



Carbon Black User Guide

Carbon Black Version: 5.0.0

Document Date: 26-January-2015

Copyrights and Notices

Copyright ©2011–2015 Bit9, Inc. All rights reserved. This product may be covered under one or more patents pending. Bit9 and Carbon Black are registered trademarks of Bit9, Inc. in the United States and other countries. Any other trademarks and product names used herein may be the trademarks of their respective owners.

This document is for use by authorized licensees of Bit9’s products. It contains the confidential and proprietary information of Bit9, Inc. and may be used by authorized licensees solely in accordance with the license agreement governing its use. This document may not be reproduced, retransmitted, or redistributed, in whole or in part, without the written permission of Bit9. Bit9 disclaims all liability for the unauthorized use of the information contained in this document and makes no representations or warranties with respect to its accuracy or completeness. Users are responsible for compliance with all laws, rules, regulations, ordinances and codes in connection with the use of the Bit9 products.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW EXCEPT WHEN OTHERWISE STATED IN WRITING BY BIT9. THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

Bit9, Inc. acknowledges the use of the following third-party software in the Carbon Black software product:

- Antlr python runtime - Copyright (c) 2010 Terence Parr
- Backbone routefilter - Copyright (c) 2012 Boaz Sender
- Backbone Upload - Copyright (c) 2014 Joe Vu, Homeslice Solutions
- Backbone Validation - Copyright (c) 2014 Thomas Pedersen, <http://thedersen.com>
- Backbone.js - Copyright (c) 2010–2014 Jeremy Ashkenas, DocumentCloud
- Canvas2Image - Copyright (c) 2011 Tommy-Carlos Williams (<http://github.com/devgeeks>)
- Code Mirror - Copyright (c) 2014 by Marijn Haverbeke marijnh@gmail.com and others
- D3js - Copyright 2013 Mike Bostock. All rights reserved
- FileSaver - Copyright (c) 2011 Eli Grey.
- Font-Awesome - Copyright Font Awesome by Dave Gandy - <http://fontawesome.io>
- Fontello - Copyright (c) 2011 by Vitaly Puzrin
- Freewall - Copyright (c) 2013 Minh Nguyen.
- FullCalendar - Copyright (c) 2013 Adam Shaw
- Gridster - Copyright (c) 2012 Ducksboard
- Heredis - Copyright (c) 2009–2011, Salvatore Sanfilippo and Copyright (c) 2010–2011, Pieter Noordhuis
- Java memcached client - Copyright (c) 2006–2009 Dustin Sallings and Copyright (c) 2009–2011 Couchbase, Inc.
- Javascript Digest Auth - Copyright (c) Marcin Michalski (<http://marcin-michalski.pl>)
- Javascript marked - Copyright (c) 2011–2014, Christopher Jeffrey (<https://github.com/chjj/>)
- Javascript md5 - Copyright (c) 1998 - 2009, Paul Johnston & Contributors All rights reserved.
- Javascript modernizr - Copyright (c) 2009_2013 Modernizr
- Javascript zip - Copyright (c) 2013 Gildas Lormeau. All rights reserved.
- Jedis - Copyright (c) 2010 Jonathan Leibusky
- Jmousetwheel - Copyright (c) 2013 Brandon Aaron (<http://brandon.aaron.sh>)
- Joyride - Copyright (c) 1998_2014 ZURB, Inc. All rights reserved.
- JQuery - Copyright (c) 2014 The jQuery Foundation.
- JQuery cookie - Copyright (c) 2013 Klaus Hartl
- JQuery flot - Copyright (c) 2007–2014 IOLA and Ole Laursen
- JQuery Foundation - Copyright (c) 2013–2014 ZURB, inc.
- JQuery placeholder - Copyright (c) Mathias Bynens <http://mathiasbynens.be/>
- JQuery sortable - Copyright (c) 2012, Ali Farhadi
- Jquery sparkline - Copyright (c) 2009–2012 Splunk, Inc.
- JQuery spin - Copyright (c) 2011–2014 Felix Gnass [fgnass@neteye.de]
- JQuery tablesorter - Copyright (c) Christian Bach.
- JQuery timepicker - Copyright (c) Jon Thornton, thornton_jon@gmail.com, <https://github.com/jonthornton>
- JQuery traffic cop - Copyright (c) Jim Cowart
- JQuery UI - Copyright (c) 2014 jQuery Foundation and other contributors
- jScrollPane - Copyright (c) 2010 Kelvin Luck

Carbon Black User Guide

- Libcurl - Copyright (c) 1996 - 2014, Daniel Stenberg, daniel@haxx.se.
- moment.js - Copyright (c) 2011–2014 Tim Wood, Iskren Chernev, Moment.js contributors
- MonthDelta - Copyright (c) 2009–2012 Jess Austin
- Mwheelintents.js - Copyright (c) 2010 Kelvin Luck
- nginx - Copyright (c) 2002–2014 Igor Sysoev and Copyright (c) 2011–2014 Nginx, Inc.
- OpenSSL - Copyright (c) 1998–2011 The OpenSSL Project. All rights reserved.
- PostgreSQL - Portions Copyright (c) 1996–2014, The PostgreSQL Global Development Group and Portions Copyright (c) 1994, The Regents of the University of California
- PostgreSQL JDBC drivers - Copyright (c) 1997–2011 PostgreSQL Global Development Group
- Pyrabbit - Copyright (c) 2011 Brian K. Jones
- Python decorator - Copyright (c) 2008, Michele Simionato
- Python flask - Copyright (c) 2014 by Armin Ronacher and contributors
- Python gevent - Copyright Denis Bilenko and the contributors, <http://www.gevent.org>
- Python gunicorn - Copyright 2009–2013 (c) Benoit Chesneau benoitc@e-engura.org and Copyright 2009–2013 (c) Paul J. Davis paul.joseph.davis@gmail.com
- Python haigha - Copyright (c) 2011–2014, Agora Games, LLC All rights reserved.
- Python hiredis - Copyright (c) 2011, Pieter Noordhuis
- Python html5 library - Copyright (c) 2006–2013 James Graham and other contributors
- Python Jinja - Copyright (c) 2009 by the Jinja Team
- Python ordereddict - Copyright (c) Raymond Hettinger on Wed, 18 Mar 2009
- Python psutil - Copyright (c) 2009, Jay Loden, Dave Daeschler, Giampaolo Rodola`
- Python pycogreen - Copyright (c) 2010–2012, Daniele Varrazzo daniele.varrazzo@gmail.com
- Python redis - Copyright (c) 2012 Andy McCurdy
- Python Seasurf - Copyright (c) 2011 by Max Countryman.
- Python simplejson - Copyright (c) 2006 Bob Ippolito
- Python sqlalchemy - Copyright (c) 2005–2014 Michael Bayer and contributors. SQLAlchemy is a trademark of Michael Bayer.
- Python sqlalchemy-migrate - Copyright (c) 2009 Evan Rosson, Jan Dittberner, Domen Ko_ar
- Python tempita - Copyright (c) 2008 Ian Bicking and Contributors
- Python urllib3 - Copyright (c) 2012 Andy McCurdy
- Python werkzeug - Copyright (c) 2013 by the Werkzeug Team, see AUTHORS for more details.
- QUnitJS - Copyright (c) 2013 jQuery Foundation, <http://jquery.org/>
- redis - Copyright (c) by Salvatore Sanfilippo and Pieter Noordhuis
- Simple Logging Facade for Java - Copyright (c) 2004–2013 QOS.ch
- Six - Copyright (c) 2010–2015 Benjamin Peterson
- Six - yum distribution - Copyright (c) 2010–2015 Benjamin Peterson
- Spymemcached / Java Memcached - Copyright (c) 2006–2009 Dustin Sallings and Copyright (c) 2009–2011 Couchbase, Inc.
- Switchery - Copyright (c) 2013–2014 Alexander Petkov
- Toastr - Copyright (c) 2012 Hans Fjallemark & John Papa.
- Underscore.js - Copyright (c) 2009–2014 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors
- Zlib - Copyright (c) 1995–2013 Jean-loup Gailly and Mark Adler
- libfreeimage.a - FreeImage open source image library.
- Protocol Buffers - Copyright (c) 2008, Google Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of the above third-party software and associated documentation files (collectively, the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notices and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE LISTED ABOVE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Carbon Black User Guide

Document Version: 5.0.0.a

Document Revision Date: January 26, 2015

Product Version: 5.0.0

Bit9, Inc.

266 Second Avenue, 2nd Floor, Waltham, MA 02451 USA

Tel: 617.393.7400

Fax: 617.393.7499

E-mail: support@bit9.com

Web: <http://www.bit9.com>

Before You Begin

This preface provides a brief orientation to *Carbon Black User Guide*.

Sections

Topic	Page
Intended Audience	8
Carbon Black Terminology	8
What this Documentation Covers	10
Other Carbon Black Documentation	12

Intended Audience

This documentation provides information for administrators and for members of Security Operations Center (SOC) and Incident Response (IR) teams who are responsible for setting up and maintaining security for endpoints and networks, as well as assessing potential vulnerabilities and detecting advanced threats. Staff who manage Carbon Black activities should be familiar with:

- Linux, Microsoft Windows, and Mac operating systems
- web applications
- desktop infrastructure (especially in-house procedures for software rollouts, patch management, and antivirus software maintenance)
- the effects of unwanted software

Carbon Black Terminology

The following table defines some of the key terms you will need to understand Carbon Black and its features:

Term	Definition
Carbon Black Enterprise Server	CentOS server which exists on the deployed network. It receives data from sensors, stores and indexes that data, and provides access to the data via the web interface. For simplicity, this is usually referred to as the “Carbon Black server” in this guide.
Carbon Black Sensor	Lightweight data-gatherers that are installed on hosts on the deployed network. They gather event data on the hosts and securely deliver it to the enterprise server for storage and indexing.
Alliance Server	Server that is managed by Bit9+Carbon Black that augments the functionality of the Carbon Black enterprise server.
Threat Intelligence Feeds	Pre-configured feeds from partners in the Carbon Black Alliance. These partners provide lists of IOCs (Indicators of Compromise) as well as contextual information based on binary and process attributes and events (MD5, IP, Domain). These attributes and events are scored and rated, and map to files in your environment.
RPM	Red Hat Package Manager, or RPM Package Manager (RPM), is the package management system used by Carbon Black. The name RPM refers to the rpm file format, files in this format, software packaged in RPM files, and the package manager itself. RPM is the baseline package format of the Linux Standard Base. Carbon Black is distributed and installed with RPMs.
Yum Repository	Yellowdog Updater, Modified (yum) is an open-source command-line package management utility for Linux operating systems that uses the RPM Package Manager. Yum depends on RPM, which uses hashes and digital signatures (digisigs) to verify the authorship and integrity of software. Yum is implemented as libraries in the Python programming language, with a small set of programs that provide a command-line interface. The RPMs that Carbon Black is packaged and installed with are hosted on a private Carbon Black yum repository.

Term	Definition
Cluster	A deployment of Carbon Black that includes multiple servers.
Master/Minion	In clustered configurations, one server is denoted as the master node and all other nodes are denoted as minions, subordinate to the master node.
Shard	A horizontal partition of data in a database or search engine. Each individual partition in a database is a shard. Each shard is held on a separate database server instance to spread load. When Carbon Black is scaled horizontally, event data is split into shards and distributed between servers in the cluster.
Solr	An open source enterprise search platform from the Apache project. Its major features include full-text search, hit highlighting, faceted search, dynamic clustering, database integration, and rich-document handling (for example, Word and PDF documents). Carbon Black uses Solr as its core data storage platform.
Data File	Computer file that is a resource for storing information which requires a computer program (executable or binary file) to run. Data files are not captured by Carbon Black.
Binary	<p>Executable file (for example, PE Windows file, ELF Linux file or Mach-O Macintosh file) that is loaded onto a computer file in binary form for computer storage and processing purposes. Carbon Black only collects binaries that execute. It does not collect scripts, batch files, or computer files that are created or modified.</p> <ul style="list-style-type: none"> • Carbon Black does collect the script or batch file name from command prompts and command lines. • Carbon Black also collects file names and paths as they are created or modified.
Process	An instance of the execution of a binary file.
MD5	Unique cryptographic hash identifier for a binary instance.
IOCs	Indicators of Compromise. Carbon Black sensors constantly monitor your computers for IOCs, and send alerts to the Carbon Black console when it detects them.
Watchlist	Fully-customizable searches that contain lists you can use to track specific IOCs. Watchlists are saved searches that are visible to all users. They can be used for searching either processes or binary executable files.

What this Documentation Covers

Carbon Black Administration and User Guide is your guide to setting up Carbon Black and day-to-day administration tasks: monitoring executable files on your network using the Carbon Black console; configuring the Carbon Black server; managing computers running the Carbon Black sensors; and managing Carbon Black Console users.

The numbered chapters in this book are aimed at the user of Carbon Black once it has been installed. They primarily describe features and how to access them through the web console interface.

The appendices cover more administrative topics, such as installing and configuring the Carbon Black Enterprise Server, integrating it with other tools, and directly controlling its activity through the APIs. Some of the appendices provide a brief overview of a topic and then point to other documents that provide the details.

The following table summarizes the contents of this guide:

Chapter	Description
1 Carbon Black Overview	Introduces Carbon Black, explains key concepts, and suggests operating strategies for managing sensors and data to provide the visibility, detection, and response capabilities in the Carbon Black solution.
2 Using the Carbon Black Console	Covers the basics of using the Carbon Black console: how to log in and out, how to navigate in the user interface from the menu system, and how to view the information Carbon Black makes available to you through UI elements such as tables, details pages, and dashboards.
3 Creating and Managing Console User Accounts	Describes how to manage access to the Carbon Black console for users and for teams of users.
4 Sensor Groups	Describes creating, editing, and deleting the sensor groups that determine what kind of information is provided by sensors and who can access the information.
5 Installing and Managing Sensors	Describes installing sensors on Windows, Mac OSX, and Linux systems, and provides an overview of how sensors work, the information that they provide, and how to modify their configuration.
6 Incident Response on Endpoints	Describes Endpoint Isolation and Live Response, two features in Carbon Black that can be used in incident response.
7 Process Search and Analysis	Describes how to perform detailed searches for processes, and then perform in-depth analysis on them.
8 Binary Search and Analysis	Describes how to search for binaries and investigate binary metadata.
9 Advanced Search Queries	Provides full details about Carbon Black query syntax and how to use it to construct advanced queries to search for processes and binaries.

Chapter	Description
10 Threat Intelligence Feeds	Describes Threat Intelligence Feeds that may be enabled on a Carbon Black server to enhance the verification, detection, visibility and analysis of threats on your endpoints.
11 Creating and Using Investigations	Describes how to work with investigations, which provide a way to group data for reporting, compliance, or retention purposes
12 Watchlists	Describes creating and using watchlists, which are saved searches that are visible to all users.
13 Console and Email Alerts	Describes the creation and management of Carbon Black alerts, which can be displayed in the console and also sent through email.
A Installing the Carbon Black Enterprise Server	Describes the steps for installing the Carbon Black Enterprise Server. Both new installations and server upgrades are covered.
B Integrating Carbon Black with a Bit9 Server	Describes the procedure for integrating a Carbon Black Enterprise Server with a Bit9 Platform Server and an overview of the additional capabilities this provides.
C Network Integrations for Feeds	Describes how feeds may be added based on a network integration to a local or cloud-based third-party device, and points to documents on the Carbon Black customer portal describing supported integrations.
D Carbon Black APIs	Provides a summary of available Carbon Black APIs and points to full documentation for them on github.
E Syslog Output for Carbon Black Events	Provides a summary of Carbon Black events output to syslog and points to more detailed syslog documents on the Carbon Black customer portal.
F Additional Administration Documents	Lists separate documents on the Carbon Black customer portal that address Carbon Black server and sensor administration topics.

Other Carbon Black Documentation

You will need some or all of the following Carbon Black documentation to accomplish tasks that are not covered in *Carbon Black User Guide*. These documents, as well as other technical support solutions documents, are available on the Bit9+Carbon Black Customer Portal website: <https://bit9.com/customer-portal>

The technical solutions documents are a source of information that is maintained as a knowledge base.

Some of these documents are updated with every new released build while others are updated only for minor or major version changes:

- *Carbon Black 5.0 Enterprise Server Sizing Guide* – This describes performance and scalability considerations in deploying Carbon Black.
- *Carbon Black 5.0 Release Notes* – This includes information about new and modified features in Carbon Black v5.0, issues resolved and general improvements in this release, and known issues and limitations. It also includes required or suggested preparatory steps before installing the server.

Contents

Intended Audience	8
Carbon Black Terminology	8
What this Documentation Covers	10
Other Carbon Black Documentation	12
1 Carbon Black Overview	19
What is Carbon Black?	20
System Architecture	23
Data Flows: Sensor, Server, and Cloud	24
Carbon Black Workflow Overview	26
2 Using the Carbon Black Console	29
Logging In	30
Logging Out	31
The Welcome Page	32
Using the Main Menu	33
Using Search Pages	36
Using Tables	39
Facet Tables and Charts	40
Results Tables	41
3 Creating and Managing Console User Accounts	43
User Account Management	44
Creating User Accounts	44
Changing Passwords	46
Deleting User Accounts	46
Creating Teams	47
Deleting Teams	50
Viewing User Activity	51
4 Sensor Groups	53
Sensor Group Overview	54
Creating Sensor Groups	54
Sensor Group Settings	55
Advanced Settings	56
Permissions	58
Event Collection	60
Moving Sensors to Another Group	61
Editing Sensor Groups	62
Deleting Sensor Groups	63
5 Installing and Managing Sensors	65
Overview	66
Installing Sensors on Windows Systems	66

Upgrading Sensors on Windows	68
Uninstalling Windows Sensors	70
Installing Sensors on Mac OSX Systems	71
Installing Sensors on Mac OSX Systems	71
Prerequisites	71
Installing Sensors	71
Install the Sensor Package on OSX clients	73
Upgrading Sensors on OSX	74
Prerequisites	74
Uninstalling Sensors on OSX	75
Installing Sensors on Linux Systems	75
Prerequisites	75
Installing the Linux Sensor Files on the Carbon Black Server	76
Download the Sensor Package	76
Manually Create the Linux Sensor Installation Package	78
Install the Linux Sensor Installation Package on Clients	79
Upgrading Sensors on Linux	79
Prerequisites	79
Upgrading Sensors	80
Manually Upgrading Sensors	80
Uninstalling Sensors on Linux	80
Managing Sensors	81
6 Incident Response on Endpoints	83
Overview	84
Isolating an Endpoint	84
Using Carbon Black Live Response	85
Live Response Endpoint Sessions	86
Registry Access in Live Response	89
Detached Session Management Mode	90
Extending Carbon Black Live Response	92
Live Response Activity Logging and Downloads	92
7 Process Search and Analysis	93
Overview	94
Entering Search Criteria	95
Additional Search Page Features	96
High-level Result Summaries	97
Related Events	98
Process Results Table	99
Analysis Preview	101
Process Analysis	103
Summary	104
Isolate Host	104
Go Live	105

Actions (Export events to CSV and Share)	105
Interactive Process Tree	106
Process Execution Details	107
Process Metadata	108
Alliance Feeds	109
Process Event Details.	110
Time Range Bar Graph	112
Process Event Details.	112
8 Binary Search and Analysis	115
Overview	116
Entering Search Criteria	117
Additional Search Page Features	118
High-level Result Summaries	119
Related Metadata.	120
Binary Search Results Table.	121
Binary Preview	122
Binary Analysis.	124
Binary Overview	125
Frequency Data.	125
Feed Information	126
General Info	126
File Version Metadata	127
Digital Signature Metadata.	128
Observed Paths	128
Observed Hosts.	129
9 Advanced Search Queries.	131
Query Criteria Details	132
Query Syntax Details	132
Terms, phrases and operators	132
Restrictions on Terms.	133
Whitespace.	133
Parenthesis	133
Negative sign	133
Double Quotes	133
Fields.	134
Datatypes.	138
domain	138
ipaddr	138
text	138
count.	139
datetime	139
keyword	139
md5.	139

path	140
bool	140
sign	140
cmdline	140
Example Searches	141
Process Search Examples	141
Binary Search Examples	144
Threat Intelligence (Alliance) Search Examples	145
10 Threat Intelligence Feeds	147
Overview	148
The Threat Intelligence Feeds Page	149
Checking for New Alliance Feeds	151
Syncing Alliance Feeds	151
Feeds and Data Sharing Settings	152
Enabling, Disabling, and Configuring a Feed	155
Creating and Adding New Feeds	157
11 Creating and Using Investigations	159
Overview	160
Creating Investigations	162
Adding Events to Investigations	163
Removing Events from Investigations	164
Adding Custom Events to Investigations	164
Deleting Investigations	165
12 Watchlists	167
Overview	168
Viewing and Searching Watchlists	168
Creating Watchlists	170
Editing Watchlists	173
Deleting Watchlists	173
13 Console and Email Alerts	175
Overview	176
Enabling Console Alerts	176
Watchlist Alerts	176
Threat Intelligence Feed Alerts	177
Viewing Alert Activity using the Dashboard	178
Managing Alerts on the Triage Alerts Page	181
Reviewing Alerts	184
Activity That Triggered the Alert: Description and Chart	185
Alert Data	187
Managing Alert Status	187
Enabling Email Alerts	189

Configuring an Email Server	189
Enabling Specific Email Alerts	190
A Installing the Carbon Black Enterprise Server	193
Overview	194
Firewall and Connectivity Requirements	194
Installing a New Carbon Black Enterprise Server	195
Initialization and Configuration Dialog (cbinit)	198
Upgrading a Carbon Black Enterprise Server	203
Server Upgrades and New Sensor Versions	203
Server Troubleshooting	204
B Integrating Carbon Black with a Bit9 Server	205
Overview	206
Built-in Compatibility Features	206
Features when Servers are Integrated	206
Activating Carbon Black-Bit9 Server Integration	207
Creating a Carbon Black User for Integration	207
Configuring and Activating the Integration	209
Viewing Integration Settings in Carbon Black	212
Regenerating the Authorization ID for Server Communication	213
Server Integration Features in the Bit9 Console	213
Sensor Information	213
File and Process Information	216
Event Information	217
Links to the Carbon Black Console	218
Correlation of Exported Data	218
C Network Integrations for Feeds	219
Integration Documents on the Customer Portal	219
D Carbon Black APIs	221
E Syslog Output for Carbon Black Events	223
Syslog Documentation on the Customer Portal	223
F Additional Administration Documents	225
Server Administration	225
Sensor Administration	225

Chapter 1

Carbon Black Overview

This chapter introduces Carbon Black, explains key concepts, and suggests operating strategies for managing sensors and data to provide the visibility, detection, and response capabilities in the Carbon Black solution.

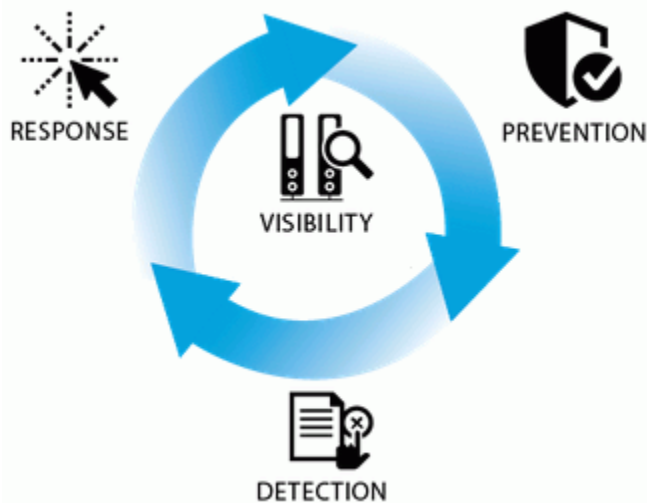
Sections

Topic	Page
What is Carbon Black?	20
System Architecture	23
Data Flows: Sensor, Server, and Cloud	24
Carbon Black Workflow Overview	26

What is Carbon Black?

