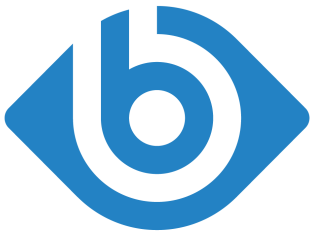
What is new in Balabit Shell Control Box 5 LTS

May 05, 2017



BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

Table of Contents

1. Preface

Welcome to Balabit Shell Control Box (SCB) version 5 LTS and thank you for choosing our product. This document describes the new features and most important changes since the latest release of SCB. The main aim of this paper is to aid system administrators in planning the migration to the new version of SCB. The following sections describe the news and highlights of SCB 5 LTS.

This document covers the Balabit Shell Control Box 5 LTS and Audit Player 2016.1 products.

For step-by-step instructions on upgrading to SCB 5 LTS see the *How to upgrade to Balabit Shell Control Box 5 LTS* guide.

Note that SCB 4 F3 has extended support period, and will be supported for 6 months after SCB 5 LTS is released. This means that 4 F3 will be supported longer than 4 F4.

1.1. Versions and releases of SCB

As of June 2011, the following release policy applies to Balabit Shell Control Box:

- *Long Term Supported or LTS releases* (for example, SCB 4 LTS) are supported for 3 years after their original publication date and for 1 year after the next LTS release is published (whichever date is later). The second digit of the revisions of such releases is 0 (for example, SCB 4.0.1). Maintenance releases to LTS releases contain only bugfixes and security updates.
- *Feature releases* (for example, SCB 4 F1) are supported for 6 months after their original publication date and for 2 months after a succeeding Feature or LTS release is published (whichever date is later). Feature releases contain enhancements and new features, presumably 1-3 new features per release. Only the last feature release is supported (for example, when a new feature release comes out, the last one becomes unsupported in 2 months).

For a full description of stable and feature releases, see *Version Policy*.

Warning
Downgrading from a feature release is not supported. If you upgrade from an LTS release (for example, 4.0) to a feature release (4.1), you have to keep upgrading with each new feature release until the next LTS version (in this case, 5.0) is published.

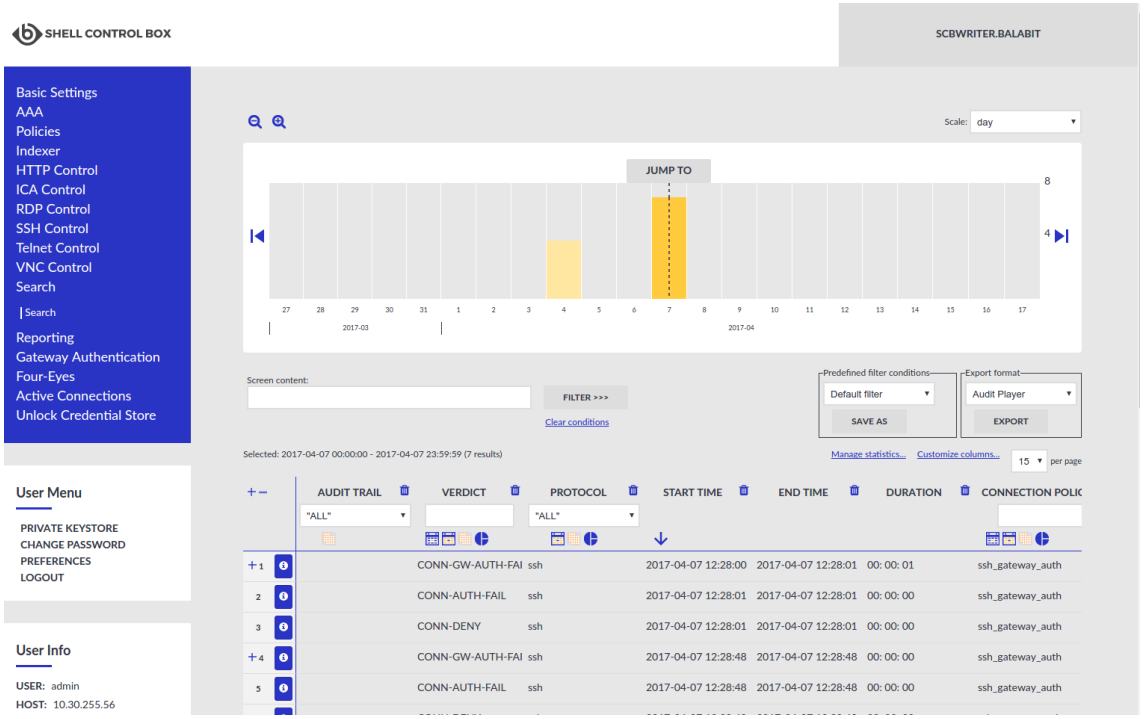
All questions, comments or inquiries should be directed to <info@balabit.com> or by post to the following address: Balabit SA 1117 Budapest, Alíz Str. 2 Phone: +36 1 398 6700 Fax: +36 1 208 0875 Web: *https://www.balabit.com/*

