STORMSHIELD V6.0

RELEASE NOTES
VERSION 6.0.32

STORMSHIELD

Date: 04 May 2020

http://extranet.skyrecon.com

TABLE OF CONTENTS

IMPORTANT

- **StormShield packages**:

  The StormShield packages now exist in the three following versions:

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

  The three packages do not come with the same features.

  For more information, see the Administrator's Guide, section Packages, option and licenses.

- **SURT**:

  If you enable and apply SURT to removable devices on agents in version 5.5 and higher, and plug in a key on a workstation in version **5.2** and lower, the `Surt.exe` file will be encrypted and become unusable.

- **Log database**:

  When updating the log database, make sure that the server has enough disk space available.

  It is recommended to have at least 1.5x the size of the log database (`.mdf` file) available on your machine.

- **Update**:

  To update StormShield, observe the following chronological order:

  1. Update the Console
  2. Update the Database
  3. Update the server (be careful to restart the machine, and not only the service)
  4. Update the Agents

  If you do not observe the updating order, StormShield's previous and new features will be altered.

- **Encryption**:

  When using **Full Disk Encryption**, NEVER choose a system restore point that is older than the encryption policy's application date.
  In the event of a restoration, this operation would destroy the NEP driver (StormShield full disk encryption) and the encrypted disk would no longer be readable.

When using **File Encryption** in Windows authentication mode, you cannot uninstall and reinstall the StormShield agent on the same computer. The encrypted data would be impossible to retrieve. Before uninstalling and reinstalling the StormShield agent, you must:

- Either revoke the already existing user key to generate a new one.
- Or change the authentication mode.

When using Full Disk Encryption under Windows 7, two synchronizations take place:

- First synchronization: hidden partition.
- Second synchronization: any other partitions.

NEVER reboot your computer while the first synchronization is in progress.

- **Antivirus**:
  - When updating or installing StormShield in version `6.0`, you have to install the `vcredist.exe` component to manage Avira licenses and password complexity.
  - Port `TCP:7080` is used on the StormShield server to update Avira.
  - Antivirus installation fails on the StormShield agent:
    - If the IP address and port are not properly configured in the configuration.
    - If the port does not correspond to the port configured for Apache when installing the server.
    - If the IP address and port configured in the configuration are blocked by a firewall (StormShield's firewall or another firewall in the corporate infrastructure).
    - If the antivirus server has not been properly installed.

- **Full support for Windows 7 SP1 and Server 2008 R2 SP1**:

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	✓	✓	✓	✓	✓
• Kernel Components	✓	✗	✓	✗	✗
• Trusted applications	✓	✓	✓	✓	✓
• WiFi Access Points	✓	✓	✓	✓	✓
• Removable Devices	✓	✓	✓	✓	✓
Configurations					
• Agent Configuration	✓	✓	✓	✓	✓
• Temporary Web Access	✓	✓	✓	✓	✓
• Learning	✓	✓	✓	✓	✓
• Antivirus Configuration (optional)	✓	✓	✓	✓	✓
Scripts					
• Tests	✓	✓	✓	✓	✓
• Actions	✓	✓	✓	✓	✓
• Batches	✓	✓	✓	✓	✓

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

INFORMATION ABOUT 6.0 VERSIONS

The table below gives information about the StormShield 6.0 versions from the 6.0.16 version:

VERSION	RELEASE DATE	BUILD
6.0.16	10/31/2014	23739
6.0.17	1/29/2015	24038
6.0.18	4/29/2015	24779
6.0.19	7/24/2015	25285
6.0.20	10/23/2015	25673
6.0.21	1/22/2016	26322
6.0.22	4/22/2016	26904
6.0.23	5/27/2016	27070
6.0.24	6/10/2016	27201
6.0.25	7/29/2016	27579
6.0.26	9/29/2016	28183
6.0.27	10/21/2016	28377
6.0.28	2/9/2017	29255
6.0.29	8/28/2017	30296
6.0.30	3/20/2018	31490
6.0.31	04/01/2019	32657
6.0.32	05/04/2020	10

SUMMARY OF NEW FUNCTIONALITIES IN STORMSHIELD 6.0

Here are the new functionalities in StormShield 6.0:

- **Enrolment of USB removable devices**:
  - In order to improve the management of data passing through a perimeter protected by StormShield, it is now possible to mark removable devices (FAT32). In conjunction with an antivirus installed on the workstation, this mark reflecting a confidence status is given to removable devices as soon as they are scanned by the antivirus.

This functionality is not an intrinsic security mecanism but it requires users to apply scenarios of validation of data before using them in a protected perimeter.

- **Sending logs customized by the user from StormShield agent**:
  - The SSUSRLOG tool allows the agent to send logs to the StormShield console using command lines, either directly, or from a .csv file. The management of these logs by StormShield is defined in the console's Log Manager.

UPDATES IN STORMSHIELD V6.0.32

- **[T4120]** OpenSSL upgraded to version 1.1.1d
  OpenSSL has been updated to version 1.1.1d. The 1.0.2 version previously used is no longer supported by OpenSSL.org.

- **[T4176]** Libxml2 upgraded to version 2.9.10
  The libxml2 version that StormShield uses to manage XML files has been upgraded to version 2.9.10. Version 2.9.6 contained vulnerabilities.

- StormShield certificates renewal
  Server and agent certificates, as well as the StormShield 6.0 root certificate, has been renewed. On Microsoft Windows Server 2003 and Windows XP operating systems, you will have to manually add the root certificate on the workstations protected by the StormShield agent. Please read the procedure on our knowledge base.

LIST OF FIXES IN STORMSHIELD V6.0.31

Agent fixes:

- **[T3096]** OpenSSL upgraded to version 1.0.2r
  The vulnerability CVE-2019-1559 has been fixed by upgrading the OpenSSL cryptographic library to version 1.0.2r. Details on this vulnerability can be found on our website https://advisories.stormshield.eu.

LIST OF FIXES IN STORMSHIELD V6.0.30

Agent fixes:

- **[T658]** Libxml2 upgraded to version 2.9.6
  The libxml2 version that StormShield uses to manage XML files has been upgraded to version 2.9.6. Version 2.9.4 contained vulnerabilities.

- **[T1654]** Incompatibility with the Spectre/Meltdown fix for Windows 7 32 bits
  The Microsoft fix against Spectre and Meltdown vulnerabilities caused an incompatibility with StormShield on Windows 7 32 bits. This issue has been fixed. In the future, if another incompatibility of this type occurs, the StormShield protections impacted would be automatically disabled.

LIST OF FIXES IN STORMSHIELD V6.0.29

Server fix:

- Apache updates
  The Apache web server has been updated to version 2.4.27. The update to this version requires running the command "skyapache.exe --update", as described in the StormShield Administrator's guide.

LIST OF FIXES IN STORMSHIELD V6.0.28

Server fixes:

- Simplification of the server's update mode
  The parameter for changing the server's update mode via the console has been removed. The default update mode is now automatic mode. The server will continue to check for new updates when the StormShield service starts. Caution: if servers have been configured in manual update mode, they must be upgraded before the console to version 6.0.28 so that they do not remain frozen in manual update mode; otherwise, switch them to automatic update mode before upgrading to version 6.0.28.

- Simplified retrieval of updates by the server
  StormShield servers' ability to retrieve their updates on remote servers will now be restricted to local folders and Windows shared folders. StormShield servers can no longer retrieve updates on FTP or HTTP servers. In the **Software Updates Settings** section in the server policy, the **Source type, Port, User name, Password** and **Remote path** parameters have been removed. The **URL/ Local path** parameter has been renamed **Updates download folder**. For more information, refer to the StormShield Administrator's guide.

- Apache updates
  The Apache web server has been upgraded to version 2.4.25. The update to this version requires running the command "skyapache.exe --update", as described in the StormShield Administrator's guide.

LIST OF FIXES IN STORMSHIELD V6.0.27

Agent fix:

- **[11556] (# CF 87486)** Random blue screen during kernel event monitoring
  Certain verifications performed as part of kernel event monitoring in the security policy could randomly cause a blue screen. These actions have been reviewed and corrected.

LIST OF FIXES IN STORMSHIELD V6.0.26

Agent fix:

- **[11258] (# CF 86869)** Compatibility of the StormShield agent with SimaPro 8.0.2
  Whenever the StormShield agent was installed on the same workstation as the SimaPro 8.0.2 software, an error displayed when launching SimaPro and it was not possible to use it. This issue has been fixed.

UPDATES IN STORMSHIELD V6.0.26

- **[11523/11525/11527]** OpenSSL upgraded to version 1.0.1u
  Vulnerabilities (CVE-2016-6304, CVE-2016-6306 and CVE-2016-2177) have been fixed by upgrading the OpenSSL cryptographic library to version 1.0.1u. Details on the vulnerability CVE-2016-6304 (OCSP Status Request extension unbounded memory growth) can be found on our website https://advisories.stormshield.eu/.