Carbon Black provides endpoint threat detection and a rapid response solution for Security Operations Center (SOC) and Incident Response (IR) teams. With Bit9+Carbon Black, enterprises can continuously monitor and record all activity on endpoints and servers. The combination of Carbon Black's endpoint visibility with the Carbon Black Threat Intelligence Cloud helps enterprises to proactively hunt for threats, customize their detection, and respond quickly. This diagram shows how the Carbon Black features work together to help you answer these questions:

- How did the problem start?
- What did the threat do?
- How many machines are infected?
- How can we resolve the threat?



Bit9+Carbon Black provides you with these solutions:

- **Visibility:** Know what's happening on every computer at all times. With Carbon Black, you have immediate real-time visibility into the files, executions, network connections, and critical system resources on every machine, and the relationships between them. You can see how every file got there, what created it, when it arrived, what it did, if it made a network connection, if it deleted itself, if a registry setting was modified, and much more.
- **Detection:** See and record everything; detect attacks in real time without signatures. Bit9's threat research team analyzes threat techniques and creates Advanced Threat Indicators to alert you to the presence of an attack. These ATIs look for the indications of a threat and are not based on signatures. Now you can detect advanced threats, zero-day attacks and other malware that evades signature-based detection tools—in real time. No waiting for signature file updates. No testing and updating .dat files. No sweeps, scans or polls. You get immediate, proactive, signature-less detection.
- **Response:** Use a recorded history to see an attack's full "kill chain"; contain and stop attacks. When you need to respond to an alert or threat, you'll instantly have the information you need to analyze, scope, contain and remediate the problem. With the

recorded details about every machine, you can “go back in time” to see what happened on any of your machines to understand the full “kill chain” of an attack. You’ll also have a copy of any binary that ever executed so you can analyze it yourself, submit it to a third party, etc. And you can contain and stop attacks by globally blocking the execution of any file automatically or with a single click.

- **Prevention.** Stop attacks with proactive, signature-less prevention techniques. With Bit9, you can choose from different forms of advanced endpoint protection to match your business and systems. Bit9’s proactive “Default-Deny” approach ensures that only software you trust can run on your machines. Bit9’s “Detect-and-Deny” technology uses ATIs to detect malware and stop its execution, and Bit9’s unique “Detonate-and-Deny” approach automatically sends every new file that arrives on any endpoint or server to leading network security tools for “detonation.” If they find malicious files, Bit9 will automatically stop them from running on all of your machines—instantly.

Carbon Black accelerates detection by going beyond signatures, and reduces the cost and complexity of incident response. Using a real-time endpoint sensor, Carbon Black delivers clear and accurate visibility and automates data acquisition by continuously recording and maintaining the relationships of every critical action on all machines, including events and event types such as executed binaries, registry modifications, file modifications, file executions, and network connections.

Carbon Black provides a cross-process event type that records an occurrence of a process that crosses the security boundary of another process. While some of these events are benign, others can indicate an attempt to change the behavior of the target process by a malicious process.



Carbon Black provides a powerful platform for detection. Unlike scan-based security solutions, Carbon Black can expand detection beyond the moment of compromise with its robust endpoint sensor and the Alliance Server, which includes:

- The Bit9 Software Reputation Service (SRS), a cloud-based intelligence database that provides highly accurate and up-to-date insight into known-good, known-bad and unproven software, giving IT and security teams actionable intelligence about the software installed in their enterprise. The capabilities of the SRS are further enhanced by feeds from leading providers, including OPSWAT, Team Cymru and others.
- Carbon Black Threat Indicators look for patterns of behavior or indicators of malicious behavior. Unlike signature-based detection, threat indicators can recognize

distinct attack characteristics based on the relationships between network traffic, binaries, processes loaded, and user accounts. Carbon Black also offers watchlists, which are fully customizable saved searches that you can use to look for specific Indicators of Compromise (IOCs).

- Third Party Attack Classification, which uses intelligence feeds from third-party sources to help you identify the type of malware and the threat actor group behind an attack. This enables security teams to have a better understanding of attacks so that they can respond more quickly and effectively. You can also leverage your own intelligence feeds to enhance response capabilities.

Carbon Black compares endpoint activity with the latest synchronization of threat intelligence feeds as it is reported. You can add intelligence feeds that you already have set up to give you zero-friction consumption of threat intelligence in Carbon Black, regardless of the source.

Carbon Black's sensor is lightweight and can be easily deployed on every endpoint, requiring little to no configuration. This enables endpoint security analysts and incident responders to deploy thousands of sensors across their environment to immediately answer key response questions.

Carbon Black's continuously-recorded sensor data is stored in a central server, which enables your team to see and understand the entire history of an attack, even if it deleted itself.

Carbon Black integrates with leading network security providers such as Check Point, Fidelis, FireEye, and Palo Alto Networks. This integration enables you to prioritize alerts that are detected on the network by correlating them with events that occurred on endpoints and servers. All of this empowers you to fully investigate your entire enterprise instantly to accelerate detection, reduce dwell time, minimize scope and immediately respond to and contain advanced threats.

You can use Carbon Black's platform APIs to customize or integrate with existing security technologies that you are using, and Security Information and Event Management systems (SIEMs).

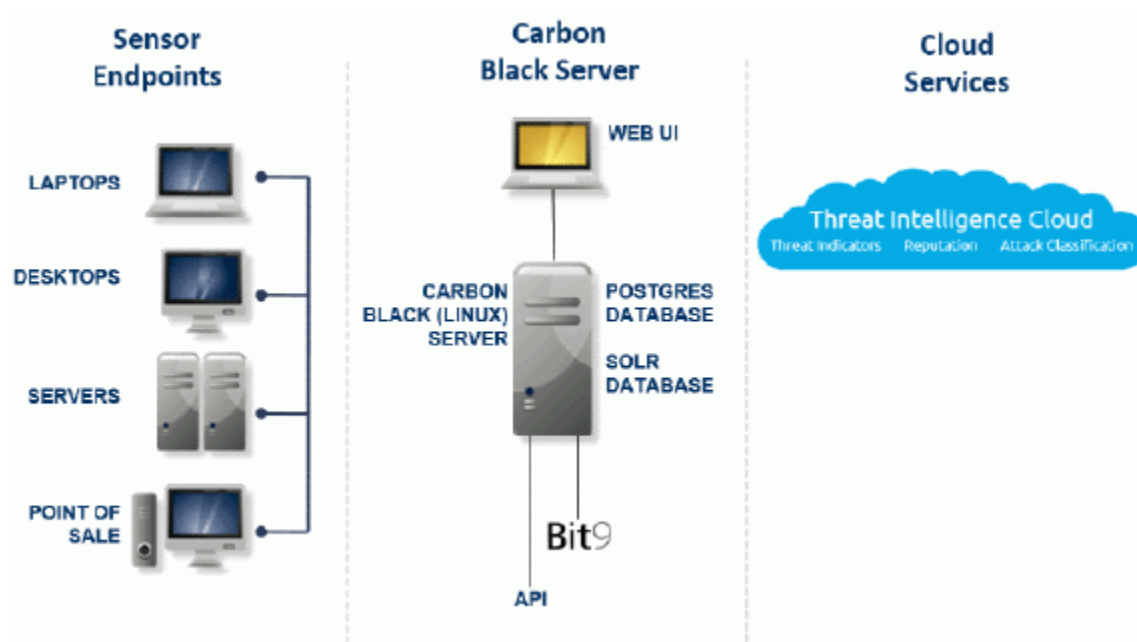
There is no one way that you can use Carbon Black. You can focus on analysis and overall health, or use it as the sentry posted at the gate, or both. For this reason, features enabled or not enabled by default might not always align with your expectations. Carbon Black is designed with as much flexibility as possible so that you can use it in the way that suits you best.

System Architecture

The Carbon Black Enterprise server software is installed on a Linux server. The Carbon Black server records events related to file changes, but copies of files and the data that changed are not recorded.

The following diagram illustrates the components of a Carbon Black installation, which are:

- Sensors that can be installed on various endpoints such as laptops, desktops, servers, and point of sale (POS) machines.
- A server that collects sensor data and makes it accessible with a web user interface or an API.
- The Threat Intelligence Cloud that includes the Bit9 Software Reputation Service (SRS), Carbon Black threat indicators, and third-party attack classification (Alliance Partner Feeds).



If your company is also using the Bit9 Platform, there is integration between it and Carbon Black. By leveraging the Bit9 Security Platform, you can contain advanced threats by globally blocking or banning them through Bit9's customizable prevention techniques in the midst of a response.

Data Flows: Sensor, Server, and Cloud

After the Carbon Black server software is installed, sensors are downloaded to endpoints and two databases are created:

- The Postgres database is used for user configuration, server configuration, and other system administration, such as the registration of sensors as they come online.
- The Solr search engine is used for all binaries, all file executions, file modifications, network connections, and registry modifications.

The following diagram illustrates the flow of data after the Carbon Black server and sensors are set up.



As soon as a sensor is installed, it begins buffering activity to report to the server. This includes:

- Currently running processes that create events
- Binary executions
- File executions and modifications
- Network connections
- Registry modifications
- Cross-process events (events that cross the security boundaries of other processes)

Every few minutes, sensors check in with the server, reporting what they have buffered, even if they are reporting that they have nothing buffered. When a sensor checks in, the server responds, letting the sensor know when to send the data and how much data to send.

As the data is sent to the server, most of it is kept in the Solr search engine, with the exception of binaries. You can configure sensor settings to allow for binary uploads. The binary uploads are not retained in the Solr database, and instead are stored in a standard data directory.

As the server records data from sensors, the data is compared with the latest synchronization from any enabled alliance feed partner. In most cases, incremental synchronizations occur hourly. Full synchronizations occur once every 24 hours by default. You can set them up to occur as often as you need them.

Most Alliance feed partners provide a list of all of the IOCs they track. Some feeds, for example, VirusTotal or Bit9, only include reports on MD5s that are observed in your enterprise. If you enable data sharing, Carbon Black pushes MD5s that are observed by sensors and binaries originating from your enterprise to the cloud. These are compared to the data that Bit9 and other third parties have on those binaries. If there is a corresponding report or record, the feed is updated to include that information.

If there is no corresponding third party report, one is requested and when available, included in the feed.

When information about a specific MD5 is included in these feeds, it remains there, even if the binary it is associated with is deleted from your endpoints and is no longer present in your environment.

Note

Results returned by Carbon Black on any search include all available data. Refer to the *Carbon Black Enterprise Server Sizing Guide* for recommendations for configuration options that affect how much data is available.

This table provides key additional information about data flows:

Table 1: Data Flow Details

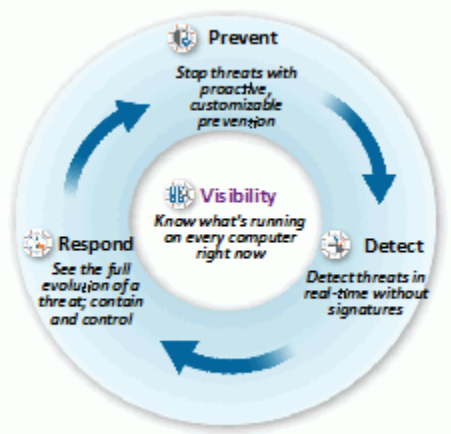
Data Flow	Description
Sensor to Server	<ul style="list-style-type: none"> • All communications are HTTPS • TCP is 443 by default, but is configurable • All communications are initiated from sensor to server (never from server to sensor). • SSL is used for confidentiality, integrity, and authentication. Sensors have the server's certificate embedded, and the server has all client certificates embedded. • Normal proxies are supported. • SSL proxies are not supported. • The server's sensor-facing interface can be configured in a DMZ to support laptops or desktops outside the corporate LAN.
Server to Alliance Server	<ul style="list-style-type: none"> • All communications are explicitly opt-in • Required for threat intelligence that is provided by Carbon Black • TCP is 433 to api.alliance.carbonblack.com • All communications are HTTPS • Proxies are supported
Server to yum Repository	<ul style="list-style-type: none"> • TCP is 443 for HTTPS to yum.carbonblack.com • TCP is 443 to a CentOS and EPEL mirror.

Carbon Black Workflow Overview

Once the Carbon Black enterprise server and sensors are installed and configured, your IT and security teams who are responsible for maintaining the health of your computer systems perform basic tasks on a regular basis to ensure that there are no threats on any computer in your enterprise.

The basic workflow is continuous: you search for threats, analyze them, resolve them, and using the tools of your choice, prevent them from happening again. As you search, you can tag any items that seem unusual or that merit further investigation and then drill down further to find out more details about those items.

Carbon Black provides you with tools to help you detect and fix threats to your system. This diagram shows the basic workflow that you use with Carbon Black:



The following table shows how Carbon Black provides solutions to the problems you face.

Table 2: Security Problems and Carbon Black Solutions

Problem	Solution
What is the entry point of the threat?	Find out how the attacker got into your systems. Get oriented with visibility into everything that is running on every computer in your enterprise using the Process Search feature.
What did the attacker do?	Look deeper into suspicious processes and events to detect evidence of damage. Select processes that look suspicious and drill deeper using the Process Analysis feature.
How many machines were compromised?	Find out the scope of the damage by digging deeper into details about detected threats by using the Process Details and Binary Details pages. Set up Threat Intelligence Feeds and Watchlists by defining characteristics of interesting activity that you want to be notified about and receiving notifications as you need them. Create Investigations of suspicious processes to keep track of key events during a given response.
How do we respond to threats?	Find out how bad the threat is, and then determine how to respond to it by seeing its full evolution, containing the threat, and then controlling it.
How do we stop the threat from happening again?	Use the Go Live feature if a problem is identified on a sensor and you need to isolate the sensor. It allows you to directly access content on endpoints that are running sensors which provide information. Set up Watchlists and Threat Intelligence Feeds that identify specific issues, and use the feeds and watchlists to perform continuous searches on your systems for immediate detection to help you stop the threat from happening again, and to ensure that you know of any new related activity.

Chapter 2

Using the Carbon Black Console

This chapter covers the basics of using the Carbon Black console: how to log in and out, how to navigate in the user interface from the menu system, and how to view the information Carbon Black makes available to you through user interface elements like tables, details pages, and dashboards. Mastering the information and tasks in this chapter will give you a head start on all other Carbon Black activities described in this guide.

Sections

Topic	Page
Logging In	30
Logging Out	31
The Welcome Page	32
Using the Main Menu	33
Using Search Pages	36
Using Tables	39

Logging In

Carbon Black has a browser-based user interface, referred to in this document as the *Carbon Black console*, for access to the Carbon Black Enterprise Server and the information it collects from sensors and threat intelligence feeds. You can log into the Carbon Black console from a web browser on any computer with access to your server. These browsers are supported:

- Google Chrome version 16 or higher
- Mozilla Firefox

To log into the Carbon Black console:

1. From any supported web browser, enter the path to the Carbon Black server.

The Carbon Black login screen displays:



2. If your browser displays a warning about the certificate, you can safely ignore the warning and click through the remaining confirmation screens. .

Note

To avoid future certificate warnings, accept the certificate permanently.

3. Enter your user name and password.
4. Click the **Login** button. The Carbon Black Welcome page displays.

Logging Out


The top right corner of Carbon Black console shows the name of the user that is currently logged in. This name also includes a menu from which you can view the profile of the logged-in user or select the Logout command.

To log out of the Carbon Black console:

1. From right end of the console banner, move the mouse cursor over the user name and choose **Logout** on the menu.

The Welcome Page

The Welcome Page provides high-level instructions for getting started with Carbon Black. Click the features that are highlighted in blue to go to the page where you define them.



Welcome to Carbon Black!

There are four steps to get started:

- 1. Download the sensor**
 - [Windows Sensor](#)
 - [OSX Sensor](#)
 - [Linux Sensor](#)

This is a sensor for the default group, with settings provided during *cbinit*. The most important setting is Server URL, as it defines how sensors will connect to this server. As your requirements grow, you can create new sensor groups, adjust settings per group, and download sensor installers for each group. You can also move existing sensors from one group to another.
- 2. Install the sensor on a computer**

The link above is the standalone executable installer. It's a ZIP archive with a digitally signed installer, a settings file and a readme. Extract the archive and run `CarbonBlackClientSetup.exe` on the target computer. The `sensorsettings.ini` file must be in the same directory, otherwise the installer won't know the Server URL.

From the Sensors page, you can also download an MSI installer. This should make deployment via Group Policy a breeze.
- 3. Confirm the sensor connected to the server**

Head over to the [sensors page](#). You should see the new computer appear within sixty seconds. If it doesn't show up, double-check the computer can reach the server via the Server URL.
- 4. Search!**

Now you're ready to pull up the [process search page](#) or the [binary search page](#) and check things out! It takes two to three minutes for data to start arriving. You may see some missing data at first, please be patient while we get everything collected and organized. If you want a fresh start from `ntoskrnl.exe`, reboot the new computer and then explore the boot process.

Using the Main Menu

The Carbon Black main menu at the top of each page allows you to easily navigate to other console pages. The menu is organized in sections according to logical task groupings, and in most cases shows a submenu of choices when you move the mouse over one of the top-level labels. Clicking on a top-level item opens the page for the first submenu choice.

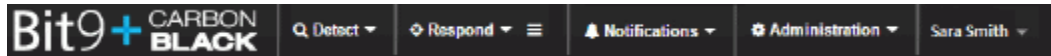


Table 3: Carbon Black Main Menu Choices

Section	Description
Detect	<p>Dashboard provides an overview of all the hosts that Carbon Black is monitoring. It displays information about the alerts found on the hosts, the users accessing the hosts, and the alert resolution status.</p> <p>Threat Intelligence provides feeds from reliable software such as VirusTotal and National Vulnerability Database. You can set up watchlists (described below), incremental synchronizations and full synchronizations with these feeds. You can also access information about process and binary matches found by each feed.</p> <p>Triage Alerts shows events that match queries defined by watchlists and Indicators of Compromise (IOCs) defined by feeds. The information that displays provides criteria that is available to use to search for specific events. The criteria that is displayed for each event is:</p> <ul style="list-style-type: none"> • Status • Username • Hostname • Feed • Watchlist • IOC • Assigned To <p>You can customize the search criteria by clicking + Add Criteria.</p> <p>Watchlists are saved queries that are performed on process events and binary data stores. The queries contain lists you can use to track specific Indicators of Compromise (IOCs). When you select a watchlist, details of the watchlist display. If you click the Search button, the full process or binary search runs, using the query that created the watch list. When the search completes, the Search Process page displays with the results.</p>

Table 3: Carbon Black Main Menu Choices (continued)


Section	Description
Respond	<p>Process Search provides an overview of the sensor process data collection from the sensors that are currently installed. Carbon Black tracks process creation, registry modifications, file modifications, DLL loads and network connections, and organizes them by process. By default, the system runs a search with *.* as criteria and displays every process that has executed. The results are sorted by the most recently executed processes, which display at the top of the list. For more information, see Chapter 7, "Process Search and Analysis."</p> <p>Binary Search shows the metadata of binary files that have been executed. Binary file data is tracked at the moment of execution. The results include every binary file that has been executed, and its metadata, in the environment. Binary file executions are identified by their MD5 hash names. For more information, see Chapter 8, "Binary Search and Analysis."</p> <p>CB Live Response is a command line page that provides direct access to sensors. Use this option if a problem is identified on a sensor and you need to isolate the sensor. This page is useful when you are performing an <i>Investigation</i> (see below), as you can directly access content on endpoints that are running sensors that are providing information. For more information, see Chapter 6, "Incident Response on Endpoints."</p> <p>Investigations are a collection of tagged process events that are products of search results which come from searching your networks and endpoints for threats. Use investigations as a way to group data for reporting, compliance, or retention purposes. For more information, see Chapter 11, "Creating and Using Investigations."</p>
	<p>Default Investigation opens the default investigation, which displays over any page that you currently have open. The default investigation consists of events that are tagged in processes from search results. You can click the icon again to delete the default investigation window. For more information, see Chapter 11, "Creating and Using Investigations."</p>
Notifications	<p>This menu contains confirmations of user actions such as tagging events and creating investigations. This information is cleared when you close the Carbon Black console.</p>

Table 3: Carbon Black Main Menu Choices (continued)

Section	Description
Administration	<p>Server Dashboard shows server storage statistics such as disk space, sensor statistics, and server communication status. For more information, see “Using Search Pages” on page 36.</p> <p>Sensors shows data for sensors and sensor groups. Much of the data on this screen relates to sensor groups, which are used to categorize sensors that share the same configuration. The dropdown menu in the upper left corner shows the group that is currently selected. You can view, define and update sensors and sensor groups on this page.</p> <p>Users enables Carbon Black administrators to add new users, view user activity, and to create teams of users. The purpose of setting up users is to define people who can log into the Carbon Black product. Teams are logical collections of users. Users can belong to several teams.</p> <p>Sharing Settings enables you to set up alliance communications settings, enable Carbon Black to gather performance information from users, set up server notification email, and to share your alert information with the Alliance Threat Intelligence Community. This page also displays your current sharing settings.</p> <p>Settings is only available to users with Global Administrator privileges. Use this page to:</p> <ul style="list-style-type: none"> • Set bandwidth throttling to control the flow of data to the server, which is helpful where bandwidth is an issue. • Define email settings for how Carbon Black sends notifications from watchlists and threat intelligence feeds. • Adjust licensing. • Review the server settings as defined in the <code>cb.conf</code> file. The <code>cb.conf</code> file allows you to check settings and configuration without touching your actual configuration. • View and edit definitions for server nodes in a cluster. • View Bit9 Platform server settings and credentials for access to the Bit9 Server. These fields are completed when integration with Bit9 Platform is configured on the Bit9 Platform side.
User name menu	<p>Profile Info shows the name, email address and teams for the user who is currently logged into the Carbon Black console. It also has a link to the user’s API token information, which is required to complete the integration with Bit9 Platform Support, and to use the Carbon Black APIs. Use this page to change the user’s password and to view and reset the user’s API token.</p> <p>Logout logs the current user out of the Carbon Black console.</p>

Using Search Pages

A primary feature in Carbon Black is the search function. You use it to look for executed processes, binaries, and threats such as Indicators of Compromise (IOCs). The search functions works the same way for many of the pages. This section provides an overview of the user interface elements that you use for searching. For detailed information about performing searches and queries, see [Chapter 7, “Process Search and Analysis,”](#) [Chapter 8, ‘Binary Search and Analysis’](#), and [Chapter 9, “Advanced Search Queries.”](#)

This is an example of a search page:

The screenshot displays the 'Search Processes' interface. At the top, there is a search bar with the placeholder text 'Contains text...' and a 'Search' button. Below the search bar, there are several filter sections for Process Name, Group, Hostname, and Parent Process. There are also four charts: Host Type (a donut chart showing server at 15% and workstation at 85%), Hour of Day, Day of Week, and Process Start Times. At the bottom, there is a table of related events showing processes like chrome.exe, googleupdate.exe, and taskeng.exe with their start times and system paths.

