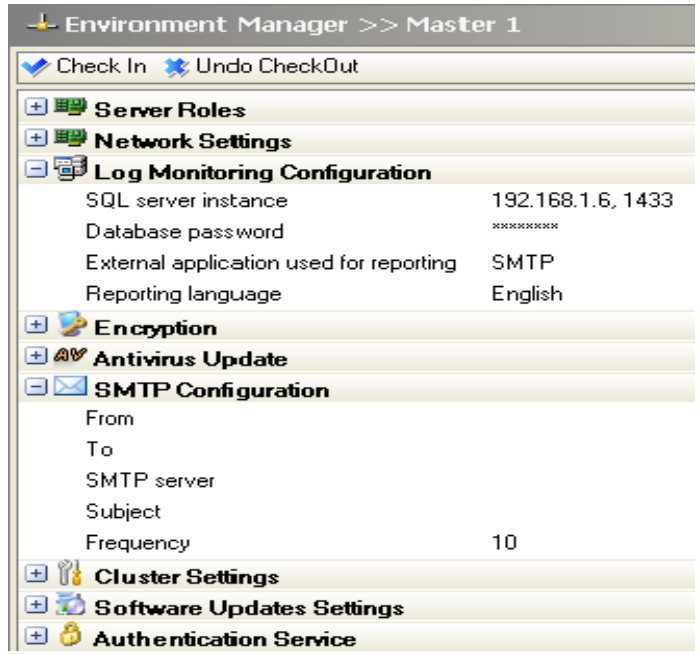
You can enable Syslog or SMTP to send logs but **not** both.

Depending on your selection, corresponding settings will be displayed in the Environment Manager (Syslog configuration or SMTP configuration panel).

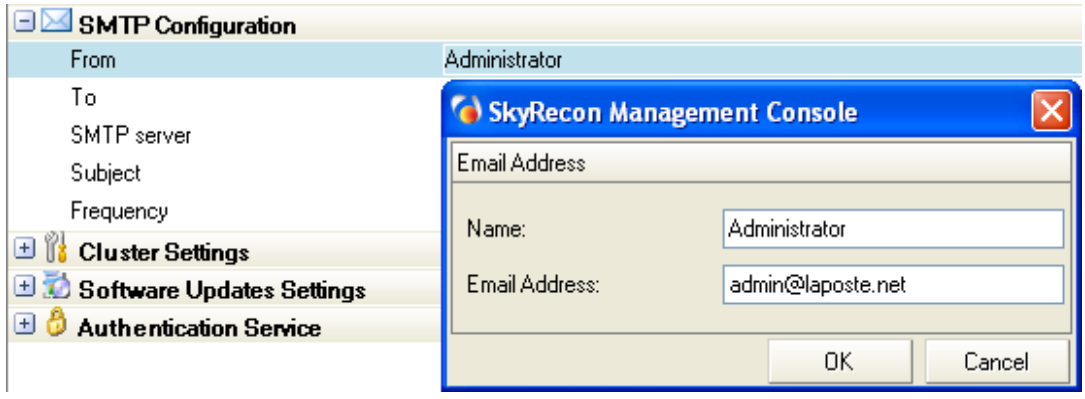
EXPORTING LOGS VIA SMTP

To export logs via SMTP, follow the steps below:

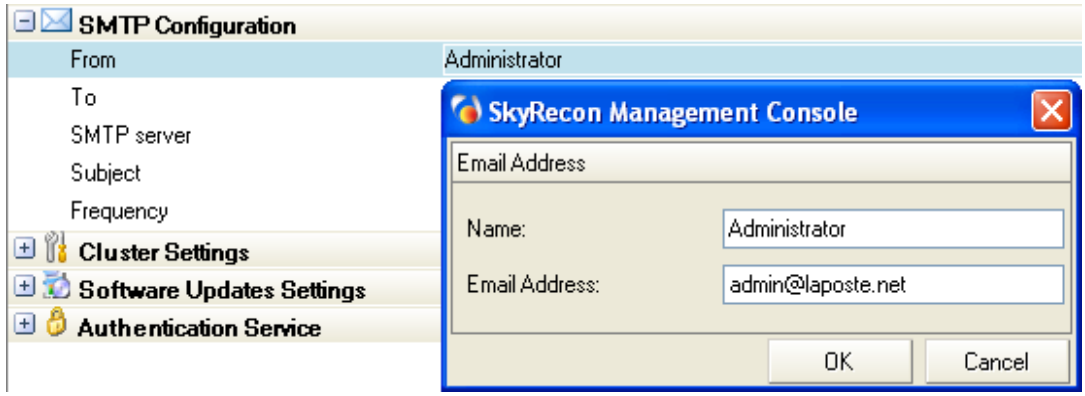
1. Select **SMTP** in **External application used for reporting**.
The **SMTP Configuration** window is displayed.



2. Define the SMTP redirection settings in the SMTP configuration panel of the primary server:
   - Click the **From** field.
   Enter the email name and address.

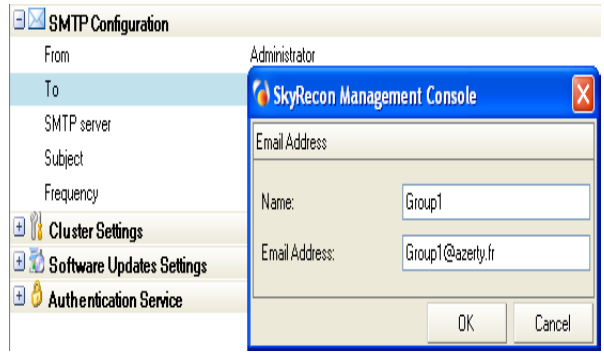


- Click the **To** field.
  Enter the email name and address.

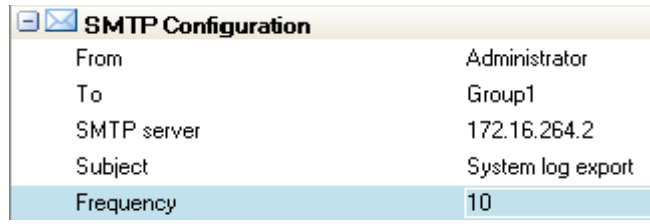


- Click the **SMTP Server** field.
  Enter the SMTP server and port information.

  If you want to use a login and a password, check the Login box and enter appropriate information.



- Enter the number of logs to be sent per message.



3. Validate your modifications.

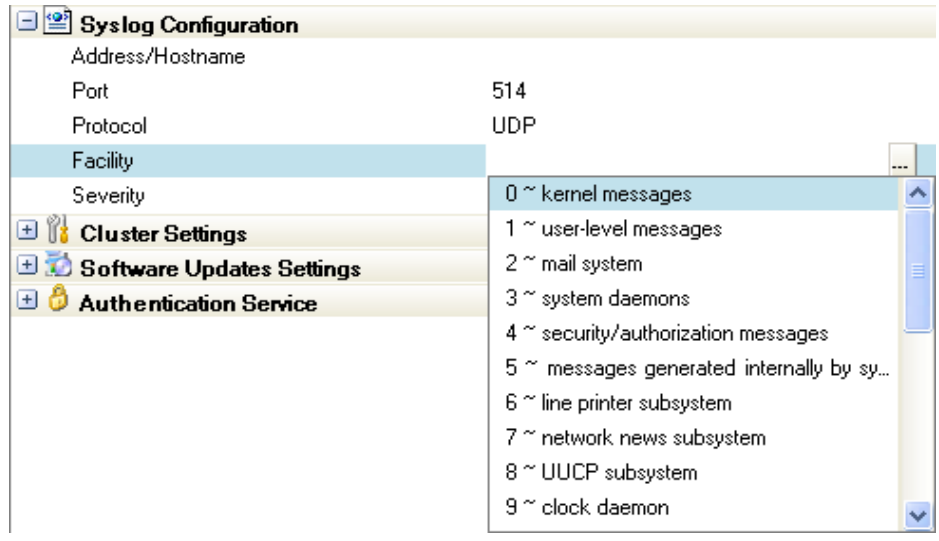
Use this feature **only** to send a few specific logs.

EXPORTING LOGS VIA SYSLOG

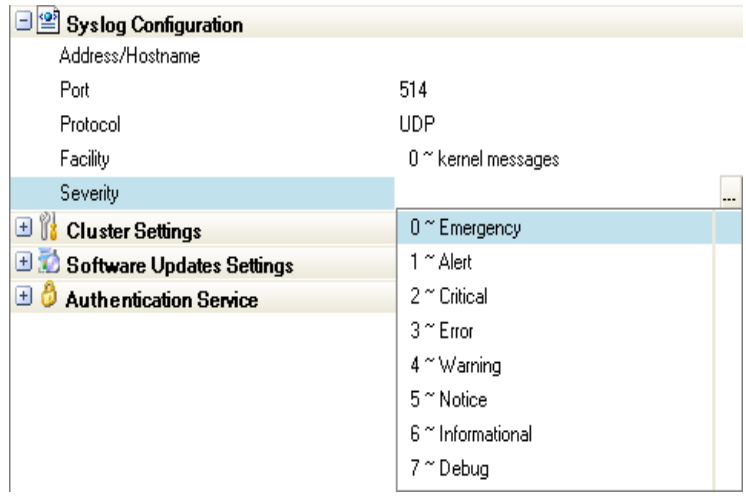
To export logs via Syslog, follow the steps below:

1. Select **Syslog** in **External application used for reporting**. The **Syslog Configuration** window is displayed.

2. Define the Syslog redirection settings in the Syslog configuration panel of the primary server:
   - In the **Address/Hostname** field, enter the IP address of the Syslog server.
   - In the **Port** field, change the port number (if necessary).
   - In the **Protocol** field, enter the protocol required (TCP or UDP).
   - Select a **Facility** level.



- Select a **Severity** level.



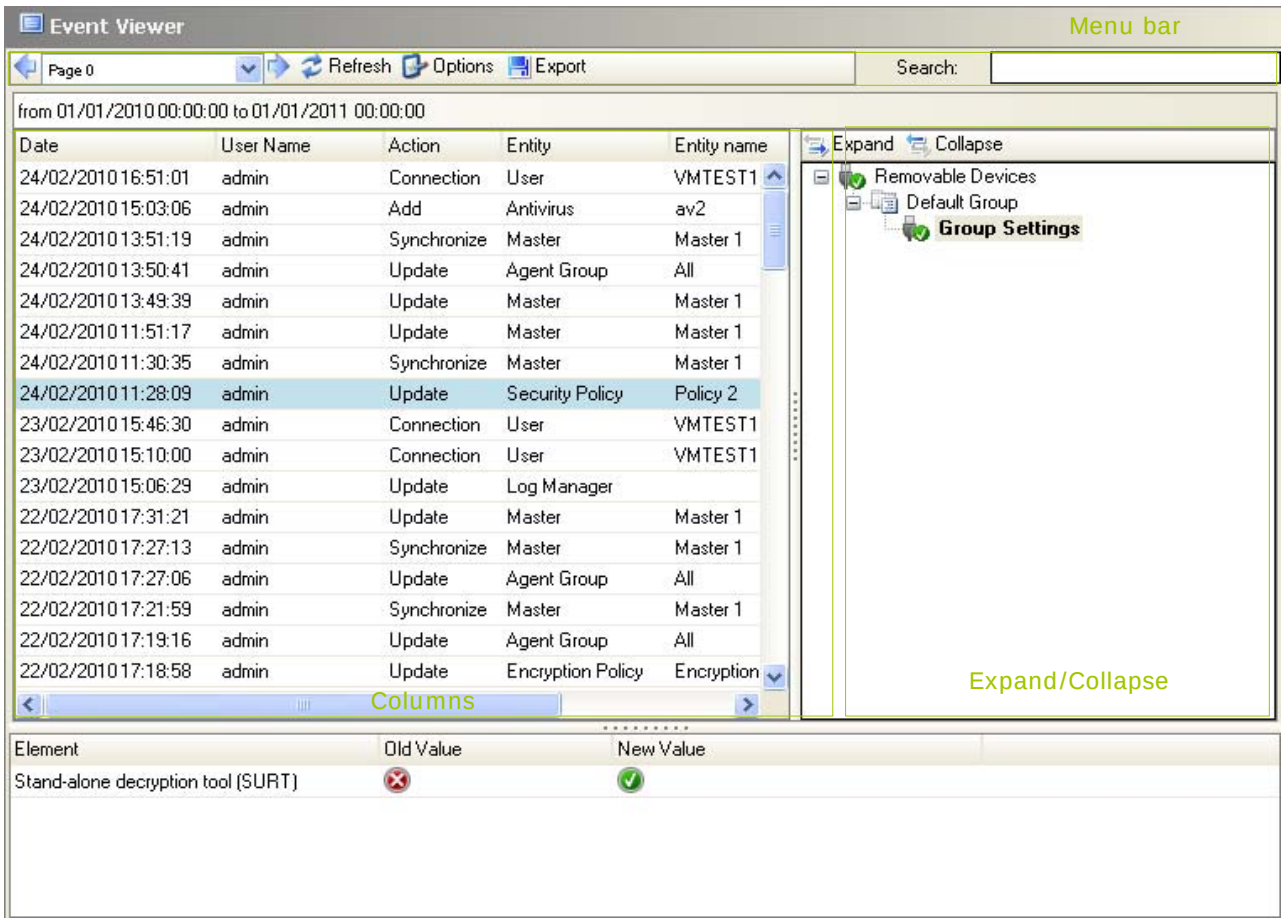
3. Validate your modifications.

Use this feature **only** to send a few specific logs.

EVENT VIEWER

OVERVIEW

All actions performed on the management console by an administrator can be recorded in logs accessible from the Event Viewer.



The administrator's actions which are recorded in the Event Viewer are the following:

- Policies:
  - Add.
  - Remove.
  - Rename.
  - Modify.

- Agent Group:
  - Add.
  - Remove.
  - Rename.
  - Modify.
- Configuration:
  - Add.
  - Remove.
  - Rename.
  - Modify.
- Script (action, test, batch, etc.):
  - Add.
  - Remove.
  - Rename.
  - Modify.
- Add an environment.
- Send a policy or configuration to a server.
- Create an administrator login.
- Change an administrator password.
- Etc.

GRAPHICAL INTERFACE

The graphical interface includes four areas:

- The menu bar.
- The columns.
- The **Expand/Collapse** panel.
- The **Details** panel.

Menu bar

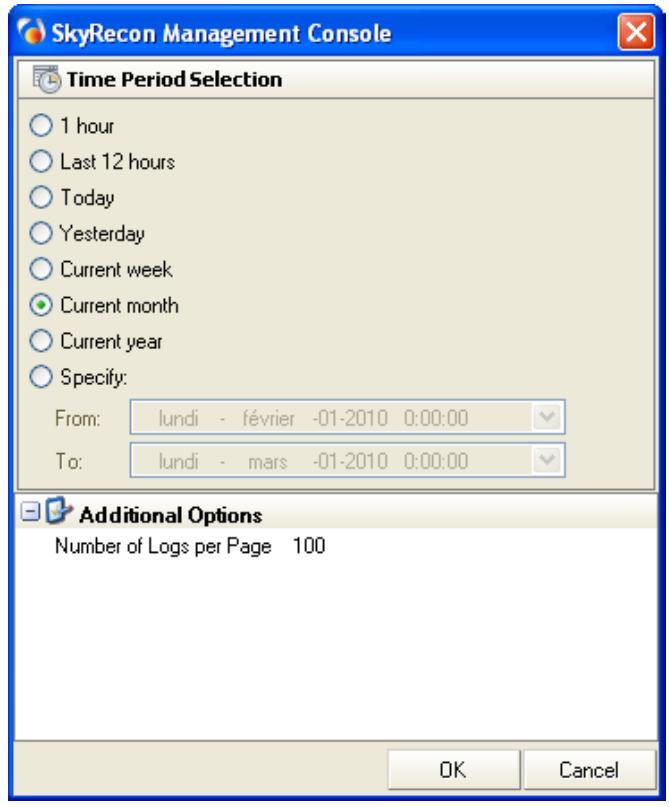
The menu bar includes the following commands:

- **Refresh:**

  Updates the display of the administrator's actions which are recorded in the Event Viewer.

- **Options:**

  Defines the display options.



  - **Time Period Selection:**

    Specifies the period of time to be used to display data in Review mode.
  - **Additional Options:**

    Specifies the number of logs to be displayed per page.

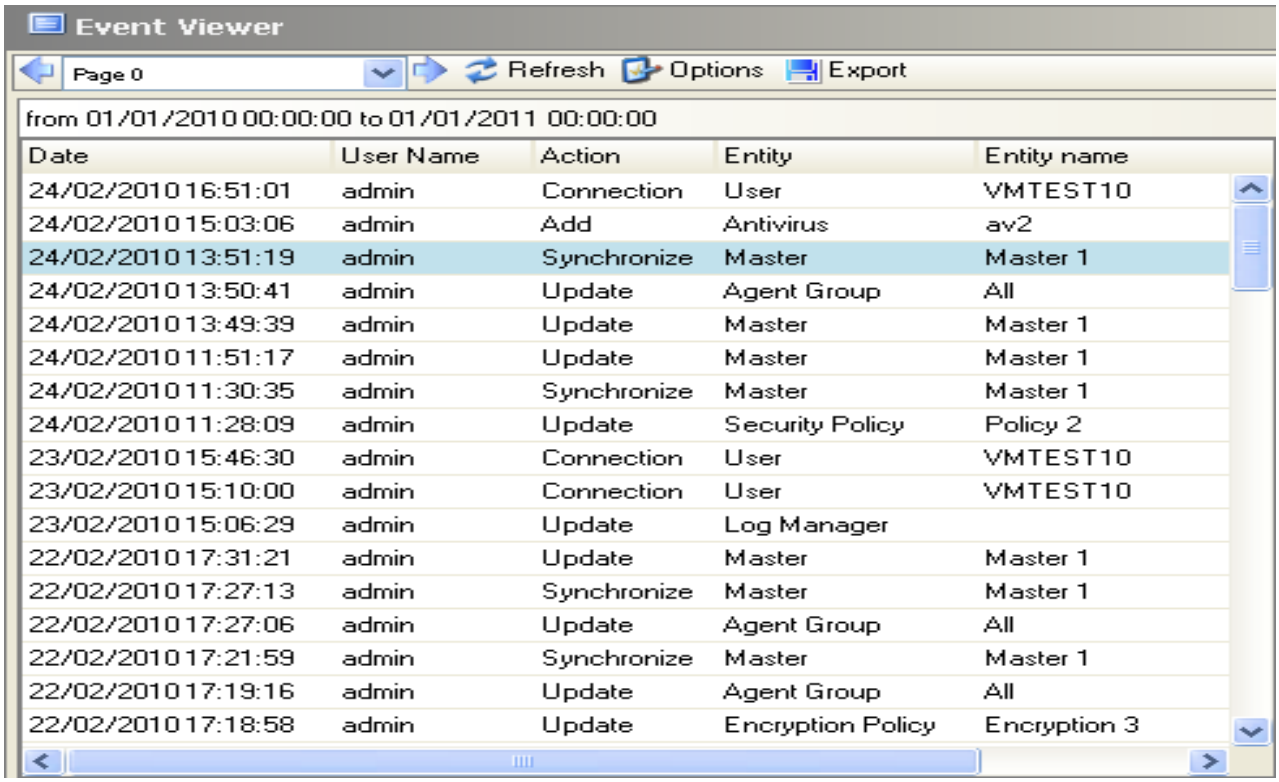
- **Export:**
  Used to save the information to a file in the XML format.
- **Search:**
  For long lists, you can use the **Search** field to locate the event quickly.

Columns

The information contained in the Event Viewer columns are the following:

- **Date**:
  Date and time of the administrator's action.
- **User Name**:
  Administrator's name.
- **Action**:
  Type of administrator's action which is reported in the Event Viewer.
  Here are a few examples of administrator's actions:
  - Synchronize.
  - Update.
  - Add.
  - Etc.
- **Entity**:
  Element associated with the administrator's action reported.
  Here are a few examples of entities:
  - Security Policy.
  - Encryption Policy.
  - Antivirus.
  - Configuration.
  - Scripts.
  - Agent Group.
  - Master server.
  - Etc.
- **Entity Name**:
  This column contains details on the administrator's action reported.
  Example:
  08/01/201011:31:37||admin||Synchronization||Master server||**Master 1**

The column specifies the name of the master server [Master1].



Date	User Name	Action	Entity	Entity name
24/02/2010 16:51:01	admin	Connection	User	VMTEST10
24/02/2010 15:03:06	admin	Add	Antivirus	av2
24/02/2010 13:51:19	admin	Synchronize	Master	Master 1
24/02/2010 13:50:41	admin	Update	Agent Group	All
24/02/2010 13:49:39	admin	Update	Master	Master 1
24/02/2010 11:51:17	admin	Update	Master	Master 1
24/02/2010 11:30:35	admin	Synchronize	Master	Master 1
24/02/2010 11:28:09	admin	Update	Security Policy	Policy 2
23/02/2010 15:46:30	admin	Connection	User	VMTEST10
23/02/2010 15:10:00	admin	Connection	User	VMTEST10
23/02/2010 15:06:29	admin	Update	Log Manager	
22/02/2010 17:31:21	admin	Update	Master	Master 1
22/02/2010 17:27:13	admin	Synchronize	Master	Master 1
22/02/2010 17:27:06	admin	Update	Agent Group	All
22/02/2010 17:21:59	admin	Synchronize	Master	Master 1
22/02/2010 17:19:16	admin	Update	Agent Group	All
22/02/2010 17:18:58	admin	Update	Encryption Policy	Encryption 3

Expand/Collapse

The **Expand/Collapse** panel displays an updated tree structure of the administrator's actions.

To display a deeper level of details on the console, click the appropriate level in the **Expand/Collapse** panel.
Example: **Group Settings**.