2. Changes since SCB 4 F4

New user interface design

The user interface has received a facelift and now has a more modern look-and-feel.

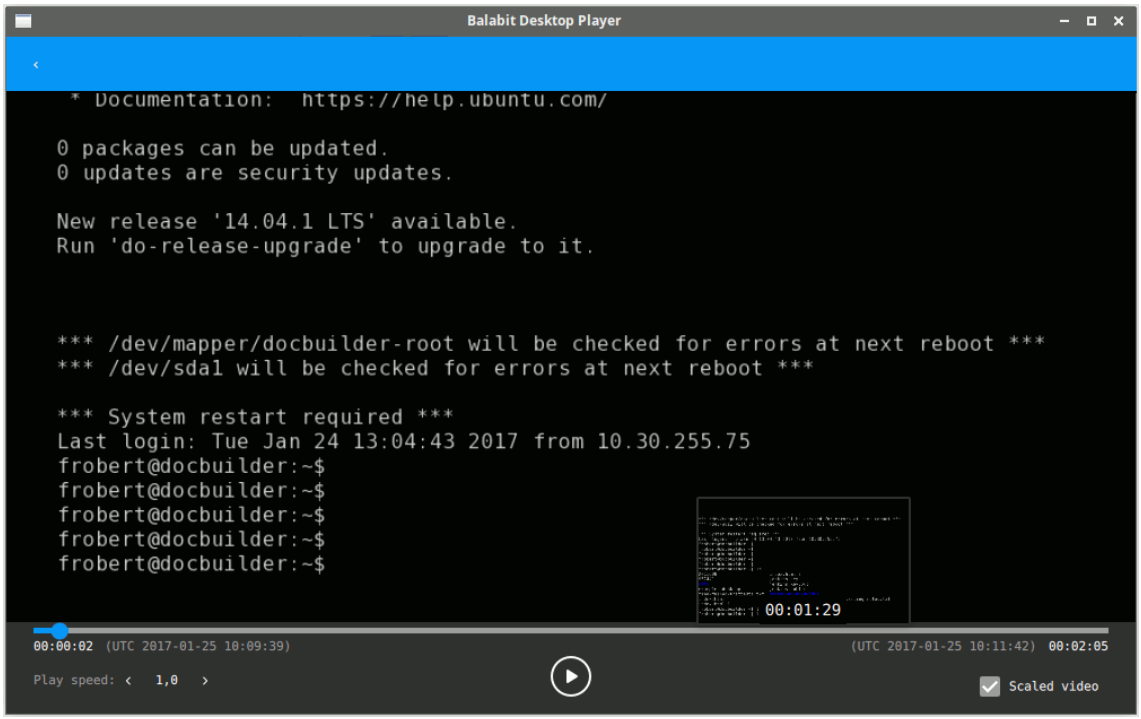
Figure 1. The Search page after the facelift



New Balabit Desktop Player

You can use the Balabit Desktop Player application to replay audit trail files that you have downloaded from the Balabit Shell Control Box.

Figure 2. Balabit Desktop Player



You can also replay these audit trails in your browser or by using the Audit Player application. Note that there are differences between these solutions:

	Audit Player	Browser	Balabit Desktop Player
Works without installation	-	✔	-
Works on any operating system	Windows	✔	Windows, Linux
Can replay TN5250 sessions	-	✔	✔
Can extract files from SCP and SFTP sessions	✔	-	From the command line
Can replay HTTP sessions	✔	-	Only exports raw files from the command line
Can start replay while rendering is in progress	✔	-	✔
Can follow 4-eyes connections	✔	-	-
Can export to PCAP	✔	-	-
Can search in the trail content	✔	✔	-
Can display user input	✔	✔	-
Export audit trail as video	-	-	✔

For further details on the Balabit Desktop Player application, see *Balabit Desktop Player User Guide*.

