



Regulatory compliance and system logging

Synopsis: The advantages of using syslog-ng Premium Edition to collect system log (syslog) and eventlog messages for policy compliance

Status: Released

Version: 2.0

Date: 09/08/2009



Table of contents

Preface.....	3
Introduction.....	4
What is system logging.....	4
Why is system logging important when dealing with policy compliance.....	4
Problems to be solved by log management.....	4
Using syslog-ng for policy compliance.....	6
PCI-DSS compliance and logging.....	6
COBIT 4.1 compliance and logging.....	8
HIPAA compliance and logging.....	10
Other important features.....	11
Secure logging using SSL/TLS.....	11
Disk-based message buffering	11
Output data into various formats.....	11
Direct database access.....	11
Select important messages.....	11
Control the rate of messages.....	11
Support for IPv4 and IPv6 environments.....	12
Flow-control	12
Heterogeneous environments.....	12
Collect logs from Microsoft Windows.....	12
Collect logs from IBM System i.....	12
Detect and log configuration changes.....	12
Further information.....	13
About BalaBit.....	13



Preface

This paper discusses the advantages of using syslog-ng Premium Edition to collect system log (syslog) and eventlog messages in compliance with regulations like the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), or the Payment Card Industry Data Security Standard (PCI-DSS). The document is recommended for technical experts and decision makers working on implementing centralized logging solutions, but anyone with basic networking knowledge can fully understand its contents. The procedures and concepts described here are applicable to version 3.0 of syslog-ng Premium Edition (PE).

This paper is organized into the following sections:

- *Introduction* briefly describes what system logging is, and why it is an important part of policy compliance.
- *Using syslog-ng for policy compliance* is a detailed list of policy requirements, including the requirements of the Payment Card Industry Data Security Standard (PCI-DSS), COBIT 4.1, and the Health Insurance Portability and Accountability Act (HIPAA) that you can address with syslog-ng Premium Edition.
- *Other important features* discusses further features of syslog-ng PE that can come handy for you when designing and implementing your system logging architecture.
- Further information contains a brief description of BalaBit IT Security and provides links where you can find out more about syslog-ng, request an evaluation version, or find a reseller.



Introduction

What is system logging

Operating systems, applications, and network devices generate text messages of various events that happen to them: a user logs in, a file is created, a network connection is opened to a remote host, etc. These messages, called log messages, are usually stored in a file on the local hard disk of the system. The aim of central system logging is to collect the log messages to a single, central log server.

For a more detailed introduction into syslog architectures, see the [Distributed syslog architectures with syslog-ng Premium Edition](#) whitepaper.

Why is system logging important when dealing with policy compliance

Log messages provide important information about the events of the network, the devices, and the applications running on these devices. Log messages can be used to detect security incidents, operational problems, and other issues like policy violations, and are useful in auditing and forensics situations. But collecting and analyzing log messages is also required directly or indirectly by several regulations, including the Sarbanes-Oxley Act (SOX), the Basel II Accord, the Health Insurance and Portability Act (HIPAA), or the Payment Card Industry Data Security Standard (PCI-DSS).

Problems to be solved by log management

There are several problems and difficulties that have to be solved when creating a usable logging infrastructure. The main problems to consider are summarized below, along with a brief description about how the syslog-ng Premium Edition (PE) application can help you to overcome these problems.

- **Many different devices and applications running on a variety of operating systems.** To start collecting log messages into a central log server, the logs must be retrieved somehow from the devices where the messages are generated. These devices (desktop computers, servers, networking devices like switches and routers, firewalls, etc.) usually use many different operating systems – all of which should send the logs to the central server. The problem with the variety of operating systems is that they use different logging solutions, with different configuration requirements and capabilities. To address this problem, syslog-ng can be installed on most common operating systems, including Linux, Solaris, HP-UX, BSD, IBM AIX, and has dedicated agent applications to collect the logs from Microsoft Windows and IBM System i platforms. Using a single logging application vastly simplifies configuration and management problems, and ensures that advanced logging capabilities (like TLS-encrypted log transfer or disk-based buffering) is available on every device. If syslog-ng cannot be installed on a device for some reason (for example, it is running a pre-built firmware which cannot be modified), a local computer running syslog-ng can accept the syslog messages from devices and relay them to the central log server.
- **Inconsistent timestamps and message format.** Different log messages often use different timestamp formats to date the messages (for example, some timestamp formats do not contain year or timezone information), making it difficult to locate the messages later, and to properly see their place in the flow of events. With syslog-ng, it is possible to convert the timestamps to a single format (e.g., as specified in the ISO 8601 standard), and also to use the date when syslog-ng server has received the message from the application or the remote host, so the stored messages will contain accurate date information even if the clock of the remote host or the application is inaccurate. The syslog-ng application provides macros and powerful message-rewriting capabilities to reformat and normalize the messages in order to convert them to a common format to ensure that the order of the data fields in the message is consistent with other messages. Supporting the new IETF syslog