Click to expand the tree structure.

Click to collapse the tree structure.

Details

After clicking the appropriate level on the **Expand/Collapse** panel, the **Details** panel will display additional information (Old Value and New Value) on the updated administrator's action.

Example:
Here is the **Details** panel after clicking **Group Settings** in the **Expand/Collapse** panel.

Chapter 18

LOGS AND ALERTS

ABOUT THIS CHAPTER

This chapter describes the logs and their graphical interfaces.

It includes the following:

- Overview.
- Agent information logs:
  - Software logs.
  - System logs.
  - Network logs.
  - Device logs.
- Certificate server logs.
- Antivirus protection logs:
  - Server installation and update.
  - Agent installation and update.
  - Detected virus.
- Sending logs customized by the user

OVERVIEW

Log data is collected by the StormShield agent on the client workstation and stored locally.

The path followed by the information used to generate reports is described below:

1. Logs are sent by the agents to the StormShield server.
2. The server sends these logs to the StormShield SQL database.
3. Logs are displayed on the SkyRecon management console.

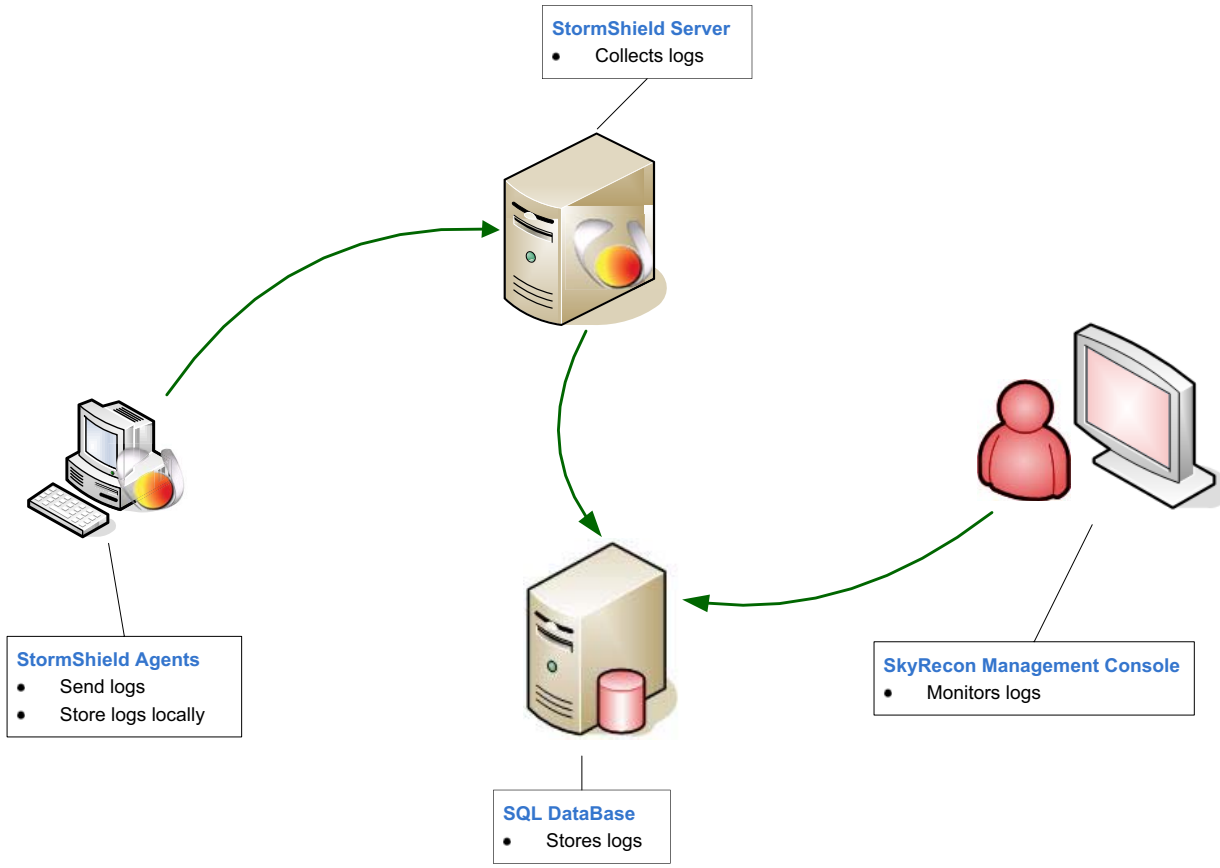


Fig. 18.1: StormShield log path

AGENT INFORMATION LOGS

SOFTWARE LOGS

Location

Information on agent activity and status is stored in a log file whose path is:

```
[Program Files]\SkyRecon\StormShieldAgent\log\software.sro
```

Variables

Each Software Log variable can assume the following values:

VARIABLE	DESCRIPTION
TIMESTAMP	Date format: Tue Apr 20 11:22:15 2010
ACTION	ERROR INFO WARN
STATUS	See table "Software log variable details", page 642.
TYPE	AGENT SERVER
MODNAME	Module name
LOG	Information message
USERID	User identifier
HOSTNAME	Agent hostname
HOSTADNAME	Agent AD name
HOSTIP	Agent IPv4 address

Table 18.1: Software log variables

Correspondence between variables and console display

Each log variable is displayed on the console as follows:

VARIABLE	CONSOLE DISPLAY
TIMESTAMP	Date
ACTION	Action
STATUS	Status
TYPE	Type
MODNAME	Mod. Name
LOG	Log

Table 18.2: Correspondence between Software log variables and console display

Details

Each log variable is associated with a keyword whose meaning is given in the table below:

VARIABLE	KEYWORD	DESCRIPTION
TIMESTAMP	20/01/2010 11:16:30	Date format
ACTION	ERROR	Blockage
	INFO	Audit
	WARN	Warning mode
STATUS	ACTION-FAILED	An action in the batch in progress returned an error
	ACTION-MISSING	Batch engine fails to interpret the action
	AGENT-IN	Agent connected
	AGENT-OUT	Agent disconnected
	AGENT-START	Agent started
	AGENT-STOP	Agent stopped
	AV_CORRUPTED	Antivirus installation corrupted. The agent has installed the antivirus but a registry key proving that the antivirus has been installed is missing.
	AV_SCAN_FINISHED	End of the antivirus scan
	AV_SCAN_INTERRUPTED	Antivirus scan interrupted

Table 18.3: Software log variable details (Sheet 1 of 7)

VARIABLE	KEYWORD	DESCRIPTION
	AV_SCAN_START	Antivirus scan started
	BAN-HOST	Host banned by the StormShield server because its certificate is used by another connected machine
	BATCH-LOG	Message
	CGI-DENIED	Certificate server denies agent certificate download request
	CGI-ERROR	Error when downloading the certificate
	CGI-INVALID	Error when downloading the certificate
	CGI-SLEEP	Certificate server is in sleep mode and cannot download certificates
	CHALLENGE_INVALID_VALUE	Invalid action or duration
	CHALLENGE-FAILED	StormShield server fails to send a token to a connected agent because the agent token key is outdated
	CHECK-FAILED	A test in the batch returned FALSE
	CHECK-MISSING	Batch engine fails to interpret the test
	CIPHER_CONF	Encryption policy has been read
	CIPHER_NEED_RECOVERY	File encryption has been disabled. Manual recovery is required
	COM-ERROR	Internal communication error
	COM-EXT	An external element has generated a StormShield log in the message
	CONF_APPLY	Application of the configuration or security policy to the agent
	CPU_CONTROL	CPU overload on the server
	CUSTOMACTION_1	Batch 1 executed
	CUSTOMACTION_2	Batch 2 executed
	CUSTOMACTION_3	Batch 3 executed
	CUSTOMACTION_4	Batch 4 executed
	CUSTOMACTION_5	Batch 5 executed
	CUSTOMACTION_ALLOWDRIVER	**Install drivers** action executed
	CUSTOMACTION_AVDAMIN	**Antivirus control** action executed
	CUSTOMACTION_NEPGUESTACCOUNT	**Create Guest Account** action executed
	CUSTOMACTION_STANDBY	**Disable Protections** action executed

Table 18.3: Software log variable details (Sheet 2 of 7)

VARIABLE	KEYWORD	DESCRIPTION
	CUSTOMACTION_STOP	**Disable Protections/Complete Stop** challenge executed
	CUSTOMACTION_UNINSTALL	**Uninstall Agent** challenge executed in %seconds
	DB_ERROR	Internal communication error with the database
	DRIVER_ERROR	Agent failed to connected to the driver
	FILE_NOT_FOUND	File cannot be found
	FLOOD_DETECTED	Log repeated and finally removed
	GET_KCM	Attempt to retrieve recovery keys denied by the server
	GET_PATCH	Patch download failed because available disk space is insufficient
	HOTSPOT_START	Beginning of the temporary web access period. Access duration is displayed in seconds
	HOTSPOT_STOP	End of the temporary web access period
	INCORRECT_DATA	The minimum configuration file present in Apache is incorrect
	INTERNAL_ERROR	Internal error (message)
	INVALID_BATCH_PARAM	The test or action in the batch includes an incorrect number of parameters at its input
	KRM_GEN	Agent has generated its unique identifier
	KU_GEN	The encryption keys assigned to the user have been downloaded
	LICENCE	Log generated if the number of agents connected to the servers exceeds the license threshold.
	LOKI_POLICY_CHANGE	Kernel protection status has changed
	LOKI_SET_CHALLENGE	Error when setting the number of reboots for driver installation
	MIGRATION_END	End of the migration of key files to the database
	MIGRATION_ERROR	Failure of the migration of key files to the database
	MIGRATION_START	Beginning of the migration of key files to the database

Table 18.3: Software log variable details (Sheet 3 of 7)

VARIABLE	KEYWORD	DESCRIPTION
	NEP_GUEST_ACCOUNT	• Add/remove a guest account • Failure to create/remove a guest account
	NEP_INSTALL_BUSY	Failure to change a password because a configuration is being applied
	NEP_INSTALL_COM_FAILURE	A communication error occurred when applying the configuration
	NEP_INSTALL_CONF_CANCELED	The application of the encryption configuration has been cancelled
	NEP_INSTALL_DISK_FAILURE	A disk-related error occurred when applying the configuration
	NEP_INSTALL_INVALID_CONF	Failure when applying the configuration. The configuration is invalid
	NEP_INSTALL_INVALID_DISK	Failure when applying the configuration. The disk is invalid
	NEP_INSTALL_INVALID_SYSTEM	Failure when applying the configuration. The operating system is invalid
	NEP_INSTALL_REBOOT	Reboot the machine to complete the application of the full disk encryption policy
	NEP_INSTALL_REGISTRY_FAILURE	A registry-based error occurred when applying the configuration
	NEP_INSTALL_SHM_FAILURE	A shared memory error occurred when applying the configuration
	NEP_INSTALL_SIMU_FAILURE	A simulation error prevents the configuration from being applied
	NEP_INSTALL_SUCCESS	Successful application of the full disk encryption configuration
	NEP_INSTALL_SYNC_FAILURE	An error occurred when synchronizing/ desynchronizing the disk
	NEP_INSTALL_SYSTEM_FAILURE	A system error prevents the configuration from being applied
	NEP_INSTALL_UNKNOWN	An unknown error prevents the configuration from being applied
	NET-INT	Network interfaces have been dumped
	NEWCERT	New certificate has been downloaded
	NO_CONF	No configuration
	OBTAIN_FILE	File cannot be obtained because available disk space is insufficient

Table 18.3: Software log variable details (Sheet 4 of 7)

VARIABLE	KEYWORD	DESCRIPTION
	ODIN_ERROR_ACCES	Agent fails to access a file for encryption/ decryption purposes
	OPTIM	• Network filtering rules hide lower rank rules (hidden rules removed to speed up processing) • An identical dynamic filtering rule already exists (the Add operation is ignored to speed up processing)
	PIPE_CALL_FROM_NAME	Error occurred when the pipe called a function
	POLICY_CHANGE	A new policy has been received. Reboot to apply the policy
	PWD_CHG_NOT_APPLY	Failure to change the password assigned to the specified user
	RECOMMENDATION	Whenever the UAC state changes (NAP or Juniper)
	RECOVER_PATH	Recovery of a machine or directory using a file including a key ring Param1: [Directory]/Param2: [File]
	RECOVERY_COMPLETE	Successful recovery
	RECOVERY_ERROR	Internal error during recovery
	RECOVERY_FAILURE	Failed recovery
	SEND_FAILED	• Data transfer to the server failed • Challenge transfer to an agent failed
	SERVER_VERSION	Displays the server version number
	SET_KEY	Displays whether the synchronization was successful or not and the time required for its completion
	SIG_ERROR	The profiling resource file is not accessible
	SSMON_SESSION_HANDLER	Error when handling session events
	SSMON_STORECAMODE_FAILURE	Error when saving information
	SSMON_STORECAMODE_INVALID	Invalid data
	START	The Userland module succeeded in connecting to its driver
	STOP	The Userland module stopped successfully
	STOPAGENTDENIED	Stop Agent action failed
	STOPAGENTEXE	Agent was stopped via stopagent.exe

Table 18.3: Software log variable details (Sheet 5 of 7)

VARIABLE	KEYWORD	DESCRIPTION
	SYNC_DIR	An error occurred when synchronizing/ desynchronizing a directory
	UAC	UAC status changed (NAP/Juniper)
	UNSET_KEY	Keys have been flushed
	UPDATING	A new patch has been downloaded onto the agent
	USER_REVOKED	Authentication on a revoked user
	WTS_SYNC	Error when creating the pipe for the SID
TYPE	AGENT	Agent
	SERVER	Server
MODNAME	ALL	
	HEIMDALL	
	HEIMDALL/THOR	
	MODACTION	
	MODAUTH	
	MODAV	
	MODCERT	
	MODCOM	
	MODDB	
	MODENFORCEMENT	
	MODFLOOD	
	MODGETCONF	
	MODKEYGEN	
	MODLDAP	
	MODMULTI	
	MODNEP	
	MODRECOVERY	
	MODROOTCERT	
	MODTOKENROOT	
	MODUPDATE	
	ODIN	

Table 18.3: Software log variable details (Sheet 6 of 7)

VARIABLE	KEYWORD	DESCRIPTION
	SSMON	
	THOR	

Table 18.3: Software log variable details (Sheet 7 of 7)

SYSTEM LOGS

Location

Information on system activity and status is stored in a log file whose path is:

```
[Program Files]\SkyRecon\StormShieldAgent\log\heimdall.sro
```

Variables

Each System Log variable can assume the following values:

VARIABLE	DESCRIPTION
TIMESTAMP	Date format: Tue Apr 20 11:22:15 2010
ACTION	See table "System log variable details", page 650.

Table 18.4: System log variables (Sheet 1 of 3)

VARIABLE	DESCRIPTION
STATUS	[BLK] [BLKCREATE] [BLKEXECUTE] [EXT-BLK] [HEAP-BLK] [LIBC-BLK] [PROFIL-BLK] [RDONLY] [STACK-BLK] [WARN] Antivirus : [ABORTED] [BLOCKED] [CLEANED] [ERASED] [FILE_UNKNOWN] [IGNORED] [MOVED] [MOVED_QUARENTINE] [MSG_ATT_DELETED] [MSG_ATT_MOVED_QUARANTINE] [MSG_ERASED] [MSG_BLOCKED] [MSG_IGNORED] [MSG_MOVED] [MSG_MOVED_CUARENTINE] [MSG_MARKED] [MSG_MARKED_MOVED] [OVERWRITTEN] [RENAMED] [WEB_FILE_MOVED_QUARANTINE] [WEB_FILE_BLOCKED] [WEB_IGNORED] For more information, see table "System log variable details", page 650.
SOURCE	Source program name
DEST	Destination program/file name
OPTION	Options

Table 18.4: System log variables (Sheet 2 of 3)

VARIABLE	DESCRIPTION
USERID	User IDentifier
RID	Unique Rule IDentifier

Table 18.4: System log variables (Sheet 3 of 3)

Correspondence between variables and console display

Each log variable is displayed on the console as follows:

VARIABLE	CONSOLE DISPLAY
TIMESTAMP	Date
ACTION	Action
STATUS	Status
SOURCE	Source
DEST	Destination
OPTION	Option
RID	RID

Table 18.5: Correspondence between System log variables and console display

Details

Each log variable is associated with a keyword whose meaning is given in the table below:

VARIABLE	KEYWORD	DESCRIPTION
TIMESTAMP	Tue Apr 20 11:22:15 2010	Date format
ACTION	ACCESS-REG	Access to registry
	ATTACH-PROCESS	Attempt to attach a process
	AV	Information on viruses
	BAD-KEY	The decryption key used to open the file is invalid

Table 18.6: System log variable details (Sheet 1 of 4)

VARIABLE	KEYWORD	DESCRIPTION
	BLOCKED-DRIVER	Driver download has been blocked Possible kernel protection values in the **Option** column under Log Monitoring > System: **1**: The driver is hidden **2**: The driver is hooked **3**: The driver's name has changed **4**: The driver file does not exist on the disk **5**: The driver is hooking
	CHECKSUM	The application hash has been modified
	COPY-PASTE	A process which is not allowed to use Copy/Paste has been blocked
	CREATE	File opening in Create mode
	DELETE	Attempt to delete a file
	EXE_ON_USB	Execution of an application from a removable device Possible values about the context of approval or deny of the execution of the application in the **Option** column under Log Monitoring > System: **0**: The user has explicitly accepted or denied the execution of the application **1**: The agent is in warning mode, the execution of the application has been automatically accepted **2**: The user has not answered or has not been able to answer (if ssmon.exe is not executed for example), the execution of the application has been automatically denied.
	HOOK	Attempt to perform a global hook
	HOOKED-DRIVER	Driver hooked by another driver For more details on kernel protection values, see BLOCKED-DRIVER.
	KEYLOG	Attempt to keylog
	LOAD-DRIVER	Notification that a new driver has been loaded For more details on kernel protection values, see BLOCKED-DRIVER.
	LOAD-OBJECT	DLL loading or shared memory use
	LOCK-KEY	Access to files encrypted with a batch is denied
	OPEN-PROCESS	Attempt to open a process
	OPEN	File opening

Table 18.6: System log variable details (Sheet 2 of 4)

VARIABLE	KEYWORD	DESCRIPTION
	OVERFLOW	Memory overflow
	PROCESS-INFORMATION	Attempt to access list of active processes
	REBOOT	Attempt to reboot the system
	RENAME	Attempt to rename a file
	SOCK-ACCEPT	Using an accept (server socket)
	SOCK-BIND	Using a bind (server socket)
	SOCK-CONNECT	Using a connect (client socket)
	SOCK-ICMP	Creation of an ICMP socket
	SOCK-LISTEN	Using a listen (server socket)
	SOCK-RAWIP	Creation of a raw or UDP socket
	SU	Attempt to elevate process privileges
	SUSPECT-DRIVER	Suspect operation performed by the driver For more details on kernel protection values, see BLOCKED-DRIVER.
	TERMINATE-PROCESS	Process was terminated (mainly due to CPU overload)
	WRITE	Attempt to write a file
STATUS	BLK	Blocked
	BLKCREATE	Blocked during creation
	BLKEXECUTE	Blocked during execution
	DYN-BLK	Blocked by a dynamic rule
	EXT-BLK	Blocked by an extension rule
	HEAP-BLK	Blocked due to heap overflow
	LEVEL-BLK	Warning and blockage by level
	LIBC-BLK	Blocked by ret-into-libc
	PROFIL-BLK	Blocked by a deviation from standard profile
	RDONLY	Enforces read-only access
	STACK-BLK	Blocked by stack overflow
	WARN	Warning without blockage
	For more information on antivirus logs, see "Detected virus", page 671.	

Table 18.6: System log variable details (Sheet 3 of 4)

VARIABLE	KEYWORD	DESCRIPTION
SOURCE		Name of the process that triggered the event Note: Even if the StormShield protection is enabled at startup, if the event occurs before the StormShield service starts, an exclamation point "!" will precede the name of the process which triggered it.
DEST		Target object path
OPTION		• Socket (default value is 0) • Hook identifier if the action type is HOOK or KEYLOG
RID		Unique Rule IDentifier **Remark**: You can double-click the log entry RID to go directly to the rule.

Table 18.6: System log variable details (Sheet 4 of 4)

NETWORK LOGS

Location

Information on network activity is stored in a log file whose path is:

```
[Program Files]\SkyRecon\StormShieldAgent\log\thor.sro
```

Variables

Each Network Log variable can assume the following values:

VARIABLE	DESCRIPTION
TIMESTAMP	Date format: Tue Apr 20 11:22:15 2010
ACTION	For more information, see table "Device log variable details", page 660.
STATUS	[INFO] [IN] [OUT] [CONNECTION_CLOSED] [IP_BLOCKED] [SCAN_IN] [SCAN_OUT] For more information, see table "Device log variable details", page 660.
METADATA	For more information, see table "Device log variable details", page 660.
IP	• SSID (WiFi) • IP fragment • IP address
PORTSRC	• Source port (TCP, UDP) • Channel (WiFi) • Type (ICMP)
PORTDST	Destination port (TCP/UDP) Code (ICMP)
PROTO1	Protocol over ethernet
PROTO2	IP protocol

Table 18.7: Network log variables (Sheet 1 of 2)

VARIABLE	DESCRIPTION
USERID	User IDentifier
RID	Unique Rule IDentifier

Table 18.7: Network log variables (Sheet 2 of 2)

Correspondence between variables and console display

Each log variable is displayed on the console as follows:

VARIABLE	CONSOLE DISPLAY
TIMESTAMP	Date
ACTION	Action
STATUS	Status
TYPE	Type
MODNAME	Mod. Name
LOG	Log

Table 18.8: Correspondence between Network log variables and console display

Details

Each log variable is associated with a keyword whose meaning is given in the table below:

VARIABLE	KEYWORD	DESCRIPTION
TIMESTAMP	Tue Apr 20 11 :22 :15 2010	Date
ACTION	ARP_ATTACKING 0x21	Identity theft attempt detected on an IP address on the network. Packet blocked.
	ARP_BLOCK 0x1	ARP stateful error (reply without request) or ARP_POISON flood
	ARP_DELETE 0x5	Entry associated with the IP address has been removed from the Windows ARP cache. Packet blocked after sending a gratuitous request (IDS set to **High** or **Critical**).