LIST OF FIXES IN STORMSHIELD V6.0.25

Agent fixes:

- **[10619]** Compatibility of the StormShield agent with Sophos antivirus
  Whenever the StormShield agent was installed on the same workstation as the McAfee encryption module (McAfee File and Removable Media Protection), a compatibility issue between both products could make the latter unstable. This issue has been fixed.

- **[10496]** Compatibility of the StormShield agent with Sophos antivirus
  Whenever the StormShield agent was installed on the same workstation as Sophos, certain applications would stop running. This random occurrence was caused by competing access between StormShield and Sophos during the installation of protection. This issue has been fixed.

UPDATES IN STORMSHIELD V6.0.25

- **[10642]** Automatic validation of temporary web access
  Whenever you create a shortcut on the user's desktop to request temporary web access ("/GrantWebAccess" argument added in the target of the shortcut to the executable file ssmon.exe), you can now add the option "/NoConfirm" in order to disable the web access confirmation window. Access will then be effective immediately.

- **[10600]** Display of the serial numbers of new licenses in the console
  For licenses that have serial numbers, they are now displayed in the license manager and in the license update menu.

- **[10726]** Libxml2 upgraded to version 2.9.4
  The libxml2 version that StormShield uses to manage XML files has been upgraded to version 2.9.4. Version 2.9.3 contained security flaws.

LIST OF FIXES IN STORMSHIELD V6.0.24

Agent fixes:

- **[10808]** Some Windows updates could not be installed on the workstation
  The StormShield agent could prevent Windows updates from being installed if the updates needed to access sensitive keys of the registry base. This issue has been fixed.

- **[10809]** Compatibility with TheGreenBow VPN Client
  The StormShield firewall and TheGreenBow VPN Client could be incompatible when the option of the VPN client Disable Split Tunneling was enabled. This issue has been fixed.

UPDATES IN STORMSHIELD V6.0.23

- **[10683]** OpenSSL updated to version 1.0.1t
  A vulnerability (CVE-2016-2107 - Attack against an AES CBC session implemented with AES-NI) has been fixed by upgrading the OpenSSL cryptographic library to version 1.0.1t. Details on this vulnerability can be found on our website https://advisories.stormshield.eu.

LIST OF FIXES IN STORMSHIELD V6.0.22

Agent fixes:

- **[9922] (# CF 86466)** Compatibility with TheGreenBow VPN Client
  TheGreenBow VPN Client (version 5.22 and upwards) did not run correctly when the SES Firewall feature was enabled on the agent. This issue has been fixed.

- **[9837] (# CF 86559)** Agent execution error
  Under certain circumstances, the corruption of the file Sigs.srn could cause an error during the execution of the agent (framework.exe). This issue has been fixed. A SIG_ERROR system log will be recorded in such cases.

Console fix:

- **[7800] (# CF 86636)** Reports filtered according to dates
  Filtering reports according to dates did not work. This issue has been fixed.

UPDATES IN STORMSHIELD V6.0.22

- **[10153]** Shortcut to temporary web access
  A shortcut can now be created on the user's desktop to quickly request temporary access to the web. You will need to create a shortcut to the executable file of the agent's graphical interface ssmon.exe on the desktop, then add the argument "/GrantWebAccess" as the target of the shortcut. This shortcut allows avoiding from going through the StormShield menu accessible from the system's status bar. For more information, refer to the StormShield 6.0 Administrator's guide.

- **[10152]** OpenSSL updated to version 1.0.1s
  OpenSSL has been updated to version 1.0.1s.

LIST OF FIXES IN STORMSHIELD V6.0.21

Agent fixes:

- **[9464]** Network filtering with several IP addresses
  In a configuration with a network interface bearing several IPv4 addresses, network filtering may fail to function correctly. This issue has been fixed.

- **[9476]** Agent/Server connection with a static route
  In a network configuration in which the agent workstation used a static route to contact the StormShield server, connections could not be set up. This issue has been fixed.

- **[9441]** Running applications from removable devices
  When the StormShield agent applied protection to control on running applications from removable devices, and it was disabled, applications could not be run from a removable device. This issue has been fixed.

- **[8972] (# CF 85869)** Chrome in 64 bits and StormShield
  The 64-bit version of the Google Chrome browser displayed an error message when it was installed with the StormShield agent. The issue occurred on all the supported 64-bit platforms (Windows 7 and Windows 8.1). This issue has been fixed.

- **[9405] (# CF 86122)** Installation of Prim'X Zone Central and StormShield
  The StormShield product's self-protection feature prevented the installation of Prim'X Zone Central. This problem is fixed.

UPDATES IN STORMSHIELD V6.0.21

- **[9751]** Libxml upgraded to version 2.9.3
  The version of libxml2 previously used (2.9.2) for managing XML files contained security flaws. The version used by StormShield is the most recent version to date (2.9.3).

- **[9712]** OpenSSL upgraded to version 1.0.1q
  The version of OpenSSL previously used (1.0.1p) contained a vulnerability that would potentially allow an attacker to cause a denial of service attack on the StormShield server. The version used by StormShield has been upgraded to version 1.0.1q.

LIST OF FIXES IN STORMSHIELD V6.0.20

Agent fixes:

- **[9183] (# CF 85358)** The agent cannot be installed on Hungarian Windows XP
  It was not possible to install the StormShield agent on the Hungarian version of Windows XP. The problem could also occur on versions of the operating system in other languages. This issue has been fixed.

- **[9137]** Warning message in the StormShield console about AVIRA license
  When synchronizing environments, the console displayed a warning message about the AVIRA antivirus license whereas the antivirus feature was not enabled on the server. This issue has been fixed.

- **[7397]** Issue when recovering from sleep mode
  When recovering from sleep mode, the workstation could freeze. This issue has been fixed.

- **[8955]** Error message when applying a file encryption policy
  When applying a file encryption policy, an error log was displayed if no letter was linked to a partition. This issue has been fixed.

- **[8577]** Issue when installing the antivirus program
  When installing the antivirus program, an error log was displayed because of an error of file copy. This issue has been fixed.

- **[8218]** Issue with file encryption
  When encrypting files, the workstation could freeze during processing. This issue has been fixed.

- **[9075]** Renaming of StormShield update file names
  When updating StormShield, the names of the update files downloaded by the agent are now in lowercase.

- **[8759]** Firewall logs and Ethernet filtering
  In the Firewall module, the log type displayed was false when a network connection was blocked at the Ethernet level (via source or destination MAC address). Now the adequate log of the type 'FW_MAC' is displayed.

- **[8888] (# CF 85872)** Slow workstation when opening the Windows session
  The workstation could be very slow because of the crash of one of the svchost processes.

- **[9201] (# CF 85838)** Incompatibility with McAfee
  On 64-bit operating systems, a BSOD occurred if McAfee Viruscan 8.8 Patch 6 was installed with StormShield. This issue has been fixed.
  On 32-bits operating systems, McAfee applications stopped unexpectedly. This issue has been fixed.

Server fix:

- **[8927] (# CF 85501)** Compliance of Syslog TCP with the RFC 6587
  Some commercial Syslog servers including the RSA server could perform a bad interpretation of logs because of a non-compliance of the Syslog emission on TCP. This issue has been fixed.

Console fixes:

- **[8551]** Logs duplicated in the Log Manager
  When logs were imported several times in the Manager, multiple copies were displayed. This issue has been fixed. A previous version of a log is now replaced by the new import.

- **[6698]** DBinstaller descriptions have been updated
  Some descriptions of features in the menus of DBinstaller were not up-to-date. This issue has been fixed.

- **[9194] (# CF 85716)** Crash of the console in ExtendedXP mode in Spanish and Portuguese
  An exception was thrown when the console was configured in ExtendedXP mode in Spanish and Portuguese. This issue has been fixed.

- **[9122]** Error when importing ExtendedXP policy templates
  Importing ExtendedXP policy templates could fail and no log was generated. This issue has been fixed.

UPDATES IN STORMSHIELD V6.0.20

- **[8308]** Apache server component updated to version 2.2.31
  The Apache server component installed with the StormShield server has been updated to version 2.2.31 in order to counter the vulnerability allowing an attacker to cause a denial of service.

- **[8859]** libxml2 library update
  There was a security vulnerability in the libxml2 library used for XML files management (configuration, policies, etc.). It has been updated to fix this issue.