protocol standard, syslog-ng makes it easy to integrate all kinds of log messages and logging clients into a common framework.

- **Protecting the integrity and confidentiality of the messages during transmission.** Log messages are important from the network-security point of view, but they may also contain sensitive information and private data like passwords, usernames, etc. Therefore, it is important that they are protected against eavesdropping when they are transmitted over the network. It is also important to verify the identity of the communicating parties (that is, the host sending the message, and the central log server) to ensure that the message is received only by its intended target (the log server), and that the message received by the server was indeed sent by the client host. The integrity of the message must be also maintained so that no unauthorized modification of the message is possible. To address these issues, the syslog-ng PE application uses the secure Transport Layer Security (TLS) protocol to encrypt the communication with the server, and authenticates both the client and the server using X.509 certificates.
- **Protecting the integrity and confidentiality of the messages stored on the log server.** Log messages must be protected even after they arrive to the log server to prevent manipulation and unauthorized access. For this reason, syslog-ng can store the log messages in encrypted and digitally signed log files. Encrypting the log files ensures that the log messages can be accessed only by authorized personnel who has the appropriate decryption key; while the digital signature prevents the unnoticed modification of the messages. It is also possible to request timestamps from an external Timestamping Authority (TSA) to add further reliability to the date of the log messages.
- **Ensuring that no messages are lost.** The syslog-ng PE application assigns a unique identifier to every message and ensures that you do not lose messages during network or system outages, because syslog-ng PE can store unsent messages on the local hard disk until the log server becomes available again. The syslog-ng PE application can also apply flow-control on the messages. Flow-control means that if the destination server or database becomes overloaded, syslog-ng PE can stop accepting messages from the sending hosts or applications. That way the senders are notified that there is a problem in the logging infrastructure and can act accordingly: for example, in an environment where policy compliance mandates all events to be logged, the applications may temporarily halt until the logging can be resumed, so there are no actions that are not logged. As an alternative to handle server downtime, syslog-ng PE can send the log messages to a backup log server if the primary server becomes unavailable.
- **Classifying log messages.** The syslog-ng application can compare the contents of the received log messages to predefined message patterns. By comparing the messages to the known patterns, syslog-ng is able to identify the exact type of the messages, and sort them into message classes. The message classes can be used to classify the type of the event described in the log message. The message classes can be customized, and for example can label the messages as user login, application crash, file transfer, etc. events. Also, syslog-ng message patterns are much easier to understand, write and maintain than the regular expressions commonly used by other products. Moreover, syslog-ng can classify tens of thousands of messages per second on average server hardware.
- **Helping SIEM devices to analyze the log messages.** Analyzing logs is an essential element of network security. While syslog-ng is not a log analyzing application, it has a number of features – including message normalization – that can aid log-analyzing engines. The syslog-ng application has powerful message filtering and sorting capabilities that make it possible to ignore trivial or low-priority messages. Since message filtering can take place already on the clients, it can save a significant amount of bandwidth by dropping unimportant messages, and decrease the load on the SIEM device at the same time. Also, since the capacity of log analyzing applications is often limited, syslog-ng can limit the number of messages sent per second. This has the benefit of flattening out message bursts and protecting the log-analyzing engine from becoming overloaded. Certain SIEM devices prefer to receive log messages from databases; syslog-ng can send the log messages directly to a database, and supports most popular databases, including MSSQL, MySQL, Oracle, and PostgreSQL.