Table 18.9: Network log variable details (Sheet 1 of 3)

VARIABLE	KEYWORD	DESCRIPTION
	ARP_POISON 0x45	ARP cache poisoning attempt detected. Packet blocked. Entry associated with the suspect IP address has been removed from the Windows ARP cache.
	ARP_POISON 0x49	ARP cache poisoning attempt detected. Packet blocked. Windows ARP cache has been updated from the previous entry.
	ARP_SPOOF 0x112	Identity theft attempt detected on the IP address. Packet accepted. Network protection (IDS set to **Critical**).
	ARP_SPOOF 0x12	Identity theft attempt detected on the IP address. Packet accepted.
	FLOOD	Repeated log entry
	FW_ICMP	Rule applied to an ICMP message. METADATA, PROTO1, IP, PROTO2, PORTSRC and PORTDST variables are filled in.
	FW_IP	Rule applied to an IP address (only METADATA, PROTO1, IP and PROTO2 variables are filled in)
	FW_MAC	Rule applied to MAC address (only METADATA and PROTO1 variables are filled in). The MAC address (hardware address of the network card) indicated in the METADATA column is the remote machine address since its local address remains the same.
	FW_PORT	Rule applied to port filtering. METADATA, PROTO1, IP, PROTO2, PORTSRC and PORTDST variables are filled in.
	PORTSCAN	Port scan detected
	STATEFUL_STATUS	PROTO1 variable indicates the stateful status code of the previously blocked packet
STATUS	CONNECTION_CLOSED	One or several connections have been closed because they are too slow
	IN	Filtering of incoming traffic
	IP_BLOCKED	Suspect IP address causing flood blocked
	OUT	Filtering of outgoing traffic

Table 18.9: Network log variable details (Sheet 2 of 3)

VARIABLE	KEYWORD	DESCRIPTION
	SCAN_IN	Incoming port scan detected
	SCAN_OUT	Outgoing port scan detected
IP	IP	IP address
METADATA		• In the case of a FLOOD, indicates the number of occurrences of the event. • Otherwise, indicates the MAC addresses.
PORTDST		Destination port number
PORTSRC		Source port number
PROTO1: PROTO2		• Protocols being filtered. • See "Protocols", page 683.
RID		Unique Rule IDentifier

Table 18.9: Network log variable details (Sheet 3 of 3)

DEVICE LOGS

The device log contains information on removable devices and WiFi activity.

Location

Information on removable device and WiFi activity is stored in a log file whose path is:

```
[Program Files]\SkyRecon\StormShieldAgent\device.sro
```

Variables

Each Device Log variable can assume the following values:

VARIABLE	DESCRIPTION
TIMESTAMP	Date format: Tue Apr 20 11:22:15 2010
ACTION	See "Device log variable details", page 660.
STATUS	Possible statuses are: [BLK] [INFO] [WARN]
SOURCE	Network card name (WiFi) Process name (mass storage device)
DEST1	File name (mass storage device) MAC address (WiFi)
DEST2	File name after renaming (mass storage device) SSID (WiFi)
SIZE	Device size
TYPE	Possible device types are: [FIREWIRE] [NETWORK] [PCMCIA] [USB]

Table 18.10: Device log variables (Sheet 1 of 2)

VARIABLE	DESCRIPTION
CLASSID	Possible classes are: [BLUETOOTH] [CDROM] [DISK] [IRDA] [MODEM] [PARALLEL] [PCMCIA] [SERIAL] [USB_ACTIVE_SYNC] [USB_APPLICATION_SPECIFIC] [USB_AUDIO] [USB_CDCDATA] [USB_COMMUNICATION] [USB_CONTENT_SECURITY] [USB_DIAGNOSTIC] [USB_HID] [USB_HUB] [USB_IMAGING] [USB_MISCELLANEOUS] [USB_PALM_SYNC] [USB_PHYSICAL] [USB_PRINTER] [USB_SMARTCARD] [USB_STORAGE] [USB_VENDOR_SPECIFIC] [USB_VIDEO] [USB_WIRELESS_CONTROLLER] [WIFI]
VENDORID	Vendor IDentifier
PRODUCTID	Product IDentifier
SERIALID	Serial IDentifier
VENDORNAME	Vendor name
PRODUCTNAME	Product name
USERID	User IDentifier
ENROLLMENTSTATE	Enrollment status
OWNERNAME	Owner of the enrolled device
RID	Unique Rule IDentifier

Table 18.10: Device log variables (Sheet 2 of 2)

Correspondence between variables and console display

Each log variable is displayed on the console as follows:

VARIABLE	CONSOLE DISPLAY
TIMESTAMP	Date
ACTION	Action
STATUS	Status
SOURCE	Source
DEST1	Destination
DEST2	Destination2
SIZE	Size
TYPE	Type
CLASSID	Class
USERNAME	Name of the user using the machine when the blockage occurred
RID	Unique Rule IDentifier

Table 18.11: Correspondence between Device log variables and console display

Details

Device log variables

Each log variable is associated with a keyword whose meaning is given in the table below:

VARIABLE	KEYWORD	DESCRIPTION
TIMESTAMP		Date format: Tue Apr 20 11:22:15 2010
ACTION	AP_ACL	Access point with ACL filtering rule (Status: WARN)
	AP_ADHOC	Access point in adhoc mode (Status: WARN)
	AP_INSECURE	Unsecured access point (Status: WARN)
	AP_WIFI	WiFi access point set to on/off (Status: WARN)
	BAD_UNPLUG	USB key incorrectly removed
	BLUETOOTH	Bluetooth device blocked
	CD	CD reading process blocked

Table 18.12: Device log variable details (Sheet 1 of 4)

VARIABLE	KEYWORD	DESCRIPTION
	CDWRITER	CD burning process blocked
	DEVICE_UNPLUG	Device plugged out
	DEVICE_PLUG	Device plugged in
	FILE_CREATE	File created (Status: INFO)
	FILE_DELETE	File deleted on the removable device (Status: INFO).
	FILE_OPEN	File opened on removable device (Status: BLK or WARN)
	FILE_OVERWRITE	File overwritten on the removable device (Status: INFO)
	FILE_READ	Data read on the removable device (Status: INFO)
	FILE_RENAME	File renamed on the removable device (Status: BLK or WARN)
	FILE_WOPEN	File opened for overwrite operation on removable device (Status: BLK or WARN)
	FILE_WRITE	Data written to a file on the removable device (Status: INFO)
	IRDA	Device using infrared port blocked
	MODEM	Modem blocked
	PARALLEL	Device connected to the parallel port blocked
	PCMCIA	PCMCIA device blocked
	SERIAL	Device connected to the serial port blocked
	USB_CLASSID	Class ID of the removable device (in the Status field)
	VOLUME_DISMOUNT	Disconnected removable device (Status: INFO)
	VOLUME_MOUNT	Connected removable device (Status: INFO)
	VOLUME_DENIED	Access to the device is forbidden. Generated if a rule specifies a filter on the enrollment status (Status : INFO)
	VOLUME_READONLY	Access to the device is read-only. Generated if a rule specifies a filter on the enrollment status (Status : INFO)
	VOLUME_READWRITE	Access to the device is authorized. Generated if a rule specifies a filter on the enrollment status (Status : INFO)
STATUS	BLK	Blocked
	INFO	Audit

Table 18.12: Device log variable details (Sheet 2 of 4)

VARIABLE	KEYWORD	DESCRIPTION
	WARN	Warning mode
SOURCE		Network card name (WiFi) Process name (removable mass storage device)
DEST1		File name
DEST2		File name after renaming (removable mass storage device) SSID (WiFi)
SIZE		Size of the device or modification
TYPE	FIREWIRE NETWORK PCMCIA USB	See "Type variables", page 664.
ClassID	BLUETOOTH CDROM DISK IRDA MODEM PARALLEL PCMCIA SERIAL USB_ACTIVE_SYNC USB_APPLICATION_SPECIFIC USB_AUDIO USB_CDCDATA USB_COMMUNICATION USB_CONTENT_SECURITY USB_DIAGNOSTIC USB_HID USB_HUB USB_IMAGING USB_MISCELLANEOUS USB_PALM_SYNC USB_PHYSICAL USB_PRINTER USB_SMARTCARD USB_STORAGE USB_VENDOR_SPECIFIC USB_VIDEO USB_WIRELESS_CONTROLLER WIFI	See "Class ID variables", page 664.

Table 18.12: Device log variable details (Sheet 3 of 4)

VARIABLE	KEYWORD	DESCRIPTION
ENROLLMENT STATE	UNENROLLED UNENROLLED_CORRUPT_ENROLL UNENROLLED_CORRUPT_FOOTPRINT ENROLLED ENROLLED_CONTENTCHANGED ENROLLED_NOTRUST TRUSTED	Refer to "Enrollment status variables", page 665
OWNERNAME		

Table 18.12: Device log variable details (Sheet 4 of 4)

WiFi variables

Each WiFi variable can assume the following values:

VARIABLE	KEYWORD	DESCRIPTION
ACTION	AP_ACL	Access point with ACL filtering rule
	AP_ADHOC	Access point in adhoc mode
	AP_INSECURE	Unsecured access point
	AP_WIFI	WiFi access point set to on/off
STATUS	WARN	Warning mode
SOURCE		Network interface name
DEST1		Access point MAC address
DEST2		Access point SSID
SIZE		Channel
TYPE		Network
CLASSID		WiFi
USERID		Information message
ID		User IDentifier

Table 18.13: WiFi variables

Type variables

Each Type variable can assume the following values:

VARIABLE	PURPOSE
FIREWIRE	Firewire access control and audit
NETWORK	WiFi access control
PCMCIA	PCMCIA access control and audit
USB	USB access control and audit

Table 18.14: Type variables

Class ID variables

Each Class ID variable can assume the following values:

VARIABLE	DESCRIPTION	PURPOSE
CDROM	CD-ROM, DVD-ROM, Blu-Ray reader	Access control, Write protection
DISK	Removable mass storage device	Access control, Audit
FLOPPY	Floppy disk drive	Heimdall
NETWORK	WiFi network	Access control
U3	U3 USB key	Access control
USB_AUDIO	USB audio card	Access control
USB_HID	USB HID devices (keyboard, mouse, graphics tablet, etc.)	Access control
USB_IMAGING	USB imaging devices (webcam, scanner, etc.)	Access control
USB_ACTIVE_SYNC	USB removable mass storage device	Class ID control
USB_APPLICATION_SPECIFIC	USB_APPLICATION_SPECIFIC class device	Class ID control
USB_CDCDATA	USB_CDCDATA class device	Class ID control
USB_COMMUNICATION	USB_COMMUNICATION class device	Class ID control
USB_CONTENT_SECURITY	USB_CONTENT_SECURITY class device	Class ID control
USB_DIAGNOSTIC	USB_DIAGNOSTIC class device	Class ID control
USB_HUB	USB_HUB class device	Class ID control
USB_MISCELLANEOUS	USB_MISCELLANEOUS class device	Class ID control

Table 18.15: Class ID variables (Sheet 1 of 2)

VARIABLE	DESCRIPTION	PURPOSE
USB_PALM_SYNC	USB_PALM_SYNC class device	Class ID control
USB_PHYSICAL	USB_PHYSICAL class device	Class ID control
USB_PRINTER	USB printer	Access control
USB_SMARTCARD	USB smart-card reader	Class ID control
USB_STORAGE	USB removable mass storage device	Class ID control
USB_VENDOR_SPECIFIC	USB_VENDOR_SPECIFIC class device	Class ID control
USB_VIDEO	USB_VIDEO class device	Class ID control
USB_WIRELESS_CONTROLLER	USB_WIRELESS_CONTROLLER class device	Class ID control
WIFI	Wireless network interface	WIFI (modap)

Table 18.15: Class ID variables (Sheet 2 of 2)

Enrollment status variables

Each Enrollment status variable can assume the following values:

VARIABLE	DESCRIPTION	ACTION
UNENROLLED	The device is not enrolled	
UNENROLLED_CORRUPT_ENROLL	The enrollment file is corrupted	The device is considered as not enrolled
UNENROLLED_CORRUPT_FOOTPRINT	The footprint file is corrupted	The device is considered as not enrolled
ENROLLED	The device is enrolled	
ENROLLED_CONTENTCHANGED	The device is enrolled but its content has changed out of the perimeter	The device is considered as enrolled
ENROLLED_NOTRUST	The device is enrolled but its trust status could not be restore	The device is considered as enrolled
TRUSTED	The device is trusted	Trust status maintained when performing operations on the device

Table 18.16: Enrollment status variables

Alert types

Removable device alerts issued by the Log Manager are the following:

- **Short Message:**

  This is the message that you can read in the list of logs on the agent computer when clicking the StormShield monitor icon .

  ```
  Block Process:%SOURCE%
  ```

- **Long Message:**

  This is the detailed message that you can read when selecting a log in StormShield Monitor on the agent computer.

  ```
  Access to [DEVICE NAME] device performed by %SOURCE% has been blocked%BR%Please contact your administrator for further information.
  ```

- **Notification Message:**

  This is the message that you can read in a pop-up on the agent (if the field is empty, no pop-up is displayed).

  ```
  Access to [DEVICE NAME] device is not allowed on this workstation.
  ```

- **External Message:**

  This is the message that you can read on the external logging system (example: Syslog).

  ```
  Access to [DEVICE NAME] device performed by %SOURCE% has been blocked.
  ```

Varaiables between **%** are replaced by the name of the resource when displayed on the agent.

CERTIFICATE SERVER LOGS

Information issued by the certificate server is stored in a log file whose path is:

`[Program Files]\SkyRecon\StormShieldServer\Apache\logs\cgi.log`

Log entries fall down into three categories:

- **Info**
  - `Info: RECOVERY certificate created [IP]:`

    A recovery certificate has been requested by the IP host and generated.
  - `Info: Permission denied [ERRCODE] [IP]:`

    Certificate download request from the IP host has been rejected.
  - `ERRCODE = e:`

    Internal error.
  - `ERRCODE = s:`

    Current date is not comprised within the certificate download period.
  - `ERRCODE = d:`

    Agent origin is not valid (the agent has been downloaded from another master server).
  - `Info: certificate created [IP]:`

    A certificate has been generated for the IP host.

- **Warning**
  - `Warning: Deleting old cgi.lock:`

    Lock file deletion has been forced. This occurs when the server is not shut down normally.

- **Error**
  - `Error: CGI is locked. Exiting process:`

    CGI has failed to access the lock file for 5 minutes. The certificate request is cancelled.
  - `Error: Invalid configuration file. Error: could not retrieve IP address:`

    The configuration file is invalid. The server failed to retrieve the IP address of the client host.
  - `Error: Wrong RECOVERY login/password:`

    The login and password set in the recovery certificate request form are not valid.
  - `Error: RECOVERY certificate creation failed [IP]:`

    An internal error occurred while using the recovery certificate request form.
  - `Error: could not retrieve request parameters [IP]:`

    The server failed to retrieve request parameters.
  - `Error: certificate creation failed [IP]:`

    An internal error occurred.

ANTIVIRUS PROTECTION LOGS

SERVER INSTALLATION AND UPDATE

Server installation and update logs are stored in the `software.sro` file (server side).

These logs contain the following information:

- **Error**
  - AV_SRV_INSTALL:
    - An error occurred when launching the installation of `sdktools`.
    - Impossible to record the `sdktools` version which has been installed in the registry base.
    - An error occurred when installing the signature repository.
    - Impossible to record the version of the signature repository which has been installed in the registry base.
    - Impossible to back up the original repository install.
  - AV_DOWNLOAD_SIGS:
    - An error occurred when downloading a new signature database from the Panda server.
  - OBTAIN_FILE:
    - File cannot be obtained because available disk space is insufficient
- **Information**
  - AV_SRV_INSTALL:
    - `sdktools` installation has started.
    - `sdktools` has been successfully installed.
    - The installation of the signature repository has started.
    - The signature repository has been successfully installed.
  - AV_SIG:
    - A new signature database is available on the server.

AGENT INSTALLATION AND UPDATE

Agent installation and update logs are stored under **Log Monitoring** in the Management and Monitoring Tools panel.

These logs contain the following information:

- **Error**
  - AV_INSTALL:
    - An error occurred when launching the installation of the antivirus administration component (`pavagent`).
    - `pavagent` installation has started even if `pavagent` has already been installed on the agent. Staff must have installed `pavagent` manually or deleted the key (indicating that `pavagent` had been previously installed) from the registry base.
    - The agent does not have the configuration required to retrieve the antivirus server address.
    - The agent fails to delete the existing file which should be replaced by the newly downloaded file.
    - Unable to download the file from the antivirus server.
    - Unable to move the downloaded file to its destination directory.
    - Unable to record the `pavagent` version which has been installed in the registry base.
    - Unable to install the antivirus protection (error code is specified).
    - Unable to record the antivirus protection which has been installed in the registry base.
  - AV_UPDATE:
    - Unable to update the file containing the trusts used for quarantine (`qutine.sif`).
    - Unable to record the `qutine.sif` version in the registry base.
  - AV_REPORT:
    - The report generated by the antivirus contains no action ID. No log can be generated.
    - Unable to allocate space to generate the source string.
    - Unable to allocate space to generate the destination string.
    - The antivirus encountered an error when generating the report. The "description" and "code" values are the values returned by the antivirus.

- AV_DEPLOY_SIG:
  - Unable to retrieve the version of the signature database currently used by the antivirus protection.
  - An error occurred when decompressing the file containing the complete signature database.
  - Unable to apply the signature file xxx.
  - Unable to retrieve the version of the signature database currently used by the antivirus protection after updating the signature database.
- AV_RESTORE:
  - An error occurred when restoring the %d. file.
- OBTAINFILE:
  - Unable to download the file because available disk space is insufficient.

- **Information**
  - AV_INSTALL:
    - The antivirus administration component (`pavagent`) has been successfully installed. The version is indicated at the end of the string.
    - `pavagent` installation has been launched.
    - The installation of the antivirus protection has been launched.
    - Reboot is required to terminate antivirus protection installation.
    - Antivirus protection has been successfully installed/updated to the version indicated.
    - Successful installation.
    - The signature database has been successfully applied.
  - AV_UPDATE:
    - The file containing the trusts used for quarantine (`qutine.sif`) has been successfully updated.
  - AV_DEPLOY_SIG:
    - A new signature database has been successfully deployed. The version is indicated.
  - AV_CONF:
    - The antivirus policy has been read.
  - AV_RESTORE:
    - The file has been restored in the %s location.

DETECTED VIRUS

Detected virus logs are stored under **Log Monitoring** in the Management and Monitoring Tools panel.

These logs contain the following information:

- **Date**.
- **Action**.
- **Status**:
  - ABORTED: The operation was aborted.
  - BLOCKED:The object has been blocked.
  - CLEANED: The object has been disinfected/neutralized.
  - ERASED:The object has been erased.
  - FILE_UNKNOWN:Action unknown.
  - IGNORED:The log has been generated but the antivirus has not modified the infected object.
  - MSG_ATT_DELETED:The attachment has been deleted.
  - MSG_ATT_MOVED_QUARANTINE:The attachment has been quarantined.
  - MSG_BLOCKED: The mail has been blocked.
  - MSG_ERASED: The mail has been destroyed.
  - MSG_IGNORED: The mail was ignored.
  - MSG_MARKED: The mail has been marked.
  - MSG_MARKED_MOVED: The mail has been marked to be moved.
  - MSG_MOVED: The mail has been moved.
  - MSG_MOVED_CUARENTINE: The mail has been quarantined.
  - MOVED: The object has been moved.
  - MOVED_QUARENTINE: The object has been quarantined.
  - OVERWRITTEN:The object has been overwritten.
  - RENAMED: The object has been renamed.
  - WEB_FILE_BLOCKED:The web file has been blocked.
  - WEB_FILE_MOVED_QUARANTINE:The web file has been quarantined.
  - WEB_IGNORED:The web file has been ignored.
- **Source**:

  This is the path of the infected object.
- **Destination**.
- **Option**:

  The virus identifier is stored in the antivirus database.
- **Username**:

  Information on the infected user.

- **RID**:

  Unique rule identifier.

- **Agent Mode**:
  - Normal.
  - Warning.
  - Standby.

All logs are recorded locally. When a virus is detected, associated logs are stored in the database.

SENDING LOGS CUSTOMIZED BY THE USER

The SSUSRLOG command-line tool allows the user to send customized logs to the StormShield console from the agent.

The tool allows directly writing the new log in the command-line interface or sending a set of logs from a CSV file. It is located in the StormShield agent directory (`ssusrlog.exe`).

The settings of these customized logs are defined in the Log Manager in the StormShield console (sending logs to a server or an external tool, pop-up windows, etc.). It is also possible to create new log status and use them with the SSUSRLOG tool. For more information, see section "Log Manager", page 620.

It is possible to create log messages for each language supported by StormShield.

To send one or few logs directly with the command-line interface, the user must use the syntax as follows:

- ssusrlog "log message" (default status: USER_LOG)
- ssusrlog LOG_STATUS "log message"

The SSUSRLOG tool automatically converts status to capital letters.

The user can add the following options:

- -e: ERROR action
- -w: WARNING action
- -i: INFO action

These values are displayed in the **Action** column in the **Log Monitoring** panel of the StormShield console. The default value is INFO.

