RELEASE NOTES

F-Secure Internet Gatekeeper

Version 5.20.646 RTM

1. General

This document contains important information regarding changes and new features in F-Secure Internet Gatekeeper. We strongly recommend that you read the entire document.

What's in This File

- System Requirements
- Product Contents
- New Features
- Known Issues
- Installation
- Contact Information and Feedback
- Third party software used in the product

2. System Requirements

To use F-Secure Internet Gatekeeper 5.20 on a computer, the computer must:

- Be x86 compatible (2Ghz or faster recommended)
- Have at least 512 MB of RAM (1 GB or more recommended)
- Have at least 5 GB of free disk space (20 GB recommended)
- Installed files need at least 1 GB of free disk space and running system needs significantly more for temporary files, logs, etc.
- Have one of the following Linux distributions installed:
  - 32-bit:
    - CentOS 5.10, 5.11, 6.4, 6.5, 6.6
    - Debian 7.4, 7.6, 7.7
    - Red Hat Enterprise Linux 5.10, 5.11, 6.4, 6.5, 6.6
    - Ubuntu 12.04.4
  - 64-bit:

- CentOS 5.10, 5.11, 6.4, 6.5, 6.6, 7.0

- Debian 7.4, 7.6, 7.7

- Red Hat Enterprise Linux 5.10, 5.11, 6.4, 6.5, 6.6, 7.0

- Ubuntu 12.04.4

- The following software must be available in the operating system:

  o Linux kernel 2.6 or later

  o Perl 5.8 or later

  o Make

  o 32-bit C and C++ runtime environment. Consult your OS documentation for installing the compatibility libraries in 64-bit environment:

    - glibc

    - libstdc++

    - libgcc1

- Support for any other and/or newer Linux distributions will be announced in future releases and/or on our web site.

For up-to-date information about supported platforms, please see our Knowledge Base:

http://www.f-secure.com/en_EMEA/support/business/

3. Product Contents

F-Secure Internet Gatekeeper is a gateway product that acts as a virus scanning proxy for HTTP, SMTP, POP, and FTP protocols.

The product uses F-Secure's scanning technologies to scan for malware. They provide outstanding protection level and fast, automatic updates to the scanning engines and anti-virus databases. With F-Secure's Security Cloud, the product can react to new threats rapidly, which keeps the users protected and enhances the protection even further.

The product can be integrated with third-party HTTP proxies with the standard ICAP protocol. The content that is submitted to the ICAP service is scanned with F-Secure's malware scanning technologies.

4. New Features

This release contains following new features, bugfixes and other changes that have been added since the 5.10.12 release.

- Added support for Japanese localization in Web UI.

- Added various missing settings in Web UI.

- Fixed CSLP-331: fsupdated is still running after turning off automatic updates.

- Fixed CSLP-344: LANG=C locale causes installer to fail.

- Fixed CTS-91677: "pass_type" and pass_type_list" options not working accurately.

- Fixed CTS-94558: Database update with fsdbupdate9.run leaves fsaua and fsupdated running when services are disabled

- Fixed CTS-95383: LAN access settings not migrated during product upgrade.

- Fixed CTS-95301: IGK leaves unexpectedly restarted proxy processes marked as busy, causing "Maximum connections" issue.

- Fixed CTS-95267: E-mail addresses of Admin notification settings cannot be set properly.

- Fixed CTS-95168: Add missing log files to logrotate.conf.

- Fixed CTS-95547: getaddrinfo_randomize expert option not working

- Removed the quick start guide and merged its contents to the admin guide.

5.00.5 => 5.10.12

- ICAP service supports scanning emails for malware and spam.

- New and improved web user interface added.

- New quick start guide added for easy installation and usage instructions.

- Fixed CTS-82476: fsaua now restart automatically when customer changes virus database download proxy settings from web user interface.

- Fixed CTS-84901: FmLib library version is not visible in the web user interface.

- Fixed CTS-86302: Added documentation for configuring HTTP proxy for anti-spam daemon (fsasd) in the administrator guide.

- Fixed CTS-91777: Fixed detecting malicious javascript and html files.

- Fixed CTS-91852: Added missing information for ICAP detections templates in administrator guide.

- Fixed CTS-91867: Improved documentation for transparent proxy bridge mode using subnet in administrator guide.

- Fixed CTS-92431: Improved detection rate for policy-based blocking for javascripts and ActiveX scripts.

- Fixed CTS-92216: Fix timeout_inactive for web servers that take more time than keepalive_timeout to start sending the reponse to IGK.

- Fixed CTS-92759: Fixed log size specification of logconv tool in administrator guide.

- Fixed CTS-92797: Fixed information for scanning daemon (fsavd) process management in administrator guide.

- Fixed CTS-92814: Parsing very large email header can lead to false detection or other unexpected result.

- Fixed CTS-92861: IGK fails to detect too long HTTP request URL.

- Fixed CTS-93579: Fixed information about connection error messages in administrator guide.

- Fixed CTS-94390: Added missing system requirements and dependencies in IGK release notes.