- **Storing the messages.** Organizations often store log messages for a long time to be able to review security incidents that are not immediately discovered, and several regulations also require the logs to be available for several months or years. Storing the log messages becomes an issue especially if the volume of log traffic is very high (e.g., a few Gigabytes per hour). To reduce the amount of logs to be stored, syslog-ng provides powerful message filtering and sorting capabilities: it can drop or separate unimportant messages, organize messages into different files or databases based on their sending host, application, or content. It can also automatically compress and encrypt the log files, and periodically start a new file so that the older files can be archived and removed from the server.



Using syslog-ng for policy compliance

Compliance is becoming more and more important in several fields – laws, regulations and industrial standards mandate increasing security awareness and the protection of sensitive data. As a result, companies have to increase the control over and the auditability of their business processes, and this makes thorough log management necessary – especially since several regulations require the centralized collection of logs (including retaining logs for an extended amount of time often spanning several years).

The syslog-ng Premium Edition application is a tool that collects log messages from the clients to a central log server, ensuring the secure transmission and storage of the log messages from a wide variety of operating systems.

PCI-DSS compliance and logging

The following table provides a detailed description of the requirements of the Payment Card Industry Data Security Standard (PCI-DSS, available at <https://www.pcisecuritystandards.org>) relevant to log management and auditing. Other compliance regulations like the Sarbanes-Oxley Act (SOX) or the Basel II Accord imply similar requirements.

<i>PCI requirement</i>	<i>How syslog-ng Premium Edition supports it</i>
3. Protect stored cardholder data	System logs may contain sensitive information such as personal identification numbers (PIN) and card validation codes. The syslog-ng PE application protects these messages by storing them in an encrypted file instead of plain text files commonly used to store log messages. It is also possible to rewrite messages and automatically remove sensitive cardholder data using the message-rewriting capabilities of syslog-ng.
4. Encrypt transmission of cardholder data across open, public networks 4.1 Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS)	Transport layer security (TLS) can be used to encrypt the communication between the clients and the log server and to protect the integrity of the messages. Using TLS-encryption also prevents third-parties from accessing or modifying the communication. The communication between the client and the server can be mutually authenticated using X.509 certificates to verify the identity of the communicating parties and prevent attackers from injecting fake messages into the log files. The syslog-ng application also helps you to be compliant with the latest standards by supporting both the BSD-syslog (RFC3164) and the IETF-syslog (RFC5424) protocols.



<i>PCI requirement</i>	<i>How syslog-ng Premium Edition supports it</i>
10.2 Implement automated audit trails for all system components.	Log messages have an important role in reconstructing events of an application, host, or a network. The syslog-ng application aids this process by ensuring that the log messages arrive to the central log server without any unwanted modification. Messages are sent encrypted using the secure TLS protocol, which is based on the reliable TCP networking protocol that ensures that the messages arrive to the log server. The disk-based buffering feature of syslog-ng PE buffers messages to the hard disk of the client, ensuring that no messages are lost even if the log server or the network connection becomes unavailable.
10.3 Record at least the following audit trail entries for all system components for each event: 10.3.1 User identification 10.3.2 Type of event 10.3.3 Date and time 10.3.4 Success or failure indication 10.3.5 Origination of event 10.3.6 Identity or name of affected data, system component, or resource.	The syslog-ng PE application can automatically add the following to log messages that omit this information: <ul style="list-style-type: none"> ● date and time in various standard formats (e.g., ISO), including timezone information ● highly customizable date and time information using macros ● the name of the client host that generated the message ● the name of the application or facility that generated the message
10.4 Synchronize all critical system clocks and times.	The syslog-ng PE server can automatically add the date and time when it received the message, so the log messages contain accurate time information – even if the clock of the client host or the application is mistimed.
10.5 Secure audit trails so they cannot be altered.	All log messages can be encrypted using public-key encryption on the central log server in a so-called logstore file. The syslog-ng application can also request timestamps for the stored data from an external Timestamping Authority (TSA) to include reliable dates in the log files.
10.5.1 Limit viewing of audit trails to those with a job-related need.	Encrypted log messages can be viewed only if the user has the required encryption key.
10.5.2 Protect audit trail files from unauthorized modifications	When stored in the logstore of the central syslog-ng server, log messages are also digitally signed to prevent modifications. The integrity of the messages is also checked when they are transmitted from the client to the log server. The communication between the clients and the log server can be mutually authenticated using X.509 certificates to prevent log-injection attacks.