LIST OF FIXES IN STORMSHIELD V6.0.19

Agent fixes:

•**[8332]** Incorrect update of the Firewall under 64-bit Windows 7
A regression has been introduced in version 6.0.17 and prevents the Firewall driver ('thor3.sra' file) from being correctly updated under the operating system 64-bit Windows 7.
If you want to update StormShield agents from this version, we recommend you to apply the steps as follows:

1. Update agents to version 6.0.18.
2. Then from version 6.0.18, update agents to version 6.0.19.

- **[8545] (# CF 85247)** Blue screen occurring when the workstation goes into sleep mode
In the Network security control tab of the security policy, when some Network Firewall rules were filtering on the MAC address, some workstations did not go properly into sleep mode. The shutdown could also be unusually long: a blue screen occurred and the computer stopped. This problem is fixed.
If you use filtering rules on MAC address, we recommend you to update to version 6.0.19.
Apply the following procedure on the impacted computers:

1. Deactivate all Network Firewall rules with MAC address filtering. You can create a "temporary" policy without MAC address filtering for these agents.

   If filtering on MAC address is defined in some Network Firewall accepting rules, some network services may not be accessible during the update process. You can then add additional accepting "IP address" rules.

2. Wait for all the machines to receive the new policy.
3. Restart the machines.
4. Update StormShield.
5. Activate the deactivated rules.

   If the procedure is not properly applied, a blue screen may occur during the update. In this case, restart the computer twice. The update will still be applied and the issue will be definitely fixed. If Microsoft Windows prompts to choose between normal restart, safe mode or system recovery, select normal restart.

   Workstations under Windows XP are not impacted. They can be normally updated.

- **[8301] (# CF 84778)** Deadlock on synchronization mechanisms
When applications used synchronization mechanisms on the workstation, a deadlock could occur when threads using these mechanisms stopped (for example applications using Mono or Unity3D). This problem is fixed.

- **[8283]** Reading and creating registry keys
When accessing a registry key, instabilities could occur under certain conditions: for example when the registry key was too long. This problem is fixed.

- **[8285]** Correction of the display of the executable file creation blocking log
  When the protection against executable file creation is enabled, now no log is sent when modifying the content of an executable file.

- **[8433]** Improvement of logs related to tokens
  Error logs displayed when exchanging tokens between the server and StormShield agents have been improved.

- **[8582] (# CF 85542)** Installing Avira antivirus on a Spanish operating system
  Now the Avira antivirus program is installed in English by default on workstations which system language is other than French.

- **[8634] (# CF 85259)** Correction of a IRQL_NOT_LESS_OR_EQUAL blue screen at machine startup
  A blue screen could happen randomly on some workstations under Windows XP.

- **[7954]** Registry keys protection
  When an applicative rule is enabled on a process concerning registry keys, the StormShield protection now stops creation and edition of keys which access is denied or of read-only keys.

- **[8702] (# CF 85696)** Compatibility between a VPN IPSec client and the StormShield firewall under 64-bit Windows 7
  Using the StormShield agent firewall (driver "thor3") and a VPN IPSec client at the same time on the same workstation under 64-bit Windows 7 could not always work. The StormShield firewall incorrectly filtered incoming packets such as UDPENCAP (encapsulation of the ESP protocol in UDP packets source/destination ports 4500). As a consequence, network flows routed by a VPN IPsec tunnel were not functional. This problem is fixed.

- **[6902]** Internet Explorer version 11 blocked
  It is now possible to block iexplore.exe version 11 thanks to network applicative rules.

Server fix:

- **[8748] (# CF 85597)** Management of log cache files enhanced
  Log cache files incorrectly formatted are now properly managed on the StormShield server.

Console fixes:

- **[8322]** Incorrect search in a log filter
  When filtering software, system, network or device logs in the **Log Monitoring** panel with the method "contains" in the **Comparison** field, the search did not find logs if the filter "Value" contained the character [_]. This problem is fixed.

- **[8254]** RootCA certificate import in the Internet Explorer certificate store
  When the console and the StormShield server synchronized for the first time, the 'RootCA' certificate was imported in the Windows/Internet Explorer certificate store. If an error occurred, the console/server synchronization did not work. This problem is fixed: the 'RootCA' certificate is no longer imported during the first synchronization.

- **[8534]** Support of special characters in the antivirus policy
  The antivirus policy now supports special characters in the **Paths to scan** and **Files to scan** fields.

- **[7571]** Checking the parent relationship of servers certificate
  When synchronizing the StormShield administration console and servers, the root authority of the servers certificate is now compared to the root authority of the administration console certificate in order to check the parent relationship.

- **[7398]** Checking in encryption, antivirus and agent configuration policies
  It is now possible to check in an encryption, antivirus and agent configuration policy when the user owns a role with the following permissions: environment control, security policies management, global security policy management and encryption policies management.

UPDATES IN STORMSHIELD V6.0.19

- **[8777]** OpenSSL update
  OpenSSL has been updated to version 1.0.1p.

- **[8257]** cURL update
  cURL has been updated to version 7.42.1.

- **[8312]** SQLite update
  Security vulnerabilities have been disclosed about SQLite. SQLite has been updated to version 3.8.10.2 in order to block these vulnerabilities.

- **[8543]** Update of the protection of files located at the root of the installation folder
  Some executable files, libraries and folders were not protected by the modlockfile protection at the root of the StormShield server and agent installation folders. Now the protection is up to date.

LIST OF FIXES IN STORMSHIELD V6.0.18

Agent fixes:

- **[8174]** OpenSSL library updated to version 1.0.1m
  In order to fix the recently discovered security vulnerability CVE-2015-0286, the OpenSSL library used by StormShield (agent, server and Apache server) has been updated to version 1.0.1m. This vulnerability is described in the STORM-2015-002 security advisory.

- **[7843] (# CF 83862)** Blue screen because of high network load
  In some particular conditions and when other security software is installed on the workstation, a blue screen could occur in the Microsoft tdx.sys driver. The StormShield driver component "baldr.sra" is one of the drivers loaded when the problem occurs. It has been modified in order to fix the problem.

- **[7865] (# CF 84101)** Firewall - Stateful TCP controls
  In some cases, the Stateful TCP analysis of TCP flows could abnormally block network packets. This problem is fixed.

- **[7892] (# CF 84562)** Agents starting very slowly with some Active Directory configurations
  In some configurations of the Active Directory, especially with an AD in WAN, the agent could take a lot of time to start. This problem is fixed.

- **[8010] (# CF 85047)** Silent crash of some applications
  Some protected processes (such as `audiodg.exe`) could stop while there were launching. This problem is fixed.

- **[7752] (# CF 84002)** Uninstalling the antivirus program only was not possible
  The `conf.srx` configuration file could not be loaded when uninstalling the antivirus program only. This problem is fixed.

- **[8023] (# CF 84332)** Crash of Word/Excel with PGP software if the Honey Pot protection is enabled
  When the Word/Excel application and other MS Office products started while the Honey Pot protection was enabled and the PGP software installed, the PGP initialization made the application crash. This problem is fixed.

- **[8051]** Agent configuration localization not applied
  In some cases, the agent did not update the language of the interface after applying policies successively modifying the language. This problem is fixed.

- **[8111]** Management of pages assigned to the Honey Pot
  The vulnerability detection module has been improved in order to manage new cases of heap spray on memory allocation.

- **[7796] (# CF 81907)** Auto-blocking of a 32-bit and 64-bit process on 64-bit OS
  In the situation where a running process is allowed to run itself whereas a protection prevents executables from starting, some cases did not work properly on 64-bit operating system. Rules about the Internet Explorer browser require explicitly allowing its executables (32 and 64 bits).

- **[7457]** libxml2 library update
  There was a security vulnerability in the libxml2 library used for XML files management (configuration, policies, etc.). It has been updated to version 2.9.2 to fix this issue.

Server fixes:

- **[8174]** OpenSSL library updated to version 1.0.1m
  In order to fix the recently discovered security vulnerability CVE-2015-0286, OpenSSL library used by StormShield (agent, server and Apache server) has been updated to version 1.0.1m. This vulnerability is described in the STORM-2015-002 security advisory.

- **[7457]** libxml2 library update
  There was a security vulnerability in the libxml2 library used for XML files management (configuration, policies, etc.). It has been updated to version 2.9.2 to fix this issue.

Console fix:

- **[8179] (#CF 84943)** Error when merging agents in the agent control panel
  Sometimes agents merger did not work. This problem is fixed.

LIST OF FIXES IN STORMSHIELD V6.0.17

Agent fixes:

- **[7414] (# CF 84210)** Excel plug-in loading error
  The Microsoft Excel plug-in "SAP BusinessObjects Extended Analytics Analyzer" did not load and could cause an "Overflow" error when the "Overflow" protection was enabled.
  This problem is fixed.

- **[7601] (# CF 83463)** Network connections blocked on workstations with StormShield agent
  The IDS ARP protections of the Firewall module could temporary block network connections on workstations provided with Windows 7 operating system and a StormShield agent. This problem is fixed.