At the top of most pages, a search field displays.



In this field you can type *search criteria* such as a string of text, combined terms, Boolean operators, and phrases. Search criteria must be entered in a standard format. Search criteria entered without syntax is treated as a full text search, and can correspond to any field, such as a filename, a host name, a registry file, or a network connection (DNS name). These searches do not use the system indexes, which could affect query performance and accuracy.

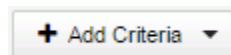
The following is an example of search criteria:

```
domain:www.carbonblack.com
```

This query would return all processes with network connections to and from domains that match the given Fully-Qualified Domain Name (FQDN).

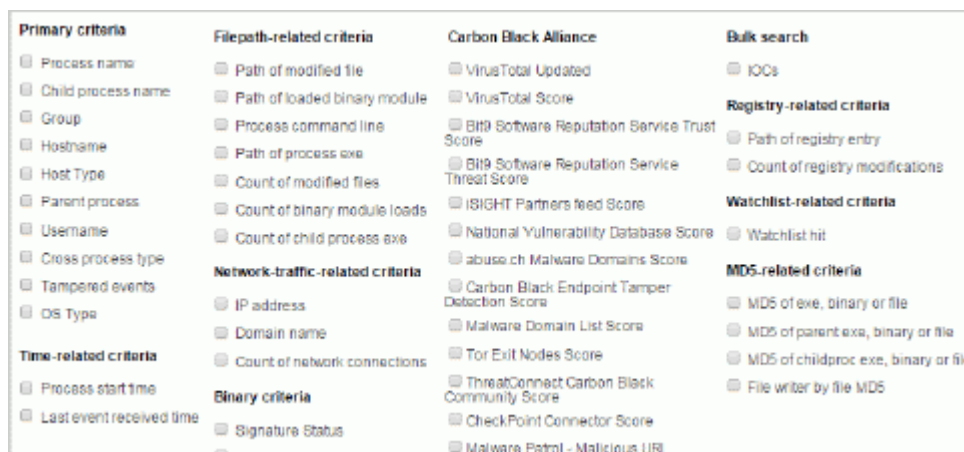
In many search fields, as you enter search criteria, the system displays the syntax for fields where the syntax must be valid, and auto-completes your criteria as you type it.

Beneath the search field, the **Add Criteria** button is displayed.



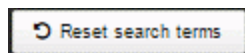
Use this in cases where you do not know which search criteria to enter or the required syntax for the search field.

When you click the **Add Criteria** button, you can select from the fields that display and enter criteria for each field. However, criteria entered this way cannot be combined using logical operators or nested to form more complex queries. Here is an example of the criteria that are available to use for search in the Search Process page:

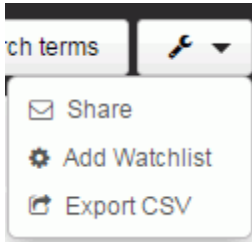


The search field and the individual criteria fields can be used independently from one another, or they can be used in combination. When used in combination, the system combines them using an "AND" operator. File names or directory names that contain spaces must be enclosed in quotation marks. Whitespaces can also be escaped by preceding the space with a backslash (“\ ”.)

At the right side of the banner where these search fields display, there is a **Reset search terms** button that you can click to remove the current search criteria and restore the default setting, which uses *.* as criteria.



At the far right side of the banner, there is a drop-down menu that provides the options to share your search criteria, add a watchlist to your search, or to export your search to a CSV file:



Search fields also appear at the top of small tables, as shown in the following example.



You can use these fields to filter the information that displays in the tables, or to search for a particular item of the type that is displayed in the table.

Using Tables

There are two types of tables that display in the Carbon Black console; small tables that display field-specific information (*facets*), and tables that display query results. The following page shows both types of tables:

The screenshot displays the Carbon Black Search Processes interface. At the top, there is a search bar with the text "Contains: text..." and a "Search" button. Below the search bar, there are several facets for filtering results:

- Process Name (50+)**: A list of processes including chrome.exe (11.0%), wmprvse.exe (3.1%), macosrvw.exe (3.1%), and ascertprotoc.othost.exe (7.9%).
- Group (1)**: A list of groups including default.group (100.0%).
- Hostname (13)**: A list of hostnames including laptop4 (69%), desktop3 (19%), desktop6 (9%), and laptop12 (3%).
- Parent Process (50+)**: A list of parent processes including svchost.exe (23.0%), searchindexer.exe (15.0%), chrome.exe (11.8%), and services.exe (9.1%).

Below the facets, there are four charts:

- Host Type**: A donut chart showing server (12%) and workstation (88%).
- Hour of Day**: A bar chart showing process counts over a 24-hour period.
- Day of Week**: A bar chart showing process counts over a week.
- Process Start Times**: A bar chart showing process counts over time.

At the bottom, there is a table of related events. The table shows 10 of 43,623 matching processes, sorted by Process start time. The table columns include Process Name, Time, Hostname, and various system metrics.

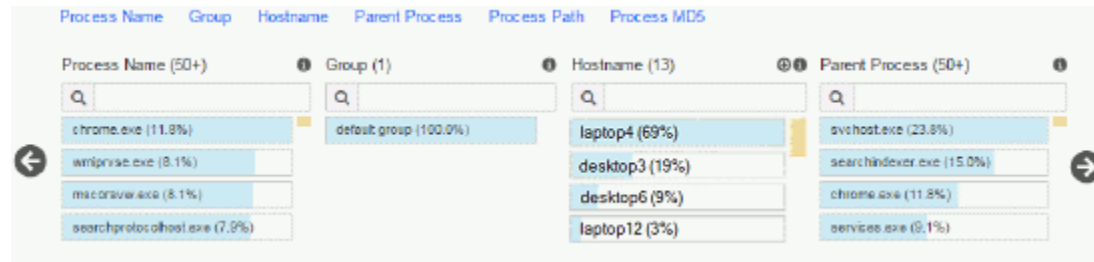
Process Name	Time	Hostname	regmod	filemod	modload	netconn	proc
chrome.exe	47 minutes ago	COMPUTERNAME	0	1	63	0	0
googleupdate.exe	48 minutes ago	COMPUTERNAME	1	0	48	0	0
taskeng.exe	48 minutes ago	COMPUTERNAME	1	0	28	0	1
chrome.exe	2 hours ago	COMPUTERNAME	0	1	63	0	0
googleupdate.exe	2 hours ago	COMPUTERNAME	1	0	48	0	0

Note

Some tables display differently from how we describe them in this section, often because they are used with unique types of data. We describe those tables in the sections where we document the features that contain them.

Facet Tables and Charts

On three main pages; Triage Alerts, Process Search, and Binary Search, beneath the **Add criteria** button, a set of *facets*, which are small tables, cross the page, with arrows on either end that enable scrolling to display additional facets.



The number of facets is fixed and so is their arrangement. Facets are used to filter the search results, and they work in conjunction with the criteria entered in the **Search** field. Beside the facet name, a number indicates the volume of results up to 50. If there are more than 50 results, the result volume displays as (50+).

Beneath each of the search fields for each facet are the results of the current search. The default search uses `*:*`, so in the Process Name facet, the top process listed is the process that has occurred more than any other process out of the total "matching processes" identified farther down on the screen. The top row is always shaded completely (100%), whether it occurred once, twice, or hundreds of times. The other rows are shaded in proportion to the number of matching results they had relative to the most frequent process. Centrally located beneath the facets is a **More** button that expands the view of facet results and adds scrollbars to them to show all of the results for each facet. Clicking any of the listed results for a facet highlights it and uses it to filter the process search results. Clicking a second time deselects the result. You can select multiple facet results.

On the Process Search and Binary Search pages, a row of charts displays under the facet tables, based on the results of the search. This is an example of the types of charts that display.

































In charts that contain bars, you can click on a bar to filter the results that display based on the information for that bar. You can hover over the information icons for specific information about each chart.

Results Tables

When you run queries using the search field described in “Using Search Pages” on page 36, the search results display in a large table at the bottom of the page, as shown in this example:

Showing 10 of 43,404 matching processes Sort by Process start time

	googleupdate.exe	25 minutes ago on COMPUTERNAME	regmod 1	filemod 0	modload 48	netconn 0	proc 0	 
c:\program files (x86)\google\update\googleupdate.exe								
	taskeng.exe	25 minutes ago on COMPUTERNAME	regmod 1	filemod 0	modload 28	netconn 0	proc 1	 
c:\windows\system32\taskeng.exe								
	chrome.exe	30 minutes ago on COMPUTERNAME	regmod 0	filemod 0	modload 62	netconn 0	proc 0	 
c:\program files (x86)\google\chrome\application\chrome.exe								
	chrome.exe	33 minutes ago on COMPUTERNAME	regmod 0	filemod 1	modload 63	netconn 0	proc 0	 
c:\program files (x86)\google\chrome\application\chrome.exe								
	googleupdate.exe	1 hours ago on COMPUTERNAME	regmod 1	filemod 0	modload 48	netconn 0	proc 0	 
c:\program files (x86)\google\update\googleupdate.exe								
	taskeng.exe	1 hours ago on COMPUTERNAME	regmod 1	filemod 0	modload 28	netconn 0	proc 1	 
c:\windows\system32\taskeng.exe								
	chrome.exe	2 hours ago on COMPUTERNAME	regmod 0	filemod 1	modload 63	netconn 0	proc 0	 
c:\program files (x86)\google\chrome\application\chrome.exe								
	googleupdate.exe	2 hours ago on COMPUTERNAME	regmod 32	filemod 1	modload 72	netconn 1	proc 0	 
c:\program files (x86)\google\update\googleupdate.exe								
	googleupdate.exe	2 hours ago on COMPUTERNAME	regmod 1	filemod 0	modload 57	netconn 0	proc 0	 
c:\program files (x86)\google\update\googleupdate.exe								
	taskeng.exe	2 hours ago on COMPUTERNAME	regmod 1	filemod 0	modload 28	netconn 0	proc 1	 
c:\windows\system32\taskeng.exe								




First ← 1 2 3 4 ... → Last

This example illustrates many of the typical elements in Carbon Black results tables. The top row contains an option to define how many results display. In most places the default number of displayed results is 10. In the top row on the right is the **Sort by** field, which provides options for sorting the results that display that are unique for each type of search.

On each row, on the left, you can see an icon for the type of process beside its name.

The following table describes icons that commonly display in rows and how to use them:

Table 4: Table icons

Icon	Description
>	If you click on the filename (highlighted in blue), or the > sign at the far right, a page with details about the file opens. For example, if the result came from a process search, the process analysis page opens, and if the result came from a binary process or watchlist page, a details page opens.
	The Preview icon opens a preview page for the result
	The Watchlist icon opens the watchlist that contains the result.
	The Tag icon indicates if the result contains an event that is included in an investigation. A gray tag icon indicates that a process does not have any events tagged for an investigation. A blue tag icon indicates that the result contains events that are tagged in an open investigation. Results that contain events that are tagged in an investigation other than an open one have a black tag icon.

Chapter 3

Creating and Managing Console User Accounts

This chapter explains how to manage access to the Carbon Black console for users and for teams of users.

Sections

Topic	Page
Creating User Accounts	44
Changing Passwords	46
Deleting User Accounts	46
Creating Teams	47
Deleting Teams	47
Viewing User Activity	51

User Account Management

Each Carbon Black console user must log into the system with a user name and password. User accounts provide system-management professionals and others who use the Carbon Black console the ability to access and manage Carbon Black features.

During Carbon Black installation, a default user account is created, and is assigned to the Global Administrator role.

You can set up users with the Global Administrator role, or with roles that have varying levels of access. The Global Administrator role has full access to all administrative, product, and sensor settings and data. You define users as Global Administrators when you are creating a user account. You define roles with different levels of access when you create teams. For information about teams, see [“Creating Teams”](#) on page 47.

Creating User Accounts

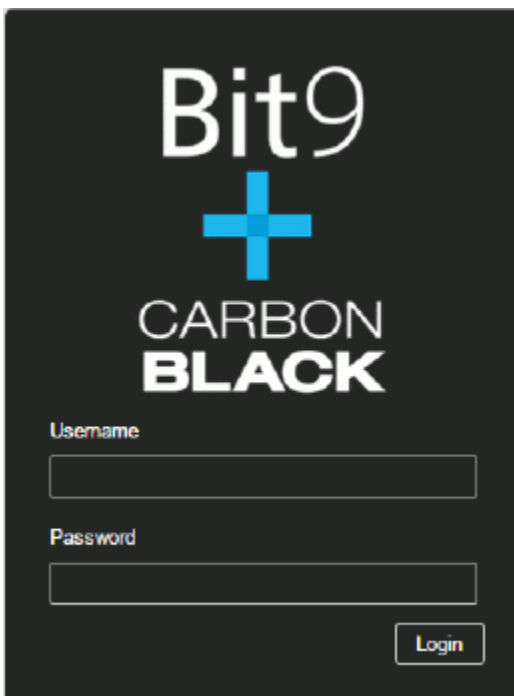
Use the URL for the Carbon Black Enterprise server and the administrative user ID and password that were created during the Carbon Black Enterprise server installation and configuration process to log into the Carbon Black console.

To create a user account:

1. From any supported web browser, enter the path to the Carbon Black Enterprise Server, for example:

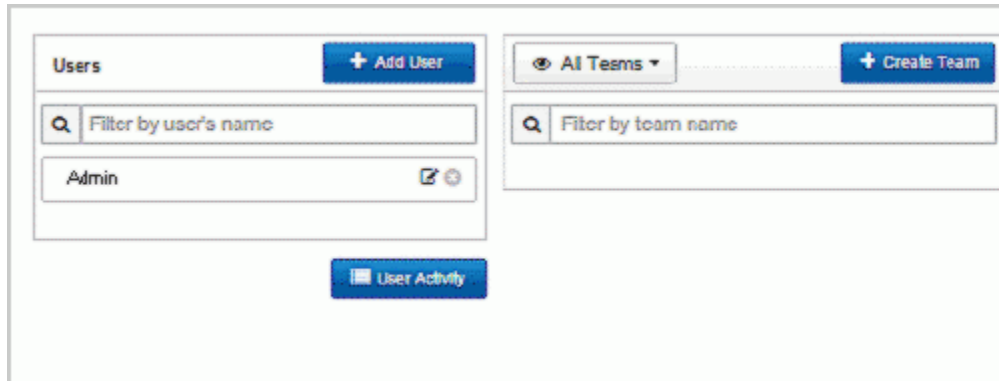
```
https://<your Carbon Black Enterprise server address>/
```

The Carbon Black login screen displays:



Enter the user name and password that were set up in the `cbinit` script during the installation process.

2. From the console menu, choose **Administration > Users**. The Users page displays.



3. Click **Add User** and enter the information described in the following table. All the fields are required.

Table 5: Add User Fields

Field	Description
Username	Name that the user enters to log into the Carbon Black console. Enter any combination of letters, numbers, or English-keyboard characters. User names are not case sensitive. Note: User names are restricted to standard, Latin alphanumeric characters. Symbols and punctuation characters are not allowed. If you attempt to create a user account with an illegal character, the Carbon Black console will display a warning dialog box.
First Name	First name of the user.
Last Name	Last name of the user.
Email address	Email address for the user.
Password	Password that authenticates this user. Enter any combination of letters, numbers, or special characters. Passwords are case sensitive. This field changes to New Password when you are editing existing accounts.
Confirm password	Retype the password to ensure that the password is the one you intended to use.
Assign to	Select the team in which to include the user. The default team is Administrators. You can select more than one team. For information about teams, see “Creating Teams” on page 47.
Global Administrator	Select this option to give the user Global Administrator privileges.

4. Click **Save changes**.

Changing Passwords

It is recommended that users change their passwords after they log in for the first time.

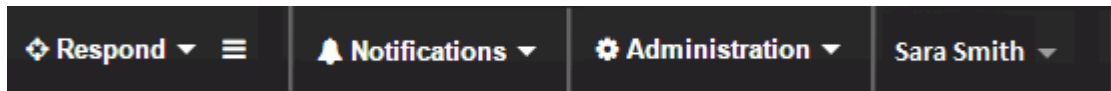
Note

If you need to change an administrator's password, contact Carbon Black support.

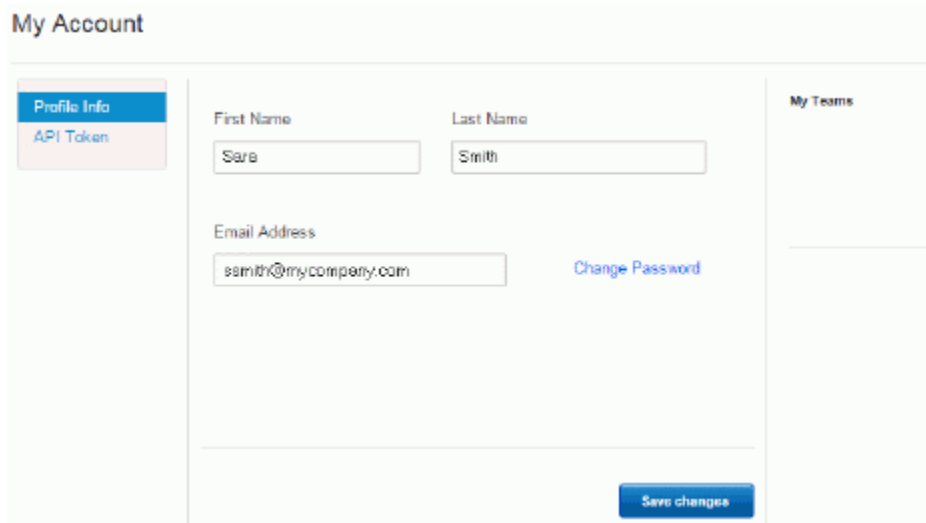
To change a user password:

1. Log into Carbon Black with the user name and password provided by the system administrator.

At the far right of the console menu, choose *yourusername* > **Profile info**.



2. The My Account window opens.



3. Click **Change Password**. The Change Password window opens. Enter your current password and your new password, and then verify your new password.
4. Click **Save changes**.

Deleting User Accounts

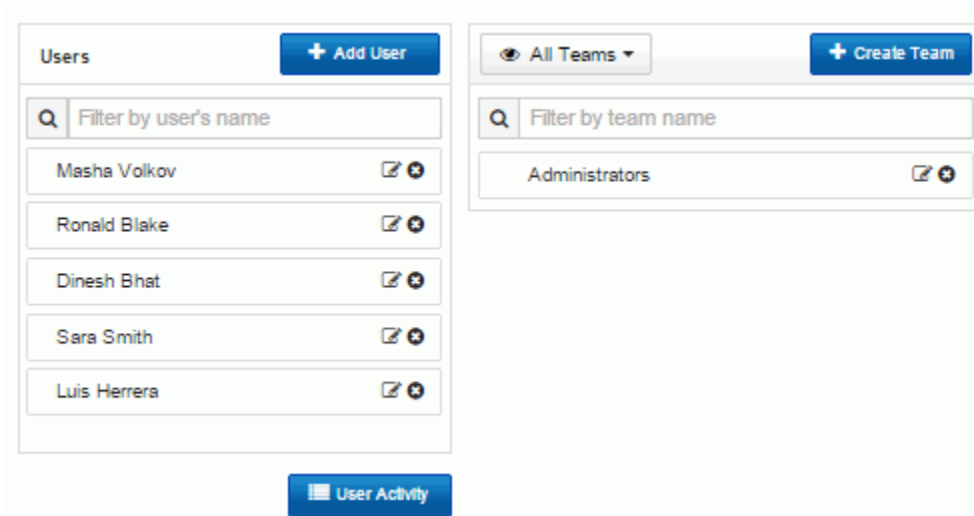
User accounts can be removed from the system, for example, when an employee no longer needs access to the Carbon Black console or leaves the company. By default, users with Global Administrator privileges can delete any account except their own. If the user with the deleted account belongs to a team, the user will automatically be removed from the team when the user account is deleted.

Note

You cannot delete the default administration account.

To delete a user account:

1. From the console menu, choose **Administration > Users**. The Users page appears:



2. Locate the user's name and click the Delete icon.
3. Respond to the confirmation prompt. To delete the account, click **OK**.

Creating Teams

A team is defined by the type of access it has to each sensor group. During Carbon Black installation, a default sensor group (called Default Group) is created and the sensor group is automatically defined with Administrator access. A default user account is also created, and is assigned to the Global Administrator role and given Administrator access to the default sensor group. You can create user roles by assigning users to teams with varying levels of privileges for sensor groups.

The types of privileges that are available are:

- Administrator
- Viewer Access
- No Access

You create teams in the **Administration** menu on the Users page. The steps for defining teams and roles are included in this sections.

The following table describes privileges and the types of access that are available for each role.

Note

If a user is defined as a Global Administrator, the Global Administrator privileges provide access to all functionality. This overrides privileges that are assigned in teams.

Table 6: Team Settings and Feature Access

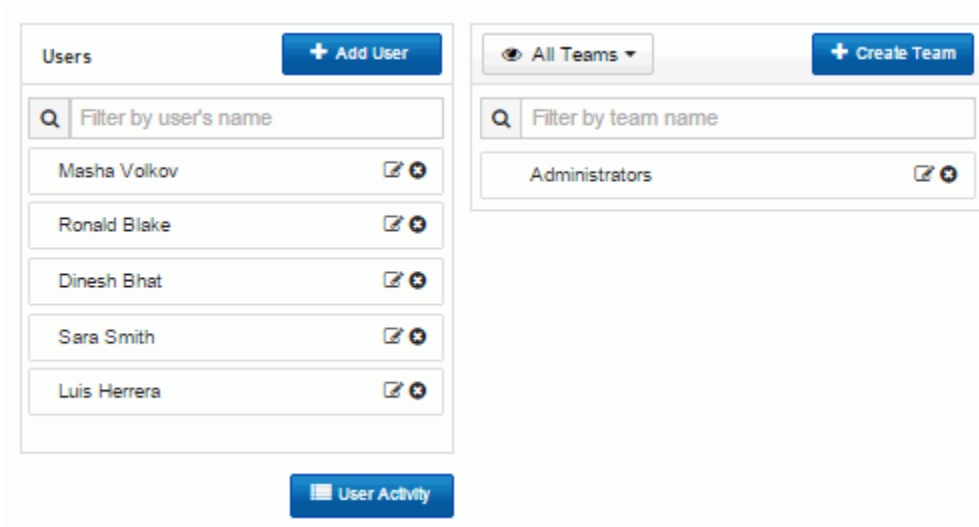
Features	Global Administrator	Administrator	Viewer Access	No Access
Administration				
Server Dashboard	Read/Write Access	No Access	No Access	No Access
Sensors and Sensor Group Settings	Read/Write Access	Read/Write Access	Read Access	No Access
Users	Read/Write Access	No Access	No Access	No Access
Sharing Settings	Read/Write Access	No Access	No Access	No Access
Settings	Read/Write Access	No Access	No Access	No Access
Detect				
Dashboard	Read/Write Access	Read/Write Access	Read/Write Access	Read/Write Access
Threat Intelligence	Read/Write Access	No Access	No Access	No Access
Triage Alerts	Read/Write Access	Read/Write Access	Read/Write Access	Read/Write Access
Watchlists	Read/Write Access	Read/Write Access	Read/Write Access	Read/Write Access
Respond				
Process Search	Read/Write Access	Read/Write Access	Read/Write Access	Access (no data displays)
Binary Search	Read/Write Access	Read/Write Access	Read/Write Access	Read/Write Access (data displays)
CB Live Response	Read/Write Access	No Access	No Access	No Access
Investigation	Read/Write Access	Read/Write Access	Read/Write Access	Read/Write Access
Notifications	Read/Write Access	Has Access	Has Access	Has Access
User Name Menu				
Profile info	Read/Write Access	Read/Write Access	Read/Write Access	Read/Write Access
Logout	Read/Write Access	Read/Write Access	Read/Write Access	Read/Write Access

The following scenario provides an example of how you could set up user accounts and teams.