<i>PCI requirement</i>	<i>How syslog-ng Premium Edition supports it</i>
10.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.	<p>The syslog-ng PE application was created exactly for this purpose: to transfer the log messages generated on the host to a central log server, where they can be stored in encrypted and digitally signed log files to prevent modifications.</p> <p>To ensure that no log messages are lost, syslog-ng supports the reliable TCP networking protocol, and can also send log messages to a backup log server in case the primary server becomes unavailable. To avoid losing messages during network outages, syslog-ng PE buffers the messages to the hard disk, and sends the messages when the server becomes available. Depending on the volume of the log traffic and the available disk space on the host, your messages are safe even in case of very long network downtime.</p> <p>Since it supports a very broad selection of operating systems and platforms, syslog-ng is ideal for massively heterogeneous environments. The supported operating systems include: Microsoft Windows, Linux, Solaris, HP-UX, IBM AIX, and IBM System i.</p>
10.5.4 Copy logs for wireless networks onto a log server on the internal LAN.	The syslog-ng PE application can relay log messages received from wireless devices and transfer them to the central log server.
10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Using TLS encryption between the clients and the log server ensures that the log messages are not modified on the network. On the log server, syslog-ng can store messages in special encrypted and digitally signed log files to prevent modifications. Timestamps for the stored data can be requested also from an external Timestamping Authority (TSA). When its configuration is changed, syslog-ng PE application automatically sends a log message to simplify the auditing of your logging infrastructure.
10.7 Retain audit trail history for at least one year, with a minimum of three months online availability.	When stored in the logstore of the central syslog-ng server, log messages can be compressed to save disk space.

COBIT 4.1 compliance and logging

Although the compliance of logging infrastructures to COBIT is seldom required by authorities, COBIT-compliance is still important, as there are certain regulations (such as the Sarbanes-Oxley Act, or the Basel II Accord) that do not specify exact technical requirements, and compliance to these regulations is often achieved by adopting a well-established framework like COBIT.

The following table discusses some sample control objectives of the Control Objectives for Information and related Technology (COBIT) 4.1, how they affect the logging infrastructure of the organizations, and how can syslog-ng PE be used to address these requirements. Please note that this list is by no means exhaustive, and other objectives may have further requirements on the logging infrastructure and log management.



COBIT 4.1 control objective	How syslog-ng Premium Edition supports it
<p>AI6 Manage Changes</p> <p>Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorized prior to implementation and reviewed against planned outcomes following implementation.</p> <p>DS9.3 Configuration Integrity Review</p> <p>Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration.</p>	<p>The syslog-ng PE application automatically detects if its configuration is changed, and automatically sends a log message about this event. That way it is easy to recognize any changes to the logging infrastructure, and detect unauthorized changes.</p>
<p>DS5.11 Exchange of Sensitive Data</p> <p>Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.</p>	<p>Transport layer security (TLS) can be used to encrypt the communication between the clients and the log server and to protect the integrity of the messages. Using TLS-encryption also prevents third-parties from accessing or modifying the communication. The communication between the client and the server can be mutually authenticated using X.509 certificates to verify the identity of the communicating parties and prevent attackers from injecting fake messages into the log files, and also from obtaining syslog data. The use of the TCP networking protocol, disk-based buffering, and the ability to send the messages to a backup server in case the primary log server becomes unavailable ensures that the log server indeed receives the sent messages.</p>
<p>DS13.3 IT Infrastructure Monitoring</p> <p>Define and implement procedures to monitor the IT infrastructure and related events. Ensure that sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.</p>	<p>The syslog-ng PE application was created exactly for this purpose: to transfer the log messages generated on the host to a central log server, where they can be stored in encrypted and digitally signed log files to prevent modifications.</p> <p>To ensure that no log messages are lost, syslog-ng supports the reliable TCP networking protocol, and can also send log messages to a backup log server in case the primary server becomes unavailable. To avoid losing messages during network outages, syslog-ng PE buffers the messages to the hard disk, and sends the messages when the server becomes available. Depending on the volume of the log traffic and the available disk space on the host, your messages are safe even in case of very long network downtime.</p> <p>Since it supports a very broad selection of operating systems and platforms, syslog-ng is ideal for massively heterogeneous environments. The supported operating systems include: Microsoft Windows, Linux, Solaris, HP-UX, IBM AIX, and IBM System i.</p>