Online disk resizing

Newly installed SCB 5 LTS virtual instances come with a simplified filesystem structure, making online disk resizing possible. That way, you can more easily accommodate the disk requirements of your stored audit trails.

Backup and archiving improvements

SCB now fully supports backups and archiving using the NFSv4 protocol. NetApp devices are also supported.

NetApp Alliance Program

Balabit became a member of the NetApp Alliance Program.

NetApp

Alliance Partner

API changes in the AA plugin

There were API changes in the AA plugin, therefore the old plugins require an update.

- The authorize hook is now mandatory, and it must return at least an ACCEPT verdict.
- The gateway_user is now a separate argument and not a value in key-value pairs.

Changes in the ticketing plugin

SCB 4 F3 and 4 F4 included a ticketing plugin framework to integrate SCB to ticketings systems, for example, to request a valid ticket ID from the user to authorize the connection. In SCB 5 LTS and later, this functionality is available using the Authentication and Authorization (AA) plugin.

You cannot use ticketing plugins in SCB 5 LTS, they must be reimplemented as AA plugins. Contact the vendor who created the ticketing plugin for you for details on updating the ticketing plugins to AA plugins. If you received the ticketing plugin from Balabit contact your service delivery partner, or <sd@balabit.com>.

REST API changes

The following new details are available about the recorded sessions when you access the *api/audit/sessions/<connection-key>* endpoint. For details on these fields, see *Section 13.1, Audited sessions* in *Using the Balabit Shell Control Box REST API*: *_connection_id*, *alerts*, *archived*, *auth_method*, *command_extracted*, *events*, *index_status*, *network_id*, *window_title_extracted*. Also, note that the *connection_policy* field now contains the name of the Connection Policy that handled the session (in earlier version it contained the key of the session, which is now available in the *connection_policy_id* field).

The timestamps returned in the REST API now use the ISO 8601 format instead of UNIX timestamp.

The events of a session and the alerts triggered by such events is available in the *api/audit/sessions/<connection-key>/events* and *api/audit/sessions/<connection-key>/alerts* endpoints. For details, see *Section 13.4, Session events* in *Using the Balabit Shell Control Box REST API* and *Section 13.3, Session alerts* in *Using the Balabit Shell Control Box REST API*.

From now on, you can search in metadata and session content at the same time, for example: `api/audit/sessions?q=protocol:ssh&content=sudo"`

The REST API now supports X.509 certificate based authentication as well.

Unsupported browsers and operating systems

Support for the following browsers and operating systems is discontinued starting from SCB 5 LTS:

- Browsers: Internet Explorer 10
- Operating systems: Windows 2003 Server, Windows Vista

Extended support period for SCB 5 LTS

Version 4 F3 has extended support period, and will be supported for 6 months after SCB 5 LTS is released.

New SNMP/email alert when a service fails

There is a new SNMP/email alert, which is triggered when a service fails. For details, see *Section 4.6.4, System related traps* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.

New authentication protocol options when authenticating users to a RADIUS server

When authenticating users to a RADIUS server, you can now specify authentication protocol options Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP). For more information, see *Procedure 5.5, Authenticating users to a RADIUS server* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.

Export/import the configuration of SCB using the console

You can now export/import the configuration of SCB from the console using a script. For further details, see *Procedure 6.5.5, Exporting and importing the configuration of SCB using the console* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.

Improved search in reports created from audit trail content

The character limit on search words when looking for specific search expressions in content subchapters has been raised from 150 to 255 characters. For details, see *Procedure 19.3, Creating reports from audit trail content* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.

3. Changes between SCB 4 LTS and 4 F4

3.1. Installation and upgrade-related improvements

Installing Balabit Shell Control Box as a Kernel-based Virtual Machine

You can deploy SCB as a virtual appliance using the *Kernel-based Virtual Machine (KVM)* solution. For details, see *Chapter 8, Installing Balabit Shell Control Box as a Kernel-based Virtual Machine* in *The Balabit Shell Control Box 5 LTS Installation Guide*.