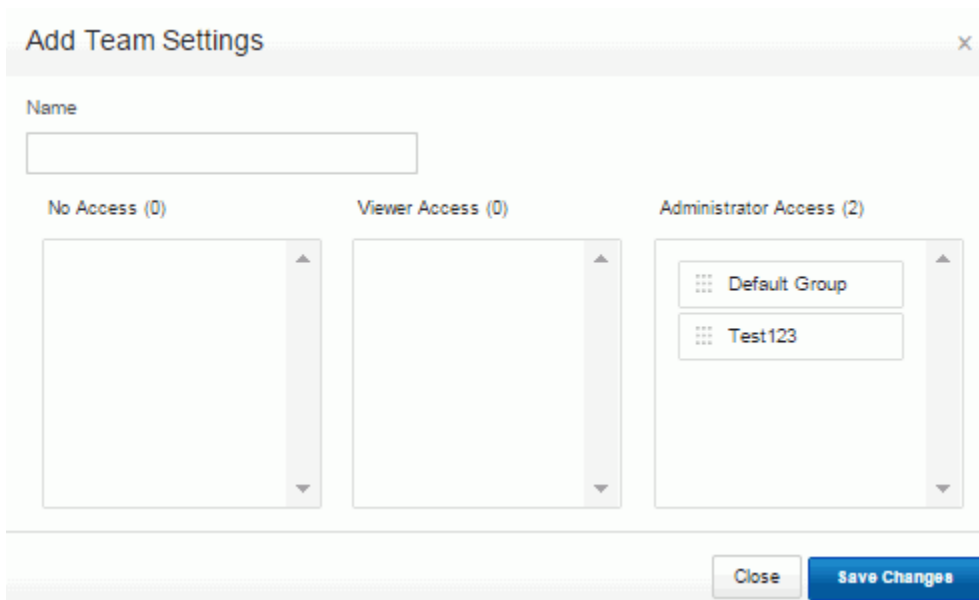
Suppose that a division of your company is based in Europe, with sites in England, France, Germany, and Italy. You have administrators in each country that oversee the computers in their countries' sites. You could assign the country administrators the role of Global Administrator, so that they can set up their users and user teams, and associate them with the sensor groups that are defined for their regions. If there are users who are responsible for computers that belong to more than one sensor group, you could add these users to multiple teams to ensure that they have the access and visibility into all the sensor groups they need to monitor.

To create teams:

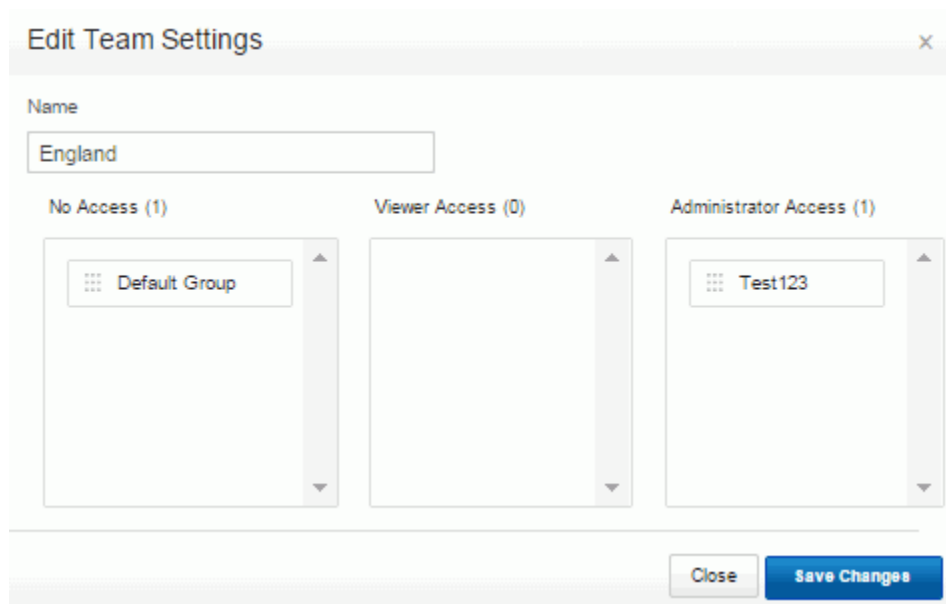
1. From the console menu, choose **Administration > Users**. The Users page opens.



2. Click the **Create Team** button. The Add Team Settings page opens.



3. In the **Name** field, enter a name for the team.
4. Drag and drop the sensor groups to the list with the type of permissions that are appropriate for this team. For example, if you want this team to have no access to the sensor group named “Default Group,” you would drag and drop the Default Group box to the No Access list.
You could assign roles to users by adding them to teams that are set up with the type of privileges that are appropriate for the role (Administrator, Viewer Access, or No Access).
This screen capture shows a team definition for a team called “England” with no access to the default sensor group and administrator access to the Test123 sensor group.



5. Click **Save Changes**.

Deleting Teams

You can delete teams from the Users page. When you delete a team, references to the team in user accounts are deleted as well, but the user accounts remain active.

To delete a Carbon Black team:

1. From the console menu, choose **Administration > Users**. The Users page displays.
2. In the list of teams, click the Delete (x) icon. The team is removed.
3. From the console menu, expand the **Notifications** menu to see a confirmation that the team has been deleted

Viewing User Activity

Carbon Black keeps an audit trail of user activity on the console.

To view user activity:

1. From the console menu, choose **Administration > Users**.
2. Click **User Activity** at the bottom of the Users column. The following information displays.

Table 7: User Activity Fields

Field	Description
Username	The user name of the user who has accessed the Carbon Black console.
Timestamp	The full date and time that the user logged into the Carbon Black console.
Remote IP	The IP address of the computer that the user logged in on.
Result	The HTTP response code when the user accesses a resource. For example, a successful authentication would show an HTTP 200 code response. If a user did not have permission to access an administrator-based resource, an HTTP 403 code would display.
Description	The HTTP response description. For example, an HTTP 200 response would show "OK" as a description, while an HTTP 403 response would show a "Requires Authentication" response.

3. Click **Export to CSV** to export the activity results in a CSV format with the filename `UserActivity.csv`.

Note

The access logs for user activity are located on the Carbon Black Enterprise server in the following file:

```
/var/log/cb/coreservices/debug.log
```


Chapter 4

Sensor Groups

This chapter describes creating, editing, and deleting sensor groups.

Sections

Topic	Page
Sensor Group Overview	54
Creating Sensor Groups	54
Sensor Group Settings	55
Advanced Settings	56
Permissions	58
Event Collection	60
Moving Sensors to Another Group	61
Editing Sensor Groups	62
Deleting Sensor Groups	63

Sensor Group Overview

Carbon Black sensors are lightweight data-gatherers that are installed on endpoints (such as laptops, desktops, and servers) on a deployed network. They gather event data on the endpoints and securely deliver it to the enterprise server for storage and indexing. Each sensor is associated with a sensor group that defines its configuration and security characteristics. One sensor group can contain many sensors, but a single sensor can only belong to one sensor group.

Sensor groups can be based on your security and organizational requirements. For example, you might base sensor groups on functional groups (such as marketing, customer service, or IT), or location.

If you move sensors from one sensor group to another, the sensors will receive security settings from the new group the next time they check back in to the server. In most cases, you do not have to reinstall the sensors when you move them. For more information, see [Chapter 5, “Installing and Managing Sensors.”](#)

Creating Sensor Groups

You can create sensor groups either before or after installing sensors. By default, sensors are installed into a sensor group named *Default Group*.

When you create sensor groups you define the following groups of settings:

- Basic sensor group settings (required), where you define the name of the sensor group and the URL that the sensor group uses to communicate with the Carbon Black Enterprise server. Carbon Black sensor-to-server communications are basically HTTPS, and behave as if the user opened a web browser to the Carbon Black Enterprise server.
- Advanced settings , where you define limits for the sensor group’s disk consumption on the host, enable VDI (Virtual Desktop Infrastructure) for sensors on virtual machines, define the site that the group belongs to, the name of the sensor executable file, the sensor upgrade policy, tamper level settings, and critical alerts settings
- Permissions, where you define the levels of access for user teams to systems in the sensor group
- Event collection, where you determine which event data to collect from the installed sensors in this group

Sensor Group Settings

In the Create Group page, on the Settings tab, the required information that you define is the sensor group name and the URL that the sensors use to communicate with the Carbon Black Enterprise server. Hover over the information icons for tips about what to enter in the fields.

To define sensor group settings:

1. From the console menu, choose **Administration > Sensors**. The Sensor page displays a list of all the installed sensors and several options at the top of the page.

Computer Name	Status	Activity	OS Version	Node Id	Sensor Version
COMPUTER3	Online	Expected in 42 seconds	Windows Server 2012 R2 Standard Edition,	0	5.0.0.41124
COMPUTER45	Online	Expected in 42 seconds	Windows Server 2012 R2 Standard Edition,	0	5.0.0.41124
COMPUTER8	Online	Expected in 42 seconds	Windows Server 2012 R2 Standard Edition,	0	5.0.0.41124
COMPUTER12	Offline	Last seen about 3 months ago	Windows 7 Service Pack 1, 32-bit	0	4.1.5.40410

2. Click the **Create Group** button. The Create Group page opens.

Create Group X

Settings
Advanced
Permissions
Event Collection

Name ⓘ

Search binary hashes with VirusTotal
Be notified of any binary flagged by VirusTotal. Information such as the filename, MD5 hash and parent process will be shared with the Bit9 Alliance partners. Any binary available on the Alliance server is deleted, saving disk space.

Server URL ⓘ

This URL is unsecure. HTTPS is recommended

Scan unknown binaries with VirusTotal
Detect new variants of known malware by sharing the full binary content of unknown executable files. Binaries will be uploaded and shared with the Bit9 Alliance partners.

Once the group is saved, you can modify in [Share Settings](#).

3. In the **Name** field, type the name of the new sensor group. Only alphanumeric characters can be used.
4. In the **Server URL** field, type the URL that the sensor group uses to communicate with the Carbon Black Enterprise server. This URL is usually the same one that is used to log into the Carbon Black Enterprise server. Use HTTPS, and specify the secure port in the URL.

Note

Be especially careful when entering or editing the server URL. An error in entering a URL can shut off communication between sensors and the server.

5. (Optional) Select **Search binary hashes with VirusTotal** to be notified of binaries flagged by VirusTotal that are found in your systems. Information such as the filename, MD5 hash and parent process will be shared with the Bit9 Alliance partners.
6. (Optional) Select **Scan unknown binaries with VirusTotal** to allow VirusTotal to scan your systems for new variants of known malware by sharing the full binary content of unknown executable files. These binaries are shared with Bit9Alliance partners.
7. You can click **Save Changes** to save the information you just defined and close the Create Group page, or you can click the **Advanced** tab to define advanced settings for the sensor group. After you save the sensor group settings, you can modify the VirusTotal options described in steps 5 and 6 in **Administration > Sharing Settings**.

Advanced Settings

You can define advanced settings in the Create Group or Edit Group Settings page. The options are the same on each page. In this procedure, we are using the Create Group page.

On the Advanced tab, you define:

- Sensor-side Maximum Disk Usage, which is the worst-case queuing capacity for sensors should the server go down
- Virtual Desktop Infrastructure (VDI) enablement for sensors on virtual machines
- Site information for throttling data from sensors
- Sensor Name (should you want to overwrite or prefix the default name of cb.exe)
- Sensor Upgrade Policy for all the sensors in this group. This is useful when sensor versions must be tested or vetted.
- Tamper Level settings
- Alerts Critical level

Hover over the information icons for tips about what to enter in the fields.

To define advanced settings for sensor groups:

1. From the console menu, choose **Administration > Sensors**. The Sensor page displays.
2. Click the **Create Group** button. The Create Group page opens.

- Click on **Advanced**. The Advanced tab opens.

- Under **Sensor-side Max Disk Usage**, there are two options that limit the sensors' disk consumption on clients: raw available space (in megabytes) or percentage of the total space available. The sensors will limit the amount of space they use on clients based on the smaller of the two values.
 - In the **MB** field, type the maximum available space on the client, in megabytes, that sensors can use.
 - In the **%** field, type the maximum percentage of total disk space on the client that sensors can use.
- Select **VDI Behavior Enabled** to enable Virtual Desktop Infrastructure (VDI) for sensors on virtual machines. Use VDI when endpoints that are virtual machines are reimaged. Sensor IDs are maintained across reimaging by hostname, mac, or other determining characteristics.

Note

VDI support must be globally enabled in order to use this feature.

- Under **Site**, select a site from the drop down menu to assign to this sensor group. You can use site definitions to define throttle settings to manage bandwidth for groups of computers. If bandwidth is an issue for this group of sensors, create or configure a site with the appropriate bandwidth settings in **Administration > Settings > Sites**, and then assign the site to this sensor group by selecting the site in this field.

7. In **Sensor Name**, enter a new name for the sensor group to overwrite or to prefix the default name of cb.exe, for example, if Operations Security (OPSEC) considerations dictate that sensors run with a non-standard or obfuscated executable name. If this option is specified, the process will run with this name instead of the default cb.exe. This will not change the Windows service display name, but it will change the name of the actual executable that is run.
8. Use the **Sensor Upgrade Policy** field to configure the upgrade policy for the sensors in this group. This field is a drop down list with the following options:
 - **Manual** - enables you to upgrade the sensors at any time to any version
 - **Always Latest** - automatically upgrades the sensors to the latest version
 - **specific version number** - a list of version numbers that you can select from. You can select a version for all the sensors, which will keep all the sensors at that specific version.

Selecting the upgrade policy of a specific version is useful when sensor versions must be tested or vetted. In most cases, there is no information loss when you upgrade the sensors.
9. Click the bar in **Tamper Level Settings** to turn these settings on or off. With tamper detection enabled, the sensor identifies attempts to modify the sensor configuration or memory and sends alerts on the attempts.
10. Click the bar in **Alerts Critical Level** to alter the critical level for alerts on a per-sensor-group basis. This directly effects the severity rating for alerts generated by this sensor group. On the **Detect > Triage Alerts** page, the severity score of an alert is determined by three components: feed rating, threat intelligence report score, and sensor criticality (i.e., server sensors could have a higher criticality than engineering workstations). For example, if there are two sensor groups with different alert criticality, when these sensor groups get alerts from the same feed and for the same report, the sensor group with the higher alert criticality will have a higher severity score on the Triage Alerts page, and servers in that group will display at the top of the queue.
11. Click **Save Changes**. The Create Group page closes and the Sensor page displays, with the name of the new group at the top left of the page.

Permissions

In the Edit Group Settings page, on the Permissions tab, you define what kind of access each team of user login accounts has to the sensors in this group.

Note

The Permissions tab displays in the Create Group page, but does not contain the teams that are available for this sensor group. After you have entered the sensor group information on the Settings tab, saved your changes, and refreshed your browser, the available teams display in the Edit Group Settings page on the Permissions tab.

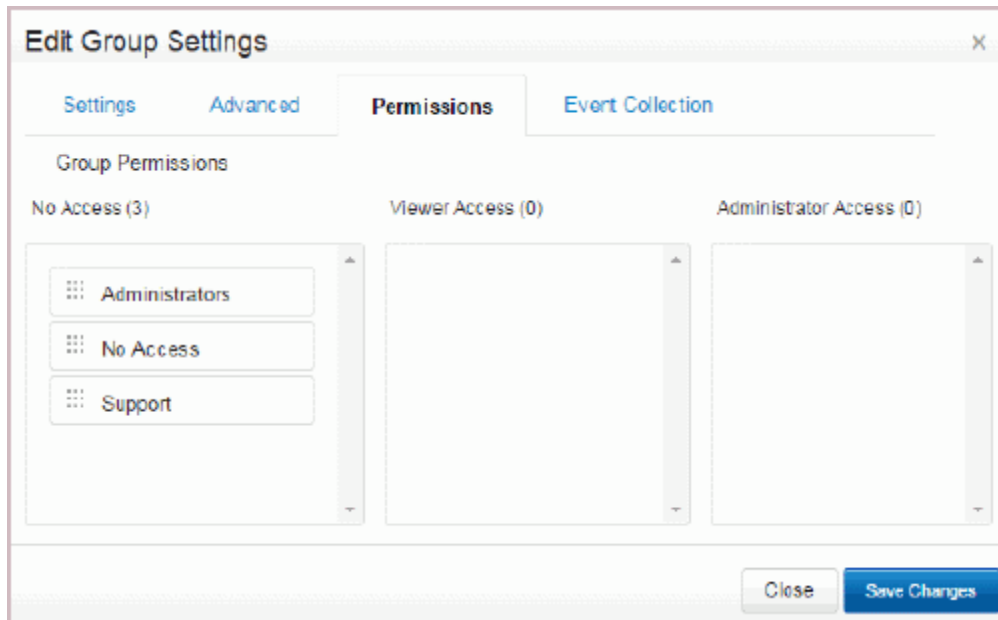
You can set up teams with roles that have varying levels of access. For information about levels of access for roles, see [Table 6, “Team Settings and Feature Access”](#), on page 48.

The Permissions tab shows which teams have either no access, viewer access, or administrator access for the products that are managed by the sensors in this group. The permission levels that are available are:

- **No Access:** when users in a team try to access or view details on a host in this sensor group, the system generates an HTTP 405 response (“The method you are using to access the file is not allowed.”)
- **Viewer Access:** users can view the data collected from hosts in this sensor group. However, users cannot make any configuration changes to this group or hosts that belong to this group.
- **Administrator Access:** users can configure the sensors’ host and group details.

To define permissions for teams in this sensor group:

1. From the console menu, choose **Administration > Sensors**. The Sensor page displays.
2. In the drop down menu at the top left of the page, select the sensor group to edit.
3. Click the **Edit Settings** tab. The Edit Settings page displays.
4. Click the **Permissions** tab. The Permissions tab displays with teams that are available in the **No Access** field:



5. Assign permissions to the teams by dragging and dropping team names to the appropriate sections. You can assign the same level of permissions to more than one team.
6. Click **Save Changes** to save your updates, and close the Edit Group Settings page, or click Event Collection to define the types of events for this sensor group to record.

Event Collection

You can define which types of events Carbon Black records for the sensors in this group by enabling or disabling the event types listed on the Event Collection tab.

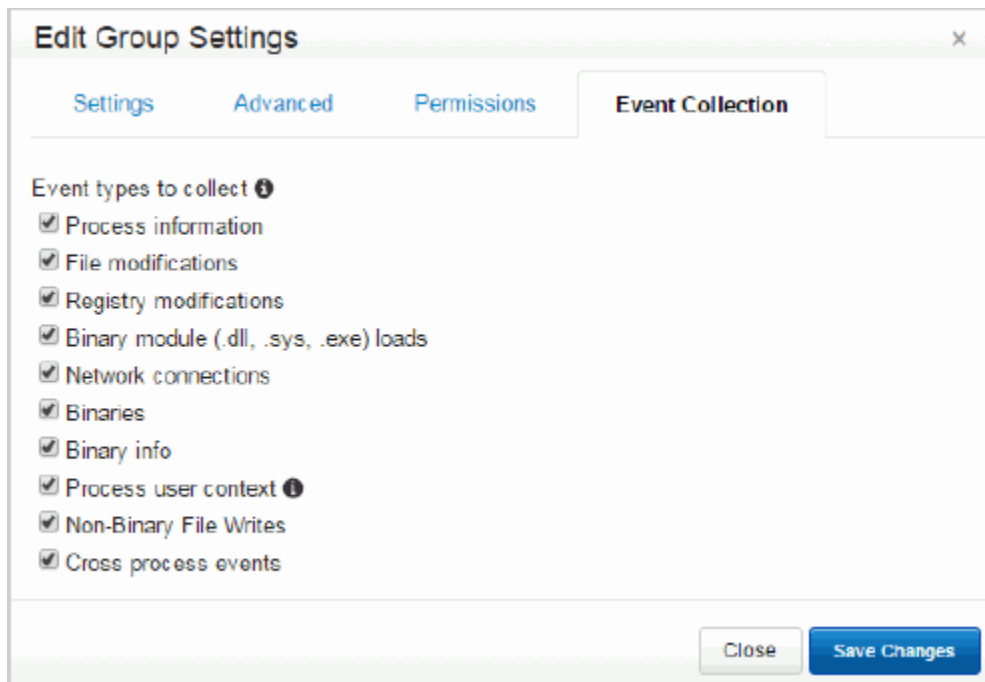
Note

Disabling event collection impacts visibility, but can improve sensor and server performance.

You can open the Event Collection tab from either the Create Group or the Edit Group Settings page. In this procedure the tab is opened in the Edit Group Settings page.

To define event collection for sensor groups:

1. From the console menu, choose **Administration > Sensors**. The Sensor page displays.
2. In the drop down menu at the top left of the page, select the sensor group to edit.
3. Click the **Edit Settings** tab. The Edit Settings page displays.
4. Click the **Event Collection** tab. It lists the options for the types of event data to collect from the installed sensors:



Most of the options are self-explanatory. However, there are two options that merit further descriptions:

- The **Process user context** option enables the Carbon Black sensor to record the user name associated with each running process. This associates endpoint activity with the operating system user account.
- The **Cross process events** option records instances when a process crosses the security boundary of another process. While some of these events are benign,

others might indicate an attempt to change the behavior of the target process by a malicious process.

Note

There are limitations on the cross process events that are reported by the sensor:

- Parent processes that create cross process events to their children are not reported.
- Cross process events that are part of the normal OS behaviors are ignored. For example, no cross process events are recorded for the Windows process `csrss.exe`.
- Cross process, open process, and open thread events are not supported on Windows XP and Windows 2003.

5. By default, all the options except for **Cross process events** are selected, and therefore, enabled. To disable an option, deselect its check box. To enable **Cross process events**, select its checkbox.
6. Click **Save Changes** to save all the updates to the sensor group.

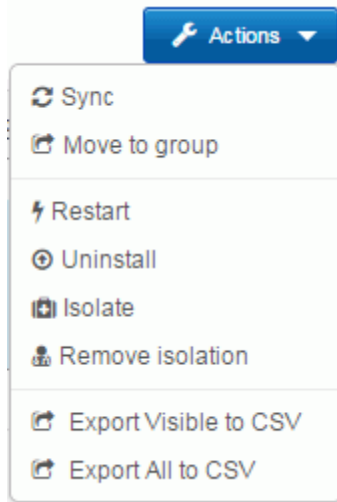
Moving Sensors to Another Group

After you create sensor groups, you can add sensors to them. By default, sensors are installed into the Default Group. On the Sensor page, you can select the group that contains the sensors to add, and then move those sensors from their original group to the new group.