- **[7449]** OpenSSL update
  StormShield used the 1.0.0m version of OpenSSL. Now the StormShield agent uses the 1.0.1j version. The TLS 1.2 protocol and the cipher suite TLS_RSA_WITH_AES_256_CBC_SHA are used for the communication between agent and server 6.0.17.
  To make the StormShield update easier, agents are still able to connect to StormShield servers in previous versions thanks to the SSL V3 protocol. The SSL V3 support will be disabled in a next version.

Server fix:

- **[7449]** OpenSSL update
  StormShield used the 1.0.0m version of OpenSSL. Now the StormShield server and the associated Apache server use the 1.0.1j version. The TLS 1.2 protocol and the cipher suite TLS_RSA_WITH_AES_256_CBC_SHA are used for the communication between agent and server 6.0.17.
  The SSL V2 and SSL V3 protocols are disabled on the Apache server which communicates with TLS 1.2 with all the clients which support TLS.
  To make the StormShield update easier, servers are still able to communicate with StormShield agents in previous versions thanks to the SSL V3 protocol. The SSL V3 support will be disabled in a next version.

> The StormShield server update does not imply the Apache server configuration update. You need to manually apply the update by executing the file `skyapache.exe --update` in `Program Files> SkyRecon>StormShield Server>Apache>conf` from an administrator command line. The former configuration files are renamed `httpd.conf.old` and `ssl.conf.old`. Restart the StormShield server to take these modifications into account.

Console fix:

- **[7640]** Synchronizing the server could fail
  Since StormShield supports TLS, the connection between the management console and the StormShield server when synchronizing the environment could regularly fail. This problem is fixed.

UPDATES IN STORMSHIELD V6.0.17

- **[7672]** Update process
  The update process has changed and allows updating the 6.0 version to a future version without risk of degrading the workstation security when it will restart with the new version installed.

- **[7677]** The Certificate conversion option has been removed
  The menu **Certificate conversion** has been removed in the StormShield management console. As a consequence, the openssl.exe binary file is no longer installed with the console.

LIST OF FIXES IN STORMSHIELD V6.0.16

Agent fixes:

- **[7177] (# CF 83998)** BSOD when starting StormShield agent under Windows 7 64 bits
  A BSOD could occur after an installation or a modification of the workstation configuration (drivers installation or update). This BSOD then constantly recurred. This problem is fixed.

- **[7269]** Vulnerability allowing the StormShield agent to be stopped
  A security vulnerability allowed stopping the StormShield agent via the Windows Service Manager. This problem is fixed.
  For more information, refer to security advisory AKSB-2014-01-FR-STM-SVC.pdf.

- **[7305]** The StormShield agent stopped when installing an update
  A regression has been introduced in version 6.0.15. This regression allowed stopping the agent when an update was installed. This problem is fixed.

- **[7241]** Kernel API not protected under Windows 7 32 bits
  Under Windows 7 32 bits, the NtOpenKeyEx Kernel API was not protected and could allow a malware to modify the registry. This problem is fixed.

- **[7246]** Renaming a registry key impossible in Warning mode
  In Warning mode, it was not possible to rename a key if the key source name or destination name was protected by StormShield. This problem is fixed.

- **[7201]** Registry protection fixed in applicative rules
  The behavior of the protection could be unpredictable and not easy to understand. This problem is fixed. See section "Updates in StormShield V6.0.16", page 43.

- **[7327] (# CF 84002)** Uninstalling Avira antivirus
  In some cases, uninstalling Avira antivirus could not work when uninstalling the StormShield agent. This problem is fixed.

- **[7396]** Protection against buffer overflow fixed
  On a 32-bit operating system and in some cases only, the RCP option of the protection against buffer overflow was not properly initialized. As a consequence, the protection could not be efficient with some processes. This problem is fixed.

- **[7483]** Ability to stop the agent with an altered StopAgent
  A regression has been introduced in version 6.0/15 and allowed stopping the StormShield agent with an altered StopAgent.exe. This problem is fixed.

Server fixes:

- **[7285]** TRACE HTTP method disabled in the Apache server provided with the StormShield server
  This HTTP method is not used by StormShield because when enabled, false positives could occur during audits by vulnerability scanners (with Nessus software for example). It is thus disabled in the Apache/StormShield server configuration.

  

  The StormShield server update does not imply the Apache server configuration update. You need to manually apply the update by executing the file `skyapache.exe --update` in `Program Files> SkyRecon>StormShield Server>Apache>conf` from an administrator command line. The former configuration files are renamed `httpd.conf.old` and `ssl.conf.old`. Restart the StormShield server to take these modifications into account.

- **[7475]** Use of the protocol TLSv1.0
  In order to reinforce the security of communications between the server and agents or consoles, the protocol TLSv1.0 has been implemented to replace the protocol SSLv3. However, in order to maintain backward compatibility during the transition period between both protocols, it is still possible to use SSLv3. StormShield can thus be a victim of the Poodle vulnerability. This backward compatibility will be removed in a future update version.
  For more information, refer to security advisory STORM-2014-02-EN.

Console fixes:

- **[7180] (# CF 84094)** Administrator rights on the database
  Administrator rights on the database could be mistakenly granted to a normal user of the StormShield console. This problem is fixed.

- **[7316] (# CF 84226)** Counting the number of StormShield agents allowed in the license
  Server-Side agents were not recorded in the number of agents allowed by the StormShield license. This problem is fixed. The number of agents allowed is now the sum of the Secure, Professional and Server-Side agents.

- **[7140] (# CF 83883)** ExtendedXP console is slow when there are many logs
  The ExtendedXP console dashboard could slowly display when there were many logs in the database. This issue has been fixed.

- **[7361]** English log for Overflow/HEAP BLK blocking process fixed
  The term "stack" has been replaced by "heap" in the English log indicating the system blocking process of the type "Overflow/Heap Blk".

- **[7340]** Improvements on the ExtendedXP console
  The following improvements have been made to the ExtendedXP console:
  - Translation of contextual menus and submenus in the **Monitoring** panel.
  - Improvement of the display of the number of log pages in the **Monitoring** panel.
  - Improvement of the behavior of the search field in the **Monitoring** panel.

- **[7136]** ExtendedXP rules import
  When importing ExtendedXP rules with the format *sczip*, rules groups were imported in alphabetical order. The rules group "Microsoft Windows", which can contain general rules, is now located at the end of the list and its rules are analyzed last.

- **[7214]** Console update
  The update program of the StormShield console was not provided in the update package. This problem is fixed.

- **[7212]** OpenSSL 1.0.0m update for the Apache server and the StormShield console
  The latest version of OpenSSL used by the Apache server and the StormShield console was not provided with a server or a console update. This issue did not have any functional impact but it is now fixed.

- **[7438] (# CF 84390)** Removable devices list fixed
  The removable devices dashboard in the security policy could display an empty list whereas USB devices had been added. This problem is fixed.

UPDATES IN STORMSHIELD V6.0.16

- **[7201]** Registry protection fixed in applicative rules
  The management of the registry access protection in applicative rules has been improved.
  Now:
  - To control the access to a key or a specific value, the whole path must be entered. For example:
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Help\v1.0\BrandingInfo\vs_100_fr-fr
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer
  - To control the access to values and subkeys of a key, the base key path must be entered followed by the wildcard character "*". For example:
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft*

  To control a key and its subkeys, both types of rules must then be used. For example:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows*

LIST OF FIXES IN STORMSHIELD V6.0.15

Agent fixes:

- **[6720]** Vulnerability CVE-2014-0139 fixed
  The cURL library used by StormShield has been updated to version 7.36.0 in order to fix the vulnerability CVE-2014-0139.

- **[6994] (# CF 83601)** AVIRA antivirus cannot be downloaded from the StormShield server
  Due to the Windows security policies defined by the administrator, the StormShield agent was not always able to download the Avira setup program. This problem is fixed.

- **[7000] (# CF 83463)** Network connections blocked on workstations with StormShield agent
  The IDS ARP protections of the Firewall module could temporary block network connections on workstations provided with Windows 7 operating system and a StormShield agent. This problem is fixed.

UPDATES IN STORMSHIELD V6.0.15

- **[6847] (# CF 83204)** Avira user configuration merged with StormShield antivirus configuration
  Configuring options in Avira administration console and keeping this configuration is now possible after synchronizing the Antivirus policy defined in StormShield. Only the settings not supported by StormShield are kept. The settings supported by StormShield overwrite the settings defined by the user.

- **[6985]** OpenSSL library updated to version 1.0.0m
  OpenSSL library used by StormShield (agent, server and console) has been updated to version 1.0.0m to fix recent security vulnerabilities. No security advisories have been published for these vulnerabilities which have been considered as minor.