SCB in Azure Marketplace

You can deploy SCB from the Microsoft Azure Marketplace, with a bring-your-own-license model. For details, see the *Balabit Shell Control Box virtual machine* page.

When deployed from the Azure Marketplace, you can use Azure File storage shares in your for Backup and Archive Policies. This is very useful as the quota for the files storage can be changed dynamically, so the cumulative size of the audit trails is not limited to the OS disk size. You can set up this share as a normal SMB shares in your Backup and Archive policies. The parameters for the policy can be obtained from the Azure portal.

SCB in Azure Cloud

You can deploy SCB as a virtual machine in the Microsoft Azure cloud computing platform. This allows you to conveniently audit access to your entire virtualized infrastructure.

Simplified, more robust upgrade process

SCB 4 F1 offers a more robust upgrade process that allows you to test upgrading your configuration and correct any problems that are not compatible with version 4 F1. Also, firmware upgrading has been simplified: instead of uploading the boot and core firmwares separately, you only have to upload a single ISO file, and SCB extract the firmwares on the box.

For details, see *Procedure 6.3.2, Upgrading SCB (single node)* in *The Balabit Shell Control Box 5 LTS Administrator Guide* and *Procedure 6.3.3, Upgrading an SCB cluster* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.

3.2. Protocol-related improvements

Credential store fallback

Until now, if you have configured SCB to use a credential store, but accessing the password or the credential store failed for some reason, SCB rejected the session. From now on, SCB automatically requests a password from the user in such scenario, so your users can access the target server. This fallback is supported in the RDP, SSH, and Telnet protocols.

Inband destination selection improvements in RDP

Using inband destination selection in RDP connections without a Terminal Services Gateway was difficult and limited, because Windows RDP clients often send only the first 9 characters of the username to the server. SCB now supports parsing key-value pairs from the username, making it possible to encode the address and port of the target server into the username of the client.

Plugin framework for authentication and authorization (AAPlugin)

SCB now includes a new plugin framework that allows you to integrate with external third-party tools to request authentication or authorization for connections that SCB monitors. As a first step, AAPlugins are supported only in RDP connections.

Such plugins allow you, for example, to request additional challenge-response information from the user or an external system (for example, LDAP or Active Directory), and permit or deny the connection based on this information. For details, *contact the Balabit Support Team*.

Windows 10 support and new client applications

SCB now supports the Remote Desktop client of Windows 10.

In addition, the Royal TSX client application running on OS X, and the WinFIOL SSH client are also supported.

Network Level Authentication in RDP without domain membership

There are scenarios when you want to use SCB to monitor RDP access to servers that accept only Network Level Authentication (NLA, also called CredSSP), but SCB is not a member of the same domain (or of a trusted domain) as the RDP server. For example, you cannot add SCB to that domain for some reason, or the RDP server is a standalone server that is not part of a domain. Now SCB support such scenarios as well.

Authentication improvements in HTTP

SCB now supports the following inband authentication methods for the HTTP protocol: Basic Access Authentication (according to *RFC2617*), and the NTLM authentication method commonly used by Microsoft browsers, proxies, and servers. This allows SCB to identify HTTP sessions better, and also makes it possible to match authorized sessions to real users.

Furthermore, for authenticated sessions, SCB can perform group-based user authorization that allows you to finetune access to your servers and services: you can now set the required group membership in the Channel policy of the HTTP connection.

Integrating ticketing systems for RDP connections

SCB provides a plugin framework to integrate SCB to external ticketing (or issue tracking) systems, allowing you to request a ticket ID from the user before authenticating on the target server. That way, SCB can verify that the user has a valid reason to access the server — and optionally terminate the connection if he does not. In addition SSH and Telnet, SCB 4 F1 adds ticketing support for the Remote Desktop (RDP) protocol.

To request a plugin that interoperates with your ticketing system, contact the *BalaBit Support Team*. For details on configuring SCB to use a plugin, see *Section 18.5, Integrating ticketing systems* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.

Telnet improvements

SCB 4 F1 supports the Telnet 5250 terminal protocol, as described in *RFC2877*. Note that the Audit Player application cannot index or replay TN5250 audit trails, only the internal indexer and audit player of SCB can process them. Also, extracting usernames from TN5250 connections is not supported.