To send a set of logs, the user can enter a CSV file as a parameter of the command line as follows:

ssusrlog -f csv_file_name

The CSV file must contain 3 columns and the separator character is a comma :

- column A: ERROR or WARN or INFO
- column B: the log status
- column C: the message

This is an example of lines of a CSV file:

WARN,USER_PASSW,The user Bob has just changed his password

ERROR,USER_PGM_EXIT,The prog.exe program has ended normally

INFO,USER_TEST,"The xx utility program has just been installed, the workstation needs to be restarted"

If the file has not been built by Microsoft Excel, you need to pay attention to how double quotes and commas are used.

The user can add the following option:

- -s: separator

If CSV files are built with international versions of Excel, the separator character may be another character than the comma. The user must declare it in the command line.

The following additional options are available for both modes:

- -verbose: displays additional information.
- -simul: displays additional information and analyzes the CSV file or the command line. Logs are not sent to StormShield. It may be useful to test tools and scripts building CSV files. This option automatically enables the "verbose" mode. In this case, the tool can be executed on a workstation without StormShield.

The following table gives examples of how to use the SSUSRLOG tool:

EXAMPLE	EXPLANATION
ssusrlog -w WIN_INFO "test number 1"	Log written in the command-line interface and sent to the console.
ssusrlog -f d:\test\ tmp.csv -s ;	Logs listed in the file `d:\test\tmp.csv` and sent to the console. The separator character is the semi-colon.
ssusrlog f d:\test\ tmp.csv -s ; -simul	Test of the log file `d:\test\tmp.csv`. The separator character is the semi-colon. Logs are not sent to StormShield.

Tableau 18.17 : Use of SSUSRLOG

SSUSRLOG return codes are:

- 0: everything is ok
- 1: empty command line, help is displayed
- 2: an error occurred

Chapter 19

TROUBLESHOOTING

ABOUT THIS CHAPTER

This chapter explains how to solve technical problems that may arise while using StormShield.

It includes the following:

- Certificates:
  - The console cannot communicate with the server.
  - The agent cannot download its certificate.
  - Unable to download certificates manually.

- Configurations:
  - Unable to apply the configuration.

- Miscellaneous:
  - Incorrect installation of the StormShield agent.
  - Agent fails to be remotely deployed.
  - Hardware conflicts.
  - Degraded performance.

For more information, log onto `https://extranet.skyrecon.com`.

CERTIFICATES

THE CONSOLE CANNOT COMMUNICATE WITH THE SERVER

If the problem is related to the certificates used to encrypt communications between the server and the console, a specific message is displayed on the SkyRecon management console (**Messages** area under **Log Manager**).

In this case, follow the steps below while respecting the order indicated:

1. Check that the certificates are located in an environment where they can be accessed by both the console and the server.

   If certificates are accessible, the problem is probably due to the certificate itself (example: the certificate has expired).

   The console will indicate the most likely reason for this in the **Message** column.

2. If there is no certificate problem, check the connectivity between the console and the server:
   - Use ping from the console to test access to the server IP address.
   - If the ping is successful, use telnet on the server address through port 16007 to test the opening of the port used for communication between the console and the server.

3. If connectivity is available, the StormShield server is effectively running on the server host machine.

   If connectivity is not available, restart the server.

4. If the problem is solved, send the configuration again.

   The console will display a message verifying that the configuration was sent and that the server received it.

THE AGENT CANNOT DOWNLOAD ITS CERTIFICATE

After installation, the agent has to download an X509 certificate to communicate securely with the server.

1. If the agent fails to download its certificate, a message is logged on the workstation.

   This message can be consulted by right-clicking the StormShield Monitor icon  displayed in the system tray and by selecting **View event logs**.

   The most common reasons for such a failure are the following:

   - The **Checking server source** option under Authentication Service is enabled on the SkyRecon management console and the agent has been downloaded from another StormShield server instance.

     Two solutions can be envisaged:

     - Reinstall an agent generated by the appropriate server.
     - Disable the **Checking server source** option in the master server configuration under Authentication service.

   - The certificate deployment period has expired.

     The period must be renewed. You can modify it on the SkyRecon management console under **Authentication Service**.

2. If the configuration is correct and the agent still cannot download its certificate:

   - Check the communication by sending a ping to the StormShield server IP address from the workstation.
   - Stop the StormShield server.
   - Run `telnet` on port 443.

     The connection should fail.

3. If the connection is established, this means that another Web server is present on the server host. Stop this server, and start the StormShield server again.

When the problem is solved, check that the agent actually downloads its certificate.

UNABLE TO DOWNLOAD CERTIFICATES MANUALLY

If you cannot access the certificate downloading page, make sure that another Web server is not already running the server host.

If manual download fails, one of the following error messages is displayed:

- `Wrong login or password`:

  The login and/or password that have been entered do not match with those defined on the SkyRecon management console.

- `The server is unable to respond to your request (server is locked)`:

  The server is locked. Try again later.

- `An internal error occurred. Please contact your administrator`:

  Server logs should be analyzed in order to diagnose the origin of the problem.

CONFIGURATIONS

UNABLE TO APPLY THE CONFIGURATION

The simplest way to check that a security configuration has been properly applied to a client workstation is to attempt an operation explicitly banned by a rule defined on the SkyRecon management console.

A good example is the rule that bans the use of Windows notepad (`notepad.exe`) to open a file with a `.txt` extension.

1. If the blocking rule works, the application will not be allowed to access the file.
2. If the blocking rule is not applied, check the following:
   - The configuration has been assigned to the target machine by the SkyRecon management console.
   - The StormShield agent is running on the client workstation. To do so, verify the StormShield Agent service status.

     If the service is not found in the list of Windows services, there has probably been a problem with agent installation.

     Correct installation is shown in the following file:

     `[Program Files]\SkyRecon\StormShieldAgent\srservice.log`
3. After verifying that the security configuration has been applied to the client workstation, check that the data collected by the agent:
   - Has effectively been sent to the server.
   - Has effectively been stored in the database.
   - Is accessible to the console.

   This data must be visible in the **Log Manager** on the console.
4. If no data is displayed on the console, check database connection.

   If the console cannot connect to the database, a message indicates this on opening the console.
5. When no connection to the database is available, you should check:
   - The database server accessibility by sending a ping to the machine that hosts the database.
   - The database engine is started (via the services or system tray icon).
6. If the database engine is running and the host machine is accessible, check the connection data that is specific to the StormShield database. To do so, verify the password in the **Database password** field and the IP address in the **SQL server instance** field in the Environment Manager.

7. If the connection to the database is active, verify that event feedback is properly configured on the console under **Console Configuration**.

   When the connection to the database is active, you can generate a log to check that the configuration has been correctly applied to the client workstation:

   - Trigger rule application on the client workstation once again.
   - Check data feedback.
   - Check the frequency of configuration updates which is also the frequency of event feedback.

Avoid updating too frequently as this may cause network saturation.

MISCELLANEOUS

INCORRECT INSTALLATION OF THE STORMSHIELD AGENT

You must use the **Administrator** account to install the StormShield agent.

If you use another account:

- The installation starts but not all of the files are copied.
- The service is not registered.
- Nothing works (including the uninstaller).

To fix the problem, you must manually remove all of the StormShield files and registry keys.

Before installing the agent, make sure that the Windows XP embedded firewall has been disabled.

AGENT FAILS TO BE REMOTELY DEPLOYED

When the **srdeployment** assistant fails to deploy the agent, the error message "`Host unreachable`" is displayed on the console.

In this case, follow the steps below while respecting the order indicated:

1. Send a `ping` command to the host IP address.
2. Check that the host `netbios C$ share` is accessible.
3. Check that **Use simple file sharing (Recommended)** is disabled.
4. Check that port `445` can be accessed by sending a `telnet` command.
5. Check that there is no connection to the host which is already open.
6. Repeat the agent deployment procedure.

HARDWARE CONFLICTS

Conflicts between drivers may sometimes cause a system crash called **BSoD** (Blue Screen of Death).
To determine the cause of the conflict, it is recommended to enable a Windows service that keeps a trace of system activity at the time of the crash.

This service is accessible from the **System Properties** panel on your workstation:

1. Click the **Advanced** tab.
2. Click **Settings** in the Startup and Recovery group.

3. From the Write debugging information group, select **Complete memory dump**.
4. Keep the default directory `%SystemRoot%\MEMORY.DMP`

   `%SystemRoot%"` usually corresponds to `c:\windows\` in Windows XP.

DEGRADED PERFORMANCE

StormShield operation has no significant impact on client workstation performance.

However, an application may repeatedly attempt to perform an operation that is blocked by StormShield. This in turn may cause CPU overload.

If workstation performance drops, it is first of all necessary to check the affected process by opening the Windows **Task Manager**.

If the affected process is indeed blocked by StormShield, a trace of the blockage will be recorded in one of the agent log files. Checking the logs will show whether the cause of the problem was indeed triggered by a StormShield-imposed blockage.

Appendix A

PROTOCOLS

ABOUT THIS APPENDIX

This appendix includes the protocol correspondence table.

PROTOCOL CORRESPONDENCE TABLE

Here is the protocol correspondence table:

CODE	MEANING
[0x0004]	"0004/IEEE 802.3 packet"
[0x0101]	"0101-1FF/Experimental"
[0x0200]	"0200/Xerox PUP protocol - see 0A00"
[0x0200]	"0200/PUP Address Translation - see 0A01"
[0x0500]	"0500/???"
[0x0400]	"0400/Nixdorf"
[0x0600]	"0600/XNS"
[0x0601]	"0601/XNS Address Translation (3Mb only)"
[0x0660]	"0660/DLOG (?)"
[0x0661]	"0661/DLOG (?)"
[0x0800]	"0800/IP protocol"
[0x0801]	"0801/X.75 Internet"
[0x0802]	"0802/NBS Internet"
[0x0803]	"0803/ECMA Internet"
[0x0804]	"0804/CHAOSnet"
[0x0805]	"0805/X.25 Level 3"
[0x0806]	"0806/Address resolution protocol"
[0x0807]	"0807/XNS Compatibility"
[0x0808]	"0808/Frame Relay ARP (RFC1701)"
[0x081C]	"081C/Symbolics Private"
[0x0888]	"0888-088A/Xyplex"
[0x0900]	"0900/Ungermann-Bass network debugger"
[0x0A00]	"0A00/Xerox IEEE802.3 PUP"
[0x0A01]	"0A01/Xerox IEEE802.3 PUP Address Translation"
[0x0BAD]	"0BAD/Banyan VINES"
[0x0BAE]	"0BAE/Banyan VINES Loopback"
[0x0BAF]	"0BAF/Banyan VINES Echo"
[0x1000]	"1000/Trailer packet"

Table A.1: Procotol correspondence table (Sheet 1 of 13)

CODE	MEANING
[0x1234]	"1234/DCA - Multicast"
[0x1600]	"1600/VALID system protocol"
[0x1989]	"1989/Artificial Horizons (\"Aviator\" dogfight simulator [on Sun])"
[0x1995]	"1995/Datapoint Corporation (RCL lan protocol)"
[0x3C00]	"3C00/3Com NBP virtual circuit datagram (like XNS SPP) not registered"
[0x3C01]	"3C01/3Com NBP System control datagram not registered"
[0x3C02]	"3C02/3Com NBP Connect request (virtual cct) not registered"
[0x3C03]	"3C03/3Com NBP Connect response not registered"
[0x3C04]	"3C04/3Com NBP Connect complete not registered"
[0x3C05]	"3C05/3Com NBP Close request (virtual cct) not registered"
[0x3C06]	"3C06/3Com NBP Close response not registered"
[0x3C07]	"3C07/3Com NBP Datagram (like XNS IDP) not registered"
[0x3C08]	"3C08/3Com NBP Datagram broadcast not registered"
[0x3C09]	"3C09/3Com NBP Claim NetBIOS name not registered"
[0x3C0A]	"3C0A/3Com NBP Delete Netbios name not registered"
[0x3C0B]	"3C0B/3Com NBP Remote adaptor status request not registered"
[0x3C0C]	"3C0C/3Com NBP Remote adaptor response not registered"
[0x3C0D]	"3C0D/3Com NBP Reset not registered"
[0x4242]	"4242/PCS Basic Block Protocol"
[0x424C]	"424C/Information Modes Little Big LAN diagnostic"
[0x4321]	"4321/THD - Diddle"
[0x4C42]	"4C42/Information Modes Little Big LAN"
[0x5208]	"5208/BBN Simnet Private"
[0x6000]	"6000/DEC Unassigned, experimental"
[0x6001]	"6001/DEC MOP dump/load"
[0x6002]	"6002/DEC MOP remote console"
[0x6003]	"6003/DEC DECNET Phase IV route"
[0x6004]	"6004/DEC LAT"
[0x6005]	"6005/DEC diagnostic protocol (at interface initialization?)"

Table A.1: Procotol correspondence table (Sheet 2 of 13)

CODE	MEANING
[0x6006]	"6006/DEC customer protocol"
[0x6007]	"6007/DEC LAVC, SCA"
[0x6008]	"6008/DEC AMBER"
[0x6009]	"6009/DEC MUMPS"
[0x6010]	"6010-6014/3Com Corporation"
[0x6558]	"6558/Trans Ether Bridging (RFC1701)"
[0x6559]	"6559/Raw Frame Relay (RFC1701)"
[0x7000]	"7000/Ungermann-Bass download"
[0x7001]	"7001/Ungermann-Bass NIUs"
[0x7002]	"7002/Ungermann-Bass diagnostic/loopback"
[0x7003]	"7003/Ungermann-Bass ??? (NMC to/from UB Bridge)"
[0x7005]	"7005/Ungermann-Bass Bridge Spanning Tree"
[0x7007]	"7007/OS/9 Microware"
[0x7009]	"7009/OS/9 Net?"
[0x7020]	"7020-7029/LRT (England) (now Sintrom)"
[0x7030]	"7030/Racal-Interlan"
[0x7031]	"7031/Prime NTS (Network Terminal Service)"
[0x7034]	"7034/Cabletron"
[0x8003]	"8003/Cronus VLN"
[0x8004]	"8004/Cronus Direct"
[0x8005]	"8005/HP Probe"
[0x8006]	"8006/Nestar"
[0x8008]	"8008/AT&T/Stanford (local use)"
[0x8010]	"8010/Excelan"
[0x8013]	"8013/SGI diagnostic type"
[0x8014]	"8014/SGI network games"
[0x8015]	"8015/SGI reserved type"
[0x8016]	"8016/SGI bounce server"
[0x8019]	"8019/Apollo DOMAIN"
[0x802E]	"802E/Tymeshare"
[0x802F]	"802F/Tigan, Inc."

Table A.1: Procotol correspondence table (Sheet 3 of 13)

CODE	MEANING
[0x8035]	"8035/Reverse addr resolution protocol"
[0x8036]	"8036/Aeonic Systems"
[0x8037]	"8037/IPX (Novell Netware?)"
[0x8038]	"8038/DEC LANBridge"
[0x8039]	"8039/DEC DSM/DDP"
[0x803A]	"803A/DEC Argonaut Console"
[0x803B]	"803B/DEC VAXELN"
[0x803C]	"803C/DEC DNS Naming Service"
[0x803D]	"803D/DEC Ethernet Encryption"
[0x803E]	"803E/DEC Distributed Time Service"
[0x803F]	"803F/DEC LAN Traffic Monitor"
[0x8040]	"8040/DEC PATHWORKS DECnet NETBIOS Emulation"
[0x8041]	"8041/DEC Local Area System Transport"
[0x8042]	"8042/DEC Unassigned"
[0x8044]	"8044/Planning Research Corp."
[0x8046]	"8046-8047/AT&T"
[0x8048]	"8048/DEC Availability Manager for Distributed Systems DECamds (but someone at DEC says not)"
[0x8049]	"8049/ExperData"
[0x805B]	"805B/Stanford V Kernel exp."
[0x805C]	"805C/Stanford V Kernel prod."
[0x805D]	"805D/Evans & Sutherland"
[0x8060]	"8060/Little Machines"
[0x8062]	"8062/Counterpoint Computers"
[0x8065]	"8065-8066/Univ. of Mass @ Amherst"
[0x8067]	"8067/Veeco Integrated Auto."
[0x8068]	"8068/General Dynamics"
[0x8069]	"8069/AT&T"
[0x806A]	"806A/Autophon"
[0x806C]	"806C/ComDesign"
[0x806D]	"806D/Compugraphic Corporation"
[0x806E]	"806E-8077/Landmark Graphics Corp."

Table A.1: Procotol correspondence table (Sheet 4 of 13)

CODE	MEANING
[0x807A]	"807A/Matra"
[0x807B]	"807B/Dansk Data Elektronik"
[0x807C]	"807C/Merit Internodal (or Univ of Michigan?)"
[0x807D]	"807D-807F/Vitalink Communications"
[0x8080]	"8080/Vitalink TransLAN III Management"
[0x8081]	"8081-8083/Counterpoint Computers"
[0x8088]	"8088-808A/Xyplex"
[0x809B]	"809B/AppleTalk"
[0x809C]	"809C-809E/Datability"
[0x809F]	"809F/Spider Systems Ltd."
[0x80A3]	"80A3/Nixdorf"
[0x80A4]	"80A4-80B3/Siemens Gammasonics Inc."
[0x80C0]	"80C0-80C3/DCA (Digital Comm. Assoc.) Data Exchange Cluster"
[0x80C4]	"80C4-80C5/Banyan Systems"
[0x80C6]	"80C6/Pacer Software"
[0x80C7]	"80C7/Applitek Corporation"
[0x80C8]	"80C8-80CC/Intergraph Corporation"
[0x80CD]	"80CD-80CE/Harris Corporation"
[0x80CF]	"80CF-80D2/Taylor Instrument"
[0x80D3]	"80D3-80D4/Rosemount Corporation"
[0x80D5]	"80D5/IBM SNA Services over Ethernet"
[0x80DD]	"80DD/Varian Associates"
[0x80DE]	"80DE-80DF/TRFS (Integrated Solutions Transparent Remote File System)"
[0x80E0]	"80E0-80E3/Allen-Bradley"
[0x80E4]	"80E4-80F0/Datability"
[0x80F2]	"80F2/Retix"
[0x80F3]	"80F3/AppleTalk AARP"
[0x80F4]	"80F4-80F5/Kinetics"
[0x80F7]	"80F7/Apollo Computer"
[0x8100]	"8100/IEEE 802.1Q VLAN tagging (XXX conflicts)"

Table A.1: Procotol correspondence table (Sheet 5 of 13)

CODE	MEANING
[0x80FF]	"80FF-8101/Wellfleet Communications (XXX conflicts)"
[0x8102]	"8102/Wellfleet BOFL (Breath OF Life) pkts [every 5-10 secs.]"
[0x8103]	"8103/Wellfleet Communications"
[0x8107]	"8107-8109/Symbolics Private"
[0x812B]	"812B/Talaris"
[0x8130]	"8130/Waterloo Microsystems Inc. (XXX which?)"
[0x8130]	"8130/Hayes Microcomputers (XXX which?)"
[0x8131]	"8131/VG Laboratory Systems"
[0x8132]	"8132-8137/Bridge Communications"
[0x8137]	"8137/Novell (old) NetWare IPX (ECONFIG E option)"
[0x8138]	"8138/Novell, Inc."
[0x8139]	"8139-813D/KTI"
[0x813F]	"813F/M/MUMPS data sharing"
[0x8145]	"8145/Vrije Universiteit (NL) Amoeba 4 RPC (obsolete)"
[0x8146]	"8146/Vrije Universiteit (NL) FLIP (Fast Local Internet Protocol)"
[0x8147]	"8147/Vrije Universiteit (NL) [reserved]"
[0x8148]	"8148/Logicraft"
[0x8149]	"8149/Network Computing Devices"
[0x814A]	"814A/Alpha Micro"
[0x814C]	"814C/SNMP over Ethernet (see RFC1089)"
[0x814D]	"814D-814E/BIIN"
[0x814F]	"814F/Technically Elite Concepts"
[0x8150]	"8150/Rational Corp"
[0x8151]	"8151-8153/Qualcomm"
[0x815C]	"815C-815E/Computer Protocol Pty Ltd"
[0x8164]	"8164-8166/Charles River Data Systems"
[0x817D]	"817D/Protocol Engines XTP"
[0x817E]	"817E/SGI/Time Warner prop."
[0x8180]	"8180/HIPPI-FP encapsulation"
[0x8181]	"8181/Scheduled Transfer STP, HIPPI-ST"

Table A.1: Procotol correspondence table (Sheet 6 of 13)

CODE	MEANING
[0x8182]	"8182-8183/Reserved for HIPPI-6400"
[0x8184]	"8184-818C/SGI prop."
[0x818D]	"818D/Motorola"
[0x8191]	"8191/PowerLAN NetBIOS/NetBEUI (PC)"
[0x819A]	"819A-81A3/RAD Network Devices"
[0x81B7]	"81B7-81B9/Xyplex"
[0x81CC]	"81CC-81D5/Apricot Computers"
[0x81D6]	"81D6-81DD/Artisoft Lantastic"
[0x81E6]	"81E6-81EF/Polygon"
[0x81F0]	"81F0-81F2/Comsat Labs"
[0x81F3]	"81F3-81F5/SAIC"
[0x81F6]	"81F6-81F8/VG Analytical"
[0x8203]	"8203-8205/QNX Software Systems Ltd."
[0x8221]	"8221-8222/Ascom Banking Systems"
[0x823E]	"823E-8240/Advanced Encryption Systems"
[0x8263]	"8263-826A/Charles River Data Systems"
[0x827F]	"827F-8282/Athena Programming"
[0x829A]	"829A-829B/Inst Ind Info Tech"
[0x829C]	"829C-82AB/Taurus Controls"
[0x82AC]	"82AC-8693/Walker Richer & Quinn"
[0x8390]	"8390/Accton Technologies (unregistered)"
[0x852B]	"852B/Talaris multicast"
[0x8582]	"8582/Kalpana"
[0x8694]	"8694-869D/Idea Courier"
[0x869E]	"869E-86A1/Computer Network Tech"
[0x86A3]	"86A3-86AC/Gateway Communications"
[0x86DB]	"86DB/SECTRA"
[0x86DD]	"86DD/IP protocol version 6"
[0x86DE]	"86DE/Delta Controls"
[0x86DF]	"86DF/ATOMIC"
[0x86E0]	"86E0-86EF/Landis & Gyr Powers"

