Changelog:
Carbon Black User Documentation

Carbon Black User Guide Version 5.1.0.c

25 November 2015

Bit9, Inc.
1100 Winter Street, Waltham, MA 02451 USA
Tel: 617.393.7400 Fax: 617.393.7499
E-mail: support@bit9.com
Web: http://www.bit9.com

Purpose

This document describes changes to the *Carbon Black User Guide* in each new edition. These changes include topics that were previously not documented or were documented elsewhere, information about new features, and corrections or enhancements to existing information. Updates to the user guide generally occur when a new version of Carbon Black is released, but may also be provided between releases.

Grammatical and spelling corrections, editing changes for improved clarity, and minor factual corrections are not listed here.

This document describes documentation changes only. For *feature* changes, corrective content to address issues, or known issues still open, see the *Carbon Black Release Notes*.

Contents

Carbon Black User Guide Version 5.1.0.c (November 25, 2015)

- Chapter 1. Carbon Black Overview, Chapter 11. Threat Intelligence Feeds – Instructions were added to open port 443 for the address threatintel.bit9.com, which is now required for certain Bit9 + Carbon Black Threat Intelligence feeds.
- Chapter 3. Managing Console User Accounts – In Table 6: Team Settings and Feature Access, the required privileges and types of access for the isolation feature are detailed.
- Chapter 5. Installing Sensors – The path for the command to manually uninstall OS X agents was incorrect in previous versions of the User Guide. The correct path, `/Application/CarbonBlack/sensoruninst.sh`, is now shown.
- Chapter 7. Incident Response on Endpoints – In "Isolating an Endpoint," a note was added describing the permissions required to utilize the isolation feature.
- Chapter 10. Advanced Search Queries –
    - In Table 33: Fields in Carbon Black Process and Binary Searches, “filemod” is a default field for process searches. This was not noted previously.
    - In several tables, some queries that showed "digisig" instead of "digsig" in the field name were corrected.
    - In both Table 33: Fields in Carbon Black Process and Binary Searches and Table 34: Fields in Carbon Black Alert Page Searches, descriptive information for several fields was updated.
    - A new section called “Searching with Binary Joins” was added, detailing how to use binary search fields as part of a process search query.

- Chapter 13. Watchlists – The procedure for creating watchlists was modified for clarity.
- Appendix B. Server Backup and Restoration – The syntax for TAR commands and SQL was revised or added to support the backup/restoration of Carbon Black servers and databases:
    - Backup: Master/Standalone Carbon Black Server
    - Backup: Minion Node Carbon Black Server
    - Full Restore: Master/Single Carbon Black Server
    - Full Restore: Minion Node Carbon Black Server
    - Native Backup: Carbon Black Solr Databases
    - Restore Server Databases from Native Backups
- Appendix I. Server VDI Support – This appendix has been reorganized and edited to better present the necessary steps for VDI support.
- Appendix J. Additional Administration Documents – Document names were obsolete and incorrect in this appendix. They have been corrected.
- Appendix K: Ports and Protocols – This new appendix describes port and protocol information for several different server communications.

Carbon Black User Guide Version 5.1.0.b (September 18, 2015)

- Chapter 1. Carbon Black Overview – Table 1 was modified to indicate that TLS 1.2 (not SSL) is used for sensor-to-server communication security.
- Chapter 5. Installing Sensors – New information was added about removing inactive sensors from the sensor list.
- Chapter 8. Process Search and Analysis –
    - Descriptions of the new EMET and Blocked fields were added to the description of process event details on Analysis Preview page.
    - On Demand feeds and EMET Protections Enabled were added to the list of elements on the Process Analysis page.
- Chapter 10. Advanced Search Queries –
    - Sections on Threat Report Search and Alert Search were added to this chapter.
    - The description of tokenization of search strings was updated to indicate that leading slashes are not tokenized.
    - Recommendations were added to avoid using leading wildcards in queries.
    - There were multiple updates and corrections in Table 33, Fields in Carbon Black Process and Binary Searches.
- Appendix B. Server Backup and Restoration –
    - New information was added to the server backup procedure to include a step for killing any Carbon Black processes not stopped by overall "stop" command.
    - The -P switch was added for certain tar commands in backup procedure.
    - Missing commands for starting or stopping clusters in certain procedures were added.
    - Instructions for restoring SSH keys on minion nodes were modified.
- Appendix D: Network Integrations for Feeds –

  - A new section was added about setting up the new Open Source Connector Repository.
  - New information was added about communication requirements info for connectors, including steps for editing iptables where needed.
  - New information was added about configuring the Fidelis XPS device and FireEye device.
  - The description of the Cyphort integration was improved.
- Appendix G: Syslog Output for Carbon Black Events –
  - Many minor improvements were made to the description of Carbon Black syslog capabilities.
  - New information was added on the Host Ingress Hit on Feed and Binary Query Hit on Feed, feed.ingress.hit.process, and feed.query.hit.process.
  - Some feed tables were missing the fields “comms_ip” and “interface_ip”. These were added to this addition.
- Appendix I: Server VDI Support – This chapter was re-edited to correct minor errors and unclear wording.
- The appendix “Server Configuration File (cb.conf)” was removed from this edition of the user guide and is now a separate document available on the Bit9 + Carbon Black Customer Portal.

Carbon Black User Guide Version 5.1.0.a (June 26, 2015)

This was the first edition of the *Carbon Black User Guide* for Version 5.1. It includes the relevant contents from the Version 5.0 user guide plus information about new features in Carbon Black v.5.1.0. Topics in the guide include installation, administration, and use of Carbon Black.

Contacting Carbon Black Support

For your convenience, Bit9 + Carbon Black Technical Support offers several channels for resolving support questions:

Technical Support Contact Options
Web: www.bit9.com
E-mail: support@bit9.com
Phone: 877.248.9098 (877.**BIT9**.098)
Fax: 617.393.7499
Hours: 8 a.m. to 8 p.m. EST

Reporting Problems

When you call or e-mail Bit9 + Carbon Black technical support, please provide the following information to the support representative:

Required Information	Description
Contact	Your name, company name, telephone number, and e-mail address
Product version	Product name and version number
Hardware configuration	Hardware configuration of the Carbon Black Server or sensor computer (processor, memory, and RAM)
Document version	For documentation issues, specify the version of the manual you are using. The date and version of the document appear after the copyright section of each manual.
Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, serious, minor, or enhancement