SCB 4 F1 can properly replay TN3270 audit trails without the upstream encryption key.

3.3. Audit trails and indexing

Audit Player indexer service EOL

The Audit Player indexer service has been deprecated and is not supported in SCB 4 F4. Before upgrading, you must configure SCB to use the Indexer service running on SCB, and install and configure external indexers. For details, see *Procedure 15.1, Configuring the internal indexer* in *The Balabit Shell Control Box 5 LTS Administrator Guide* and *Section 15.2, Configuring external indexers* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.

If you need help to estimate the required number and resources of the external indexers, *contact the Balabit Support Team*.

Warning
Enabling the indexer without any previous estimations is dangerous and might result in overloading the box.

The indexer does not support USB Hardware security modules (HSMs). If your audit trails are encrypted and the related private keys are stored on a HSM, DO NOT UPGRADE to SCB 4 F4.

Indexing improvements in graphical protocols

To optimize indexing resources and improve the speed and performance of Optical Character Recognition in graphical protocols, you can now configure **Indexer policies** for every Connection policy to specify the languages typically used in these connections. For example, if you know that your users use only a few languages in their connections (for example, because they use the Remote Desktop Protocol (RDP) to access only English and French software), then setting these languages in the Indexer policy improves accuracy and reduces the time required to perform character recognition.

For details, see *Chapter 15, Indexing audit trails* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.

Indexing Arabic text in graphical protocols

To make the audit trails of graphical protocols easier to review and manage in forensic situations, SCB 4 F3 adds support for Optical Character Recognition for languages that use Arabic characters. That way your auditors can search in the content of the graphical protocols, for example, in the texts typed or seen by a user in RDP, even if the text is Arabic.

Audit Player improvements

Audit Player version 2016.1 handles IPv6 metadata, and Citrix ICA connections that use the H.264 codec.

Scaling audit trail processing

If SCB audits lots of connections, processing and indexing the created audit trails requires significant computing resources, which may not be available in the SCB appliance. To decrease the load on the SCB appliance, you can install the indexer service on external Linux hosts. These external indexer hosts run the same indexer service as the SCB appliance, and can index audit trails, or generate screenshots and replayable video files from the audit trails as needed. The external indexers register on SCB, wait for SCB to send an audit trail to process, process the audit trail, then return the processed data to SCB. The external indexer hosts do not store any data, thus any sensitive data is available on the host while it is being processed.