- **[7040]** Update process
  StormShield agents update process has been completely revised. Agents update is now faster (between 5 and 15 seconds versus more than 2 minutes before) and more reliable thanks to direct communication between the different components involved in the update.

UPDATE AND FIXES IN STORMSHIELD V6.0.14

Update:

- **[6951]** ExtendedXP administration mode added to the StormShield console
  A new simplified administration interface has been added to the StormShield administration console. This interface is for use by the ExtendedXP service's customers. For more information, refer to the StormShield 6.0 Administrator's guide.

Agent fixes:

- **[6866] (# CF 83166)** Error logs improved for Agent/Server SSL connections
  In some error cases, logs dealing with SSL connections between agents and servers were not complete (empty string). This issue has been fixed.

- **[6890]** Connection of the agent to the StormShield server to check for updates
  When looking for updates availability, an agent could connect to the invalid IP address 0.0.0.0. This blocked the update process. This issue has been fixed.

- **[6842] (# CF 82967) and [6966] (# CF 83470)** BSOD when connecting a removable device
  When connecting a USB removable device, a BSOD could occur either randomly or because of the software environment. This issue has been fixed.

- **[6935] (# CF 83073)** Memory leak when the operating system is installed in c:\WINNT
  If the StormShield agent was installed on an operating system located in c:\WINNT, an error when loading the applicative rules file caused a memory leak. The workstation could not be used then. This issue has been fixed.

Server fix:

- **[6927] (# CF 83467)** StormShield server crash
  A regression has been introduced while improving logs insertion in database. The StormShield server was not working properly because of this regression. This issue has been fixed.

LIST OF FIXES IN STORMSHIELD V6.0.13

Agent fixes:

- **[6467] (# CF 82398)** Modules display issue when debugging a process
  A problem preventing modules loading events (DLL) from being displayed when debugging a process is fixed.

- **[6479] (# CF 82252)** Unusually high usage of the CPU by ssmon.exe
  A problem made a ssmon.exe thread be played in a loop indefinitely. As a consequence, the thread consumed many CPU resources. This issue has been fixed.

- **[6518] (# CF 80745)** Network connections blocked on workstations with StormShield agent
  In some cases, the IDS ARP protections of the Firewall module could temporary blocked network connections on workstations provided with a StormShield agent. This issue has been fixed.

- **[6566] (# CF 82622)** Driver corruption message display
  When the kernel components protection was enabled, in some cases the protection could indicate the corruption of some drivers (such as `vga.sys`). This issue has been fixed.

- **[6556]** .cpl extension added to the protected extensions list
  The extension `.cpl` has been added to the list of the extensions blocked by the setting "Executable file creation" in the security policy. This extension is blocked for the level "High" and "Critical".

- **[6645] (# CF 82988)** BSOD when opening a process
  On a workstation with the StormShield agent, when any process opened another process and tried to duplicate a resource from this process whereas it had just ended, a BSOD occurred. This problem is fixed.

- **[6734] (# CF 83101)** Wi-Fi was not blocked
  Under Windows XP, Wi-Fi connections could go through if no network rule was applied. This problem is fixed. This was a regression introduced in version 6.0.07.

- **[6789] (# CF 83048)** BSOD when opening files
  On a workstation with the StormShield agent, when any process tried to access a file, a BSOD could occur. This problem is fixed.

Server fixes:

- **[6729] (# CF 83115)** SQL server overload
  A new log about removable devices activities stored on the database could overload the SQL server if the database already contained many logs. This problem is fixed.

- **[6674]** Apache server component updated to version 2.2.27
  In order to fix the vulnerability CVE-2014-0098, the Apache server component installed with the StormShield server has been updated to version 2.2.27.

Console fixes:

- **[5632] (# CF 82420)** Sorting by date in the devices enrollment window is not working
  When the user wanted to sort enrolled removable devices by date, they were sorted out according to their alphabetical order and not to their chronological order. Sorting by date is now functional.

- **[6516]** Improvement of logs merger in the console
  The speed of the logs merger in the console manager has been improved. Now it is faster to merge logs according to criteria such as the host name or the AD identifier.

- **[6352, 6699]** DBInstaller cannot be used with MS SQL 2012
  It was not possible to use the database maintenance features provided by DBInstaller when using a MS SQL 2012 server.

UPDATES IN STORMSHIELD V6.0.13

- **[6654]** Improvement of logs merger in the database
  The StormShield server has been modified to improve logs merger in the database on SQL 2008 servers or higher versions with several processors. This improvement requires a standard or enterprise version of SQL Server. It does not apply to SQL Server Express and SQL Server 2005.

- **[6524]** Temporary storage of logs on files
  The StormShield server temporarily stores logs on files. This applies to logs waiting to be merged in the database. In case of unexpected shutdown of the server, pending logs are thus no longer lost.
  These files are stored in the sub-folder: "`Log\Cache`" in the StormShield installation directory. According to the security policies applied to agents, you may need to keep a few gigabytes of available disk space for these files.

LIST OF FIXES IN STORMSHIELD V6.0.11

Agent fixes:

- **[6099] (# CF 82000)** Autoencryption of the standalone encryption application (SURT)
  When an encrypted USB key containing the SURT encryption application was connected to a workstation protected by a StormShield agent without encryption policy for removable devices, the file `surt.exe` on the key was encrypted because of a bug. The SURT application became then unusable on a workstation without StormShield. This issue has been fixed.

- **[6071]** Crash of the framework.exe application when connecting a removable device
  The `framework.exe` application crashed when connecting a removable device. This issue has been fixed.

- **[6107] (# CF 81907)** Applications freezed if accessing .exe was not authorized
  A bug prevented an application from opening its own binary file. As a consequence, on Windows 7, some applications such as `iexplore.exe` could not restart, which could make the application close. This issue has been fixed.

- **[6126]** Flaws allowing the main application of the framework.exe agent to be stopped
  Two flaws enabled the voluntary shutdown of the `framework.exe` agent application. This issue has been fixed. For more information, refer to security advisories AKSB-2013-03-EN-STM-JOB.docx and AKSB-2013-04-EN-STM-X64.docx.

- **[6002] and [5984]** Workstation random crash
  Two bugs could occur randomly and make the workstation crash. This issue has been fixed.

- **[6203]** Dump file not correctly written when a BSOD occurred on Windows 7 64 bits
  A bug prevented the Dump file from being written when a blue screen occurred on Windows 7 64 bits. This issue has been fixed.

- **[5880]** Accesses to removable devices blocked when the agent is disabled
  A bug prevented to access files on a removable device when the agent had been explicitly stopped with `StopAgent.exe`. This issue has been fixed.

- **[6250]** Compatibility with the different access methods to files improved
  A better management of access methods to files has been implemented in order to improve the security of the application control module.

- **[5934] (# CF 79498)** Freeze after a change of the encryption password in SSO mode
  A bug blocked the user on the connection window at Windows start-up if the surface encryption password in SSO mode had been changed. This issue has been fixed.

- **[5989] (# CF 82161)** Bug fix on the network section of applicative rules
  On 64-bit operating systems, application network rules did not block the flow as expected. This issue has been fixed.

- **[5875]** Incorrect flows filtering in hotspot mode "Temporary web access"
  A bug made all TCP and UDP ports open when using a temporary Internet access. This issue has been fixed. Now, only ports defined in the administration console are authorized.

- **[6246]** Security of agent/server communications improved
  Under certain conditions, when the communication is established between the agent and the StormShield server, a bug about the use of SSL tunnel certificates could occur. This issue has been fixed.

Server fixes:

- **[5972] (# CF 81293)** Compatibility with syslog protocol improved
  The date format of emitted syslog messages has been improved in order to enhance compatibility with syslog servers.

- **[6214]** Overloaded servers during agents initialization
  When massively deploying StormShield agents, the server could be overloaded by certificates generation requests (generation is executed during the agent initialization). This issue has been fixed.

Console fixes:

- **[5808]** Connection error to the database during bases backup in the DBInstaller application
  A connection error to the database during bases backup in the DBInstaller application is fixed. This error occurred when the user chose to connect using the Windows authentication.

- **[6141]** Memory overflow when entering a password in the proxy configuration fixed
  In the antivirus configuration of an "Agent" policy, the maximum length of the proxy password must not exceed 39 characters in order to match the limit imposed by the configuration interface of Avira Antivirus 2013.

- **[6065] (# CF 82018)** Error in retrieving the serial number of some USB removable devices
  A problem with reading identification information of USB removable devices is fixed in the console and on the StormShield agent. Devices which vendor ID includes the special character "_" are now supported.

UPDATES IN STORMSHIELD V6.0.11

- **[5886]** Modification of the extension of console policies files
  The console now exports and imports policies with the extension `*.scep` (StormShield Console Exported Policy) by default in order to be directly identified when importing policies in the version 6.0 of StormShield. It is still possible to export and import policies and configurations with the extension `*.srxml`.