<i>COBIT 4.1 control objective</i>	<i>How syslog-ng Premium Edition supports it</i>
<p>PO2.4 Integrity Management</p> <p>Define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.</p>	<p>Using TLS encryption between the clients and the log server ensures that the log messages are not modified on the network. On the log server, syslog-ng can store messages in special encrypted and digitally signed log files to prevent modifications. It is also possible to store a copy of the messages digitally signed and encrypted in the logstore, and another copy in a database (syslog-ng can directly send messages into Oracle, MySQL, and other databases); the database can be used for everyday log processing, analyzing, and reporting purposes, and the messages can be compared to the copies stored in the logstore to detect any unwanted changes.</p>



HIPAA compliance and logging

The Health Insurance Portability and Accountability Act (HIPAA) has few direct requirements about logging, but it requires the protection and encryption of sensitive information as it is transmitted over the network and stored on a computer. As log messages may contain such information, the logging infrastructure must comply with these requirements as well.

The following table discusses some sample requirement of HIPAA, how they affect the logging infrastructure of the organizations, and how can syslog-ng PE address these requirements. Please note that this list is by no means exhaustive, and other requirements may be applicable to the logging infrastructure and log management.

<i>HIPAA Security Rule</i>	<i>How syslog-ng Premium Edition supports it</i>
164.312(e)(1) Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Transport layer security (TLS) can be used to encrypt the communication between the clients and the log server and to protect the integrity of the messages. Using TLS-encryption also prevents third-parties from accessing or modifying the communication. The communication between the client and the server can be mutually authenticated using X.509 certificates to verify the identity of the communicating parties and prevent attackers from injecting fake messages into the log files, and also from obtaining syslog data. The use of the TCP networking protocol, disk-based buffering, and the ability to send the messages to a backup server in case the primary log server becomes unavailable ensures that the log server indeed receives the sent messages.
164.312(e)(2)(i) Integrity Controls (A): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Using TLS encryption between the clients and the log server ensures that the log messages are not modified on the network. On the log server, syslog-ng can store messages in special encrypted and digitally signed log files to prevent modifications. It is also possible to store a copy of the messages digitally signed and encrypted in the logstore, and another copy in a database (syslog-ng can directly send messages into Oracle, MySQL, and other databases); the database can be used for everyday log processing, analyzing, and reporting purposes, and the messages can be compared to the copies stored in the logstore to detect any unwanted changes.
164.312(e)(2)(ii) Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	The syslog-ng PE application can encrypt log messages while they are transferred from their origin to the central log server, and store them on the central log server in an encrypted, digitally signed format. Timestamps for the stored data can be requested also from an external Timestamping Authority (TSA).



Other important features

This section highlights some of the features of syslog-ng PE that were not discussed in detail so far, but are useful to know about.

Secure logging using SSL/TLS

Log messages may contain sensitive information that should not be accessed by third parties. Therefore, syslog-ng Premium Edition uses the Transport Layer Security (TLS) protocol to encrypt the communication. TLS also allows the mutual authentication of the host and the server using X.509 certificates.

Disk-based message buffering

The Premium Edition of syslog-ng stores messages on the local hard disk if the central log server or the network connection becomes unavailable. The syslog-ng application automatically sends the stored messages to the server when the connection is reestablished, in the same order the messages were received. The disk buffer is persistent – no messages are lost even if syslog-ng is restarted.

Output data into various formats

The syslog-ng application does not limit what you can do with your log messages: it is meant to provide you with the most effective way to collect them. You can store your logs in files, databases, or pass them to a log analyzing application: syslog-ng PE can customize the messages into the format you want. You can even reorganize the contents of the log messages if you are not content with the original message format – or if it makes your log analyzing application more effective.