Table A.1: Procotol correspondence table (Sheet 7 of 13)

CODE	MEANING
[0x8700]	"8700-8710/Motorola"
[0x8739]	"8739/Control Technology Inc. RDP Without IP"
[0x873A]	"873A/Control Technology Inc. Mcast Industrial Ctrl Proto."
[0x873B]	"873B-873C/Control Technology Inc. Proprietary"
[0x876B]	"876B/TCP/IP Compression (RFC1701)"
[0x876C]	"876C/IP Autonomous Systems (RFC1701)"
[0x876D]	"876D/Secure Data (RFC1701)"
[0x8808]	"8808/802.3x flow control packet"
[0x880B]	"880B/PPP (obsolete by PPPOE)"
[0x8820]	"8820/Hitachi Cable (Optoelectronic Systems Laboratory)"
[0x8847]	"8847/MPLS Unicast"
[0x8848]	"8848/MPLS Multicast"
[0x8856]	"8856/Axis Communications AB proprietary bootstrap/ config"
[0x8863]	"8863/PPP Over Ethernet Discovery Stage"
[0x8864]	"8864/PPP Over Ethernet Session Stage"
[0x8888]	"8888/HP LanProbe test?"
[0x9000]	"9000/Loopback: used to test interfaces"
[0x9001]	"9001/3Com (Formerly Bridge Communications), XNS Systems Management"
[0x9002]	"9002/3Com (Formerly Bridge Communications), TCP/IP Systems Management"
[0x9003]	"9003/3Com (Formerly Bridge Communications), loopback detection"
[0xAAAA]	"AAAA/DECNET? Used by VAX 6220 DEBNI"
[0xFAF5]	"FAF5/Sonix Arpeggio"
[0xFF00]	"FF00/BBN VITAL-LanBridge cache wakeups"
[0x0]	"HOPOPT/IPv6 Hop-by-Hop Option"
[0x1]	"ICMP/Internet Control Message"
[0x2]	"IGMP/Internet Group Management"
[0x3]	"GGP/Gateway-to-Gateway"
[0x4]	"IP/IP in IP encapsulation"
[0x5]	"ST/Stream"

Table A.1: Procotol correspondence table (Sheet 8 of 13)

CODE	MEANING
[0x6]	"TCP/Transmission Control"
[0x7]	"CBT/CBT"
[0x8]	"EGP/Exterior Gateway Protocol"
[0x9]	"IGP/any private interior gateway"
[0xa]	"BBN-RCC-MON/BBN RCC Monitoring"
[0xb]	"NVP-II/Network Voice Protocol"
[0xc]	"PUP/PUP"
[0xd]	"ARGUS/ARGUS"
[0xe]	"EMCON/EMCON"
[0xf]	"XNET/Cross Net Debugger"
[0x10]	"CHAOS/Chaos"
[0x11]	"UDP/User Datagram"
[0x12]	"MUX/Multiplexing"
[0x13]	"DCN-MEAS/DCN Measurement Subsystems"
[0x14]	"HMP/Host Monitoring"
[0x15]	"PRM/Packet Radio Measurement"
[0x16]	"XNS-IDP/XEROX NS IDP"
[0x17]	"TRUNK-1/Trunk-1"
[0x18]	"TRUNK-2/Trunk-2"
[0x19]	"LEAF-1/Leaf-1"
[0x1a]	"LEAF-2/Leaf-2"
[0x1b]	"RDP/Reliable Data Protocol"
[0x1c]	"IRTP/Internet Reliable Transaction"
[0x1d]	"ISO-TP4/ISO Transport Protocol Class 4"
[0x1e]	"NETBLT/Bulk Data Transfer Protocol"
[0x1f]	"MFE-NSP/MFE Network Services Protocol"
[0x20]	"MERIT-INP/MERIT Internodal Protocol"
[0x21]	"SEP/Sequential Exchange Protocol"
[0x22]	"3PC/Third Party Connect Protocol"
[0x23]	"IDPR/Inter-Domain Policy Routing Protocol"
[0x24]	"XTP/XTP"

Table A.1: Procotol correspondence table (Sheet 9 of 13)

CODE	MEANING
[0x25]	"DDP/Datagram Delivery Protocol"
[0x26]	"IDPR-CMTP/IDPR Control Message Transport Proto"
[0x27]	"TP++/TP++ Transport Protocol"
[0x28]	"IL/IL Transport Protocol"
[0x29]	"IPv6/"
[0x2a]	"SDRP/Source Demand Routing Protocol"
[0x2b]	"IPv6-Route/Routing Header for IPv6"
[0x2c]	"IPv6-Frag/Fragment Header for IPv6"
[0x2d]	"IDRP/Inter-Domain Routing Protocol"
[0x2e]	"RSVP/Reservation Protocol"
[0x2f]	"GRE/General Routing Encapsulation"
[0x30]	"MHRP/Mobile Host Routing Protocol"
[0x31]	"BNA/"
[0x32]	"ESP/Encap Security Payload"
[0x33]	"AH/Authentication Header"
[0x34]	"I-NLSP/Integrated Net Layer Security TUBA"
[0x35]	"SWIPE/IP with Encryption"
[0x36]	"NARP/NBMA Address Resolution Protocol"
[0x37]	"MOBILE/IP Mobility"
[0x38]	"TLSP/Transport Layer Security Protocol using Kryptonet key management"
[0x39]	"SKIP/SKIP"
[0x3a]	"IPv6-ICMP/ICMP for IPv6"
[0x3b]	"IPv6-NoNxt/No Next Header for IPv6"
[0x3c]	"IPv6-Opts/Destination Options for IPv6"
[0x3d]	"any host internal protocol"
[0x3e]	"CFTP/CFTP"
[0x3f]	"any local network"
[0x40]	"SAT-EXPAK/SATNET and Backroom EXPAK"
[0x41]	"KRYPTOLAN/"
[0x42]	"RVD/MIT Remote Virtual Disk Protocol"
[0x43]	"IPPC/Internet Pluribus Packet Core"

Table A.1: Procotol correspondence table (Sheet 10 of 13)

CODE	MEANING
[0x44]	"any distributed file system"
[0x45]	"SAT-MON/SATNET Monitoring"
[0x46]	"VISA/VISA Protocol"
[0x47]	"IPCV/Internet Packet Core Utility"
[0x48]	"CPNX/Computer Protocol Network Executive"
[0x49]	"CPHB/Computer Protocol Heart Beat"
[0x4a]	"WSN/Wang Span Network"
[0x4b]	"PVP/Packet Video Protocol"
[0x4c]	"BR-SAT-MON/Backroom SATNET Monitoring"
[0x4d]	"SUN-ND/SUN ND PROTOCOL-Temporary"
[0x4e]	"WB-MON/WIDEBAND Monitoring"
[0x4f]	"WB-EXPAK/WIDEBAND EXPAK"
[0x50]	"ISO-IP/ISO Internet Protocol"
[0x51]	"VMTP"
[0x52]	"SECURE-VMTP/SECURE-VMTP"
[0x53]	"VINES"
[0x54]	"TTP"
[0x55]	"NSFNET-IGP/NSFNET-IGP"
[0x56]	"DGP/Dissimilar Gateway Protocol"
[0x57]	"TCF"
[0x58]	"EIGRP"
[0x59]	"OSPFIGP"
[0x5a]	"Sprite-RPC/Sprite RPC Protocol"
[0x5b]	"LARP/Locus Address Resolution Protocol"
[0x5c]	"MTP/Multicast Transport Protocol"
[0x5d]	"AX.25/AX.25 Frames"
[0x5e]	"IPIP/IP-within-IP Encapsulation Protocol"
[0x5f]	"MICP/Mobile Internetworking Control Pro."
[0x60]	"SCC-SP/Semaphore Communications Sec. Pro."
[0x61]	"ETHERIP/Ethernet-within-IP Encapsulation"
[0x62]	"ENCAP/Encapsulation Header"

Table A.1: Procotol correspondence table (Sheet 11 of 13)

CODE	MEANING
[0x63]	"any private encryption scheme"
[0x64]	"GMTP"
[0x65]	"IFMP/Ipsilon Flow Management Protocol"
[0x66]	"PNNI/PNNI over IP"
[0x67]	"PIM/Protocol Independent Multicast"
[0x68]	"ARIS"
[0x69]	"SCPS"
[0x6a]	"QNX"
[0x6b]	"A/N/Active Networks"
[0x6c]	"IPComp/IP Payload Compression Protocol"
[0x6d]	"SNP/Sitara Networks Protocol"
[0x6e]	"Compaq-Peer/Compaq Peer Protocol"
[0x6f]	"IPX-in-IP"
[0x70]	"VRRP/Virtual Router Redundancy Protocol"
[0x71]	"PGM/PGM Reliable Transport Protocol"
[0x72]	"any 0-hop protocol"
[0x73]	"L2TP/Layer Two Tunneling Protocol"
[0x74]	"DDX/D-II Data Exchange DDX"
[0x75]	"IATP/Interactive Agent Transfer Protocol"
[0x76]	"STP/Schedule Transfer Protocol"
[0x77]	"SRP/SpectraLink Radio Protocol"
[0x78]	"UTI"
[0x79]	"SMP/Simple Message Protocol"
[0x7a]	"SM"
[0x7b]	"PTP/Performance Transparency Protocol"
[0x7c]	"ISIS over IPv4"
[0x7d]	"FIRE"
[0x7e]	"CRTP/Combat Radio Transport Protocol"
[0x7f]	"CRUDP/Combat Radio User Datagram"
[0x80]	"SSCOPMCE"
[0x81]	"IPLT"

Table A.1: Procotol correspondence table (Sheet 12 of 13)

CODE	MEANING
[0x82]	"SPS/Secure Packet Shield"
[0x83]	"PIPE/Private IP Encapsulation within IP"
[0x84]	"SCTP/Stream Control Transmission Protocol"
[0x85]	"FC/Fibre Channel"
[0x86]	"RSVP-E2E-IGNORE"
[0x87]	"Mobility Header"
[0x88]	"UDPLite"

Table A.1: Procotol correspondence table (Sheet 13 of 13)

Appendix B

FILES EXEMPTED FROM ENCRYPTION

ABOUT THIS APPENDIX

This appendix includes the list of the files exempted from encryption.

FILE LIST

Some files that are automatically initialized upon computer start-up will never be encrypted, namely Windows system files and StormShield files.

Here is the list of files that will never be encrypted:

FILES EXEMPTED FROM ENCRYPTION
*.386
*.a
*.bat
*.cab
*.com
*.cpl
*.cur
*.dat
*.desklink
*.dev
*.dll
*.drv
*.exe
*.ico
*.job
*.jod
*.la
*.lib
*.lnk
*.log
*.o
*.ocx
*.p12
*.pdb
*.pfx
*.reg

Table B.1: List of files exempted from encryption (Sheet 1 of 3)

FILES EXEMPTED FROM ENCRYPTION
*.scf
*.sra
*.srk
*.srn
*.sro
*.srx
*.sys
*\boot.ini
*\bootfont.bin
*\bootmgr
*\bootsect.dos
*\desktop.htt
*\desktop.ini
*\ntldr
*\ntuser.ini
*\ntuser.pol
System Volume Information
temporary internet files
|programfiles|*
|systemdrive|\Boot*
|systemdrive|\BOOTSECT.BAK
|systemdrive|\Documents and Settings\All Users*
|systemdrive|\Documents and Settings\Default User*
|systemdrive|\Documents and Settings\LocalService*
|systemdrive|\Documents and Settings\NetworkService*
|systemdrive|\progra~1*
|systemdrive|\programdata*
|systemroot|*
|userprofile|\application data\microsoft\crypto*
|userprofile|\application data\microsoft\protect*
|userprofile|\application data\microsoft\systemcertificates*

Table B.1: List of files exempted from encryption (Sheet 2 of 3)

FILES EXEMPTED FROM ENCRYPTION
|userprofile|\appdata\roaming\microsoft\crypto*
|userprofile|\appdata\roaming\microsoft\protect*
|userprofile|\appdata\roaming\microsoft\systemcertificates*
|users|\default*
|users||username|\ntuser.dat*

Table B.1: List of files exempted from encryption (Sheet 3 of 3)

Appendix C

FILE ENCRYPTION ERROR CODES

ABOUT THIS APPENDIX

This appendix includes the list of the error codes related to file encryption.

ERROR CODE LIST

Here is the list of the error codes related to file encryption:

CODE	MEANING
00000000	STATUS_SUCCESS
00000000	STATUS_WAIT_0
00000001	STATUS_WAIT_1
00000002	STATUS_WAIT_2
00000003	STATUS_WAIT_3
0000003F	STATUS_WAIT_63
00000080	STATUS_ABANDONED
00000080	STATUS_ABANDONED_WAIT_0
000000BF	STATUS_ABANDONED_WAIT_63
000000C0	STATUS_USER_APC
00000100	STATUS_KERNEL_APC
00000101	STATUS_ALERTED
00000102	STATUS_TIMEOUT
00000103	STATUS_PENDING
00000104	STATUS_REPARSE
00000105	STATUS_MORE_ENTRIES
00000106	STATUS_NOT_ALL_ASSIGNED
00000107	STATUS_SOME_NOT_MAPPED
00000108	STATUS_OPLOCK_BREAK_IN_PROGRESS
00000109	STATUS_VOLUME_MOUNTED
0000010A	STATUS_RXACT_COMMITTED
0000010B	STATUS_NOTIFY_CLEANUP
0000010C	STATUS_NOTIFY_ENUM_DIR
0000010D	STATUS_NO_QUOTAS_FOR_ACCOUNT
0000010E	STATUS_MASTER_TRANSPORT_CONNECT_FAILED
00000110	STATUS_PAGE_FAULT_TRANSITION
00000111	STATUS_PAGE_FAULT_DEMAND_ZERO
00000112	STATUS_PAGE_FAULT_COPY_ON_WRITE

Table C.1: Error codes related to file encryption (Sheet 1 of 36)

CODE	MEANING
00000113	STATUS_PAGE_FAULT_GUARD_PAGE
00000114	STATUS_PAGE_FAULT_PAGING_FILE
00000115	STATUS_CACHE_PAGE_LOCKED
00000116	STATUS_CRASH_DUMP
00000117	STATUS_BUFFER_ALL_ZEROS
00000118	STATUS_REPARSE_OBJECT
00000119	STATUS_RESOURCE_REQUIREMENTS_CHANGED
00000120	STATUS_TRANSLATION_COMPLETE
00000121	STATUS_DS_MEMBERSHIP_EVALUATED_LOCALLY
00000122	STATUS_NOTHING_TO_TERMINATE
00000123	STATUS_PROCESS_NOT_IN_JOB
00000124	STATUS_PROCESS_IN_JOB
00000125	STATUS_VOLSNAP_HIBERNATE_READY
00000126	STATUS_FSFILTER_OP_COMPLETED_SUCCESSFULLY
00010001	DBG_EXCEPTION_HANDLED
00010002	DBG_CONTINUE
40000000	STATUS_OBJECT_NAME_EXISTS
40000001	STATUS_THREAD_WAS_SUSPENDED
40000002	STATUS_WORKING_SET_LIMIT_RANGE
40000003	STATUS_IMAGE_NOT_AT_BASE
40000004	STATUS_RXACT_STATE_CREATED
40000005	STATUS_SEGMENT_NOTIFICATION
40000006	STATUS_LOCAL_USER_SESSION_KEY
40000007	STATUS_BAD_CURRENT_DIRECTORY
40000008	STATUS_SERIAL_MORE_WRITES
40000009	STATUS_REGISTRY_RECOVERED
4000000A	STATUS_FT_READ_RECOVERY_FROM_BACKUP
4000000B	STATUS_FT_WRITE_RECOVERY
4000000C	STATUS_SERIAL_COUNTER_TIMEOUT
4000000D	STATUS_NULL_LM_PASSWORD
4000000E	STATUS_IMAGE_MACHINE_TYPE_MISMATCH

Table C.1: Error codes related to file encryption (Sheet 2 of 36)

CODE	MEANING
4000000F	STATUS_RECEIVE_PARTIAL
40000010	STATUS_RECEIVE_EXPEDITED
40000011	STATUS_RECEIVE_PARTIAL_EXPEDITED
40000012	STATUS_EVENT_DONE
40000013	STATUS_EVENT_PENDING
40000014	STATUS_CHECKING_FILE_SYSTEM
40000015	STATUS_FATAL_APP_EXIT
40000016	STATUS_PREDEFINED_HANDLE
40000017	STATUS_WAS_UNLOCKED
40000018	STATUS_SERVICE_NOTIFICATION
40000019	STATUS_WAS_LOCKED
4000001A	STATUS_LOG_HARD_ERROR
4000001B	STATUS_ALREADY_WIN32
4000001C	STATUS_WX86_UNSIMULATE
4000001D	STATUS_WX86_CONTINUE
4000001E	STATUS_WX86_SINGLE_STEP
4000001F	STATUS_WX86_BREAKPOINT
40000020	STATUS_WX86_EXCEPTION_CONTINUE
40000021	STATUS_WX86_EXCEPTION_LASTCHANCE
40000022	STATUS_WX86_EXCEPTION_CHAIN
40000023	STATUS_IMAGE_MACHINE_TYPE_MISMATCH_EXE
40000024	STATUS_NO_YIELD_PERFORMED
40000025	STATUS_TIMER_RESUME_IGNORED
40000026	STATUS_ARBITRATION_UNHANDLED
40000027	STATUS_CARDBUS_NOT_SUPPORTED
40000028	STATUS_WX86_CREATEWX86TIB
40000029	STATUS_MP_PROCESSOR_MISMATCH
4000002A	STATUS_HIBERNATED
4000002B	STATUS_RESUME_HIBERNATION
4000002C	STATUS_FIRMWARE_UPDATED
4000002D	STATUS_DRIVERS_LEAKING_LOCKED_PAGES

Table C.1: Error codes related to file encryption (Sheet 3 of 36)

CODE	MEANING
40010001	DBG_REPLY_LATER
40010002	DBG_UNABLE_TO_PROVIDE_HANDLE
40010003	DBG_TERMINATE_THREAD
40010004	DBG_TERMINATE_PROCESS
40010005	DBG_CONTROL_C
40010006	DBG_PRINTEXCEPTION_C
40010007	DBG_RIPEXCEPTION
40010008	DBG_CONTROL_BREAK
40010009	DBG_COMMAND_EXCEPTION
80000001	STATUS_GUARD_PAGE_VIOLATION
80000002	STATUS_DATATYPE_MISALIGNMENT
80000003	STATUS_BREAKPOINT
80000004	STATUS_SINGLE_STEP
80000005	STATUS_BUFFER_OVERFLOW
80000006	STATUS_NO_MORE_FILES
80000007	STATUS_WAKE_SYSTEM_DEBUGGER
8000000A	STATUS_HANDLES_CLOSED
8000000B	STATUS_NO_INHERITANCE
8000000C	STATUS_GUID_SUBSTITUTION_MADE
8000000D	STATUS_PARTIAL_COPY
8000000E	STATUS_DEVICE_PAPER_EMPTY
8000000F	STATUS_DEVICE_POWERED_OFF
80000010	STATUS_DEVICE_OFF_LINE
80000011	STATUS_DEVICE_BUSY
80000012	STATUS_NO_MORE_EAS
80000013	STATUS_INVALID_EA_NAME
80000014	STATUS_EA_LIST_INCONSISTENT
80000015	STATUS_INVALID_EA_FLAG
80000016	STATUS_VERIFY_REQUIRED
80000017	STATUS_EXTRANEOUS_INFORMATION
80000018	STATUS_RXACT_COMMIT_NECESSARY

Table C.1: Error codes related to file encryption (Sheet 4 of 36)

CODE	MEANING
8000001A	STATUS_NO_MORE_ENTRIES
8000001B	STATUS_FILEMARK_DETECTED
8000001C	STATUS_MEDIA_CHANGED
8000001D	STATUS_BUS_RESET
8000001E	STATUS_END_OF_MEDIA
8000001F	STATUS_BEGINNING_OF_MEDIA
80000020	STATUS_MEDIA_CHECK
80000021	STATUS_SETMARK_DETECTED
80000022	STATUS_NO_DATA_DETECTED
80000023	STATUS_REDIRECTOR_HAS_OPEN_HANDLES
80000024	STATUS_SERVER_HAS_OPEN_HANDLES
80000025	STATUS_ALREADY_DISCONNECTED
80000026	STATUS_LONGJUMP
80000027	STATUS_CLEANER_CARTRIDGE_INSTALLED
80000028	STATUS_PLUGPLAY_QUERY_VETOED
80000029	STATUS_UNWIND_CONSOLIDATE
8000002A	STATUS_REGISTRY_HIVE_RECOVERED
8000002B	STATUS_DLL_MIGHT_BE_INSECURE
8000002C	STATUS_DLL_MIGHT_BE_INCOMPATIBLE
80010001	DBG_EXCEPTION_NOT_HANDLED
80130001	STATUS_CLUSTER_NODE_ALREADY_UP
80130002	STATUS_CLUSTER_NODE_ALREADY_DOWN
80130003	STATUS_CLUSTER_NETWORK_ALREADY_ONLINE
80130004	STATUS_CLUSTER_NETWORK_ALREADY_OFFLINE
80130005	STATUS_CLUSTER_NODE_ALREADY_MEMBER
C0000001	STATUS_UNSUCCESSFUL
C0000002	STATUS_NOT_IMPLEMENTED
C0000003	STATUS_INVALID_INFO_CLASS
C0000004	STATUS_INFO_LENGTH_MISMATCH
C0000005	STATUS_ACCESS_VIOLATION
C0000006	STATUS_IN_PAGE_ERROR