- Ret-to-Libc protection
  The Ret-to-Libc (RCP) protection is now functional for 32-bit applications on 64-bit operating systems.

LIST OF FIXES IN STORMSHIELD V6.0.10

Agent fixes:

- **[5877] (# CF 81705)** Random blue screen (BSOD) caused by the odin-sys driver
  In the StormShield driver `odin-sys.sra` (removable devices encryption management), a bug could randomly engender a BSOD. This issue has been fixed.

- **[5817]** Full disk encryption impossible on 64-bit operating systems
  A bug introduced in version 6.0.09 prevented the implementation of full disk encryption on 64-bit operating systems. This issue has been fixed.

- **[5962]** Vulnerability in the Microsoft Detours library
  The fix of the vulnerability discovered in the Microsoft Detours library has been inteThe vulnerability allowed an attacker to run malicious code if Ret-to-lib-C (RCP) or Copy/Paste protection was enabled.grated into StormShield. The vulnerability allowed an attacker to run malicious code if Ret-to-lib-C (RCP) or Copy/Paste protection was enabled.
  For more information, refer to security advisory AKSB-2013-02-EN-STM-DETOURS.PDF

- **[6043]** Disk decryption impossible
  When uninstalling the StormShield agent, a bug introduced in version 6.0.09 prevented disk decryption. This issue has been fixed.

LIST OF FIXES IN STORMSHIELD V6.0.09

Agent fixes:

- **[5691] (# CF 80810)** Access blocked when browsing a USB key
  When the default access to removable devices was set to **Denied**, browsing the structure of a USB key was impossible. This problem impacted Windows Vista and higher versions of Windows. This issue has been fixed.

- **[5673] (# CF 80768)** Isolation of a workstation when using network firewall rules with MAC addresses
  When one of the network firewall rules included a MAC address, all incoming and outgoing connections of a workstation could be blocked. This issue has been fixed.

- **[5679]** Access to .srx files impossible outside the StormShield agent directory
  Access to `.srx` files located outside the StormShield agent directory was not possible. To allow an application access `.srx` files, it is now possible to add an extension rule for the `.srx` extension in the **Extension Rules** category of the security policy and specify applications allowed to open `.srx` files in **Application**.

- **[5416] (# CF 79148)** Blue screen (BSOD) in the Ret-Lib-C protection against memory overflow
  A BSOD could display in the Ret-Lib-C protection against memory overflow. This occurred when the Windows DEP protection was disabled on the machine (`/noexecute=Alwaysoff` in the `boot.ini` file). This issue has been fixed.
  For more information, refer to **http://support.microsoft.com/kb/875352**.

- **[5662] (# CF 80999)** cycle.srn file corrupted
  The StormShield agent was unable to manage the `cycle.srn` learning file when it was corrupted. This issue has been fixed.

UPDATES IN STORMSHIELD V6.0.09

- **[5786]** Implementation of a specific channel for log upload
  - Log upload is now performed on the secured TCP port 16004. If port 16004 is not accessible, logs are uploaded on the secured TCP port 16005.
  - Log upload periods are now managed via the new **Logs upload period** parameter of the server configuration.
  - The policy update time still relies on the **Token refresh time** parameter. When tokens are refreshed, new policies are updated, if necessary. If the server cannot contact the clients, after a period equivalent to twice the token refresh time, the clients contact the server in order to update their policies.

- **[5579]** Secure communication between the software part and StormShield drivers
  To improve the robustness of the StormShield agent, communication between the software part and the StormShield drivers has been secured.

- **[5620]** Improvement of the Agent Monitoring panel
  Several internal fixes have been implemented in the Agent Monitoring panel in order to improve the fluidity in the presence of thousands of agents.

LIST OF FIXES IN STORMSHIELD V6.0.08

Agent fixes:

- **[5482] (# CF 78519) (# CF 80342)** USB 3.0 controllers support
  USB 3.0 controllers are now supported on 32 and 64-bit versions of Windows 7 operating system.

- **[5479] (# CF 80182)** Inactivity of StormShield when SURT starts
  In some configurations, the StormShield agent remained idle when the SURT application started at user connection. This issue has been fixed.

- **[5541] (# CF 80884)** Network connection lost if no firewall rule is defined in StormShield
  When no firewall rule was defined in StormShield and if other firewall software were installed on the workstation, the network connection could be lost. This problem started in version 6.0.07 and is fixed. x

Server fixes:

- Limitation of connections to the StormShield server
  The number of connections from a same IP address to the StormShield server was limited to 10. This number is now unlimited.

- **[5547]** Apache server update
  The `mod_rewrite` module has been removed from the StormShield Apache server configuration after a security vulnerability has been discovered. For more information, see Security Bulletin CVE-2013-1862.

  

  The StormShield server update does not imply the Apache server configuration update. You need to manually apply the update by executing the file `skyapache.exe --update` in `Program Files> SkyRecon>StormShield Server>Apache>conf` from an administrator command line. The former configuration files are renamed `httpd.conf.old` and `ssl.conf.old`. Restart the StormShield server to take these modifications into account.

- **[5574]** SQL installation without SA account
  The installation of the StormShield server and the maintenance of the SQL database (via DBInstaller) without SA account is now possible when choosing the Windows authentication.

  

  When maintaining the database (DBInstaller) with the Windows authentication, the user running `DBInstaller.exe` needs to have the database administration privileges. Contact your database administrator.

  

  When installing the SQL server with the Windows authentication, the SA account is automatically deactivated and renamed.

UPDATES IN STORMSHIELD V6.0.08

- **[5431]** Scalability
  The maximum limit for the number of simultaneous connections to a server is increased from 100 to 1000.

  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).

- **[5545]** Visual C++ 2008 redistributable packages update
  Ressources provided with StormShield include the Microsoft Visual C++ 2008 SP1 redistributable packages.

  These redistributable packages are not automatically installed when applying the 6.0.08 patch. You need to manually install them on the StormShield servers and consoles. If you are installing the 6.0.08 version, these redistributable packages are automatically installed.

- **[5504]** Compatibility with MS SQL Server 2012 databases
  The MS SQL Server 2012 databases are now supported by StormShield.

- **[5581]** Confirmation request for executing a program on a removable device
  The new parameter **Execution control on removable device** is available in the security policy. If it is enabled, a confirmation is requested from the user when an application starts from a removable device.

The confirmation message to the user can be customized. In **Log Manager**, choose the type **System Logs** and edit the notification message of the lines (#.)?EXE_ON_USB BLKEXECUTE and (#.)?EXE_ON_USB WARN. The message will display in the confirmation window on the agent. If the user accepts the execution of the program, a warning log is created. If the user rejects the execution, an information log is created.

VARIABLE	KEYWORD	DESCRIPTION
	EXE_ON_USB	Execution of an application from a removable device. Possible values about the context of approval or denial of the execution of the application in the **Option** column under **Log Monitoring > System** are: **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 launched for example), the execution of the application has been automatically denied.

To properly enable this new feature, it is necessary to update the log database once the server and the console have been updated.

To do so: start the application `c:\Program Files\SkyRecon\SkyRecon Management Console\DBInstall\DbInstaller.exe`, and then use the "Configuration database maintenance" tool. Enter the configuration database password, choose the "Update" operation and follow the wizard instructions.

LIST OF FIXES IN STORMSHIELD V6.0.07

Agent fixes:

- **[5303] (# CF 79968)** Random crash of the framework.exe process when the Kernel component protection is enabled
  When the Kernel component protection was enabled, the framework.exe process unexpectedly ended soon after the workstation started and in some configurations of the user workstation.

- **[5301]** Crash of the framework.exe process when restarting the workstation after the installation
  The framework.exe process unexpectedly ended when restarting the workstation after installing the agent.

- **[5343] (# CF 80055)** Crash of the StormShield agent when applying new encryption policies
  The framework.exe process unexpectedly ended when scanning files to apply encryption policies if new empty files only were found.

- **[5423]** Check of the patches files improved
  Verif_patch.exe was untimely called in order to check the integrity of update files. This issue has been fixed.

- **[5458]** Random blue screen (BSOD) after patch installation
  On 32-bit systems (except Windows XP), a BSOD could occur after installing a patch before restarting the workstation. This issue has been fixed.

- **[5380] (# CF 80010)** Fix of the blackscreen at session login
  The StormShield firewall is now deactivated if no firewall rule is defined in StormShield network policies.

UPDATE IN STORMSHIELD V6.0.07

- **[5428]** New antivirus version
  The antivirus has been updated to use the Avira 2013 engine.

  Before updating the StormShield server, it is necessary to stop and disable the "Avira Security Management Center Internet Update Manager" service.