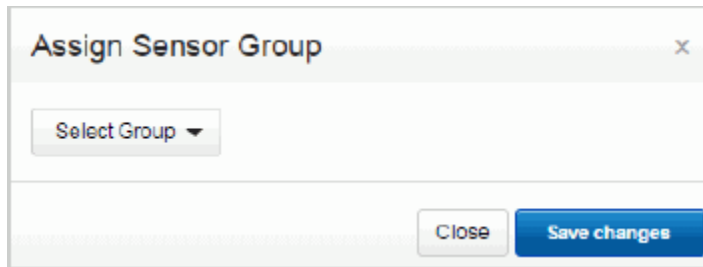
To add sensors to sensor groups:

1. From the console menu, choose **Administration > Sensors**. The Sensor page displays.
2. From the sensor group drop-down menu at the top left side of the page, select the group that contains the sensors you want to move to another group. Initially, this will most likely be the Default Group.
3. In the list of sensors at the bottom of the page, select the checkboxes next to the sensors to move.

4. Click **Actions > Move to group**.



The Assign Sensor Group window opens.



5. Click **Select Group**, and then click the sensor group to move the sensors to. The selected sensors are removed from the list of the current group, and display in the list of their new group.
6. Click **Save changes**. The sensors are moved to the new group. Select the new group from the menu at the top right of the page to see the updated list of sensors.

Editing Sensor Groups

After you create a sensor group and save your changes, you can open the Edit Group Settings window to change any of the settings you previously defined. The Edit Group Settings page and the Create Group page contain the same tabs and options.

As noted in [“Permissions”](#) on page 58, you must use the Edit Group Settings page to define permissions for teams using the sensor group.

After you make changes in the Edit Group Settings page and save your changes, the changes will not take effect until the next time the sensors report to the Carbon Black Enterprise server..

Note

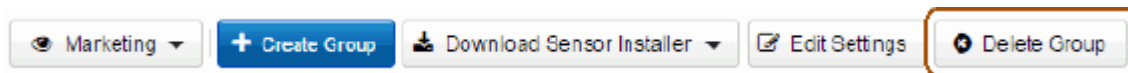
If any changes are made to the Carbon Black Enterprise server URL and the URL becomes incorrect, you will lose communication with the deployed sensors.

Deleting Sensor Groups

You can delete sensor groups on the Sensor page. When you delete a sensor group, the teams for which you defined permissions will no longer have access to the sensors that belonged to the group.

To delete sensor groups:

1. From the console menu, choose **Administration** > **Sensors**. The Sensor page displays.
2. From the sensor group drop-down menu at the top left side of the page, select the sensor group to delete.
3. Click **Delete Group** at the top right side of the page.



A confirmation message displays, saying that any sensors remaining in this group will be moved to the default group. Click **OK**. The sensor group is removed from the dropdown list on the right.

Chapter 5

Installing and Managing Sensors

This chapter describes installing sensors on Windows, Mac OSX, and Linux systems, and provides an overview of how sensors work and the information that they provide.

Sections

Topic	Page
Overview	66
Installing Sensors on Windows Systems	66
Installing Sensors on Mac OSX Systems	71
Installing Sensors on Linux Systems	75
Managing Sensors	81

Overview

Carbon Black sensors are lightweight data-gatherers that are installed on endpoints (such as laptops, desktops, and servers) on a deployed network. They gather event data on the endpoints and securely deliver it to the enterprise server for storage and indexing.

You install sensors on servers and endpoints in your enterprise. As soon as a sensor is installed, it begins buffering activity to report to the server.

This chapter describes how to install sensors, and how to manage them.

Installing Sensors on Windows Systems

This section describes the steps to install, upgrade, and uninstall the Carbon Black Windows sensor.

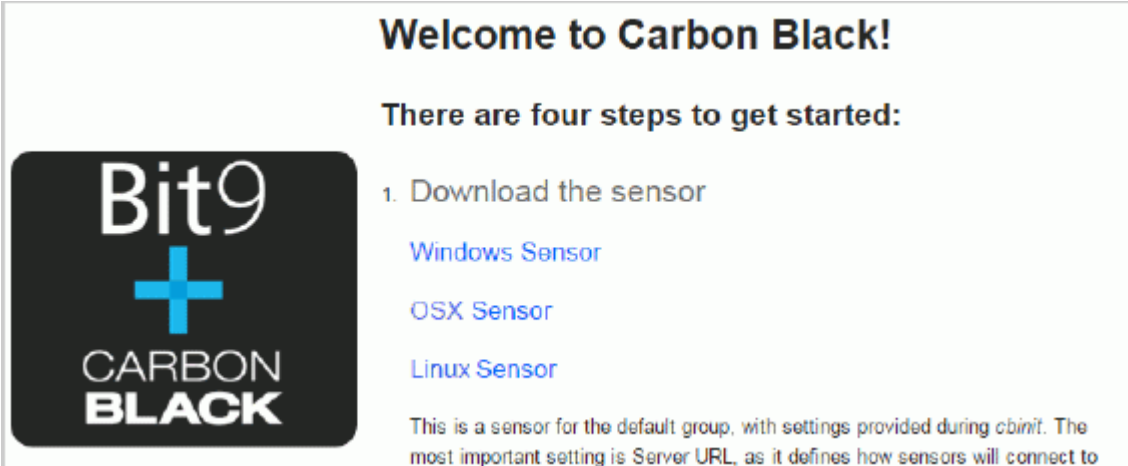
You must download a sensor installer and install sensors (one per computer) on Windows computers to begin collecting data.

Note

When you download a sensor from the Welcome page, the sensor is automatically included in the default sensor group. If you want the sensor to belong to another sensor group, download the package from the Sensor Group page.

To download the sensor package from the Welcome page:

1. Log into the Carbon Black Enterprise server. For information, see [“Logging In”](#) on page 30. The Welcome page displays:



Welcome to Carbon Black!

There are four steps to get started:

1. Download the sensor
 - [Windows Sensor](#)
 - [OSX Sensor](#)
 - [Linux Sensor](#)

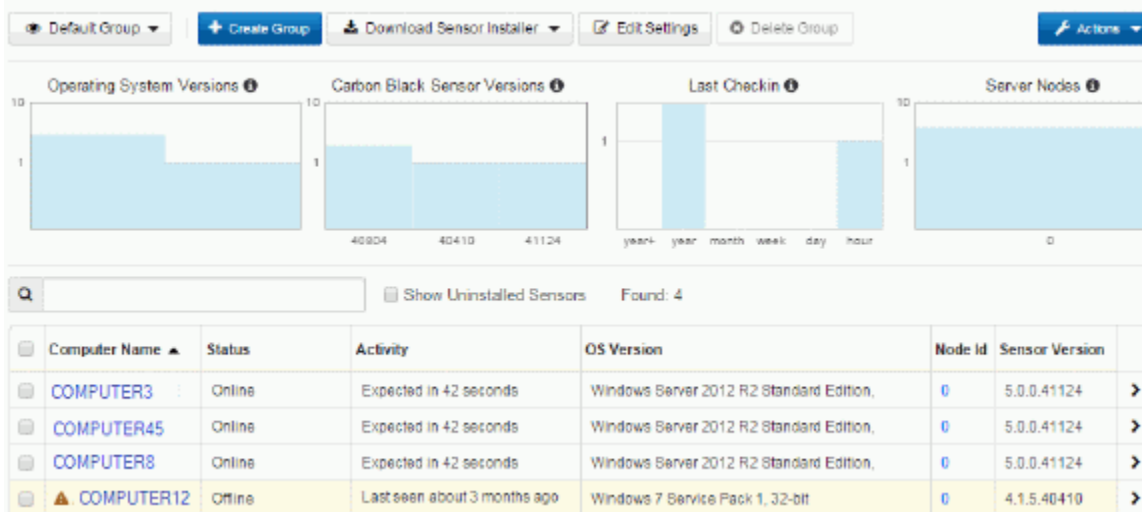
This is a sensor for the default group, with settings provided during *cbinit*. The most important setting is Server URL, as it defines how sensors will connect to

2. Click **Windows Sensor**. The Windows Sensor .zip file is downloaded to the server.

To download the sensor package from the Sensor Group page

You must be logged into the Carbon Black console with read permissions for a specific sensor group.

1. Log into the Carbon Black console. For instructions, see “[Logging In](#)” on page 30.
2. From the menu, choose **Administration > Sensors**. The Sensors page displays:



3. Click the **Edit Settings** button. The Settings tab in the Edit Group Settings page displays:

Edit Group Settings ✕

Settings
Advanced
Permissions
Event Collection

Name ⓘ

Search binary hashes with VirusTotal

Be notified of any binary flagged by VirusTotal. Information such as the filename, MD5 hash and parent process will be shared with the Bit9 Alliance partners. Any binary available on the Alliance server is deleted, saving disk space.

Server URL ⓘ

Scan unknown binaries with VirusTotal

Detect new variants of known malware by sharing the full binary content of unknown executable files. Binaries will be uploaded and shared with the Bit9 Alliance partners.

Once the group is saved, you can modify in [Share Settings](#).

Close
Save Changes

4. Verify that the **Server URL** field is correct. If this field is not correct, the sensors will not be able to communicate with the server.

Note

This IP address or server name must be usable by the sensor. If the Carbon Black Enterprise server appears with a different IP address from the locally-bound IP address to the sensor hosts, use the appropriate IP address or name.

If no changes are necessary, click **Close** to exit the window. Otherwise, click **Save Changes**.

5. On the Sensors page, click **Download Sensor Installer** and then select **Windows Standalone EXE**. The following file is downloaded:

CarbonBlackExeInstaller-<version number>-Default Group.zip

Note

To use an MSI installer to install sensors on remote installations of sensors on multiple endpoints, select **Windows MSI for GPO Installation**. For more information, see [https://technet.microsoft.com/en-us/library/hh147307\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx)

6. Transfer the .zip file to a Windows computer (XPSP3 or higher, either 32- or 64-bit).
7. Extract the .zip file.

Note

Do not just open the file. The contents must be unzipped.

8. Run `CarbonBlackClientSetup.exe`. On Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012, you are prompted for elevation as required.

Upgrading Sensors on Windows

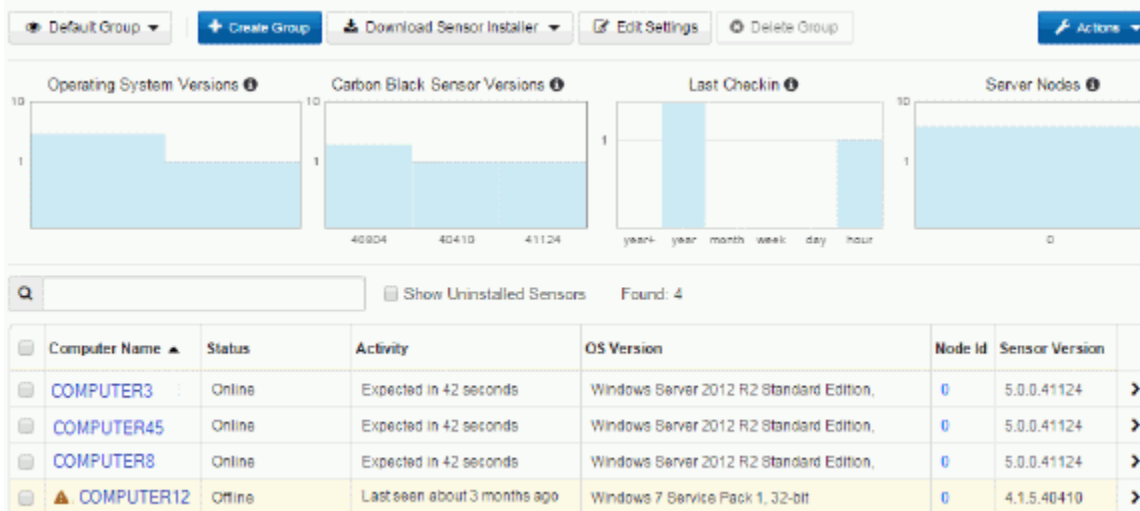
A new server version might include a new sensor version. Check the release notes or contact Customer Support if you have any questions.

If a new sensor version is included, you need to decide if you want the sensor to be deployed immediately to existing sensor installations, or if you want to install only server updates.

This can be configured on the Carbon Black console.

To upgrade sensors:

1. Log into the Carbon Black console. For instructions, see “[Logging In](#)” on page 30.
2. From the menu, choose **Administration > Sensors**. The Sensors page displays:



3. Click the **Edit Settings** button. The Settings tab in the Edit Group Settings page displays:

Edit Group Settings ✕

Settings
Advanced
Permissions
Event Collection

Name ⓘ

Server URL ⓘ

Search binary hashes with VirusTotal

Be notified of any binary flagged by VirusTotal. Information such as the filename, MD5 hash and parent process will be shared with the Bit9 Alliance partners. Any binary available on the Alliance server is deleted, saving disk space.

Scan unknown binaries with VirusTotal

Detect new variants of known malware by sharing the full binary content of unknown executable files. Binaries will be uploaded and shared with the Bit9 Alliance partners.

Once the group is saved, you can modify in [Share Settings](#).

4. Click on **Advanced**. The Advanced tab opens.

The screenshot shows the 'Create Group' dialog box with the 'Advanced' tab selected. The 'Sensor Upgrade Policy' dropdown menu is set to 'Manual'. The 'Tamper Level Settings' slider is set to 'Off' and the 'Alerts Critical Level' slider is set to 'Low'. The 'VDI Behavior Enabled' checkbox is checked.

5. In **Sensor Upgrade Policy**, if **Always Latest** is selected, the server will automatically upgrade sensors to the latest sensor version. If you want to keep the sensors at a specific version, select that version number from the Sensor Upgrade Policy menu prior to upgrading. If you want to continue using whatever sensor versions are already installed, regardless of the version, select **Manual**.

Uninstalling Windows Sensors

You can uninstall sensors using the Carbon Black console.

To uninstall sensors:

1. Log into the Carbon Black console. For instructions, see [“Logging In”](#) on page 30.
2. From the menu, choose **Administration > Sensors**. The Sensors page displays.
3. Select the checkbox next to the sensor(s) to uninstall.
4. On the right side of the menu at the top of the page, click **Actions > Uninstall**.
5. Click **OK** in the Confirmation dialog box. The sensor(s) are uninstalled.

Note

The sensor will receive the uninstall request the next time it checks in with the server, which can be anytime between 30 seconds to several minutes, depending on the number of active sensors and the server load.

Uninstalled sensors will no longer be visible in lists of hosts and sensors unless the **Show Uninstalled Sensors** checkbox is selected.

For the latest updates, known issues, and troubleshooting information, refer to the *Server Install* (server_install.pdf) document on the Customer Portal.

Installing Sensors on Mac OSX Systems

This section describes the steps to install, upgrade, and uninstall the Carbon Black Mac OSX sensor.

You must download a sensor installer and install sensors on Mac OSX computers (one sensor per computer) to begin collecting data.

Installing Sensors on Mac OSX Systems

Prerequisites

You must have the Carbon Black Enterprise server installed with version 4.2.2 or later.

Installing Sensors

The Carbon Black OSX sensor installation is a manual process and consists of two primary steps:

1. Installing the sensor files on the Carbon Black server for distribution to endpoints and
2. Installing the sensor package on the endpoints.

Note

If you have installed Carbon Black Enterprise server version 5.0, or 4.2.2 or later, and the OSX sensor RPM is installed on the Carbon Black Enterprise Server, if you have access to the Carbon Black console, you can download the Default Sensor group OSX sensor installer package from the Carbon Black Welcome page or from the “Download Sensor Installer” option on the Sensors page (for sensor groups for which you have read permissions). If you follow that procedure, you can skip the procedure for creating the OSX sensor installation package as described immediately below in [“Installing the OSX Sensor Files on the Carbon Black Enterprise Server”](#) procedure for creating the OSX sensor installation package.

However, if you are upgrading sensor versions, the following steps apply.

Installing the OSX Sensor Files on the Carbon Black Enterprise Server

With version 4.2.2 Carbon Black repo and higher, the OSX sensor is available for download and installation on the Carbon Black server via the YUM packaging system.

To download and install the OSX sensor files to the server:

1. Verify that the repository that is configured on the Carbon Black Enterprise server has access to the OSX sensor RPM by running:


```
yum info cb-osx-sensor
```

2. Install the OSX sensor package on your Carbon Black server by running:

```
yum install cb-osx-sensor
```

and answer `Y` to the confirmation
3. Retart the Carbon Black Services by issuing this command

```
service cb-enterprise restart
```

Access the OSX Sensor Package

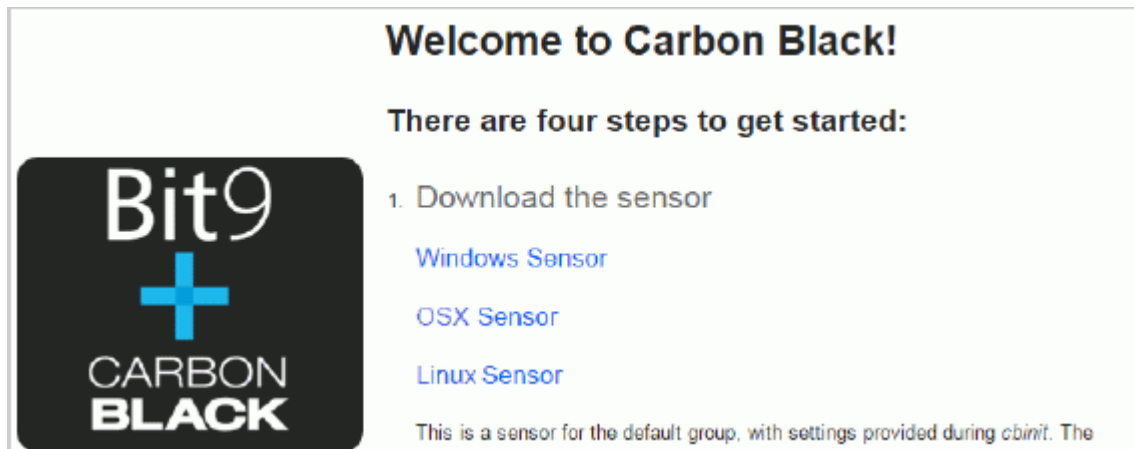
You can download the sensor package from the Carbon Black console or manually create it (for instructions on manually creating the sensor package, see [“To manually create the OSX sensor installation package:”](#) on page 73). Ensure that you complete the instructions in [“Installing the OSX Sensor Files on the Carbon Black Enterprise Server”](#) on page 71 before you perform this procedure.

Note

When you download a sensor from the Welcome page, the sensor is automatically included in the default sensor group. If you want the sensor to belong to another sensor group, download the package from the Sensor Group page.

To download the sensor package from the Welcome page:

1. Log onto the Carbon Black Enterprise server. For information, see [“Logging In”](#) on page 30. The Welcome page displays:

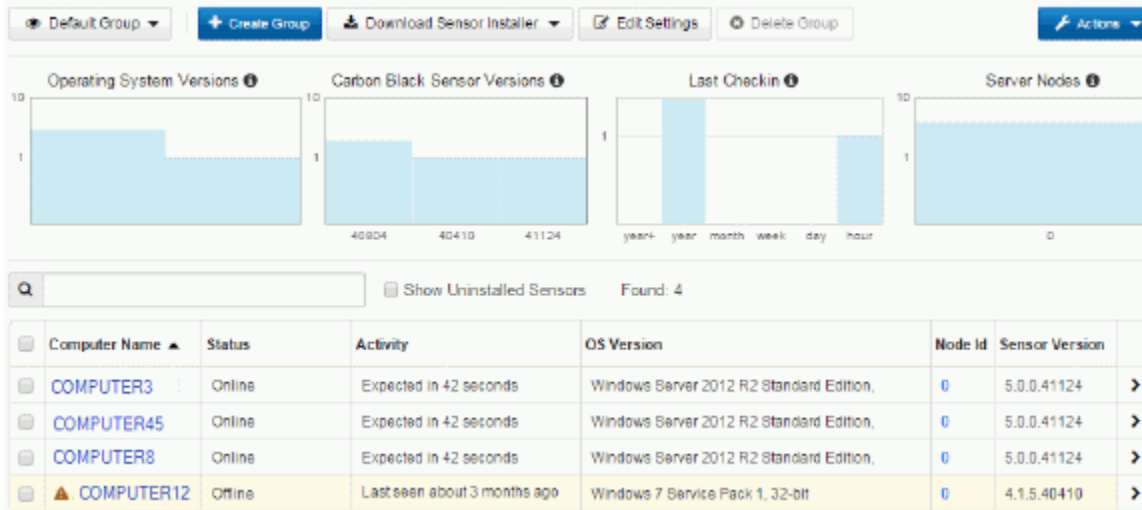


2. Click **OSX Sensor**. The OSX sensor .zip file is downloaded to the server.

To download the sensor package from the Sensor Group page

You must be logged into the Carbon Black console with read permissions for a specific sensor group.

1. From the menu, choose **Administration > Sensors**. The Sensors page displays:



2. Click **Download Sensor Installer** button and select **OSX Standalone PKG**. The Sensor package file is downloaded to your system.

To manually create the OSX sensor installation package:

Create the installation package on the Carbon Black Enterprise server.

Run the following command:

```
/usr/share/cb/cbsensorinstallergen -installer-file=[path to OSX .pkg file] -os=osx -package-path=[directory path to save the output package]
```

You can use the `-sensor-group` option to target the installer to a specific sensor group.

Note

The value for the `-sensor-group` option must be enclosed in quotes if the name includes spaces, for example: `-sensor-group="Web Server Sensor Group"`

The default sensor group is `Default Group`. The `-help` option displays command line help for the script. The output file is a `.zip` file that contains the installer and the `sensorsettings.ini` file that are required for installation.

Install the Sensor Package on OSX clients

1. Copy the `.zip` sensor installation package to the OSX client.
2. Extract the `.zip` file.

Note

Do not just open the file. The contents must be unzipped.

Run the .pkg file and follow the installation prompts. You can run this file by double-clicking it, or by using a silent installer, for example:

```
installer -pkg <CarbonBlackClientSetup-osx-v(XYZ) .pkg -target/
```

This will install the OSX sensor using the configuration that is provided in the sensorsettings.ini file.

At this point, the OSX sensor is installed and running. The sensors pane in the Carbon Black Enterprise server administrative interface shows the sensor as registered and checking in.

Upgrading Sensors on OSX

A new server version might include a new sensor version. Check the release notes or contact Customer Support if you have any questions.

If a new sensor version is included, you need to decide if you want the sensor to be deployed immediately to existing sensor installations, or if you want to install only server updates. This can be configured on the Carbon Black console.

You can upgrade OSX clients that are running the Carbon Black OSX sensor automatically on the Carbon Black Enterprise server, or manually on the endpoint. The server-based OSX sensor upgrade is a global (all-or-none) setting in the cb.conf file on the Carbon Black Enterprise server. Unlike the installer package, the OSX sensor .pkg file does not require any preprocessing.

Prerequisites

You must have a Carbon Black enterprise server installation of version 4.2.2 or higher.

There must be an OSX endpoint that is running a previous version of the Carbon Black OSX Sensor.

You must have a newer version of the OSX sensor downloaded and installed on the Carbon Black Enterprise server.

To upgrade sensors on the server:

1. Ensure that the OSX sensor package is installed on your Carbon Black Enterprise server by following the steps in [“Installing Sensors on Mac OSX Systems”](#) on page 71.
2. Modify the cb.conf setting `SensorUpgradeOsx` (the cb.conf file is located in `/etc/cb/cb.conf`):
 - a. When no upgrade is desired, this setting is set to `Manual` or `None` (the default is `Manual`).
 - b. To enable the OSX sensors to upgrade to a new sensor version, change this setting to the version number of the OSX sensor upgrade package installed in step 1, for example: `SensorUpgradeOsx=4.1.0.12345`
3. Restart Carbon Black Enterprise, for example, run

```
service cb-enterprise restart
```

On the next checkin, the OSX sensors will perform the upgrade to the new OSX sensor version.