Table C.1: Error codes related to file encryption (Sheet 5 of 36)

CODE	MEANING
C0000007	STATUS_PAGEFILE_QUOTA
C0000008	STATUS_INVALID_HANDLE
C0000009	STATUS_BAD_INITIAL_STACK
C000000A	STATUS_BAD_INITIAL_PC
C000000B	STATUS_INVALID_CID
C000000C	STATUS_TIMER_NOT_CANCELED
C000000D	STATUS_INVALID_PARAMETER
C000000E	STATUS_NO_SUCH_DEVICE
C000000F	STATUS_NO_SUCH_FILE
C0000010	STATUS_INVALID_DEVICE_REQUEST
C0000011	STATUS_END_OF_FILE
C0000012	STATUS_WRONG_VOLUME
C0000013	STATUS_NO_MEDIA_IN_DEVICE
C0000014	STATUS_UNRECOGNIZED_MEDIA
C0000015	STATUS_NONEXISTENT_SECTOR
C0000016	STATUS_MORE_PROCESSING_REQUIRED
C0000017	STATUS_NO_MEMORY
C0000018	STATUS_CONFLICTING_ADDRESSES
C0000019	STATUS_NOT_MAPPED_VIEW
C000001A	STATUS_UNABLE_TO_FREE_VM
C000001B	STATUS_UNABLE_TO_DELETE_SECTION
C000001C	STATUS_INVALID_SYSTEM_SERVICE
C000001D	STATUS_ILLEGAL_INSTRUCTION
C000001E	STATUS_INVALID_LOCK_SEQUENCE
C000001F	STATUS_INVALID_VIEW_SIZE
C0000020	STATUS_INVALID_FILE_FOR_SECTION
C0000021	STATUS_ALREADY_COMMITTED
C0000022	STATUS_ACCESS_DENIED
C0000023	STATUS_BUFFER_TOO_SMALL
C0000024	STATUS_OBJECT_TYPE_MISMATCH
C0000025	STATUS_NONCONTINUABLE_EXCEPTION

Table C.1: Error codes related to file encryption (Sheet 6 of 36)

CODE	MEANING
C0000026	STATUS_INVALID_DISPOSITION
C0000027	STATUS_UNWIND
C0000028	STATUS_BAD_STACK
C0000029	STATUS_INVALID_UNWIND_TARGET
C000002A	STATUS_NOT_LOCKED
C000002B	STATUS_PARITY_ERROR
C000002C	STATUS_UNABLE_TO_DECOMMIT_VM
C000002D	STATUS_NOT_COMMITTED
C000002E	STATUS_INVALID_PORT_ATTRIBUTES
C000002F	STATUS_PORT_MESSAGE_TOO_LONG
C0000030	STATUS_INVALID_PARAMETER_MIX
C0000031	STATUS_INVALID_QUOTA_LOWER
C0000032	STATUS_DISK_CORRUPT_ERROR
C0000033	STATUS_OBJECT_NAME_INVALID
C0000034	STATUS_OBJECT_NAME_NOT_FOUND
C0000035	STATUS_OBJECT_NAME_COLLISION
C0000037	STATUS_PORT_DISCONNECTED
C0000038	STATUS_DEVICE_ALREADY_ATTACHED
C0000039	STATUS_OBJECT_PATH_INVALID
C000003A	STATUS_OBJECT_PATH_NOT_FOUND
C000003B	STATUS_OBJECT_PATH_SYNTAX_BAD
C000003C	STATUS_DATA_OVERRUN
C000003D	STATUS_DATA_LATE_ERROR
C000003E	STATUS_DATA_ERROR
C000003F	STATUS_CRC_ERROR
C0000040	STATUS_SECTION_TOO_BIG
C0000041	STATUS_PORT_CONNECTION_REFUSED
C0000042	STATUS_INVALID_PORT_HANDLE
C0000043	STATUS_SHARING_VIOLATION
C0000044	STATUS_QUOTA_EXCEEDED
C0000045	STATUS_INVALID_PAGE_PROTECTION

Table C.1: Error codes related to file encryption (Sheet 7 of 36)

CODE	MEANING
C0000046	STATUS_MUTANT_NOT_OWNED
C0000047	STATUS_SEMAPHORE_LIMIT_EXCEEDED
C0000048	STATUS_PORT_ALREADY_SET
C0000049	STATUS_SECTION_NOT_IMAGE
C000004A	STATUS_SUSPEND_COUNT_EXCEEDED
C000004B	STATUS_THREAD_IS_TERMINATING
C000004C	STATUS_BAD_WORKING_SET_LIMIT
C000004D	STATUS_INCOMPATIBLE_FILE_MAP
C000004E	STATUS_SECTION_PROTECTION
C000004F	STATUS_EAS_NOT_SUPPORTED
C0000050	STATUS_EA_TOO_LARGE
C0000051	STATUS_NONEXISTENT_EA_ENTRY
C0000052	STATUS_NO_EAS_ON_FILE
C0000053	STATUS_EA_CORRUPT_ERROR
C0000054	STATUS_FILE_LOCK_CONFLICT
C0000055	STATUS_LOCK_NOT_GRANTED
C0000056	STATUS_DELETE_PENDING
C0000057	STATUS_CTL_FILE_NOT_SUPPORTED
C0000058	STATUS_UNKNOWN_REVISION
C0000059	STATUS_REVISION_MISMATCH
C000005A	STATUS_INVALID_OWNER
C000005B	STATUS_INVALID_MASTER_GROUP
C000005C	STATUS_NO_IMPERSONATION_TOKEN
C000005D	STATUS_CANT_DISABLE_MANDATORY
C000005E	STATUS_NO_LOGON_SERVERS
C000005F	STATUS_NO_SUCH_LOGON_SESSION
C0000060	STATUS_NO_SUCH_PRIVILEGE
C0000061	STATUS_PRIVILEGE_NOT_HELD
C0000062	STATUS_INVALID_ACCOUNT_NAME
C0000063	STATUS_USER_EXISTS
C0000064	STATUS_NO_SUCH_USER

Table C.1: Error codes related to file encryption (Sheet 8 of 36)

CODE	MEANING
C0000065	STATUS_GROUP_EXISTS
C0000066	STATUS_NO_SUCH_GROUP
C0000067	STATUS_MEMBER_IN_GROUP
C0000068	STATUS_MEMBER_NOT_IN_GROUP
C0000069	STATUS_LAST_ADMIN
C000006A	STATUS_WRONG_PASSWORD
C000006B	STATUS_ILL_FORMED_PASSWORD
C000006C	STATUS_PASSWORD_RESTRICTION
C000006D	STATUS_LOGON_FAILURE
C000006E	STATUS_ACCOUNT_RESTRICTION
C000006F	STATUS_INVALID_LOGON_HOURS
C0000070	STATUS_INVALID_WORKSTATION
C0000071	STATUS_PASSWORD_EXPIRED
C0000072	STATUS_ACCOUNT_DISABLED
C0000073	STATUS_NONE_MAPPED
C0000074	STATUS_TOO_MANY_LUIDS_REQUESTED
C0000075	STATUS_LUIDS_EXHAUSTED
C0000076	STATUS_INVALID_SUB_AUTHORITY
C0000077	STATUS_INVALID_ACL
C0000078	STATUS_INVALID_SID
C0000079	STATUS_INVALID_SECURITY_DESCR
C000007A	STATUS_PROCEDURE_NOT_FOUND
C000007B	STATUS_INVALID_IMAGE_FORMAT
C000007C	STATUS_NO_TOKEN
C000007D	STATUS_BAD_INHERITANCE_ACL
C000007E	STATUS_RANGE_NOT_LOCKED
C000007F	STATUS_DISK_FULL
C0000080	STATUS_SERVER_DISABLED
C0000081	STATUS_SERVER_NOT_DISABLED
C0000082	STATUS_TOO_MANY_GUIDS_REQUESTED
C0000083	STATUS_GUIDS_EXHAUSTED

Table C.1: Error codes related to file encryption (Sheet 9 of 36)

CODE	MEANING
C0000084	STATUS_INVALID_ID_AUTHORITY
C0000085	STATUS_AGENTS_EXHAUSTED
C0000086	STATUS_INVALID_VOLUME_LABEL
C0000087	STATUS_SECTION_NOT_EXTENDED
C0000088	STATUS_NOT_MAPPED_DATA
C0000089	STATUS_RESOURCE_DATA_NOT_FOUND
C000008A	STATUS_RESOURCE_TYPE_NOT_FOUND
C000008B	STATUS_RESOURCE_NAME_NOT_FOUND
C000008C	STATUS_ARRAY_BOUNDS_EXCEEDED
C000008D	STATUS_FLOAT_DENORMAL_OPERAND
C000008E	STATUS_FLOAT_DIVIDE_BY_ZERO
C000008F	STATUS_FLOAT_INEXACT_RESULT
C0000090	STATUS_FLOAT_INVALID_OPERATION
C0000091	STATUS_FLOAT_OVERFLOW
C0000092	STATUS_FLOAT_STACK_CHECK
C0000093	STATUS_FLOAT_UNDERFLOW
C0000094	STATUS_INTEGER_DIVIDE_BY_ZERO
C0000095	STATUS_INTEGER_OVERFLOW
C0000096	STATUS_PRIVILEGED_INSTRUCTION
C0000097	STATUS_TOO_MANY_PAGING_FILES
C0000098	STATUS_FILE_INVALID
C0000099	STATUS_ALLOTTED_SPACE_EXCEEDED
C000009A	STATUS_INSUFFICIENT_RESOURCES
C000009B	STATUS_DFS_EXIT_PATH_FOUND
C000009C	STATUS_DEVICE_DATA_ERROR
C000009D	STATUS_DEVICE_NOT_CONNECTED
C000009E	STATUS_DEVICE_POWER_FAILURE
C000009F	STATUS_FREE_VM_NOT_AT_BASE
C00000A0	STATUS_MEMORY_NOT_ALLOCATED
C00000A1	STATUS_WORKING_SET_QUOTA
C00000A2	STATUS_MEDIA_WRITE_PROTECTED

Table C.1: Error codes related to file encryption (Sheet 10 of 36)

CODE	MEANING
C00000A3	STATUS_DEVICE_NOT_READY
C00000A4	STATUS_INVALID_GROUP_ATTRIBUTES
C00000A5	STATUS_BAD_IMPERSONATION_LEVEL
C00000A6	STATUS_CANT_OPEN_ANONYMOUS
C00000A7	STATUS_BAD_VALIDATION_CLASS
C00000A8	STATUS_BAD_TOKEN_TYPE
C00000A9	STATUS_BAD_MASTER_BOOT_RECORD
C00000AA	STATUS_INSTRUCTION_MISALIGNMENT
C00000AB	STATUS_INSTANCE_NOT_AVAILABLE
C00000AC	STATUS_PIPE_NOT_AVAILABLE
C00000AD	STATUS_INVALID_PIPE_STATE
C00000AE	STATUS_PIPE_BUSY
C00000AF	STATUS_ILLEGAL_FUNCTION
C00000B0	STATUS_PIPE_DISCONNECTED
C00000B1	STATUS_PIPE_CLOSING
C00000B2	STATUS_PIPE_CONNECTED
C00000B3	STATUS_PIPE_LISTENING
C00000B4	STATUS_INVALID_READ_MODE
C00000B5	STATUS_IO_TIMEOUT
C00000B6	STATUS_FILE_FORCED_CLOSED
C00000B7	STATUS_PROFILING_NOT_STARTED
C00000B8	STATUS_PROFILING_NOT_STOPPED
C00000B9	STATUS_COULD_NOT_INTERPRET
C00000BA	STATUS_FILE_IS_A_DIRECTORY
C00000BB	STATUS_NOT_SUPPORTED
C00000BC	STATUS_REMOTE_NOT_LISTENING
C00000BD	STATUS_DUPLICATE_NAME
C00000BE	STATUS_BAD_NETWORK_PATH
C00000BF	STATUS_NETWORK_BUSY
C00000C0	STATUS_DEVICE_DOES_NOT_EXIST
C00000C1	STATUS_TOO_MANY_COMMANDS

Table C.1: Error codes related to file encryption (Sheet 11 of 36)

CODE	MEANING
C00000C2	STATUS_ADAPTER_HARDWARE_ERROR
C00000C3	STATUS_INVALID_NETWORK_RESPONSE
C00000C4	STATUS_UNEXPECTED_NETWORK_ERROR
C00000C5	STATUS_BAD_REMOTE_ADAPTER
C00000C6	STATUS_PRINT_QUEUE_FULL
C00000C7	STATUS_NO_SPOOL_SPACE
C00000C8	STATUS_PRINT_CANCELLED
C00000C9	STATUS_NETWORK_NAME_DELETED
C00000CA	STATUS_NETWORK_ACCESS_DENIED
C00000CB	STATUS_BAD_DEVICE_TYPE
C00000CC	STATUS_BAD_NETWORK_NAME
C00000CD	STATUS_TOO_MANY_NAMES
C00000CE	STATUS_TOO_MANY_SESSIONS
C00000CF	STATUS_SHARING_PAUSED
C00000D0	STATUS_REQUEST_NOT_ACCEPTED
C00000D1	STATUS_REDIRECTOR_PAUSED
C00000D2	STATUS_NET_WRITE_FAULT
C00000D3	STATUS_PROFILING_AT_LIMIT
C00000D4	STATUS_NOT_SAME_DEVICE
C00000D5	STATUS_FILE_RENAMED
C00000D6	STATUS_VIRTUAL_CIRCUIT_CLOSED
C00000D7	STATUS_NO_SECURITY_ON_OBJECT
C00000D8	STATUS_CANT_WAIT
C00000D9	STATUS_PIPE_EMPTY
C00000DA	STATUS_CANT_ACCESS_DOMAIN_INFO
C00000DB	STATUS_CANT_TERMINATE_SELF
C00000DC	STATUS_INVALID_SERVER_STATE
C00000DD	STATUS_INVALID_DOMAIN_STATE
C00000DE	STATUS_INVALID_DOMAIN_ROLE
C00000DF	STATUS_NO_SUCH_DOMAIN
C00000E0	STATUS_DOMAIN_EXISTS

Table C.1: Error codes related to file encryption (Sheet 12 of 36)

CODE	MEANING
C00000E1	STATUS_DOMAIN_LIMIT_EXCEEDED
C00000E2	STATUS_OPLOCK_NOT_GRANTED
C00000E3	STATUS_INVALID_OPLOCK_PROTOCOL
C00000E4	STATUS_INTERNAL_DB_CORRUPTION
C00000E5	STATUS_INTERNAL_ERROR
C00000E6	STATUS_GENERIC_NOT_MAPPED
C00000E7	STATUS_BAD_DESCRIPTOR_FORMAT
C00000E8	STATUS_INVALID_USER_BUFFER
C00000E9	STATUS_UNEXPECTED_IO_ERROR
C00000EA	STATUS_UNEXPECTED_MM_CREATE_ERR
C00000EB	STATUS_UNEXPECTED_MM_MAP_ERROR
C00000EC	STATUS_UNEXPECTED_MM_EXTEND_ERR
C00000ED	STATUS_NOT_LOGON_PROCESS
C00000EE	STATUS_LOGON_SESSION_EXISTS
C00000EF	STATUS_INVALID_PARAMETER_1
C00000F0	STATUS_INVALID_PARAMETER_2
C00000F1	STATUS_INVALID_PARAMETER_3
C00000F2	STATUS_INVALID_PARAMETER_4
C00000F3	STATUS_INVALID_PARAMETER_5
C00000F4	STATUS_INVALID_PARAMETER_6
C00000F5	STATUS_INVALID_PARAMETER_7
C00000F6	STATUS_INVALID_PARAMETER_8
C00000F7	STATUS_INVALID_PARAMETER_9
C00000F8	STATUS_INVALID_PARAMETER_10
C00000F9	STATUS_INVALID_PARAMETER_11
C00000FA	STATUS_INVALID_PARAMETER_12
C00000FB	STATUS_REDIRECTOR_NOT_STARTED
C00000FC	STATUS_REDIRECTOR_STARTED
C00000FD	STATUS_STACK_OVERFLOW
C00000FE	STATUS_NO_SUCH_PACKAGE
C00000FF	STATUS_BAD_FUNCTION_TABLE

Table C.1: Error codes related to file encryption (Sheet 13 of 36)

CODE	MEANING
C0000100	STATUS_VARIABLE_NOT_FOUND
C0000101	STATUS_DIRECTORY_NOT_EMPTY
C0000102	STATUS_FILE_CORRUPT_ERROR
C0000103	STATUS_NOT_A_DIRECTORY
C0000104	STATUS_BAD_LOGON_SESSION_STATE
C0000105	STATUS_LOGON_SESSION_COLLISION
C0000106	STATUS_NAME_TOO_LONG
C0000107	STATUS_FILES_OPEN
C0000108	STATUS_CONNECTION_IN_USE
C0000109	STATUS_MESSAGE_NOT_FOUND
C000010A	STATUS_PROCESS_IS_TERMINATING
C000010B	STATUS_INVALID_LOGON_TYPE
C000010C	STATUS_NO_GUID_TRANSLATION
C000010D	STATUS_CANNOT_IMPERSONATE
C000010E	STATUS_IMAGE_ALREADY_LOADED
C000010F	STATUS_ABIOS_NOT_PRESENT
C0000110	STATUS_ABIOS_LID_NOT_EXIST
C0000111	STATUS_ABIOS_LID_ALREADY_OWNED
C0000112	STATUS_ABIOS_NOT_LID_OWNER
C0000113	STATUS_ABIOS_INVALID_COMMAND
C0000114	STATUS_ABIOS_INVALID_LID
C0000115	STATUS_ABIOS_SELECTOR_NOT_AVAILABLE
C0000116	STATUS_ABIOS_INVALID_SELECTOR
C0000117	STATUS_NO_LDT
C0000118	STATUS_INVALID_LDT_SIZE
C0000119	STATUS_INVALID_LDT_OFFSET
C000011A	STATUS_INVALID_LDT_DESCRIPTOR
C000011B	STATUS_INVALID_IMAGE_NE_FORMAT
C000011C	STATUS_RXACT_INVALID_STATE
C000011D	STATUS_RXACT_COMMIT_FAILURE
C000011E	STATUS_MAPPED_FILE_SIZE_ZERO

Table C.1: Error codes related to file encryption (Sheet 14 of 36)

CODE	MEANING
C000011F	STATUS_TOO_MANY_OPENED_FILES
C0000120	STATUS_CANCELLED
C0000121	STATUS_CANNOT_DELETE
C0000122	STATUS_INVALID_COMPUTER_NAME
C0000123	STATUS_FILE_DELETED
C0000124	STATUS_SPECIAL_ACCOUNT
C0000125	STATUS_SPECIAL_GROUP
C0000126	STATUS_SPECIAL_USER
C0000127	STATUS_MEMBERS_MASTER_GROUP
C0000128	STATUS_FILE_CLOSED
C0000129	STATUS_TOO_MANY_THREADS
C000012A	STATUS_THREAD_NOT_IN_PROCESS
C000012B	STATUS_TOKEN_ALREADY_IN_USE
C000012C	STATUS_PAGEFILE_QUOTA_EXCEEDED
C000012D	STATUS_COMMITMENT_LIMIT
C000012E	STATUS_INVALID_IMAGE_LE_FORMAT
C000012F	STATUS_INVALID_IMAGE_NOT_MZ
C0000130	STATUS_INVALID_IMAGE_PROTECT
C0000131	STATUS_INVALID_IMAGE_WIN_16
C0000132	STATUS_LOGON_SERVER_CONFLICT
C0000133	STATUS_TIME_DIFFERENCE_AT_DC
C0000134	STATUS_SYNCHRONIZATION_REQUIRED
C0000135	STATUS_DLL_NOT_FOUND
C0000136	STATUS_OPEN_FAILED
C0000137	STATUS_IO_PRIVILEGE_FAILED
C0000138	STATUS_ORDINAL_NOT_FOUND
C0000139	STATUS_ENTRYPOINT_NOT_FOUND
C000013A	STATUS_CONTROL_C_EXIT
C000013B	STATUS_LOCAL_DISCONNECT
C000013C	STATUS_REMOTE_DISCONNECT
C000013D	STATUS_REMOTE_RESOURCES

Table C.1: Error codes related to file encryption (Sheet 15 of 36)

CODE	MEANING
C000013E	STATUS_LINK_FAILED
C000013F	STATUS_LINK_TIMEOUT
C0000140	STATUS_INVALID_CONNECTION
C0000141	STATUS_INVALID_ADDRESS
C0000142	STATUS_DLL_INIT_FAILED
C0000143	STATUS_MISSING_SYSTEMFILE
C0000144	STATUS_UNHANDLED_EXCEPTION
C0000145	STATUS_APP_INIT_FAILURE
C0000146	STATUS_PAGEFILE_CREATE_FAILED
C0000147	STATUS_NO_PAGEFILE
C0000148	STATUS_INVALID_LEVEL
C0000149	STATUS_WRONG_PASSWORD_CORE
C000014A	STATUS_ILLEGAL_FLOAT_CONTEXT
C000014B	STATUS_PIPE_BROKEN
C000014C	STATUS_REGISTRY_CORRUPT
C000014D	STATUS_REGISTRY_IO_FAILED
C000014E	STATUS_NO_EVENT_PAIR
C000014F	STATUS_UNRECOGNIZED_VOLUME
C0000150	STATUS_SERIAL_NO_DEVICE_INITED
C0000151	STATUS_NO_SUCH_ALIAS
C0000152	STATUS_MEMBER_NOT_IN_ALIAS
C0000153	STATUS_MEMBER_IN_ALIAS
C0000154	STATUS_ALIAS_EXISTS
C0000155	STATUS_LOGON_NOT_GRANTED
C0000156	STATUS_TOO_MANY_SECRETS
C0000157	STATUS_SECRET_TOO_LONG
C0000158	STATUS_INTERNAL_DB_ERROR
C0000159	STATUS_FULLSCREEN_MODE
C000015A	STATUS_TOO_MANY_CONTEXT_IDS
C000015B	STATUS_LOGON_TYPE_NOT_GRANTED
C000015C	STATUS_NOT_REGISTRY_FILE