- Fixed CTS-94834: Added information about orsp_file_check for HTTP proxy in administrator guide.

4.10.17 => 5.00.5

- Support for F-Secure Real Time Protection Network was added to the HTTP proxy. When enabled, common files are identified by rapidly updating black and white lists. This saves system resources and improves the protection.

- The malware scanning capabilities are now available by a standard ICAP interface. This enables integration with third party proxies that support ICAP.

- The list of supported distributions was reworked to focus on the most popular, current and actively supported distributions.

- Removed dependency to Java, which is a common source of security vulnerabilities. Java runtime environment is no longer distributed with the product. As a consequence, this release does not contain a web UI, but is also significantly smaller and lighter. Configuration is done by editing the configuration files directly.

- Improved quality of RPM packages.

- Improved the output from IGK init scripts.

- Fixed CTS-91383: Added an option to control whether to transparently re-establish keepalive upstream HTTP connections.

If you are upgrading from a version earlier than 4.10.17 ,4.11.8 or 4.12.5, see the release notes of version 4.12.5 for a list of earlier changes.

5. Known Issues

- Upgrading from any 2.X or 3.X version is not supported. Please uninstall the old version completely before installing F-Secure Internet Gatekeeper 5.20.

- Upgrading from 4.X Japanese version of the product(virusgw) to international version(fsigk) is not supported. Follow the instruction in admin guide of the product to migrate settings from old(virusgw) installation to F-Secure Internet Gatekeeper 5.10(fsigk) installation.

- Credentials for accessing services using HTTP proxy (http_proxyauth_user and http_proxyauth_pass in fsigk.ini) have certain limitations. Only the following printable ASCII characters are allowed: letters, digits and the following special characters: -._~!$&'()*+,;=

- If you use rpm to upgrade the product to the 5.20 release, the product configuration files are reset to the factory defaults. The upgrade process renames the old configuration files by attaching an .rpmorig extension. This does not affect the main configuration file, fsigk.ini. As a workaround, you can rename the backup files back to their original names.

Please see our Knowledge Base for up-to-date information about known problems and possible workarounds:
http://www.f-secure.com/en_EMEA/support/business/

6. Installation

The product can be installed from an RPM package, or a tar package.

6.1. RPM installation or upgrade

First download the rpm package, then run the following command as root user:

rpm -Uvh fsigk-5.20.646-0.i386.rpm

After the installation, open http://<HOSTNAME>:9012/ with your web browser and use the default username and password to log in and configure the product. See the admin guide for information on how to configure the product with the web user interface.

6.2. Installing using a tar package

First download the tar package, then run the following commands as root user:

tar zxf fsigk-5.20.646.tar.gz

cd fsigk-5.20.646

make install

After the installation, open http://<HOSTNAME>:9012/ with your web browser and use the default username and password to log in and configure the product. See the admin guide for information on how to configure the product with the web user interface.

7. Contact Information and Feedback

To provide feedback or report problems, please see:

http://support.f-secure.com/

Please make sure that you tell the product version and Linux distribution you are using when contacting us.

8. Third party software used in the product

Commtouch 7.03.0049

Copyright (C) 1991-2010 Commtouch Software, Ltd. www.commtouch.com
[http://www.cyren.com]

Berkeley DB 1.85

Copyright (c) 1991, 1993, 1994 The Regents of the University of California. All rights reserved.
[http://www.oracle.com/technetwork/database/database-technologies/berkeleydb/overview/index.html]

JSON-C 0.9

Copyright (c) 2009-2012 Eric Haszlakiewicz
Copyright (c) 2004, 2005 Metaparadigm Pte Ltd
[https://github.com/json-c/json-c]

Libevent 2.0.21

Copyright (c) 2000-2007 Niels Provos <provos@citi.umich.edu>
Copyright (c) 2007-2010 Niels Provos and Nick Mathewson
[http://libevent.org/]

Linux PAM userdb module 1.1.1.1

Copyright (c) Cristian Gafton <gafton@redhat.com>, 1999. All rights reserved.
[http://www.linux-pam.org/]

libaes 0.03

Copyright (c) 2001, Dr Brian Gladman <brg@gladman.uk.net>, Worcester, UK. All rights reserved.
[http://libaes.sourceforge.net/]

MD5 message-digest algorithm

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.
[http://www.ietf.org/rfc/rfc1321.txt]

TCP wrapper utilities 7.6

Copyright 1995 by Wietse Venema.
[ftp://ftp.porcupine.org/pub/security/index.html]

SQlite3 3.8.1

The author disclaims copyright to this source code (Public Domain).
[http://www.sqlite.org/]

Transparent Proxying patches for Linux kernel 2.6

Copyright (C) 2007-2008 BalaBit IT Ltd.
[http://www.balabit.com/support/community/products/tproxy]

Civetweb 1.4

Copyright (c) 2004-2013 Sergey Lyubka Copyright (c) 2013 No Face Press, LLC (Thomas Davis)
[https://github.com/sunsetbrew/civetweb]