To upgrade sensors manually:

1. Download or create a Carbon Black OSX Sensor installer zip file by following the steps in [“Access the OSX Sensor Package”](#) on page 72.
2. Copy the OSX sensor installation package to the OSX client(s) to be upgraded.
3. Unzip the .zip file.

Note

Do not just open the file. The contents must be unzipped.

4. Install the new sensor version by running the .pkg file in the location where the new sensor installation package was unzipped. You can run this file by double-clicking it, or by using a silent installer, for example:
`installer -pkg <CarbonBlackClientSetup-osx-v(XYZ) .pkg -target/`
 When the .pkg file completes, the OSX sensor will be installed and running. The sensors pane on the Carbon Black Enterprise server in the administrative interface will show the sensor as registered and checking in.

Uninstalling Sensors on OSX

To uninstall sensors, you can either use the Carbon Black console and follow the instructions in [“Uninstalling Windows Sensors”](#) on page 70, or you can follow the steps described here.

To uninstall sensors manually:

- On the OSX client where the sensor is installed, run the following command:
`/opt/cbsensor/sensoruninstall.sh`

When this process is complete, the endpoint will stop reporting events and binaries to the Carbon Black server.

For the latest updates, known issues, and troubleshooting information, refer to the *Sensor Osx Install* (sensor_osx_install.pdf) document on the Customer Portal.

Installing Sensors on Linux Systems

This section describes the steps to install, upgrade, and uninstall the Carbon Black Linux sensor.

You must download a sensor installer and install one or more sensors on Linux computers to begin collecting data.

With version 4.2.2 or higher of the Carbon Black repository, the Linux sensor is available for download and installation on the Carbon Black Enterprise server with the YUM packaging system.

Prerequisites

You must have the following in place before installing the sensor:

- A Carbon Black enterprise server installation version 4.2.2 or higher.
- OpenSSL version 1.0.1 or higher.

The Carbon Black Linux sensor installation is a manual process and consists of two steps:

1. Installing the sensor files on the Carbon Black server for distribution to endpoints
2. Installing the sensor package on the endpoints

Note

With Carbon Black enterprise server installation version 4.2.2 or higher and the Linux sensor RPM installed on the Carbon Black enterprise server, if you have web UI access, you can download the Linux sensor installer package for the the default sensor group from the Carbon Black console Welcome page or from **Administration > Sensors > Download Sensor Installer** (for those groups that you have read permissions to). If you download the install package from the Carbon Black console pages, you can skip the creation of the Linux sensor installation package that is described below.

Installing the Linux Sensor Files on the Carbon Black Server

To download and install the Linux sensor files on the server:

1. Verify that the Carbon Black repository that is configured on the Carbon Black Enterprise server has access to the Linux sensor RPM by running:

```
yum info cb-linux-sensor
```
2. Install the Linux sensor package on your Carbon Black Enterprise server:

```
yum install cb-linux-sensor
```


and answer **Y** to the confirmation.
3. Start the Carbon Black services by running:

```
service cb-enterprise restart
```

Download the Sensor Package

You can download the sensor package from the Carbon Black console or manually create it (for instructions on manually creating the sensor package, see [“To create the Linux sensor installation package manually:”](#) on page 78). Ensure that you complete the [“Installing the Linux Sensor Files on the Carbon Black Server”](#) on page 76 before you perform this procedure.

Note

When you download a sensor from the Welcome page, the sensor is automatically included in the default sensor group. If you want the sensor to belong to another sensor group, download the package from the Sensor Group page.

To download the sensor package from the Welcome page:

1. Log into the Carbon Black Enterprise server. For information, see [“Logging In”](#) on page 30. The Welcome page displays:



Welcome to Carbon Black!

There are four steps to get started:

1. Download the sensor
 - [Windows Sensor](#)
 - [OSX Sensor](#)
 - [Linux Sensor](#)

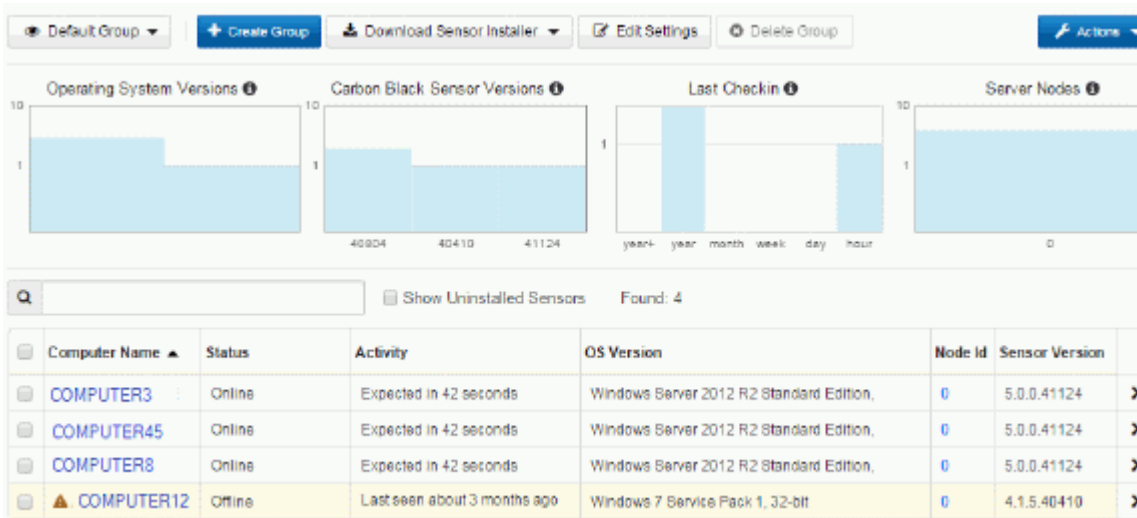
This is a sensor for the default group, with settings provided during *cbinit*. The most important setting is **Sensor ID**, as it defines how sensors will connect to

2. Click **Linux Sensor**. The Linux sensor *.tar.gz file is downloaded to the server.

To download the sensor package from the Sensor Group page

You must be logged into the Carbon Black console with read permissions for a specific sensor group.

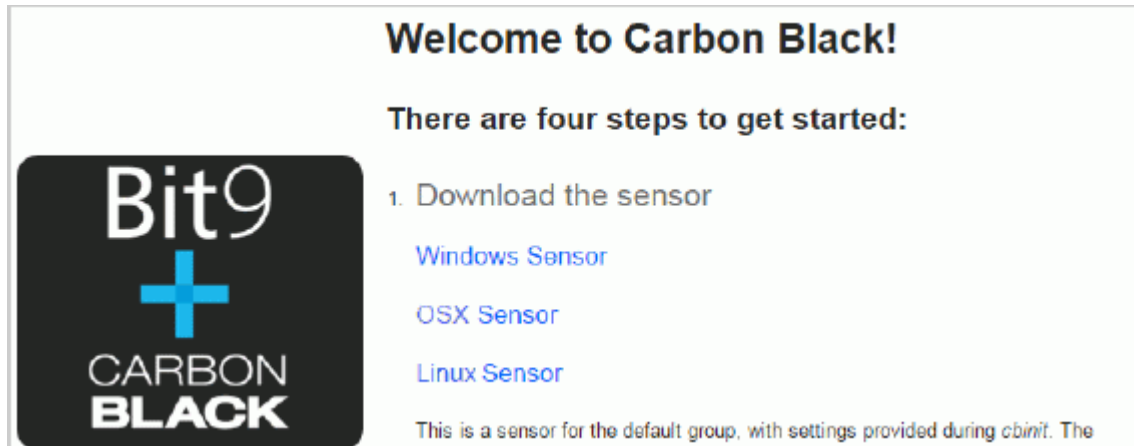
1. From the menu, choose **Administration > Sensors**. The Sensors page displays:



The screenshot shows the Carbon Black console interface for the Sensors page. At the top, there are navigation buttons: "Default Group", "Create Group", "Download Sensor Installer", "Edit Settings", "Delete Group", and "Actions". Below these are four charts: "Operating System Versions", "Carbon Black Sensor Versions", "Last Checkin", and "Server Nodes". A search bar and "Show Uninstalled Sensors" checkbox are visible above a table of sensors. The table has columns for Computer Name, Status, Activity, OS Version, Node Id, and Sensor Version. Four sensors are listed: COMPUTER3, COMPUTER45, COMPUTER8, and COMPUTER12. COMPUTER12 is highlighted in yellow and has a warning icon.

Computer Name	Status	Activity	OS Version	Node Id	Sensor Version
COMPUTER3	Online	Expected in 42 seconds	Windows Server 2012 R2 Standard Edition,	0	5.0.0.41124
COMPUTER45	Online	Expected in 42 seconds	Windows Server 2012 R2 Standard Edition,	0	5.0.0.41124
COMPUTER8	Online	Expected in 42 seconds	Windows Server 2012 R2 Standard Edition,	0	5.0.0.41124
COMPUTER12	Offline	Last seen about 3 months ago	Windows 7 Service Pack 1, 32-bit	0	4.1.5.40410

2. Click **Download Sensor Installer** button and select **Linux Standalone RPM**. The Sensor package file is downloaded to your system.



Welcome to Carbon Black!

There are four steps to get started:

1. Download the sensor
 - Windows Sensor
 - OSX Sensor
 - Linux Sensor

This is a sensor for the default group, with settings provided during cbinit. The

3. Click **Linux Sensor**. The Linux sensor .zip file is downloaded to the server.

Manually Create the Linux Sensor Installation Package

The installation package must be created on the Carbon Black Enterprise server. Use a script to package the install files with the server settings.

To create the Linux sensor installation package manually:

1. Install the Carbon Black Linux sensor files on the server following the steps described in [“Installing the Linux Sensor Files on the Carbon Black Server”](#) on page 76.
2. Run the following command:

```
/usr/share/cb/cbsensorinstallergen -installer-file=[path to Linux .rpm file],[path to Linux .sh file] -os=linux-package-path=[dir path to save the output package]
```

You can use the `-sensor-group` option to target the installer to a specific sensor group.

Note

The value for the `-sensor-group` option must be enclosed in quotes if the name includes spaces, for example: `-sensor-group="Web Server Sensor Group"`

The default is `Default Group`. The `-help` option displays command line help for the script.

The output file is a gzipped tar file that contains the installer, an installer script (.sh) and the `sensorsettings.ini` file, which are required for installation. A `readme.txt` is also included that contains the Carbon Black Enterprise server and sensor group name that a sensor would register with upon installation.

Install the Linux Sensor Installation Package on Clients

1. Copy the .tar.gz sensor installation package to the client.
2. Untar the .tar.gz file, for example, at a command prompt, from the directory where this file is located, type:

```
tar -zxvf .tar.gz
```

Note

Do not just open the file. The contents must be unzipped.

3. Run the .sh file and follow any installation prompts. This will install the Linux sensor using the configuration that is provided in the sensorsettings.ini file.

After you complete these steps, the Linux sensor will be installed and running. The sensors pane in the Administrative section of the Carbon Black console should show the sensor as registered and checking in.

Upgrading Sensors on Linux

A new server version might include a new sensor version. Check the release notes or contact Customer Support if you have any questions.

If a new sensor version is included, you need to decide if you want the sensor to be deployed immediately to existing sensor installations, or if you want to install only server updates.

This can be configured on the Carbon Black console.

Linux clients that are running the Carbon Black Linux sensor can be upgraded automatically via the server or manually at the endpoint. Currently, the server-based Linux sensor upgrade is a global (all-or-none) setting in the cb.conf file on the Carbon Black enterprise server. Unlike the installer package, the Linux sensor upgrade .tar.gz file does not require any preprocessing.

Prerequisites

You must have the following in place before upgrading sensors:

- A Carbon Black enterprise server installation version 4.2.2 or higher
- A linux endpoint running a previous version of the Carbon Black Linux Sensor.
- A newer version of the Linux sensor downloaded and installed on the Carbon Black server (for instructions on how to do this, see step 3 in [“Installing the Linux Sensor Files on the Carbon Black Server”](#) on page 76).

Upgrading Sensors

To enable a Linux sensor upgrade package for deployment via the server:

1. Install the Linux sensor package on your Carbon Black server by following the steps described in [“Installing the Linux Sensor Files on the Carbon Black Server”](#) on page 76.
2. Modify the cb.conf setting `SensorUpgradeLinux`:
 - a. When no upgrade is desired, this setting is set to `Manual` or `None`.
 - b. To enable the Linux sensors to upgrade to the newer sensor, change this setting to the version number of the Linux sensor upgrade package used in step 1, for example:

```
SensorUpgradeLinux=4.2.1.12345
```
3. Restart Carbon Black Enterprise, for example, by running the command:

```
service cb-enterprise restart
```

On the next checkin, the Linux sensors will perform the upgrade to the new Linux sensor version.

Manually Upgrading Sensors

1. Install the Linux sensor package on your Carbon Black Enterprise server by following the steps described in [“Installing the Linux Sensor Files on the Carbon Black Server”](#) on page 76.
2. Access the tar.gz file:
 - a. Download this file from the Welcome page on the Carbon Black console
 - b. Create a Carbon Black Linux Sensor installer by following the steps in [“Manually Create the Linux Sensor Installation Package”](#) on page 78.
3. Copy the Linux sensor installation package to the Linux client(s) that will be upgraded
4. Untar the tar.gz file (do not just open, the contents need to be unzipped on disk), for example, at a command prompt, from the directory where this file is located, type:

```
tar -zxvf .tar.gz
```
5. Uninstall the current Linux sensor by running the following command:

```
/opt/cbsensor/sensoruninstall.sh
```

After you run this command, the endpoint will stop reporting events and binaries to the Carbon Black enterprise server.
6. Install the new sensor version by running the .sh file in the location where the new sensor install package was untarred. At this point, the Linux sensor will be installed and running. The Sensors page in the Carbon Black console Administration menu shows the sensor as registered and checking in.

Uninstalling Sensors on Linux

To uninstall sensors, you can either use the Carbon Black console and follow the instructions in [“Uninstalling Windows Sensors”](#) on page 70, or you follow the steps described here.

To uninstall sensors on Linux manually:

- On the Linux client where the sensor is installed, run the following command:
`/opt/cbsensor/sensoruninstall.sh`

When this process is complete, the endpoint will stop reporting events and binaries to the Carbon Black server.

For the latest updates, known issues, and troubleshooting information, refer to the *Sensor Linux Install* (sensor_linux_install.pdf) document on the Customer Portal.

Managing Sensors

As soon as a sensor is installed, it begins buffering activity to report to the server. This includes all currently running processes that create events, and all binaries, all file executions, file modifications, network connections, and registry modifications.

Every few minutes sensors check in with the Carbon Black Enterprise server and report what they have buffered, even if they are reporting that they have nothing buffered.

When a sensor checks in, the server responds, letting the sensor know when to send the data, and how much data to send.

As the server records data from sensors, it is compared with the latest synchronization from any enabled Alliance Feed Partner. In most cases incremental synchronizations occur hourly and full synchronizations occur once every 24 hours.

Each sensor is associated with a sensor group that defines its configuration and security characteristics. One sensor group can contain many sensors, but a single sensor can only belong to one sensor group.

You can monitor the following information about sensors (per sensor group) from the **Administration > Sensors** page in the Carbon Black console:

- Distribution of operating systems for computers
- Distribution of Carbon Black sensor versions for computers
- Distribution of Carbon Black sensor checkins for computers
- Distribution of sensors by server nodes or cluster nodes
- Computer names with sensors installed on them and high-level status information.

To search for a sensor, you can enter information about the sensor into the Search box on the Sensors page.

Click the name of a computer to open the Sensor Details page with detailed sensor information.

You can also target specific types of event information for sensors to collect.

For more information about sensors and sensor groups, see [“Sensor Groups”](#) on page 53.

Other features that can help you manage sensors and work with the information they capture are:

- Isolating an endpoint with a suspicious process or threat that has been detected on it.
- Directly responding to a threat detected on an endpoint

For information about these features, see [Chapter 6, “Incident Response on Endpoints.”](#)

Chapter 6

Incident Response on Endpoints

This chapter describes Endpoint Isolation and Live Response, two features in Carbon Black that can be used in incident response.

Sections

Topic	Page
Overview	84
Isolating an Endpoint	84
Using Carbon Black Live Response	85
Live Response Endpoint Sessions	86
Detached Session Management Mode	90
Live Response Activity Logging and Downloads	92

Overview

When a process analysis or another Carbon Black tool, shows you that there is a malicious file or process on one or more of your endpoints, you may choose to respond in a number of different ways, ranging from continued monitoring to re-imaging the affected systems. Carbon Black provides two ways to respond to threats directly from the console:

- **Endpoint Isolation** —You can isolate a computer from the rest of the network, leaving only connections needed for access to its sensor by the Carbon Black server.
- **Carbon Black Live Response** —You can open a command interface to directly access any sensor-managed system.

These features can be used together or separately. For example, if you found a malicious process currently running on a sensor-managed computer, you could isolate that computer immediately to prevent the spread of the problem and then use Carbon Black Live Response to end the process and perform any other file removal or other repairs needed. On the other hand, if the incident that Carbon Black identified is not ongoing, isolation may not be necessary. In that case, you could use Carbon Black Live Response to remediate or further investigate it on machines that were affected.

Neither Sensor Isolation nor Carbon Black Live Response announces its presence on an affected sensor. With Sensor Isolation, the user would likely become aware quickly that they had lost network access, but they would not know why. With Carbon Black Live Response, actions you take on a computer might affect a user's access to files or programs, but there would be no indication that Carbon Black tools are responsible unless you chose to make the user aware of that.

In addition to the tools described in this chapter, if you are also managing your endpoints with the Bit9 Platform, you can use Bit9 Platform control features to investigate incidents and modify rules to prevent future occurrences. See [Appendix B, "Integrating Carbon Black with a Bit9 Server,"](#) for details of features available when the two platforms are connected.

Isolating an Endpoint

You can isolate one or more endpoints from the rest of your network and the internet through the Carbon Black Console. When an endpoint is isolated, its connectivity is limited to the following:

- The Carbon Black server can communicate with an isolated computer.
- To allow the Carbon Black server to communicate with the sensor, ARP, DNS and DHCP services remain operational on the sensor's host. In addition, ICMP (e.g., ping) will remain operational on Windows operating systems prior to Vista.

Once isolated, an endpoint remains isolated under most circumstances until its isolation state is removed through the console. Note, however, that if an isolated system is rebooted, it will stop being isolated until it checks in with the Carbon Black server, which normally occurs every few minutes.

To isolate one or more endpoints from the network:

1. On the Carbon Black Console menu, choose **Administration > Sensors**.
2. On the Sensors page, check the box next to each endpoint you want to isolate.

3. On the Actions menu, choose **Isolate**.
4. In the confirmation dialog, if you are certain you want to isolate these computers, click **OK**. The computer is isolated from all but the Carbon Black server and the network services necessary to connect the two.

With the systems that showed malicious activity isolated, you can proceed with whatever remediation steps you plan to take, including Carbon Black Live Response. When you are finished, restoring connectivity to the systems is as simple as isolating them was.

To end network isolation for one or more endpoints:

1. On the Carbon Black Console menu, choose **Administration > Sensors**.
2. On the Sensors page, check the box next to each endpoint for which you want to restore network connectivity.
3. On the Actions menu, choose **Remove isolation**.
4. In the confirmation dialog, if you are certain you want to restore these computers to network connectivity, click **OK**. The computer returns to the network with the same access it had prior to being isolated.

Using Carbon Black Live Response

Carbon Black Live Response opens a command interface for direct access to any sensor-managed system. Responders can perform remote live investigations, intervene in ongoing attacks, and instantly remediate endpoint threats. For example, Live Response allows a responder to view directory contents, kill processes, modify the registry, and get files from sensor-managed computers. [Table 8, “Carbon Black Live Response Session Commands”](#) on page 88 shows the complete set of Live Response commands.

To use Live Response, you must have it enabled in the Carbon Black Enterprise Server configuration settings. This is done by editing the `cb.conf` file on the Carbon Black server:

```
# Enable/Disable cblr functionality. Disabled by default
CbLREnabled=True.
```

Also, a user must have Global administrator status to access sensors with Live Response.

Important

This feature should be used in full compliance with your organization's policy on accessing other user's computers and files. Consider the capabilities of described here when making decisions about giving users access to the Carbon Black console and also when choosing the Sensor Group to put computers in.

There are two different modes for Live Response:

- **Attached Mode** —When you activate Live Response for a specific endpoint, you create and attach to a *session*. The interface for a session includes information about the endpoint and a command window for interacting with the endpoint. See [“Live Response Endpoint Sessions”](#) on page 86.
- **Detached Mode** —You can enter Live Response without being attached to a particular session through the **Respond > Go Live** command on the console menu.

This interface includes commands to manage and access existing sessions as well as other commands that are useful outside of a session. See “[Detached Session Management Mode](#)” on page 90.

Live Response Endpoint Sessions

To access an endpoint using Carbon Black Live Response, a user must have Global administrator privileges. A "session" must first be created with the sensor you want to access. A session indicates that the sensor is connected to the Carbon Black server to receive real-time commands. Sessions are created and attached to automatically when you click the 'Go Live' button on the Sensor Details or Process Analyze pages. If you enter the Carbon Black Live Response console using the **Respond > Go Live** command from the console menu, to access an endpoint you must first create a session and then attach to it:

```
[CB Live]# session new [sensor_id]
[CB Live]# attach [provided_session_id]
```

You can have sessions with multiple sensors active at the same time. Use the 'detach' command to detach from a session but leave it active. Use the 'session close' command to end a session with the sensor. Sessions will timeout when they are not attached and active for 5 minutes.

Each session has a unique numeric ID. Up to 10 sessions can be running at any one time, and multiple users can be attached to the same session.

Important

More than one Carbon Black console user can attach to the same session with an endpoint at the same time. If more than one user submits a command through the session at approximately the same time, each command must finish executing before the next one can begin. Also, one user could undo or otherwise modify what another is doing. Consider this if more than one user has Live Response access to an endpoint.

To create and attach to a Carbon Black Live Response sensor session:

1. Go to the Sensor details page for the computer you want to access by double-clicking on the computer name wherever it appears as a link. If you are not already on a page that shows the computer name:
 - a. On the Carbon Black Console menu, choose **Administration > Sensors**.
 - b. On the Sensors page, double-click the name of the computer.
2. On the Sensor details page, click the **Go Live>** button.

The Live Response page appears, with a command window on the left and an information panel on the right. The command window prompt shows the name of the host and the current directory in which Live Response is active. The information panel includes Host Details, Alerts related to the host, and Running Processes on the host.