Table C.1: Error codes related to file encryption (Sheet 16 of 36)

CODE	MEANING
C000015D	STATUS_NT_CROSS_ENCRYPTION_REQUIRED
C000015E	STATUS_DOMAIN_CTRLR_CONFIG_ERROR
C000015F	STATUS_FT_MISSING_MEMBER
C0000160	STATUS_ILL_FORMED_SERVICE_ENTRY
C0000161	STATUS_ILLEGAL_CHARACTER
C0000162	STATUS_UNMAPPABLE_CHARACTER
C0000163	STATUS_UNDEFINED_CHARACTER
C0000164	STATUS_FLOPPY_VOLUME
C0000165	STATUS_FLOPPY_ID_MARK_NOT_FOUND
C0000166	STATUS_FLOPPY_WRONG_CYLINDER
C0000167	STATUS_FLOPPY_UNKNOWN_ERROR
C0000168	STATUS_FLOPPY_BAD_REGISTERS
C0000169	STATUS_DISK_RECALIBRATE_FAILED
C000016A	STATUS_DISK_OPERATION_FAILED
C000016B	STATUS_DISK_RESET_FAILED
C000016C	STATUS_SHARED_IRQ_BUSY
C000016D	STATUS_FT_ORPHANING
C000016E	STATUS_BIOS_FAILED_TO_CONNECT_INTERRUPT
C0000172	STATUS_PARTITION_FAILURE
C0000173	STATUS_INVALID_BLOCK_LENGTH
C0000174	STATUS_DEVICE_NOT_PARTITIONED
C0000175	STATUS_UNABLE_TO_LOCK_MEDIA
C0000176	STATUS_UNABLE_TO_UNLOAD_MEDIA
C0000177	STATUS_EOM_OVERFLOW
C0000178	STATUS_NO_MEDIA
C000017A	STATUS_NO_SUCH_MEMBER
C000017B	STATUS_INVALID_MEMBER
C000017C	STATUS_KEY_DELETED
C000017D	STATUS_NO_LOG_SPACE
C000017E	STATUS_TOO_MANY_SIDS
C000017F	STATUS_LM_CROSS_ENCRYPTION_REQUIRED

Table C.1: Error codes related to file encryption (Sheet 17 of 36)

CODE	MEANING
C0000180	STATUS_KEY_HAS_CHILDREN
C0000181	STATUS_CHILD_MUST_BE_VOLATILE
C0000182	STATUS_DEVICE_CONFIGURATION_ERROR
C0000183	STATUS_DRIVER_INTERNAL_ERROR
C0000184	STATUS_INVALID_DEVICE_STATE
C0000185	STATUS_IO_DEVICE_ERROR
C0000186	STATUS_DEVICE_PROTOCOL_ERROR
C0000187	STATUS_BACKUP_CONTROLLER
C0000188	STATUS_LOG_FILE_FULL
C0000189	STATUS_TOO_LATE
C000018A	STATUS_NO_TRUST_LSA_SECRET
C000018B	STATUS_NO_TRUST_SAM_ACCOUNT
C000018C	STATUS_TRUSTED_DOMAIN_FAILURE
C000018D	STATUS_TRUSTED_RELATIONSHIP_FAILURE
C000018E	STATUS_EVENTLOG_FILE_CORRUPT
C000018F	STATUS_EVENTLOG_CANT_START
C0000190	STATUS_TRUST_FAILURE
C0000191	STATUS_MUTANT_LIMIT_EXCEEDED
C0000192	STATUS_NETLOGON_NOT_STARTED
C0000193	STATUS_ACCOUNT_EXPIRED
C0000194	STATUS_POSSIBLE_DEADLOCK
C0000195	STATUS_NETWORK_CREDENTIAL_CONFLICT
C0000196	STATUS_REMOTE_SESSION_LIMIT
C0000197	STATUS_EVENTLOG_FILE_CHANGED
C0000198	STATUS_NOLOGON_INTERDOMAIN_TRUST_ACCOUNT
C0000199	STATUS_NOLOGON_WORKSTATION_TRUST_ACCOUNT
C000019A	STATUS_NOLOGON_SERVER_TRUST_ACCOUNT
C000019B	STATUS_DOMAIN_TRUST_INCONSISTENT
C000019C	STATUS_FS_DRIVER_REQUIRED
C0000202	STATUS_NO_USER_SESSION_KEY
C0000203	STATUS_USER_SESSION_DELETED

Table C.1: Error codes related to file encryption (Sheet 18 of 36)

CODE	MEANING
C0000204	STATUS_RESOURCE_LANG_NOT_FOUND
C0000205	STATUS_INSUFF_SERVER_RESOURCES
C0000206	STATUS_INVALID_BUFFER_SIZE
C0000207	STATUS_INVALID_ADDRESS_COMPONENT
C0000208	STATUS_INVALID_ADDRESS_WILDCARD
C0000209	STATUS_TOO_MANY_ADDRESSES
C000020A	STATUS_ADDRESS_ALREADY_EXISTS
C000020B	STATUS_ADDRESS_CLOSED
C000020C	STATUS_CONNECTION_DISCONNECTED
C000020D	STATUS_CONNECTION_RESET
C000020E	STATUS_TOO_MANY_NODES
C000020F	STATUS_TRANSACTION_ABORTED
C0000210	STATUS_TRANSACTION_TIMED_OUT
C0000211	STATUS_TRANSACTION_NO_RELEASE
C0000212	STATUS_TRANSACTION_NO_MATCH
C0000213	STATUS_TRANSACTION_RESPONDED
C0000214	STATUS_TRANSACTION_INVALID_ID
C0000215	STATUS_TRANSACTION_INVALID_TYPE
C0000216	STATUS_NOT_SERVER_SESSION
C0000217	STATUS_NOT_CLIENT_SESSION
C0000218	STATUS_CANNOT_LOAD_REGISTRY_FILE
C0000219	STATUS_DEBUG_ATTACH_FAILED
C000021A	STATUS_SYSTEM_PROCESS_TERMINATED
C000021B	STATUS_DATA_NOT_ACCEPTED
C000021C	STATUS_NO_BROWSER_SERVERS_FOUND
C000021D	STATUS_VDM_HARD_ERROR
C000021E	STATUS_DRIVER_CANCEL_TIMEOUT
C000021F	STATUS_REPLY_MESSAGE_MISMATCH
C0000220	STATUS_MAPPED_ALIGNMENT
C0000221	STATUS_IMAGE_CHECKSUM_MISMATCH
C0000222	STATUS_LOST_WRITEBEHIND_DATA

Table C.1: Error codes related to file encryption (Sheet 19 of 36)

CODE	MEANING
C0000223	STATUS_CLIENT_SERVER_PARAMETERS_INVALID
C0000224	STATUS_PASSWORD_MUST_CHANGE
C0000225	STATUS_NOT_FOUND
C0000226	STATUS_NOT_TINY_STREAM
C0000227	STATUS_RECOVERY_FAILURE
C0000228	STATUS_STACK_OVERFLOW_READ
C0000229	STATUS_FAIL_CHECK
C000022A	STATUS_DUPLICATE_OBJECTID
C000022B	STATUS_OBJECTID_EXISTS
C000022C	STATUS_CONVERT_TO_LARGE
C000022D	STATUS_RETRY
C000022E	STATUS_FOUND_OUT_OF_SCOPE
C000022F	STATUS_ALLOCATE_BUCKET
C0000230	STATUS_PROPSET_NOT_FOUND
C0000231	STATUS_MARSHALL_OVERFLOW
C0000232	STATUS_INVALID_VARIANT
C0000233	STATUS_DOMAIN_CONTROLLER_NOT_FOUND
C0000234	STATUS_ACCOUNT_LOCKED_OUT
C0000235	STATUS_HANDLE_NOT_CLOSABLE
C0000236	STATUS_CONNECTION_REFUSED
C0000237	STATUS_GRACEFUL_DISCONNECT
C0000238	STATUS_ADDRESS_ALREADY_ASSOCIATED
C0000239	STATUS_ADDRESS_NOT_ASSOCIATED
C000023A	STATUS_CONNECTION_INVALID
C000023B	STATUS_CONNECTION_ACTIVE
C000023C	STATUS_NETWORK_UNREACHABLE
C000023D	STATUS_HOST_UNREACHABLE
C000023E	STATUS_PROTOCOL_UNREACHABLE
C000023F	STATUS_PORT_UNREACHABLE
C0000240	STATUS_REQUEST_ABORTED
C0000241	STATUS_CONNECTION_ABORTED

Table C.1: Error codes related to file encryption (Sheet 20 of 36)

CODE	MEANING
C0000242	STATUS_BAD_COMPRESSION_BUFFER
C0000243	STATUS_USER_MAPPED_FILE
C0000244	STATUS_AUDIT_FAILED
C0000245	STATUS_TIMER_RESOLUTION_NOT_SET
C0000246	STATUS_CONNECTION_COUNT_LIMIT
C0000247	STATUS_LOGIN_TIME_RESTRICTION
C0000248	STATUS_LOGIN_WKSTA_RESTRICTION
C0000249	STATUS_IMAGE_MP_UP_MISMATCH
C0000250	STATUS_INSUFFICIENT_LOGON_INFO
C0000251	STATUS_BAD_DLL_ENTRYPOINT
C0000252	STATUS_BAD_SERVICE_ENTRYPOINT
C0000253	STATUS_LPC_REPLY_LOST
C0000254	STATUS_IP_ADDRESS_CONFLICT1
C0000255	STATUS_IP_ADDRESS_CONFLICT2
C0000256	STATUS_REGISTRY_QUOTA_LIMIT
C0000257	STATUS_PATH_NOT_COVERED
C0000258	STATUS_NO_CALLBACK_ACTIVE
C0000259	STATUS_LICENSE_QUOTA_EXCEEDED
C000025A	STATUS_PWD_TOO_SHORT
C000025B	STATUS_PWD_TOO_RECENT
C000025C	STATUS_PWD_HISTORY_CONFLICT
C000025E	STATUS_PLUGPLAY_NO_DEVICE
C000025F	STATUS_UNSUPPORTED_COMPRESSION
C0000260	STATUS_INVALID_HW_PROFILE
C0000261	STATUS_INVALID_PLUGPLAY_DEVICE_PATH
C0000262	STATUS_DRIVER_ORDINAL_NOT_FOUND
C0000263	STATUS_DRIVER_ENTRYPOINT_NOT_FOUND
C0000264	STATUS_RESOURCE_NOT_OWNED
C0000265	STATUS_TOO_MANY_LINKS
C0000266	STATUS_QUOTA_LIST_INCONSISTENT
C0000267	STATUS_FILE_IS_OFFLINE

Table C.1: Error codes related to file encryption (Sheet 21 of 36)

CODE	MEANING
C0000268	STATUS_EVALUATION_EXPIRATION
C0000269	STATUS_ILLEGAL_DLL_RELOCATION
C000026A	STATUS_LICENSE_VIOLATION
C000026B	STATUS_DLL_INIT_FAILED_LOGOFF
C000026C	STATUS_DRIVER_UNABLE_TO_LOAD
C000026D	STATUS_DFS_UNAVAILABLE
C000026E	STATUS_VOLUME_DISMOUNTED
C000026F	STATUS_WX86_INTERNAL_ERROR
C0000270	STATUS_WX86_FLOAT_STACK_CHECK
C0000271	STATUS_VALIDATE_CONTINUE
C0000272	STATUS_NO_MATCH
C0000273	STATUS_NO_MORE_MATCHES
C0000275	STATUS_NOT_A_REPARSE_POINT
C0000276	STATUS_IO_REPARSE_TAG_INVALID
C0000277	STATUS_IO_REPARSE_TAG_MISMATCH
C0000278	STATUS_IO_REPARSE_DATA_INVALID
C0000279	STATUS_IO_REPARSE_TAG_NOT_HANDLED
C0000280	STATUS_REPARSE_POINT_NOT_RESOLVED
C0000281	STATUS_DIRECTORY_IS_A_REPARSE_POINT
C0000282	STATUS_RANGE_LIST_CONFLICT
C0000283	STATUS_SOURCE_ELEMENT_EMPTY
C0000284	STATUS_DESTINATION_ELEMENT_FULL
C0000285	STATUS_ILLEGAL_ELEMENT_ADDRESS
C0000286	STATUS_MAGAZINE_NOT_PRESENT
C0000287	STATUS_REINITIALIZATION_NEEDED
80000288	STATUS_DEVICE_REQUIRES_CLEANING
80000289	STATUS_DEVICE_DOOR_OPEN
C000028A	STATUS_ENCRYPTION_FAILED
C000028B	STATUS_DECRYPTION_FAILED
C000028C	STATUS_RANGE_NOT_FOUND
C000028D	STATUS_NO_RECOVERY_POLICY

Table C.1: Error codes related to file encryption (Sheet 22 of 36)

CODE	MEANING
C000028E	STATUS_NO_EFS
C000028F	STATUS_WRONG_EFS
C0000290	STATUS_NO_USER_KEYS
C0000291	STATUS_FILE_NOT_ENCRYPTED
C0000292	STATUS_NOT_EXPORT_FORMAT
C0000293	STATUS_FILE_ENCRYPTED
40000294	STATUS_WAKE_SYSTEM
C0000295	STATUS_WMI_GUID_NOT_FOUND
C0000296	STATUS_WMI_INSTANCE_NOT_FOUND
C0000297	STATUS_WMI_ITEMID_NOT_FOUND
C0000298	STATUS_WMI_TRY_AGAIN
C0000299	STATUS_SHARED_POLICY
C000029A	STATUS_POLICY_OBJECT_NOT_FOUND
C000029B	STATUS_POLICY_ONLY_IN_DS
C000029C	STATUS_VOLUME_NOT_UPGRADED
C000029D	STATUS_REMOTE_STORAGE_NOT_ACTIVE
C000029E	STATUS_REMOTE_STORAGE_MEDIA_ERROR
C000029F	STATUS_NO_TRACKING_SERVICE
C00002A0	STATUS_SERVER_SID_MISMATCH
C00002A1	STATUS_DS_NO_ATTRIBUTE_OR_VALUE
C00002A2	STATUS_DS_INVALID_ATTRIBUTE_SYNTAX
C00002A3	STATUS_DS_ATTRIBUTE_TYPE_UNDEFINED
C00002A4	STATUS_DS_ATTRIBUTE_OR_VALUE_EXISTS
C00002A5	STATUS_DS_BUSY
C00002A6	STATUS_DS_UNAVAILABLE
C00002A7	STATUS_DS_NO_RIDS_ALLOCATED
C00002A8	STATUS_DS_NO_MORE_RIDS
C00002A9	STATUS_DS_INCORRECT_ROLE_OWNER
C00002AA	STATUS_DS_RIDMGR_INIT_ERROR
C00002AB	STATUS_DS_OBJ_CLASS_VIOLATION
C00002AC	STATUS_DS_CANT_ON_NON_LEAF

Table C.1: Error codes related to file encryption (Sheet 23 of 36)

CODE	MEANING
C00002AD	STATUS_DS_CANT_ON_RDN
C00002AE	STATUS_DS_CANT_MOD_OBJ_CLASS
C00002AF	STATUS_DS_CROSS_DOM_MOVE_FAILED
C00002B0	STATUS_DS_GC_NOT_AVAILABLE
C00002B1	STATUS_DIRECTORY_SERVICE_REQUIRED
C00002B2	STATUS_REPARSE_ATTRIBUTE_CONFLICT
C00002B3	STATUS_CANT_ENABLE_DENY_ONLY
C00002B4	STATUS_FLOAT_MULTIPLE_FAULTS
C00002B5	STATUS_FLOAT_MULTIPLE_TRAPS
C00002B6	STATUS_DEVICE_REMOVED
C00002B7	STATUS_JOURNAL_DELETE_IN_PROGRESS
C00002B8	STATUS_JOURNAL_NOT_ACTIVE
C00002B9	STATUS_NOINTERFACE
C00002C1	STATUS_DS_ADMIN_LIMIT_EXCEEDED
C00002C2	STATUS_DRIVER_FAILED_SLEEP
C00002C3	STATUS_MUTUAL_AUTHENTICATION_FAILED
C00002C4	STATUS_CORRUPT_SYSTEM_FILE
C00002C5	STATUS_DATATYPE_MISALIGNMENT_ERROR
C00002C6	STATUS_WMI_READ_ONLY
C00002C7	STATUS_WMI_SET_FAILURE
C00002C8	STATUS_COMMITMENT_MINIMUM
C00002C9	STATUS_REG_NAT_CONSUMPTION
C00002CA	STATUS_TRANSPORT_FULL
C00002CB	STATUS_DS_SAM_INIT_FAILURE
C00002CC	STATUS_ONLY_IF_CONNECTED
C00002CD	STATUS_DS_SENSITIVE_GROUP_VIOLATION
C00002CE	STATUS_PNP_RESTART_ENUMERATION
C00002CF	STATUS_JOURNAL_ENTRY_DELETED
C00002D0	STATUS_DS_CANT_MOD_MASTERGROUPID
C00002D1	STATUS_SYSTEM_IMAGE_BAD_SIGNATURE
C00002D2	STATUS_PNP_REBOOT_REQUIRED

Table C.1: Error codes related to file encryption (Sheet 24 of 36)

CODE	MEANING
C00002D3	STATUS_POWER_STATE_INVALID
C00002D4	STATUS_DS_INVALID_GROUP_TYPE
C00002D5	STATUS_DS_NO_NEST_GLOBALGROUP_IN_MIXEDDOMAIN
C00002D6	STATUS_DS_NO_NEST_LOCALGROUP_IN_MIXEDDOMAIN
C00002D7	STATUS_DS_GLOBAL_CANT_HAVE_LOCAL_MEMBER
C00002D8	STATUS_DS_GLOBAL_CANT_HAVE_UNIVERSAL_MEMBER
C00002D9	STATUS_DS_UNIVERSAL_CANT_HAVE_LOCAL_MEMBER
C00002DA	STATUS_DS_GLOBAL_CANT_HAVE_CROSSDOMAIN_MEMBER
C00002DB	STATUS_DS_LOCAL_CANT_HAVE_CROSSDOMAIN_LOCAL_MEMBER
C00002DC	STATUS_DS_HAVE_MASTER_MEMBERS
C00002DD	STATUS_WMI_NOT_SUPPORTED
C00002DE	STATUS_INSUFFICIENT_POWER
C00002DF	STATUS_SAM_NEED_BOOTKEY_PASSWORD
C00002E0	STATUS_SAM_NEED_BOOTKEY_FLOPPY
C00002E1	STATUS_DS_CANT_START
C00002E2	STATUS_DS_INIT_FAILURE
C00002E3	STATUS_SAM_INIT_FAILURE
C00002E4	STATUS_DS_GC_REQUIRED
C00002E5	STATUS_DS_LOCAL_MEMBER_OF_LOCAL_ONLY
C00002E6	STATUS_DS_NO_FPO_IN_UNIVERSAL_GROUPS
C00002E7	STATUS_DS_MACHINE_ACCOUNT_QUOTA_EXCEEDED
C00002E8	STATUS_MULTIPLE_FAULT_VIOLATION
C00002E9	STATUS_CURRENT_DOMAIN_NOT_ALLOWED
C00002EA	STATUS_CANNOT_MAKE
C00002EB	STATUS_SYSTEM_SHUTDOWN
C00002EC	STATUS_DS_INIT_FAILURE_CONSOLE
C00002ED	STATUS_DS_SAM_INIT_FAILURE_CONSOLE
C00002EE	STATUS_UNFINISHED_CONTEXT_DELETED
C00002EF	STATUS_NO_TGT_REPLY
C00002F0	STATUS_OBJECTID_NOT_FOUND

Table C.1: Error codes related to file encryption (Sheet 25 of 36)

CODE	MEANING
C00002F1	STATUS_NO_IP_ADDRESSES
C00002F2	STATUS_WRONG_CREDENTIAL_HANDLE
C00002F3	STATUS_CRYPTO_SYSTEM_INVALID
C00002F4	STATUS_MAX_REFERRALS_EXCEEDED
C00002F5	STATUS_MUST_BE_KDC
C00002F6	STATUS_STRONG_CRYPTO_NOT_SUPPORTED
C00002F7	STATUS_TOO_MANY_PRINCIPALS
C00002F8	STATUS_NO_PA_DATA
C00002F9	STATUS_PKINIT_NAME_MISMATCH
C00002FA	STATUS_SMARTCARD_LOGON_REQUIRED
C00002FB	STATUS_KDC_INVALID_REQUEST
C00002FC	STATUS_KDC_UNABLE_TO_REFER
C00002FD	STATUS_KDC_UNKNOWN_ETYPE
C00002FE	STATUS_SHUTDOWN_IN_PROGRESS
C00002FF	STATUS_SERVER_SHUTDOWN_IN_PROGRESS
C0000300	STATUS_NOT_SUPPORTED_ON_SBS
C0000301	STATUS_WMI_GUID_DISCONNECTED
C0000302	STATUS_WMI_ALREADY_DISABLED
C0000303	STATUS_WMI_ALREADY_ENABLED
C0000304	STATUS_MFT_TOO_FRAGMENTED
C0000305	STATUS_COPY_PROTECTION_FAILURE
C0000306	STATUS_CSS_AUTHENTICATION_FAILURE
C0000307	STATUS_CSS_KEY_NOT_PRESENT
C0000308	STATUS_CSS_KEY_NOT_ESTABLISHED
C0000309	STATUS_CSS_SCRAMBLED_SECTOR
C000030A	STATUS_CSS_REGION_MISMATCH
C000030B	STATUS_CSS_RESETS_EXHAUSTED
C0000320	STATUS_PKINIT_FAILURE
C0000321	STATUS_SMARTCARD_SUBSYSTEM_FAILURE
C0000322	STATUS_NO_KERB_KEY
C0000350	STATUS_HOST_DOWN