  When installing the antivirus on the agent, you need to restart the workstation twice. When updating the agent, you need to restart the workstation three times. StormShield asks the user to restart the workstation at the relevant times.

LIST OF FIXES IN STORMSHIELD V6.0.06

After replacing the SkyRecon Systems certificate in February 2013, the workstation needs to be restarted twice in order to complete the installation of the StormShield agent update. A pop-up window indicates you need to restart.

Agent fixes:

- **[5167] (# CF 78532)** Impossible to define firewall rules on ethernet frames on Vista workstations and higher
  Firewall rules on ethernet frames (rules on MAC addresses, on the ethernet protocol and on the integrity check at the ethernet level) were not taken into account on workstations under Microsoft Windows Vista and higher versions. The protection now works.

- **[5102] (# CF 78593)** Impossible to encrypt a USB key with BitLocker
  On a workstation protected by StormShield, it was impossible to encrypt a USB device with Bitlocker ToGo. This issue has been fixed.

BitLocker toGo encryption is not compatible with StormShield file encryption neither with the enrollment mechanism.

- **[5178] (# CF 79154)** Full disk encryption impossible on some laptops
  Full disk encryption did not work on some laptop models. This issue has been fixed.

- **[5240] (# CF 78548)** StormShield blocked with 3.XXOldConfiguration
  In some cases, the workstation equipped with StormShield applied the 3.XXOldConfiguration configuration and no network access was possible. This issue has been fixed.

After restarting the workstation, it is necessary to be connected to the StormShield server for the right configuration to be applied again.

LIST OF FIXES IN STORMSHIELD V6.0.05

Agent fix:

- **[5049] (#CF 78562)** Problem when mounting a USB key
  On a workstation protected by StormShield, StormShield did not allow the correct mounting of "mass storage" USB keys if a SD cards reader or equivalent was connected to the USB interface. This problem when mounting USB keys could result in "black screens". This issue has been fixed.

LIST OF FIXES IN STORMSHIELD V6.0.04

Server fix:

- **[4940]** Apache server update
  Apacher server version 2.0.64 has been updated to version 2.2.22. The new version fixes different security vulnerabilities: CVE-2011-3192, CVE-2011-3368 and CVE-2011-0419.

> The StormShield server update does not imply the Apache server configuration update. You need to manually apply the update by executing the file "skyapache.exe --update" in Program Files> SkyRecon>StormShield Server>Apache>conf from an administrator command line. The former configuration files are renamed httpd.conf.old and ssl.conf.old. Restart the StormShield server to take these modifications into account.

LIST OF FIXES IN STORMSHIELD V6.0.03

Agent fixes:

- **[2606] (#ETU-64389-614)** Multiple firewalls support on 64-bit versions of Windows
  On a workstation protected by StormShield under 64-bit Windows OS, traffic rules prevented the possible rules defined by other firewalls from being applied. Rules from all firewalls of the system are now taken into account when filtering network frames.

- **[2601] (#FLY-75562-903)** Blue screen (BSOD)
  On a workstation protected by StormShield, in some cases, applying file encryption could cause a BSOD. This issue has been fixed.

- **[2588] (#CKV-39291-875)** sr footprint file deletion
  When revoking an enrolled USB device, the sr footprint file located on the enrolled device was not deleted. The file is now deleted if the device is connected to the workstation performing the revocation.

LIST OF FIXES IN STORMSHIELD V6.0.02

Agent fixes:

- **[2574] (# DSY-93056-101)** Full disk encryption on 64-bit systems
  The full disk encryption did not correctly apply on 64-bit systems. In this case, an alert of the "error" type was reported during the full disk encryption and the encryption password was systematically requested when activating the agent. This problem is fixed.

- **[2573] (# MOQ-70740-360)** Multicast traffic stopped
  On a workstation protected by StormShield, the multicast traffic generated by an application was not received by the host machine. StormShield now authorizes a workstation to receive its own multicast traffic.

COMPATIBILITY BETWEEN WINDOWS® VERSIONS AND STORMSHIELD

Here are the Windows versions which are compatible with **StormShield 6.0**:

WINDOWS	PROFESSIONAL EDITION	SECURE EDITION	SERVER-SIDE EDITION	AVP OPTION
XP SP3 - 32bits	✓	✓	-	✓
7 SP1 - 32bits	✓	✓	-	✓
7 SP1 - 64bits	✓	✓	-	✓
Server 2003			✓	
Server 2008 R2	-	-	✓	-

Tableau 1.1 : Compatibility between Windows versions and StormShield

UNSUPPORTED HARDWARE AND SOFTWARE DURING DISK ENCRYPTION

The unsupported hardware and software during disk encryption are the following:

- Software RAID and dynamic disks.
- Partition management and disk cloning tools.
- Hard drives with sector size other than 512 bytes.
- Extended partitions are not supported by full disk encryption. Only disks containing primary partitions can be encrypted.
- Multiboot (several operating systems on the same partition or on two separated partitions) is not supported by disk encryption.
- Boot loaders other than Microsoft Windows boot loader are not supported by disk encryption.

KNOWN INCOMPATIBILITIES

Known incompatibilities are the following:

ID	INCOMPATIBILITIES	WORKAROUND
1365	**Description**: Possible application crash when **SuperCopier** is installed with the StormShield agent.	Uninstall SuperCopier.
1082	**Description**: The **Hummingbird** application cannot be installed when the StormShield agent is activated. **Cause**: The StormShield agent is incompatible with the WinPCAP driver and the Hummingbird application installer.	Install the Hummingbird application before installing the StormShield agent.
1124	**Description**: A **BSOD** is displayed when the user tries to open a **VPN Cisco** client connection. **Cause**: Incompatibility between the `vsdatant.sys` driver (Zone Alarm Firewall) and StormShield.	Rename the `vsdatant.sys` driver for deactivation.
1633	**Description**: A **BSOD** is displayed with **Promax** when installing StormShield. **Cause**: Incompatibility between the aksfridge.sys driver and StormShield.	No solution. (#ZVQ-26686-729)
1645	**Description**: A bootable device cannot be created with the HP USB Disk Storage Format Tool. The following error message is displayed between [format end] and [start copy file] on the device: "FAILED TO MAKE THE DEVICE DOS-BOOTABLE". **Cause**: When a device is removed from a computer, StormShield denies access to the latter as long as StormShield checks whether or not the device is encrypted. During this process, the HP software mounts and unmounts the device several times in a row.	No solution. (#FKX-94147-408)
1846	**Description**: Incompatibility between StormShield and the Digital Persona smart-card authentication system. Files encrypted by StormShield cannot be accessed when using Windows authentication. **Cause**: If Digital Persona is installed after StormShield, the former removes StormShield's GINA dll and the authentication system.	Install StormShield after Digital Persona. (#DNX-52479-415)

Tableau 1.2 : Known incompatibilities (Page 1/5)

ID	INCOMPATIBILITIES	WORKAROUND
1466	**Description**: The web page used to download agents and browsed with Microsoft Internet Explorer 6 SP2 cannot be displayed.	Update Internet Explorer or use another web browser which is more recent.
2060	**Description**: Incompatibility between StormShield and the Aboutkey tool which checks for the presence of the Guardant Stealth II dongle. **Cause**: The dongle driver is incompatible with the device control system.	No solution.
2137	**Description**: Incompatibility between StormShield and Sophos SafeGuard Enterprise (encryption tool). USB keys are displayed in Computer, but their content cannot be accessed. USB hard disks can only be accessed in read-only mode. **Cause**: The encryption tool is incompatible with the device control system. SafeGuard detects if another driver implements a filter and in this case, denies access to devices.	Modify the registry base in order to load the StormShield driver `odin-sys.sra` before the SafeGuard Enterprise driver. **Procedure**: 1. Stop the StormShield agent with `stopagent.exe` 2. Go to registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder` 3. Edit the `List` value and add an **Odin** entry above the **Primary Disk** entry (Safeguard Enterprise driver) See "Modifying the registry key ServiceGroupOrder", page 70. 4. Go to registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\odin` 5. Add the `Group` value (string type) and assign the value `Odin` in the **Value data** field. See "Adding a value to the registry key odin", page 70. 6. Reboot. (#BSX-16078-335)

Tableau 1.2 : Known incompatibilities (Page 2/5)