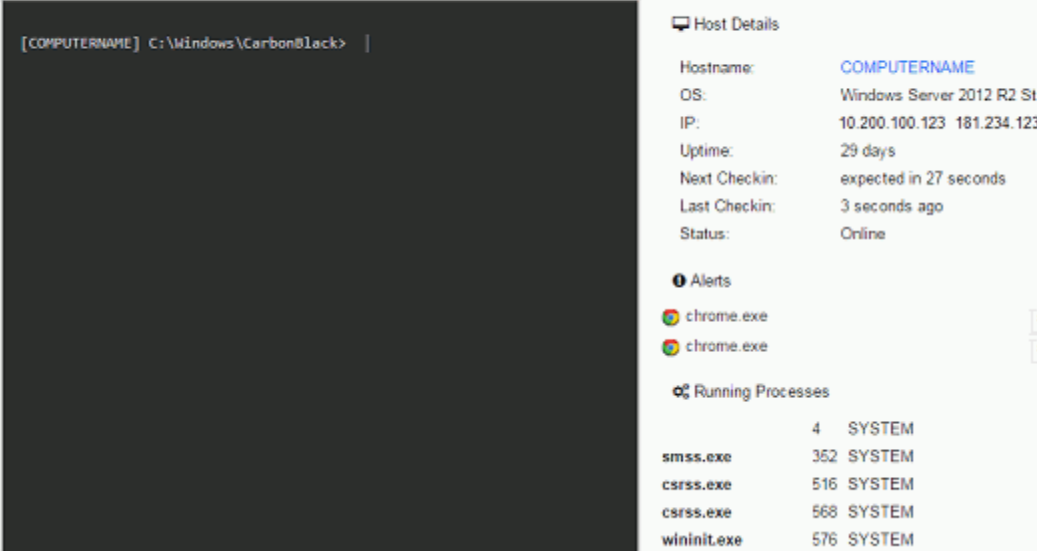
There is a status indicator (dot) and message immediately above the command window:

 - **Green** -- The sensor is connected and a session has been established. The host name is shown.

- **Orange** -- The Carbon Black server is waiting for the sensor to check in, or no host is connected because no session is attached.
- **Grey** -- A session cannot be established with the sensor, e.g., because it the sensor is disabled or the host is off-line.

>_ Live Response

● COMPUTERNAME



Host Details

Hostname: COMPUTERNAME
 OS: Windows Server 2012 R2 St
 IP: 10.200.100.123 181.234.123
 Uptime: 29 days
 Next Checkin: expected in 27 seconds
 Last Checkin: 3 seconds ago
 Status: Online

Alerts

chrome.exe
 chrome.exe

Running Processes

Process Name	PID	PPID	Session Name
smss.exe	4	SYSTEM	
csrss.exe	352	SYSTEM	
csrss.exe	516	SYSTEM	
csrss.exe	568	SYSTEM	
wininit.exe	576	SYSTEM	

3. To view a list of the available commands, click in the command window area and enter the **help** command. You can get information about a specific command by entering:

help *commandname*

Table 8 shows the complete set of Live Response commands. In the descriptions, remote host refers to the host being accessed via Live Response and local host refers to the host on which the user is running the Carbon Black console. These commands are all run in the SYSTEM context.

Note

Be sure to use the commands and options as documented here. Although some of the Carbon Black Live Response commands are the same as commands in the DOS command interface, the available options are specific to Live Response.

Table 8: Carbon Black Live Response Session Commands

Command	Description
archive	Get an archive (gzip tarball) of all the session data for this session, including commands run and files downloaded; the archive is downloaded to the computer on which you are running the Carbon Black console using the browser's download method
argparse	Test how Live Response parses CLI arguments. This command helps determine whether there are any interpretation issues; for example, it can reveal whether spaces or other special characters are properly escaped.
cd <i>[dir]</i>	Change current working directory; absolute, relative, drive-specific, and network share paths may be used
clear	Clear console screen; cls command can also be used for this purpose
delete <i>[path]</i>	Delete the file specified in the path argument
detach	Detach from current Live Response session. If a session has no attachments, it remains alive until it times out (5 minutes by default).
dir	Return list of files in current directory, or the specified directory if that is added to the command, e.g. dir c:\temp
drives	List drives on the remote host
exec <i>[processpath]</i>	<p>Execute a background process specified in the processpath argument on the current remote host; by default, process execution returns immediately and output is to stdout and stderr. Options (may be combined):</p> <ul style="list-style-type: none"> • exec -o <i>outputfile processpath</i> – Redirect the process output to the specified remote file, which you can download • exec -w <i>processpath</i> – Wait for the process to exit before returning <p>You could combine the options as shown in the example below to execute and capture the output from a script: exec -o c:\output.txt -w c:\scripts\some_script.cmd</p> <p>The full path to the process, for example, c:\windows\system32\notepad.exe, must be provided for the processpath argument.</p>
execfg <i>[processpath]</i>	<p>Execute a process on the remote host and return stdout/stderr</p> <p>For example: execfg c:\windows\system32\ipconfig /all prints the output of ipconfig to the screen.</p>
files <i>[-s session]</i> <i>[action] [option]</i>	Perform actions over cache stored session files
get <i>[path]</i>	Get file specified in the path argument from remote host and download to the host running the Carbon Black console for this session

Command	Description
help	Show the Live Response session commands with a brief description of each; if a command name is added, show the description of the specified command, with additional details (such as options) if available; e.g. help dir
hexdump	Output first 50 bytes of file in hexdump format
kill	Terminate specified process
mkdir	Make a directory on the remote host
ps	Get list of processes from remote host
put <i>[remotepath]</i>	Put a file from the host on which the console is being run onto the remote host at the specified path; the file to be put is specified in the Open dialog of the browser once the command is entered in Live Response.
pwd	Print current working directory
reg	View and/or modify Windows registry settings. The syntax of this command is: reg <i>[action] [key] [options]</i> See “Registry Access in Live Response” on page 89 or use help reg in the Live Response command window for details.

As the table shows, some commands provide information and others actually allow you to modify an endpoint. If you choose, you can try some of the information commands to become familiar with the interface before proceeding with any changes. Status and error messages should inform you of any connection or command error issues, but you can also use the **dir** or **pwd** commands to confirm your connection.

To end a Live Response session with a computer:

- In the Live Response command window, enter the **detach** command.
The session with that computer ends and the general **[CB Live]#** prompt replaces the computer-specific prompt.

Sessions also timeout after lack of activity. The default timeout value is 5 minutes.

Registry Access in Live Response

In a Live Response session, the **reg** command provides direct access to the remote computer’s Windows Registry.

The syntax of the Live Response reg command is:

```
[CB Live]# reg [action] [key or value] [options]
```

[Table 9](#) shows the reg command actions and their options. These options are intended to mirror the Windows default reg.exe command syntax. For all reg command actions, key paths can take hive references in either short or long form: HKLM or HKEY_LOCAL_MACHINE.

Table 9: Live Response Registry (reg) Command Actions

Action	Description
query	<p>Format: reg query [key or value] [options]</p> <p>Options:</p> <p>(<i>none</i>) – If no option switch is specified, query for the specified key</p> <p>-v – Query for the specified value</p> <p>Example:</p> <pre>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run</pre>
add	<p>Format: reg add [key] [options]</p> <p>Options:</p> <p>-v – Value for the key to be added</p> <p>-d – Data for the key to be added</p> <p>-t – Type of the key to be added; accepted types are:</p> <ul style="list-style-type: none"> • REG_NONE • REG_BINARY • REG_SZ • REG_EXPAND_SZ • REG_MULTI_SZ • REG_DWORD • REG_DWORD_BIG_ENDIAN • REG_QWORD <p>Example:</p> <pre>reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run -v calc -t REG_SZ -d c:\windows\system32\calc.exe</pre>
delete	<p>Format: reg delete [key or value] [options]</p> <p>Options:</p> <p>(<i>none</i>) – If no option switch is specified, delete the specified key</p> <p>-v – Delete the specified value</p> <p>Example:</p> <pre>reg delete HKLM\Software\Microsoft\Windows\CurrentVersion\Run -v calc</pre>

Detached Session Management Mode

You can enter Live Response without a specific session. In this mode, you can take certain actions that do not require current access to an endpoint, such as viewing the sessions that are active or examining files uploaded to the server as a result of a session. You also can attach to (join) an existing session or create a new one. [Table 10](#) shows the available commands in Live Response Management Mode.

Some commands in detached mode are accessible by users who do not have Global administrator privileges, but most are not, and attempting to use them returns an error message in the command window.

To open a Live Response command window without a session:

- On the Carbon Black console menu, choose **Respond > Go Live**.
The Live Response page is displayed. In this mode, the prompt in the command window shows **[CB Live]#** without the name of an endpoint.

Table 10: Live Response Management Mode Commands

Command	Description
archive <i>[id]</i>	Get an archive (gzip tarball) of all the session data for the session whose ID is provided.
argparse	Test how Live Response parses CLI arguments. This command helps determine whether there are any interpretation issues.
attach <i>[id]</i>	Attach to the session whose ID is provided. The session command can be used to find the ID of an existing session or create a new one. A session must be in <i>active</i> or <i>pending</i> state to be attached.
clear	Clear console screen; cls command can also be used for this purpose
files -s <i>[id]</i>	Perform actions over cache stored files for the session whose ID is provided.
help	Show the commands available in this mode with a brief description of each
help <i>command</i>	Show the description of the specified command, with additional details (such as options) if available; e.g. help dir
sensor <i>[options]</i>	List sensors managed by this Carbon Black server. Options: -i <i>[1.2.3.4]</i> -- Return all sensors with specified IP address. -n <i>[host_str]</i> -- Return all sensors with matching host name. -a -- Return all sensors. Searches are case-sensitive substring searches for both host name and IP address. An option must be used with this command. If both -n and -i are specified, only -i is used.
session	Manage Live Response sessions. With no argument, lists all open sessions and their ID numbers, which can be used with the attach command. Options: <ul style="list-style-type: none"> • session new <i>[id]</i> – Creates a new session for the sensor whose ID number is provided. Note that you provide a <i>sensor</i> ID, not a session ID. • session list [-v] – Lists existing sessions. If the -v option is included, closed sessions are included. This option (without -v) is the default when no additional arguments are used. • close <i>[id]</i> – Close the session whose ID is provided.

Extending Carbon Black Live Response

Because the built-in commands in Carbon Black Live Response include “put file” and “create process”, responders can arbitrarily extend the capabilities of Live Response beyond the built-ins commands. For example, and investigators could take the following series of actions:

- Upload yara.exe and search memory for your custom yara signatures
- Upload winpmem.exe and dump a memory image
- Upload sbag.exe and parse the registry for Shellbags artifacts
- Upload a custom powershell script and execute it with powershell.exe

Although the library of built-in commands in Carbon Black Live Response will grow, it will never include every command for every situation. The ability to use “put file” and “create process” together assures that you have the freedom to add utilities you need for forensics and incident response. Additional capabilities are provided by a Live Response API, described at:

https://github.com/carbonblack/cbapi/tree/5.0.0/sensor_apis#carbon-black-live-response-sensor-api

Live Response Activity Logging and Downloads

Live Response activity is logged both on sensors that are accessed and on the Carbon Black server.

For any sensor accessed by Live Response, commands executed during the session are logged in the Sensor.log file, which is in the Carbon Black sensor installation folder on the endpoint.

On the Carbon Black Enterprise Server, Live Response activity can be reviewed in the following files:

- **/var/log/cb/liveresponse/debug.log** – This is where you would go to begin troubleshooting a Live Response issue. It contains debug information related to the functional operation of the Live Response components and communication between sensor and server.
- **/etc/cb/liveresponse-logger.conf** -- This is where you can change the level of information in the debug.log.
- **/var/log/cb/audit/liveresponse.log** – This file is for auditing Carbon Black Live activity. It keeps a log of all commands executed on an endpoint and the username/account information of the person who executed each one.
- **/var/cb/data/liveresponse** – This directory is where files that are get and put using Live Response are stored. It also contains the output of all commands executed. For example if you do a process listing, the list goes into this directory in JSON format. If you download a file (for example, using the archive command), that also appears in this directory (under /tmp) as well as on the host running the Carbon Black browser.

You can change the length of time Live Response data is retained by editing the ??? parameter in the **cb.conf** file.

Chapter 7

Process Search and Analysis

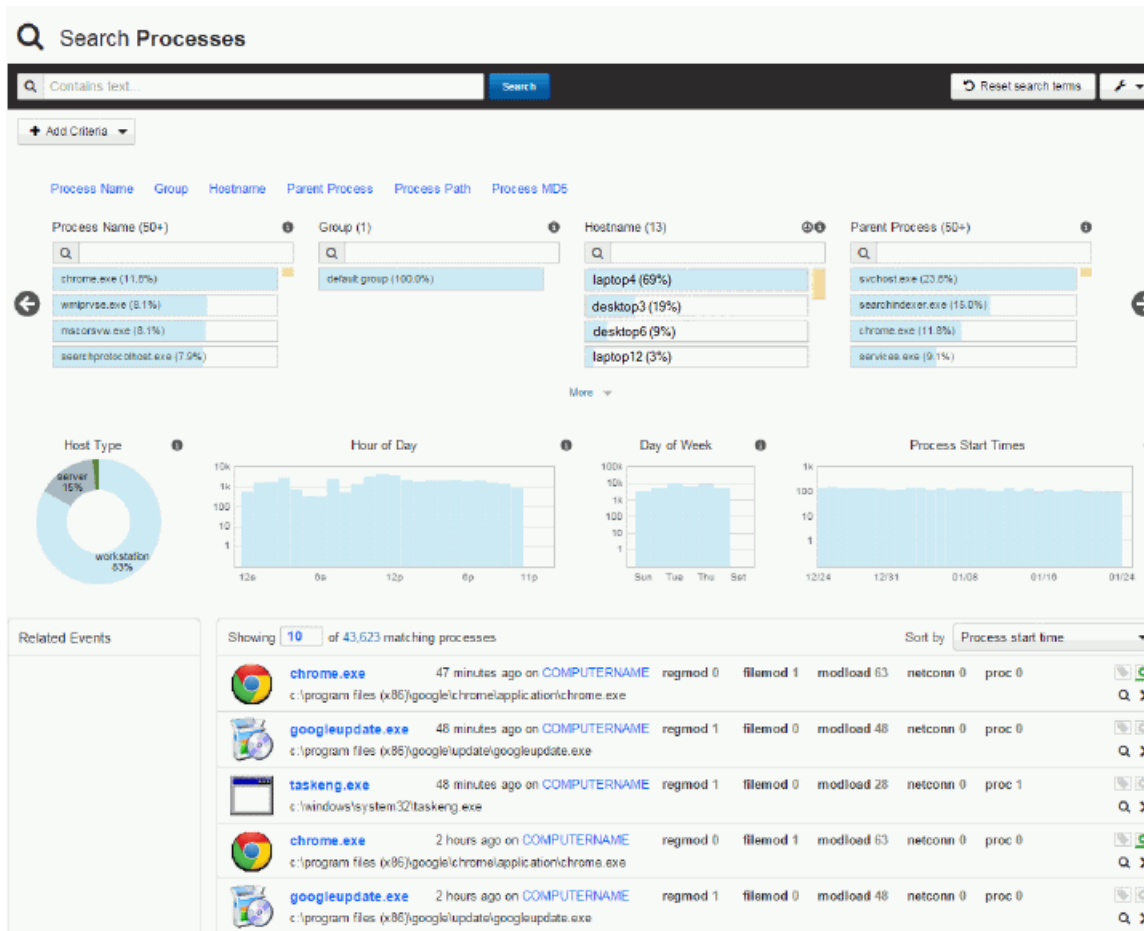
This chapter describes how to perform detailed searches for processes, and then perform in-depth analysis on them.

Sections

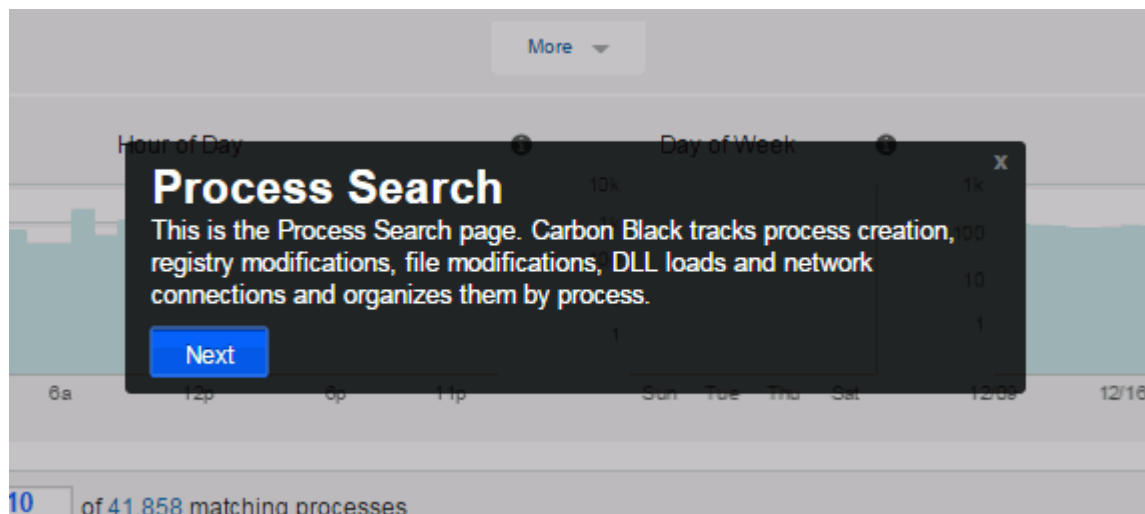
Topic	Page
Overview	94
Entering Search Criteria	95
Additional Search Page Features	96
High-level Result Summaries	97
Related Events	98
Process Results Table	99
Analysis Preview	101
Process Analysis	103

Overview

When you are aware of an incident that could be a threat -- for example, you receive a customer call reporting unusual software behavior or an alert from a threat intelligence report or watchlist -- you can search all your systems and endpoints for processes that indicate Indicators of Compromise (IOCs). With Carbon Black, sensors collect data automatically so that you can immediately start analyzing IOCs and finding solutions. You can discover how and where the threat started by using **Respond > Process Search**.



The first time that you open the Process Search page, a short tour with a series of information windows opens that provides an overview of the Process Search feature.



Click **Next** in each tour window to learn about how to use each section of this page.

Entering Search Criteria

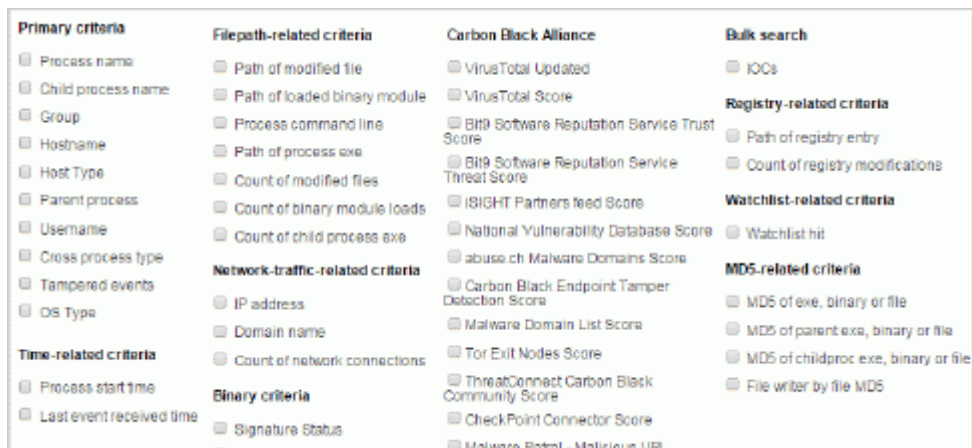
You use the Process Search feature to start your investigation into potential threats. The section “[Using Search Pages](#)” on page 36 provides an overview of the search functionality of Carbon Black. This section describes how to perform simple searches for processes using search strings and pre-defined search criteria. For detailed information about using queries in Carbon Black, see [Chapter 9, “Advanced Search Queries.”](#)

You can enter keyword searches or pre-defined search criteria in the **Search** box at the top of the page. While you type in criteria, the correct syntax displays. If you do not enter any search criteria, the system runs a search with `*.*`, every process that has executed, ranked according to process start time, with the most frequently executed processes at the top. You can also sort the results according to the count of events or last update time.

The **Search** box and the criteria fields can be used independently from one another, or they can be used in combination. When used in combination, the system combines them using an `AND` operator.

To perform a process search:

1. From the console menu, choose **Respond > Process Search**. The Search Processes page displays.
2. In the **Search** box:
 - Type a search string (must be formatted with the correct syntax) or
 - Click **Add Criteria**. The predefined search criteria options display:



3. Select the check box of a field. A dialog box displays with options to specify the criteria for the field. Repeat to use more than one field for the search.

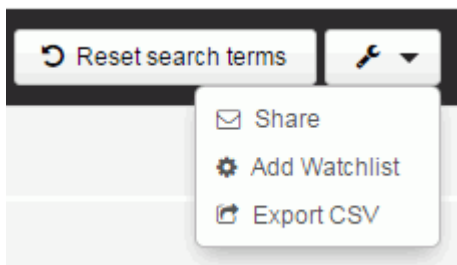
Note

The system combines multiple fields using the AND operator for the search criteria.

4. Click **Search**. The results of the search display in a series of small tables and graphs, and rows at the bottom of the page.

Additional Search Page Features

In the right top corner of the page, the **Actions** button provides several options:



- **Share:** Use this option share query strings with other people. You can e-mail the URL of the Carbon Black Enterprise server with a query string to another Carbon Black user. That user can then use that string to view the same results in their own Carbon Black user interface.
- **Add Watchlist:** Use this option to create a watchlist that is based on the current query string. A watchlist is a saved search that you can use to track specific Indicators of Compromise (IOCs).

- **Export CSV:** Use this option to export the first 1000 process search results to a .csv file in a comma separated value format for reporting, retention, or compliance. Each row will contain the URL to the details of each result on the table.

Note

To export more than 1000 rows, you must configure API functionality to capture and save the data. For information about configuring APIs, see [Appendix D, “Carbon Black APIs.”](#)

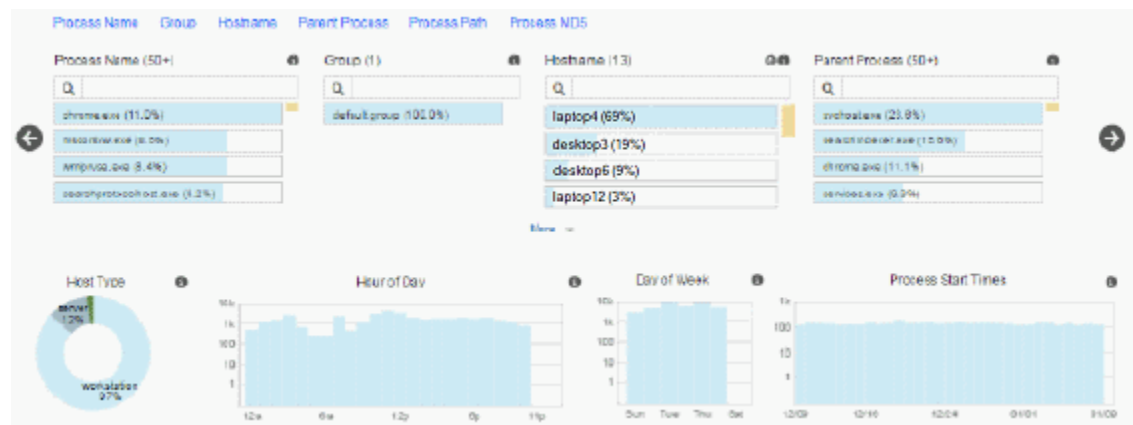
The **Reset search terms** button removes all search criteria and restores the default view using *.* as criteria.

High-level Result Summaries

When you click **Search**, the Search Processes page updates the results data with information that is specific to the search criteria that you used. The results display in a variety of formats that enable you to quickly find any process or file that seems suspicious.

A summary of the results displays in facets (small tables and graphs that provide high-level result data). Each process that matches your search criteria displays in a row below the facets.

The following illustration shows two rows of facets:



Facets provide a high-level summary of your current search results. Click the information icons to learn more about each facet.