Direct database access

Storing your log messages in a database allows you to easily search and query the messages and interoperate with log analyzing applications. The Premium Edition of syslog-ng supports the following databases: MSSQL, MySQL, Oracle, and PostgreSQL.

Select important messages

You can use various filters – ranging from very simple to really complex ones – to select messages based on their content, source, or other parameters. This is useful if you do not want to send every message to the central server, or you have to process messages differently based on their content. The syslog-ng application can dynamically create directories, files, and database tables using macros.

Control the rate of messages

You can control the number of messages syslog-ng PE sends to the central server to ensure that sudden message bursts do not consume the bandwidth of other important applications, or to flatten the load of the server. Controlling the number of sent messages is useful also if you have a database or a log analyzing application on the server that can process only a limited number of messages. Using disk-based buffering together with the rate-limiting feature of syslog-ng PE prevents the loss of messages, and helps to use the resources effectively without overloading backend systems.



Support for IPv4 and IPv6 environments

You can deploy syslog-ng in both types of networks, and use the same system logging tool across your entire network infrastructure.

Flow-control

Flow-control uses a control window to determine if there is free space in the output buffer of syslog-ng for new messages. If the output buffer is full, then the destination cannot accept new messages for some reason: for example, it is overloaded, or the network connection became unavailable. In such cases, syslog-ng stops reading messages from the sending applications or hosts until some messages have been successfully sent to the destination.

Heterogeneous environments

The syslog-ng application is the ideal choice to collect logs in massively heterogeneous environments using several different operating systems and hardware platforms, including Linux, Windows, Unix, BSD, Sun Solaris, HP-UX, and AIX. For a complete list of platforms supported by syslog-ng Premium Edition, visit <http://www.balabit.com/network-security/syslog-ng/central-syslog-server/>.

Collect logs from Microsoft Windows

Using syslog-ng Agent for Windows, you can collect messages from logfiles and eventlog groups, and transfer all log messages to the central syslog server using encrypted, reliable TCP connections. That way you can integrate your Windows-based and UNIX-based devices into the same logging infrastructure. The syslog-ng Agent for Windows application can be managed centrally from your Domain Controller.

Collect logs from IBM System i

Using syslog-ng Agent for IBM System i, you can collect application and system messages, as well as messages from the System i security audit journal. The collected messages are forwarded to the central syslog server using encrypted, reliable TCP connections. That way you can integrate your IBM System i devices into the same logging infrastructure as your UNIX and other devices.

Detect and log configuration changes

The syslog-ng Premium Edition application will automatically detect when its configuration is modified and send a log message about the change, simplifying the audit of your syslog infrastructure.



Further information

About BalaBit

BalaBit IT Security is a developer of network security solutions satisfying the highest standards. BalaBit was founded and is currently owned by Hungarian individuals. Its main products are the syslog-ng system logging software, which is the most widely used alternative syslog solution of the world; [Zorp, a modular proxy gateway](#) capable of inspecting over twenty protocols, including encrypted ones like SSL and SSH, and the [BalaBit Shell Control Box](#), an appliance that can transparently control, audit, and replay SSH, RDP, and Telnet traffic.

To learn more about syslog-ng, request an evaluation version, find a reseller, or buy syslog-ng directly from BalaBit, visit the following links:

- [The syslog-ng homepage](#)
- [syslog-ng manuals, guides, and other documentation](#)
- [Register and request an evaluation version](#)
- [Find a reseller](#)
- [Buy syslog-ng in the BalaBit Webshop](#)



All questions, comments or enquiries should be directed to info@balabit.com or by post to the following address:
BalaBit IT Security 1115 Budapest, Bártfai str. 54.
Phone: +36 1 371-0540 Fax: +36 1 208-0875 Web: <http://www.balabit.com/>

Copyright © 2009 BalaBit IT Security Ltd. Some rights reserved.
This document is published under the Creative Commons Attribution-Noncommercial-No Derivative Works (by-nc-nd) 3.0 license.
[The latest version is always available at http://www.balabit.com/support/documentation/](http://www.balabit.com/support/documentation/)