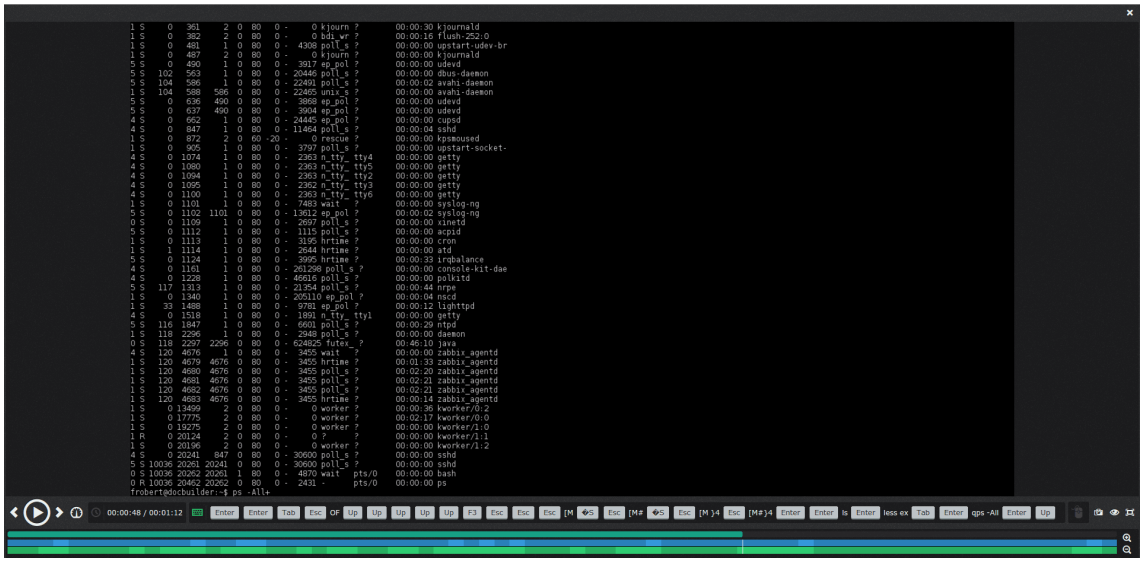
IPv6 support for the audited traffic

SCB now supports the auditing of IPv6 environments. You can audit IPv4 clients accessing IPv6 servers, IPv6 clients accessing IPv4 servers, and naturally, IPv6 clients accessing IPv6 servers. You can also use IPv6 addresses with inband destination selection.

Replaying audit trails in your browser

With SCB 4 F1, you can conveniently replay audit trails in your browser, without having to install extra software.

Figure 3. Replaying audit trails in your browser



Directly search for commands and window titles

When using the indexer service of SCB (that is, not the Audit Player application), you can directly search in the detected window titles or the commands of the audit trails. For example, the `command:sudo` search expression will return the relevant audit trails from terminal connections, while the `title:properties` search expression will return audit trails from graphical connections. For details, see *Section Searching in commands and window titles* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.

Figure 4. Searching for commands in terminal connections

3.4. REST API

More SCB features accessible using the REST API

To make integrating SCB into various management systems easier and more complete, you can now use the following SCB features using the RESTful API:

- Upload and update plugins using the API. For details, see *Section Upload a plugin* in *Using the Balabit Shell Control Box REST API*.
- You can search in the indexed content of the sessions, and also filter the search results based on the date of the session. The new REST-based search allows for much faster and flexible searching of session metadata and content. The search syntax follows the Lucene syntax, so you can group search terms, negate expressions, and so on. Note that the search interface over REST currently does not support the fine-tuned authorization capabilities that are available in the browser or over the RPC API. Fine-grained authorization is planned for the next SCB release (5 LTS).For details, see *Section 13.2, Searching in the session database* in *Using the Balabit Shell Control Box REST API*.

The documentation of the REST API received a major update, including sections on several previously undocumented features, an index of the API parameters, and a reorganization of the reference chapter.

For details, see *Using the Balabit Shell Control Box REST API*.

Search connection metadata via the REST API

You can now access and search connection metadata using the REST API, allowing you, for example, to access this information from external applications, or to run timed queries automatically.

For details, see *Section 13.2, Searching in the session database* in *Using the Balabit Shell Control Box REST API*.

More SCB features accessible using the REST API

To make integrating SCB into various management systems easier and more complete, you can now access the several SCB features using the RESTful API, including:

- *Section 15.1, Usermapping policy* in *Using the Balabit Shell Control Box REST API*
- *Section 6.10, User lists* in *Using the Balabit Shell Control Box REST API*
- *Section 14.1, Reporting* in *Using the Balabit Shell Control Box REST API*
- *Section 10.1, SSH connections* in *Using the Balabit Shell Control Box REST API*

Other features will be available via the REST API in future releases.

For details, see *Using the Balabit Shell Control Box REST API*.

Configuring SCB using a REST API

To make integrating SCB into various management systems possible, you can now access SCB using a RESTful API. Currently the API supports only the parts of the configuration that are changed most often at large enterprises, namely Channel policies.

Other features will be available via the REST API in future releases.

For details, see *Using the Balabit Shell Control Box REST API*.

3.5. Compliance and awards

HPE Security ArcSight CEF Certification

SCB has received the HPE Security ArcSight CEF Certification, and can send logs to the HPE ArcSight Data Platform via a syslog-ng relay (syslog-ng Premium Edition 5 F6 or syslog-ng Open Source Edition 3.8 and later).

Cybersecurity Excellence Awards

The Balabit Shell Control Box was a finalist of the *2016 Cybersecurity Excellence Awards* in the Privileged Access Management category. Another Balabit product, the syslog-ng Store Box (SSB), won in the Forensics category. Cybersecurity Excellence Awards are rewarded each year to individuals, products and companies that demonstrate excellence, innovation and leadership in information security. Nominees are awarded based on the content of their nomination and the popular vote by the Information Security Community.

Balabit Shell Control Box wins at SC Awards Europe

The Balabit Shell Control Box has won the *SC Awards Europe in Best Identity Management category*.