ID	INCOMPATIBILITIES	WORKAROUND

Fig. 1 : Modifying the registry key `ServiceGroupOrder`

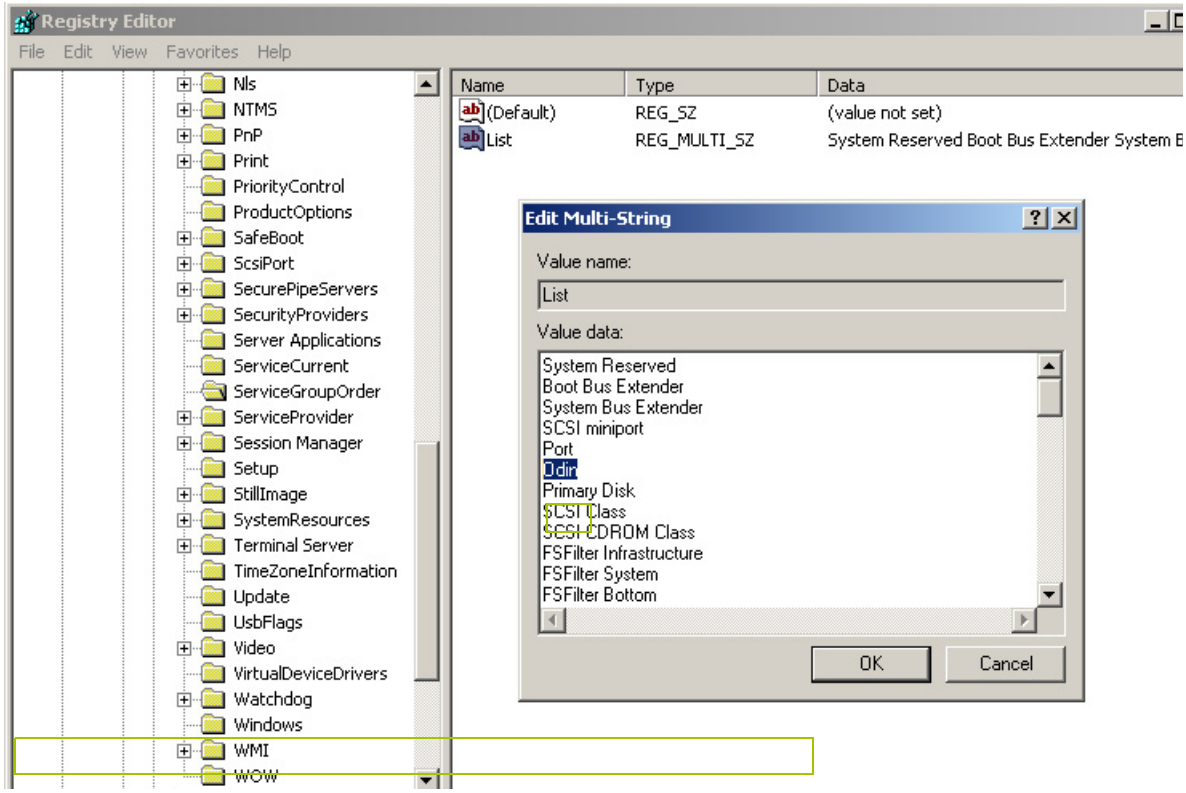

Fig. 2 : Adding a value to the registry key `odin`

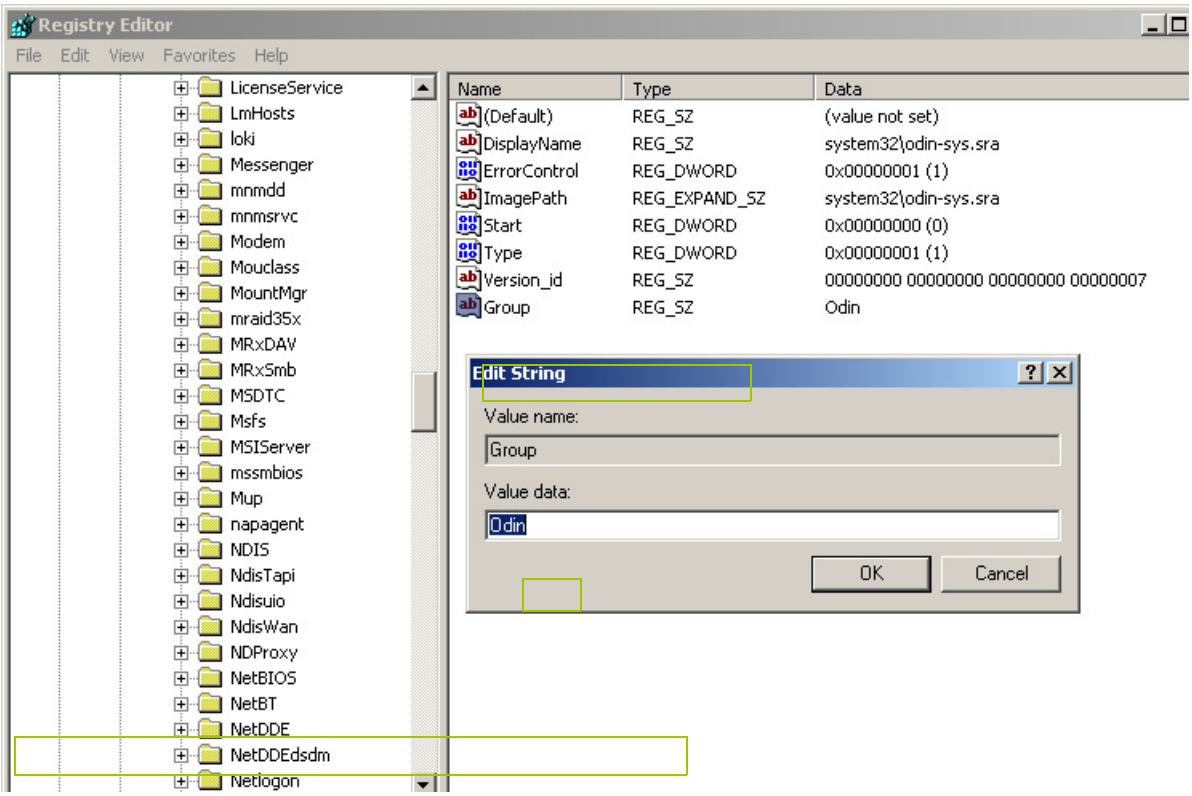

Tableau 1.2 : Known incompatibilities (Page 3/5)

ID	INCOMPATIBILITIES	WORKAROUND
2235	**Description**: A **BSOD** is displayed after installing Daemon Tools Lite. **Cause**: The tool is incompatible with full disk encryption.	No solution.
2240	**Description**: Incompatibility between StormShield and Vodafone MobileConnect. **Cause**: The Vodafone software is incompatible with the Protection against memory overflow.	Update Vodafone MobileConnect to version 9.04.
2512	**Description**: Incompatibility between StormShield and BitDefender. **Cause**: Incompatibility with a driver installed by BitDefender. BitDefender destroys some StormShield processes because it detects that intrusive operations are performed.	No solution.
5180	**Description**: Incompatibility with BitLocker To Go (StormShield file encryption). **Cause**: BitLocker To Go and StormShield operations overlapping.	No solution. StormShield file encryption must be deactivated for removable devices. No rule must include condition on removable device enrollment.
	Description: Incompatibility with F-Secure application on 64-bit operating systems. **Cause**: Incompatibility with auto-protection in StormShield.	Disable option **Use advanced process monitoring** in the DeepGuard settings in F-Secure.
	Description: A BSOD occurs when using StormShield with a solution embedding Safenet aksfridge.sys, Aksdf.sys or Hardlock.sys drivers.	The version 6.62 or later of Safenet drivers (Sentinel HASP/LDK) includes a fix for this problem.
	Description: Incompatibility with the CISCO client VPN application and the ORANGE BUSINESS EVERYWHERE VPN on Windows Seven x64 with a Stormshield Endpoint Security firewall policy. The connection to the VPN is established but it is not possible to browse: there is no input or output byte. **Cause**: The StormShield internal firewall blocks the VPN communication. By deactivating the driver Thor3, the issue no longer occurs.	You must disable the StormShield firewall to use the VPN and StormShield. As an administrator, run the command: C:\Users\Administrator>"C:\Program Files (x86)\SkyRecon\StormShield Agent\Uninstall_thor3.exe" -U Since versions 5.7/15 and 6.0/08, if you do not use any firewall policy, this one is disabled.
	Description: MTP USB devices cannot be blocked.	No solution.
	Description: SD card and eSata devices cannot be blocked.	No solution.

Tableau 1.2 : Known incompatibilities (Page 4/5)

ID	INCOMPATIBILITIES	WORKAROUND
	Description: The Avira 2013 antivirus software cannot be installed on Windows XP SP2.	Avira 2013 is not supported on Windows XP SP2. Windows XP SP3 minimum is required.
9418	**Description**: Incompatibility with the extension "Office Editing for Docs, Sheets and Slides" for Google Chrome. Opening a document with this extension fails and displays either an error or a blank page.	No solution.

Tableau 1.2 : Known incompatibilities (Page 5/5)