Table C.1: Error codes related to file encryption (Sheet 26 of 36)

CODE	MEANING
C0000351	STATUS_UNSUPPORTED_PREAUTH
C0000352	STATUS_EFS_ALG_BLOB_TOO_BIG
C0000353	STATUS_PORT_NOT_SET
C0000354	STATUS_DEBUGGER_INACTIVE
C0000355	STATUS_DS_VERSION_CHECK_FAILURE
C0000356	STATUS_AUDITING_DISABLED
C0000357	STATUS_PRENT4_MACHINE_ACCOUNT
C0000358	STATUS_DS_AG_CANT_HAVE_UNIVERSAL_MEMBER
C0000359	STATUS_INVALID_IMAGE_WIN_32
C000035A	STATUS_INVALID_IMAGE_WIN_64
C000035B	STATUS_BAD_BINDINGS
C000035C	STATUS_NETWORK_SESSION_EXPIRED
C000035D	STATUS_APPHELP_BLOCK
C000035E	STATUS_ALL_SIDS_FILTERED
C000035F	STATUS_NOT_SAFE_MODE_DRIVER
C0000361	STATUS_ACCESS_DISABLED_BY_POLICY_DEFAULT
C0000362	STATUS_ACCESS_DISABLED_BY_POLICY_PATH
C0000363	STATUS_ACCESS_DISABLED_BY_POLICY_PUBLISHER
C0000364	STATUS_ACCESS_DISABLED_BY_POLICY_OTHER
C0000365	STATUS_FAILED_DRIVER_ENTRY
C0000366	STATUS_DEVICE_ENUMERATION_ERROR
00000367	STATUS_WAIT_FOR_OPLOCK
C0000368	STATUS_MOUNT_POINT_NOT_RESOLVED
C0000369	STATUS_INVALID_DEVICE_OBJECT_PARAMETER
C000036A	STATUS_MCA_OCCURED
C000036B	STATUS_DRIVER_BLOCKED_CRITICAL
C000036C	STATUS_DRIVER_BLOCKED
C000036D	STATUS_DRIVER_DATABASE_ERROR
C000036E	STATUS_SYSTEM_HIVE_TOO_LARGE
C000036F	STATUS_INVALID_IMPORT_OF_NON_DLL
40000370	STATUS_DS_SHUTTING_DOWN

Table C.1: Error codes related to file encryption (Sheet 27 of 36)

CODE	MEANING
C0000380	STATUS_SMARTCARD_WRONG_PIN
C0000381	STATUS_SMARTCARD_CARD_BLOCKED
C0000382	STATUS_SMARTCARD_CARD_NOT_AUTHENTICATED
C0000383	STATUS_SMARTCARD_NO_CARD
C0000384	STATUS_SMARTCARD_NO_KEY_CONTAINER
C0000385	STATUS_SMARTCARD_NO_CERTIFICATE
C0000386	STATUS_SMARTCARD_NO_KEYSET
C0000387	STATUS_SMARTCARD_IO_ERROR
C0000388	STATUS_DOWNGRADE_DETECTED
C0000389	STATUS_SMARTCARD_CERT_REVOKED
C000038A	STATUS_ISSUING_CA_UNTRUSTED
C000038B	STATUS_REVOCATION_OFFLINE_C
C000038C	STATUS_PKINIT_CLIENT_FAILURE
C000038D	STATUS_SMARTCARD_CERT_EXPIRED
C000038E	STATUS_DRIVER_FAILED_PRIOR_UNLOAD
C000038F	STATUS_SMARTCARD_SILENT_CONTEXT
C0000401	STATUS_PER_USER_TRUST_QUOTA_EXCEEDED
C0000402	STATUS_ALL_USER_TRUST_QUOTA_EXCEEDED
C0000403	STATUS_USER_DELETE_TRUST_QUOTA_EXCEEDED
C0000404	STATUS_DS_NAME_NOT_UNIQUE
C0000405	STATUS_DS_DUPLICATE_ID_FOUND
C0000406	STATUS_DS_GROUP_CONVERSION_ERROR
C0000407	STATUS_VOLSNAP_PREPARE_HIBERNATE
C0000408	STATUS_USER2USER_REQUIRED
C0000409	STATUS_STACK_BUFFER_OVERRUN
C000040A	STATUS_NO_S4U_PROT_SUPPORT
C000040B	STATUS_CROSSREALM_DELEGATION_FAILURE
C000040C	STATUS_REVOCATION_OFFLINE_KDC
C000040D	STATUS_ISSUING_CA_UNTRUSTED_KDC
C000040E	STATUS_KDC_CERT_EXPIRED
C000040F	STATUS_KDC_CERT_REVOKED

Table C.1: Error codes related to file encryption (Sheet 28 of 36)

CODE	MEANING
C0000410	STATUS_PARAMETER_QUOTA_EXCEEDED
C0000411	STATUS_HIBERNATION_FAILURE
C0000412	STATUS_DELAY_LOAD_FAILED
C0000413	STATUS_AUTHENTICATION_FIREWALL_FAILED
C0000414	STATUS_VDM_DISALLOWED
C0000415	STATUS_HUNG_DISPLAY_DRIVER_THREAD
C0009898	STATUS_WOW_ASSERTION
C0010001	DBG_NO_STATE_CHANGE
C0010002	DBG_APP_NOT_IDLE
C0020001	RPC_NT_INVALID_STRING_BINDING
C0020002	RPC_NT_WRONG_KIND_OF_BINDING
C0020003	RPC_NT_INVALID_BINDING
C0020004	RPC_NT_PROTSEQ_NOT_SUPPORTED
C0020005	RPC_NT_INVALID_RPC_PROTSEQ
C0020006	RPC_NT_INVALID_STRING_UUID
C0020007	RPC_NT_INVALID_ENDPOINT_FORMAT
C0020008	RPC_NT_INVALID_NET_ADDR
C0020009	RPC_NT_NO_ENDPOINT_FOUND
C002000A	RPC_NT_INVALID_TIMEOUT
C002000B	RPC_NT_OBJECT_NOT_FOUND
C002000C	RPC_NT_ALREADY_REGISTERED
C002000D	RPC_NT_TYPE_ALREADY_REGISTERED
C002000E	RPC_NT_ALREADY_LISTENING
C002000F	RPC_NT_NO_PROTSEQS_REGISTERED
C0020010	RPC_NT_NOT_LISTENING
C0020011	RPC_NT_UNKNOWN_MGR_TYPE
C0020012	RPC_NT_UNKNOWN_IF
C0020013	RPC_NT_NO_BINDINGS
C0020014	RPC_NT_NO_PROTSEQS
C0020015	RPC_NT_CANT_CREATE_ENDPOINT
C0020016	RPC_NT_OUT_OF_RESOURCES

Table C.1: Error codes related to file encryption (Sheet 29 of 36)

CODE	MEANING
C0020017	RPC_NT_SERVER_UNAVAILABLE
C0020018	RPC_NT_SERVER_TOO_BUSY
C0020019	RPC_NT_INVALID_NETWORK_OPTIONS
C002001A	RPC_NT_NO_CALL_ACTIVE
C002001B	RPC_NT_CALL_FAILED
C002001C	RPC_NT_CALL_FAILED_DNE
C002001D	RPC_NT_PROTOCOL_ERROR
C002001F	RPC_NT_UNSUPPORTED_TRANS_SYN
C0020021	RPC_NT_UNSUPPORTED_TYPE
C0020022	RPC_NT_INVALID_TAG
C0020023	RPC_NT_INVALID_BOUND
C0020024	RPC_NT_NO_ENTRY_NAME
C0020025	RPC_NT_INVALID_NAME_SYNTAX
C0020026	RPC_NT_UNSUPPORTED_NAME_SYNTAX
C0020028	RPC_NT_UUID_NO_ADDRESS
C0020029	RPC_NT_DUPLICATE_ENDPOINT
C002002A	RPC_NT_UNKNOWN_AUTHN_TYPE
C002002B	RPC_NT_MAX_CALLS_TOO_SMALL
C002002C	RPC_NT_STRING_TOO_LONG
C002002D	RPC_NT_PROTSEQ_NOT_FOUND
C002002E	RPC_NT_PROCNUM_OUT_OF_RANGE
C002002F	RPC_NT_BINDING_HAS_NO_AUTH
C0020030	RPC_NT_UNKNOWN_AUTHN_SERVICE
C0020031	RPC_NT_UNKNOWN_AUTHN_LEVEL
C0020032	RPC_NT_INVALID_AUTH_IDENTITY
C0020033	RPC_NT_UNKNOWN_AUTHZ_SERVICE
C0020034	EPT_NT_INVALID_ENTRY
C0020035	EPT_NT_CANT_PERFORM_OP
C0020036	EPT_NT_NOT_REGISTERED
C0020037	RPC_NT_NOTHING_TO_EXPORT
C0020038	RPC_NT_INCOMPLETE_NAME

Table C.1: Error codes related to file encryption (Sheet 30 of 36)

CODE	MEANING
C0020039	RPC_NT_INVALID_VERS_OPTION
C002003A	RPC_NT_NO_MORE_MEMBERS
C002003B	RPC_NT_NOT_ALL_OBJS_UNEXPORTED
C002003C	RPC_NT_INTERFACE_NOT_FOUND
C002003D	RPC_NT_ENTRY_ALREADY_EXISTS
C002003E	RPC_NT_ENTRY_NOT_FOUND
C002003F	RPC_NT_NAME_SERVICE_UNAVAILABLE
C0020040	RPC_NT_INVALID_NAF_ID
C0020041	RPC_NT_CANNOT_SUPPORT
C0020042	RPC_NT_NO_CONTEXT_AVAILABLE
C0020043	RPC_NT_INTERNAL_ERROR
C0020044	RPC_NT_ZERO_DIVIDE
C0020045	RPC_NT_ADDRESS_ERROR
C0020046	RPC_NT_FP_DIV_ZERO
C0020047	RPC_NT_FP_UNDERFLOW
C0020048	RPC_NT_FP_OVERFLOW
C0030001	RPC_NT_NO_MORE_ENTRIES
C0030002	RPC_NT_SS_CHAR_TRANS_OPEN_FAIL
C0030003	RPC_NT_SS_CHAR_TRANS_SHORT_FILE
C0030004	RPC_NT_SS_IN_NULL_CONTEXT
C0030005	RPC_NT_SS_CONTEXT_MISMATCH
C0030006	RPC_NT_SS_CONTEXT_DAMAGED
C0030007	RPC_NT_SS_HANDLES_MISMATCH
C0030008	RPC_NT_SS_CANNOT_GET_CALL_HANDLE
C0030009	RPC_NT_NULL_REF_POINTER
C003000A	RPC_NT_ENUM_VALUE_OUT_OF_RANGE
C003000B	RPC_NT_BYTE_COUNT_TOO_SMALL
C003000C	RPC_NT_BAD_STUB_DATA
C0020049	RPC_NT_CALL_IN_PROGRESS
C002004A	RPC_NT_NO_MORE_BINDINGS
C002004B	RPC_NT_GROUP_MEMBER_NOT_FOUND

Table C.1: Error codes related to file encryption (Sheet 31 of 36)

CODE	MEANING
C002004C	EPT_NT_CANT_CREATE
C002004D	RPC_NT_INVALID_OBJECT
C002004F	RPC_NT_NO_INTERFACES
C0020050	RPC_NT_CALL_CANCELLED
C0020051	RPC_NT_BINDING_INCOMPLETE
C0020052	RPC_NT_COMM_FAILURE
C0020053	RPC_NT_UNSUPPORTED_AUTHN_LEVEL
C0020054	RPC_NT_NO_PRINC_NAME
C0020055	RPC_NT_NOT_RPC_ERROR
40020056	RPC_NT_UUID_LOCAL_ONLY
C0020057	RPC_NT_SEC_PKG_ERROR
C0020058	RPC_NT_NOT_CANCELLED
C0030059	RPC_NT_INVALID_ES_ACTION
C003005A	RPC_NT_WRONG_ES_VERSION
C003005B	RPC_NT_WRONG_STUB_VERSION
C003005C	RPC_NT_INVALID_PIPE_OBJECT
C003005D	RPC_NT_INVALID_PIPE_OPERATION
C003005E	RPC_NT_WRONG_PIPE_VERSION
C003005F	RPC_NT_PIPE_CLOSED
C0030060	RPC_NT_PIPE_DISCIPLINE_ERROR
C0030061	RPC_NT_PIPE_EMPTY
C0020062	RPC_NT_INVALID_ASYNC_HANDLE
C0020063	RPC_NT_INVALID_ASYNC_CALL
400200AF	RPC_NT_SEND_INCOMPLETE
C0140001	STATUS_ACPI_INVALID_OPCODE
C0140002	STATUS_ACPI_STACK_OVERFLOW
C0140003	STATUS_ACPI_ASSERT_FAILED
C0140004	STATUS_ACPI_INVALID_INDEX
C0140005	STATUS_ACPI_INVALID_ARGUMENT
C0140006	STATUS_ACPI_FATAL
C0140007	STATUS_ACPI_INVALID_SUPERNAME

Table C.1: Error codes related to file encryption (Sheet 32 of 36)

CODE	MEANING
C0140008	STATUS_ACPI_INVALID_ARGTYPE
C0140009	STATUS_ACPI_INVALID_OBJTYPE
C014000A	STATUS_ACPI_INVALID_TARGETTYPE
C014000B	STATUS_ACPI_INCORRECT_ARGUMENT_COUNT
C014000C	STATUS_ACPI_ADDRESS_NOT_MAPPED
C014000D	STATUS_ACPI_INVALID_EVENTTYPE
C014000E	STATUS_ACPI_HANDLER_COLLISION
C014000F	STATUS_ACPI_INVALID_DATA
C0140010	STATUS_ACPI_INVALID_REGION
C0140011	STATUS_ACPI_INVALID_ACCESS_SIZE
C0140012	STATUS_ACPI_ACQUIRE_GLOBAL_LOCK
C0140013	STATUS_ACPI_ALREADY_INITIALIZED
C0140014	STATUS_ACPI_NOT_INITIALIZED
C0140015	STATUS_ACPI_INVALID_MUTEX_LEVEL
C0140016	STATUS_ACPI_MUTEX_NOT_OWNED
C0140017	STATUS_ACPI_MUTEX_NOT_OWNER
C0140018	STATUS_ACPI_RS_ACCESS
C0140019	STATUS_ACPI_INVALID_TABLE
C0140020	STATUS_ACPI_REG_HANDLER_FAILED
C0140021	STATUS_ACPI_POWER_REQUEST_FAILED
C00A0001	STATUS_CTX_WINSTATION_NAME_INVALID
C00A0002	STATUS_CTX_INVALID_PD
C00A0003	STATUS_CTX_PD_NOT_FOUND
400A0004	STATUS_CTX_CDM_CONNECT
400A0005	STATUS_CTX_CDM_DISCONNECT
C00A0006	STATUS_CTX_CLOSE_PENDING
C00A0007	STATUS_CTX_NO_OUTBUF
C00A0008	STATUS_CTX_MODEM_INF_NOT_FOUND
C00A0009	STATUS_CTX_INVALID_MODEMNAME
C00A000A	STATUS_CTX_RESPONSE_ERROR
C00A000B	STATUS_CTX_MODEM_RESPONSE_TIMEOUT

Table C.1: Error codes related to file encryption (Sheet 33 of 36)

CODE	MEANING
C00A000C	STATUS_CTX_MODEM_RESPONSE_NO_CARRIER
C00A000D	STATUS_CTX_MODEM_RESPONSE_NO_DIALTONE
C00A000E	STATUS_CTX_MODEM_RESPONSE_BUSY
C00A000F	STATUS_CTX_MODEM_RESPONSE_VOICE
C00A0010	STATUS_CTX_TD_ERROR
C00A0012	STATUS_CTX_LICENSE_CLIENT_INVALID
C00A0013	STATUS_CTX_LICENSE_NOT_AVAILABLE
C00A0014	STATUS_CTX_LICENSE_EXPIRED
C00A0015	STATUS_CTX_WINSTATION_NOT_FOUND
C00A0016	STATUS_CTX_WINSTATION_NAME_COLLISION
C00A0017	STATUS_CTX_WINSTATION_BUSY
C00A0018	STATUS_CTX_BAD_VIDEO_MODE
C00A0022	STATUS_CTX_GRAPHICS_INVALID
C00A0024	STATUS_CTX_NOT_CONSOLE
C00A0026	STATUS_CTX_CLIENT_QUERY_TIMEOUT
C00A0027	STATUS_CTX_CONSOLE_DISCONNECT
C00A0028	STATUS_CTX_CONSOLE_CONNECT
C00A002A	STATUS_CTX_SHADOW_DENIED
C00A002B	STATUS_CTX_WINSTATION_ACCESS_DENIED
C00A002E	STATUS_CTX_INVALID_WD
C00A002F	STATUS_CTX_WD_NOT_FOUND
C00A0030	STATUS_CTX_SHADOW_INVALID
C00A0031	STATUS_CTX_SHADOW_DISABLED
C00A0032	STATUS_RDP_PROTOCOL_ERROR
C00A0033	STATUS_CTX_CLIENT_LICENSE_NOT_SET
C00A0034	STATUS_CTX_CLIENT_LICENSE_IN_USE
C00A0035	STATUS_CTX_SHADOW_ENDED_BY_MODE_CHANGE
C00A0036	STATUS_CTX_SHADOW_NOT_RUNNING
C0040035	STATUS_PNP_BAD_MPS_TABLE
C0040036	STATUS_PNP_TRANSLATION_FAILED
C0040037	STATUS_PNP_IRQ_TRANSLATION_FAILED

Table C.1: Error codes related to file encryption (Sheet 34 of 36)

CODE	MEANING
C0040038	STATUS_PNP_INVALID_ID
C0150001	STATUS_SXS_SECTION_NOT_FOUND
C0150002	STATUS_SXS_CANT_GEN_ACTCTX
C0150003	STATUS_SXS_INVALID_ACTCTXDATA_FORMAT
C0150004	STATUS_SXS_ASSEMBLY_NOT_FOUND
C0150005	STATUS_SXS_MANIFEST_FORMAT_ERROR
C0150006	STATUS_SXS_MANIFEST_PARSE_ERROR
C0150007	STATUS_SXS_ACTIVATION_CONTEXT_DISABLED
C0150008	STATUS_SXS_KEY_NOT_FOUND
C0150009	STATUS_SXS_VERSION_CONFLICT
C015000A	STATUS_SXS_WRONG_SECTION_TYPE
C015000B	STATUS_SXS_THREAD_QUERIES_DISABLED
C015000C	STATUS_SXS_ASSEMBLY_MISSING
4015000D	STATUS_SXS_RELEASE_ACTIVATION_CONTEXT
C015000E	STATUS_SXS_PROCESS_DEFAULT_ALREADY_SET
C015000F	STATUS_SXS_EARLY_DEACTIVATION
C0150010	STATUS_SXS_INVALID_DEACTIVATION
C0150011	STATUS_SXS_MULTIPLE_DEACTIVATION
C0150012	STATUS_SXS_SYSTEM_DEFAULT_ACTIVATION_CONTEXT_EMPTY
C0150013	STATUS_SXS_PROCESS_TERMINATION_REQUESTED
C0150014	STATUS_SXS_CORRUPT_ACTIVATION_STACK
C0150015	STATUS_SXS_CORRUPTION
C0130001	STATUS_CLUSTER_INVALID_NODE
C0130002	STATUS_CLUSTER_NODE_EXISTS
C0130003	STATUS_CLUSTER_JOIN_IN_PROGRESS
C0130004	STATUS_CLUSTER_NODE_NOT_FOUND
C0130005	STATUS_CLUSTER_LOCAL_NODE_NOT_FOUND
C0130006	STATUS_CLUSTER_NETWORK_EXISTS
C0130007	STATUS_CLUSTER_NETWORK_NOT_FOUND
C0130008	STATUS_CLUSTER_NETINTERFACE_EXISTS
C0130009	STATUS_CLUSTER_NETINTERFACE_NOT_FOUND

Table C.1: Error codes related to file encryption (Sheet 35 of 36)

CODE	MEANING
C013000A	STATUS_CLUSTER_INVALID_REQUEST
C013000B	STATUS_CLUSTER_INVALID_NETWORK_PROVIDER
C013000C	STATUS_CLUSTER_NODE_DOWN
C013000D	STATUS_CLUSTER_NODE_UNREACHABLE
C013000E	STATUS_CLUSTER_NODE_NOT_MEMBER
C013000F	STATUS_CLUSTER_JOIN_NOT_IN_PROGRESS
C0130010	STATUS_CLUSTER_INVALID_NETWORK
C0130011	STATUS_CLUSTER_NO_NET_ADAPTERS
C0130012	STATUS_CLUSTER_NODE_UP
C0130013	STATUS_CLUSTER_NODE_PAUSED
C0130014	STATUS_CLUSTER_NODE_NOT_PAUSED
C0130015	STATUS_CLUSTER_NO_SECURITY_CONTEXT
C0130016	STATUS_CLUSTER_NETWORK_NOT_INTERNAL
C0130017	STATUS_CLUSTER_POISONED

Table C.1: Error codes related to file encryption (Sheet 36 of 36)

INDEX

A

C

E

F

I

K

L

M

P

Q

R

S

T

U

V

W

http://extranet.skyrecon.com