FSTEK certification

SCB has obtained the Federal Service for Technical and Export Control (FSTEK) certification, which is compulsory for information security products in Russia.

Reports and PCI DSS compliance

To help you comply with the regulations of the Payment Card Industry Data Security Standard (PCI DSS), SCB can generate reports on the compliance status of SCB. Note that this is not a fully-featured compliance report: it is a tool to enhance and complement your compliance report by providing information available in SCB. For details, see *Procedure 19.7, Creating PCI DSS reports* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.

The charts in the general operational reports of SCB have been redesigned. In addition, you can replace the Balabit logo on the cover page of SCB reports with your own logo. For details, see *Procedure 19.2, Configuring custom reports* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.

3.6. Other

New guides

Separate installation guide. To improve how information is organized in the documentation set and make it easier for users to find information relevant to their roles we have moved the chapters related to installing

SCB to a separate installation guide For more information on the installation guide, see *The Balabit Shell Control Box 5 LTS Installation Guide*.

Getting your SCB ready for Blindspotter. Blindspotter is the real-time user behavior analytics tool developed by Balabit, that can monitor the behavior of your privileged users based on the data extracted from SCB sessions. *Configuring Balabit Shell Control Box for Blindspotter* collects the most important configuration tasks to prepare your SCB installation to integrate with *Blindspotter*.

Auto-assign option for web gateway authentication

The new auto-assign option simplifies using the web gateway authentication if your users have multiple connections. After you enable auto-assignment, your users can turn on auto-assigning for their connections on the web gateway authentication page. After that, your users do not need to access the SCB web interface to assign every connection individually, it will happen automatically after the initial login. Note that this feature is available only in SCB version 4.4.1 and later.

10Gbit interface support

The SCB T-10 appliance is equipped with a dual-port SFP+ interface card labeled A and B. You can use the 10Gbit interface both for proxy traffic and for local services. This means that these interfaces can be used for the same purposes as the other 3 physical interfaces. That way, you can use SCB without any additional changes even if your network devices support only 10Gbit, and you must connect SCB to a 10Gbit-only network.

Splunk integration

Balabit provides an add-on and an app for Splunk, integrating SCB logs into Splunk, and making SCB information available in other Splunk apps, for example, in the Splunk Enterprise Security app. The *BalabitSCB Add-On for Splunk* and the *BalabitSCB App for Splunk* are both available for free in the *splunkbase*.

For details, see *Procedure 4.5.1, Configuring system logging* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.

Integration with Blindspotter

SCB now supports the operation of Blindspotter, the real-time user behavior analytics solution of Balabit. Blindspotter is a monitoring tool that maps and profiles user behavior to reveal human risk, and can analyze user behavior using the data from the audit trails recorded by SCB. *Learn more about SCB*

Flexible network configuration and VLAN support

To improve the networking flexibility of SCB and make it easier to integrate into complex environments, the networking configuration of SCB has been significantly changed. The most important improvements are as follows:

- The Bastion and Router modes of operation have been removed, and now you can use SCB in both transparent and non-transparent connections. SCB will automatically handle nontransparent (Bastion-mode) and transparent (Router-mode) connections simultaneously.
- Bridge mode has been removed from SCB.
- The network interfaces labeled as LAN1, LAN2, and LAN 3 (earlier labeled as external, internal, and management) of the appliance were dedicated to specific tasks, and you could not use them for other purposes. Now you can configure and use them any way you need to. For example, you can receive transparent connections on LAN1 and LAN2, and route them to LAN3.

- You can configure multiple logical interfaces for every physical interface. Each logical interface can belong to a different VLAN, and have multiple alias IP addresses.
- You can configure the services available on SCB (for example, remote SSH access to SCB, access to the web interface, and so on) to be available only on specific IP addresses and ports. You can also restrict access to these services based on the IP address or network of the clients.
- You can control how SCB routes unmanaged traffic (that is, traffic that passes SCB but is not inspected or audited) between its network interfaces. You can connect interface pairs, and SCB will route all unmanaged traffic between the specified interface pairs.

For details, see *Section 2.3, Modes of operation* in *The Balabit Shell Control Box 5 LTS Administrator Guide* and *Section 4.3, Network settings* in *The Balabit Shell Control Box 5 LTS Administrator Guide*.