There are two rows of facets. The top row of facets that display are tables that provide the following information:

- **Process Name:** Shows unique names of processes that match your search criteria
- **Group:** Shows the activity distributed among the configured sensor groups whose processes match the search criteria
- **Hostname:** Shows the hostnames of the currently installed sensors with processes that match the search criteria
- **Parent Process:** Shows the parent processes that create child processes and that match the search criteria.

- **Process Path:** Shows the full physical path of the executables from which a process was executed.
- **Process MD5:** Shows the MD5 hash value of the executable for each matching process.

The second row of facets are graphs that provide the following information:

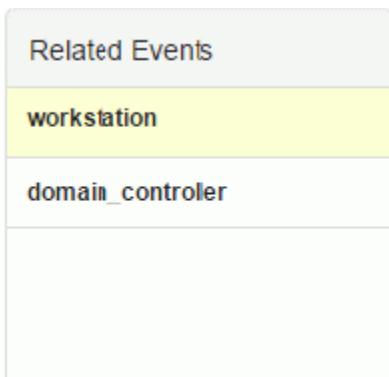
- **Host Type:** Shows a breakdown of computers with matching processes by the percentage of workstations, servers, and domain controllers with processes that match the search criteria.
- **Hour of Day:** Shows the hour of day each process was started in the computer's local time zone.
- **Day of Week:** Shows the day each process was started in the computer's local time zone.
- **Process Start Times:** Shows the number of processes that were started each day, for the most recent 30 days. The start times are displayed in Greenwich Mean Time (GMT).

By looking at the facets, you can quickly see the names and number of processes that match your search criteria, and the names and quantity of hosts on which they executed. You can also determine if the paths to the processes are legitimate.

In the Process MD5 facet, hover on one of the MD5 hashes to display its details. Below the MD5 details, rows for each process that executed the binary display.

Related Events

Below the facets and to the left of the table of process search results, the Related Events panel displays:



Related Events
workstation
domain_controller
server

The related events that display in the illustration above reflect search results using the following query (created using fields from the Search Criteria window):

```
host_type:"workstation", host_type:"domain_controller",  
host_type:"server"
```











If you hover over an item in Related Events, rows that correspond with the selected common elements are highlighted, as shown in the following example:

Related Events	Showing 10 of 145 matching processes						Sort by
notepad.exe	 notepad.exe	about 2 months ago on COMPUTER...	regmod 0	filemod 0	modload 26	netcon	
server	 explorer.exe	about 2 months ago on COMPUTER...	regmod 534	filemod 99	modload 24	netcon	
workstation	 notepad.exe	about 4 months ago on DESKTOP6	regmod 0	filemod 0	modload 25	netcon	
c:\windows\system32\notepad.exe	 notepad.exe	about 4 months ago on LAPTOP5	regmod 0	filemod 0	modload 25	netcon	

The process results that are highlighted are from executable files that were run on domain controller computers.

Process Results Table

At the bottom of the page, to the right of Related Events, the results table displays. Each row provides details about an executed process that matches the search criteria.

Showing 10 of 40,643 matching processes		Sort by
 chrome.exe	16 minutes ago on COMPUTERNAME	regmod 0 filemod 1 modload 63 netconn 0 pro
 googleupdate.exe	43 minutes ago on COMPUTERNAME	regmod 1 filemod 0 modload 48 netconn 0 pro
 taskeng.exe	43 minutes ago on COMPUTERNAME	regmod 1 filemod 0 modload 28 netconn 0 pro
 chrome.exe	47 minutes ago on COMPUTERNAME	regmod 0 filemod 0 modload 62 netconn 0 pro
 chrome.exe	1 hours ago on COMPUTERNAME	regmod 0 filemod 1 modload 63 netconn 0 pro
 wmiprvse.exe	1 hours ago on COMPUTERNAME	regmod 0 filemod 1 modload 42 netconn 0 pro
 googleupdate.exe	2 hours ago on COMPUTERNAME	regmod 1 filemod 0 modload 48 netconn 0 pro
 taskeng.exe	2 hours ago on COMPUTERNAME	regmod 1 filemod 0 modload 28 netconn 0 pro
 chrome.exe	2 hours ago on COMPUTERNAME	regmod 0 filemod 1 modload 63 netconn 0 pro
 googleupdate.exe	3 hours ago on COMPUTERNAME	regmod 1 filemod 0 modload 48 netconn 0 pro

First ← 1 2 3 4 ...

Above the search results you can see how many process executions match the search criteria and the filters you selected.

The **Sort by** menu provides the following options:

- None
- Process last update time
- Process start time (default)
- Process name
- Count of Network connections
- Count of Registry modifications
- Count of File modifications
- Count of Binary loads

On each row, the following information displays:

Table 11: Search results table row details





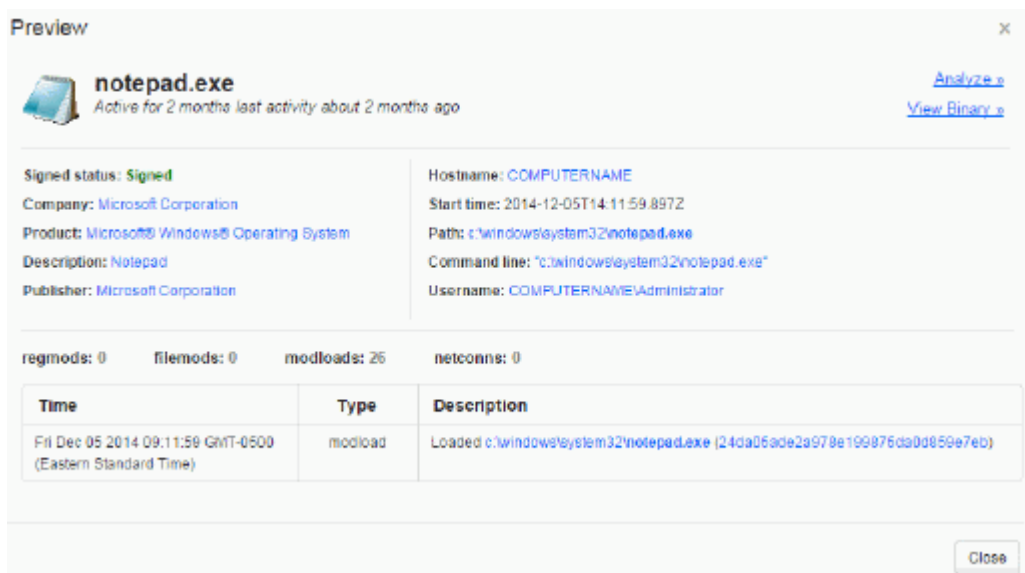
Title	Description
	Shows the icon of the process or program that was executed.
Process Name	Shows the name of the executable file that was run, for example, <code>notepad.exe</code> . Underneath the process name, the path on the file system from which the process was executed displays.
Execution Time	Shows the time of the most recent execution of the process.
regmod	Shows the number of Windows registry modifications that were made by the execution of this process.
filemod	Shows the number of files that were modified by the execution of this process.
modload	Shows the number of modules that were loaded by the execution of this process.
netconn	Shows the number of network connections that the execution of this process either attempted or established.
proc	Shows the number of child processes that were generated from the execution of this process.
>	Shows the Process Analysis page with details about the process executable file. For more information about process analysis, see "Process Analysis" on page 103.
	Shows the Analysis Preview page, which provides a more detailed summary of information about the process execution than the information in this table, but less information than the Process Analysis page. For more information, see "Analysis Preview" on page 101.
	Shows if the process execution was seen by an existing watchlist. If the icon is gray, the process execution was not seen by a watchlist. If the icon is green, the process execution was seen by a watchlist. Click on the icon to open the watchlist.

Table 11: Search results table row details (continued)


Title	Description
	<p>Shows if the result contains an event that is included in an investigation. An investigation is a collection of tagged process events that are products of search results. A gray tag icon indicates that a process does not have any events tagged for an investigation. A blue tag icon indicates that the result contains events that are tagged in an open investigation. Results that contain events that are tagged in an investigation other than an open one have a black tag icon. For more information about investigations, see Chapter 11, “Creating and Using Investigations.”</p>

Analysis Preview

If you click the magnifying glass icon in a row in the results table, the Analysis Preview page displays:



Preview x

 **notepad.exe**
Active for 2 months last activity about 2 months ago [Analyze](#)
[View Binary](#)

Signed status: Signed	Hostname: COMPUTERNAME
Company: Microsoft Corporation	Start time: 2014-12-05T14:11:59.897Z
Product: Microsoft® Windows® Operating System	Path: c:\windows\system32\notepad.exe
Description: Notepad	Command line: "c:\windows\system32\notepad.exe"
Publisher: Microsoft Corporation	Username: COMPUTERNAME\Administrator

regmods: 0 filemods: 0 modloads: 26 netconns: 0

Time	Type	Description
Fri Dec 05 2014 09:11:59 GMT-0500 (Eastern Standard Time)	modload	Loaded c:\windows\system32\notepad.exe (24da06ade2a978e199876da0d0659e7eb)

This page provides a quick overview of the following details of the selected process execution:

Metadata:

- **Signed status:** Shows if the process executable file is signed by the publisher.
- **Company:** Shows the company name of the process executable file.
- **Product:** Shows the product for which the process executable file was created.
- **Description:** Shows a text description of the process executable file.
- **Publisher:** Shows the official publisher of the process executable file.

Execution details:

- **Hostname:** Shows the name of the host on which the process was run.
- **Start time:** Shows the full timestamp for the time when the process was run.
- **Path:** Shows the physical path from which the process was run.
- **Command line:** Shows the full command line specific to the execution of this process.
- **Username:** Shows the user on the given host who executed the process. The format is `<domain>\<username>`.

Process event details:

- **Regmods:** Shows the number of Windows registry modifications that were made by the process execution.
- **Filemods:** Shows the number of files that were modified by the execution of this process.
- **Modloads:** Shows the number of modules that were loaded by this process execution.
- **Netconns:** Shows the number of network connections that this process execution either attempted or established.
- **Childprocs:** Shows child process start times, end times, and the PIDs of the selected parent process.
- **Crossprocs:** Shows occurrences of processes that cross the security boundary of other processes.

Additional details:

- **Time:** Shows the full timestamp for a data source (data sources are regmod, filemod, modload, or netconn). The time is displayed for the sensor's time zone.
- **Type:** Shows the type of data source.
- **Description:** Shows information about the event in context with the event type. For example, for filemods, the path of the file that was modified would display in this field.

At the top right of the page, the following options display:

- **Analyze:** Click to open the Process Analysis page, which provides a more granular analysis of the process executable file (this is the same page that opens when you click the Process Analysis icon (>) in the Search Processes page).
- **View Binary:** Click to view the detailed binary analysis page for the process executable file. For more information, see [Chapter 8, "Binary Search and Analysis."](#)

Process Analysis

After you have detected a threat and searched process executables, when you find a process that merits investigation, you can open the Process Analysis page. The Process Analysis page is where all the activity collected for a specific process by Carbon Black is represented. The following illustration shows the details of the process executable file:

C:\windows\system32\wbem\wmiprvse.exe

Process Analysis
 wmiprvse.exe on COMPUTERNAME by SYSTEM - was active for under one second 9 hours ago
 Command line: c:\windows\system32\wbem\wmiprvse.exe -embedding

Process: wmiprvse.exe
 OS Type: windows
 Path: c:\windows\system32\wbem\wmiprvse.exe
 Username: SYSTEM
 MD5: ce6d08350d0a1278e9a97e94023d1800
 Start Time: 2015-01-23T14:12:13.156Z

wmiprvse.exe: Signed by Microsoft Corporation
 Company: Microsoft Corporation
 Product: Microsoft Windows® Operating System
 Description: WMI Provider Host
 Signed: Signed
 Publisher: Microsoft Corporation

Filter bar: Type, Dir, Invest, Threat, Terms, Feeds, Sig, Pub, File Action, File Type, Domain, IP, Reg Action, Reg Hive, Child Path, Child MD5

Filters:
 Type: modload (42), filemod (1)
 Directories: c:\windows\system32 (35), c:\windows\system32\wbem, c:\windows\system32\wbem, c:\windows\system32\wbem, c:\windows\system32\wbem
 Investigation: Untagged (43)
 Threat Level: Known Good (28), Known Bad (0)
 Search Terms: c:\windows\system32\wbem
 Feeds: SR5Trust (28), None (15)

Timeline: 14:12:13:100 to 14:12:13:280

Time	Type	Description
2015-01-23 14:12:13.296 GMT	modload	Loaded c:\windows\system32\dpapi.dll Signed (92abf534e992c61730c24f003bbe192a)
2015-01-23 14:12:13.296 GMT	modload	Loaded c:\windows\system32\msasn1.dll Signed (7da935827bc3f48bae14Eba4b2755f1ad)

The Process Analysis page contains the following elements and options to help you investigate more deeply into the details of the process. Each item is described in the sections that follow.

- Title
- Isolate host
- Go Live >_
- Actions (Export events to CSV and Share)
- Interactive process tree
- Process execution details
- Process metadata
- Alliance feeds
- Process details facets
- Time range bar graph
- Events view

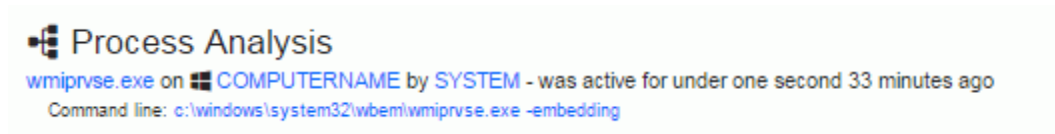
Summary

The title information shows the general process execution details. Using our example of `C:\windows\system32\wbem\wmiprvse.exe`, the format of the information that displays is:

`<Process name> on <Hostname> by <Hostname>\<User> - active for <Time> about <Time> ago`

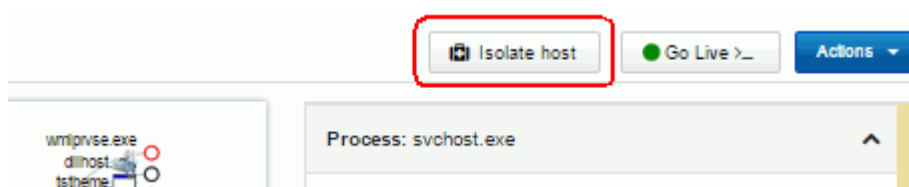
Command line: `<Executable file path>`

For example, the title information that displays for our example is:



Isolate Host

The Isolate host button displays at the top right of the Process Analysis page:

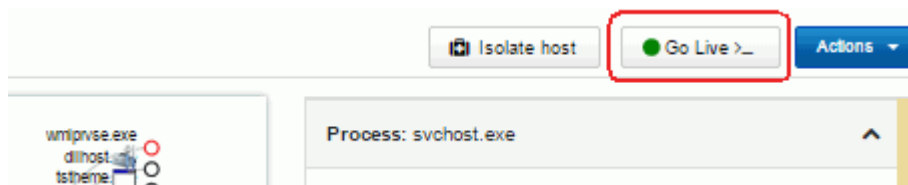


Use this option to isolate a computer. For example, you might discover that suspicious files have been executing from a particular computer and you want to prevent them from spreading to other computers in your network. When a computer (host) is isolated, connections to the Carbon Black Enterprise server such as DHCP and DNS are maintained, but all other connections are blocked or terminated. The user is not notified by Carbon Black, even though the computer will not work as expected.

The computer remains isolated until this option is disabled or the computer reboots. See [“Isolating an Endpoint”](#) on page 84 for more information.

Go Live

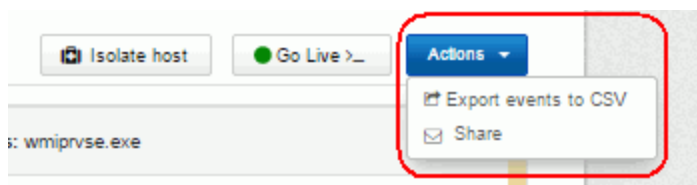
The **Go Live** button displays at the top right of the Process Analysis page:



This option is useful when you are investigating an Indicator of Compromise (IOC), because once you have identified a computer with suspicious activity, you can directly access the content on that system. You can open an interactive live session to the end-point host and execute commands in real time, to help isolate or eradicate the threat. For more information about this feature, see [“Using Carbon Black Live Response”](#) on page 85.

Actions (Export events to CSV and Share)

The **Actions** button gives you access to the **Export** and **Share** options:



The Export events to CSV option creates the following .csv files in a reports.zip archive, and downloads the archive to your local computer:

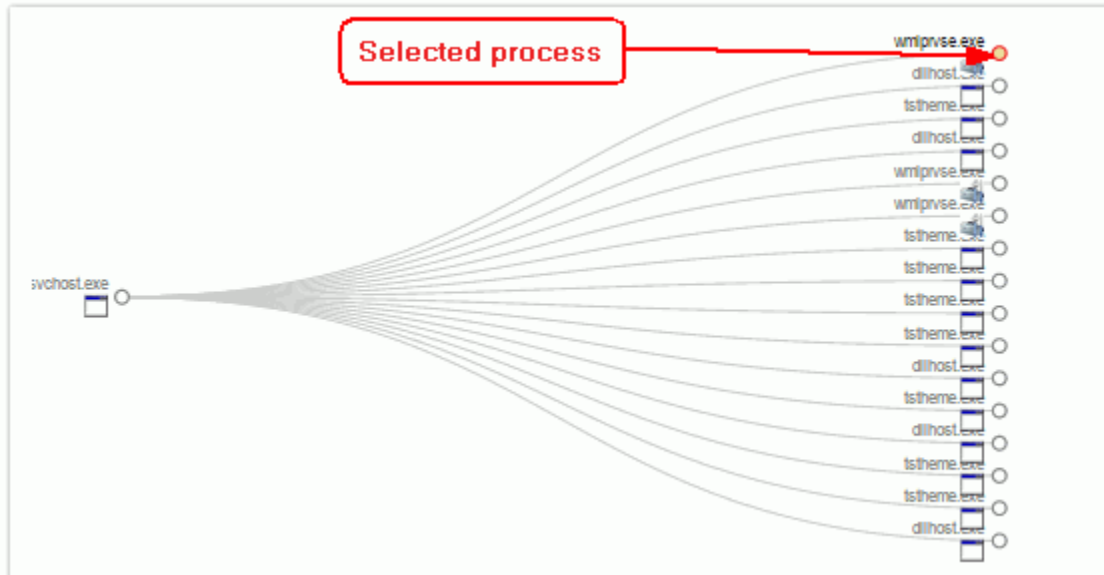
- summary.txt (contains information about the current view)
- process.txt (contains information about the processes)
- filemods.csv
- modloads.csv
- netconns.csv
- regmods.csv

The .csv files contain the information in the **Description** fields for each type that display in the results table at the bottom of the Process Analysis window. For more information, see [“Process Event Details”](#) on page 110.

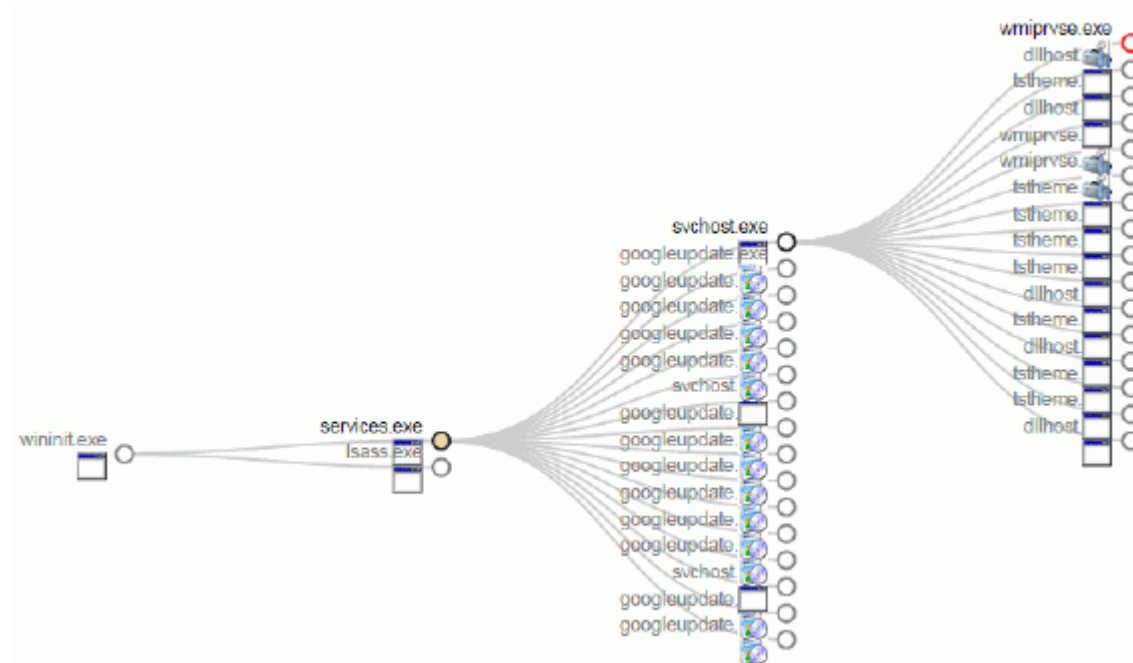
The **Share** option opens the Carbon Black user’s default email client, creates an email, and includes the details from the summary.txt file (path, MD5, start timestamp, last updated timestamp, hostname, and full command line), as well as a URL that accesses the same page in which the **Share** button was clicked.

Interactive Process Tree

By default, the graphical process tree view displays the parent process of the selected process executable file in a search result, with the relevant child process already selected (shown in gold, with a red circle), as shown in this example:



You can interact with this view by clicking other child and parent processes, for example, to continue identifying a possible issue.



The process tree always shows the process event that is selected, and includes its parent process and all child processes. Processes that are siblings to the selected process also display. To expand or collapse elements in the process tree, click once to select a process event, and click once more to expand or collapse that branch of the tree.

Note

When you click on other child or parent processes, the Process Analysis page is updated in context to show the new selected process details, including the summary tables and graphs.

Process Execution Details

Details about the process execution display in the panel on the upper right side of the Process Analysis page:



The screenshot displays a panel titled "Process: rundll32.exe" with an upward arrow. Below the title, the following details are listed:

- OS Type: (unknown)
- Path: [c:\windows\systemwow64\rundll32.exe](#)
- Username: [SYSTEM](#)
- MD5: [be1dae43dfbca94fb6b4157c1b16923e](#)
- Start Time: 2014-02-18T10:44:03.443Z

Below this section, the text "rundll32.exe: Signed by Microsoft Corporation" is shown with an upward arrow. Underneath, the following signed file information is displayed:

- Company: [Microsoft Corporation](#)
- Product: [Microsoft® Windows® Operating System](#)
- Description: [Windows host process \(Rundll32\)](#)
- Signed: **Signed**
- Publisher: [Microsoft Corporation](#)

At the bottom of the panel, there is a search icon followed by the text "Alliance Feeds 6 hit(s) in 6 report(s)" and an upward arrow.

The following information displays:

Table 12: Process Analysis: Process Execution Details

Field	Description
Process	Shows the name of the process executable file.
OS Type	Shows the operating system on which the process was executed.
Path	Shows the physical path from which the process was executed.
Username	Shows the name of the user on the host computer who executed the process. The format is: <Hostname>\<User>.
MD5	Shows the MD5 hash value of the process.
Start Time	Shows the full pastime for the process execution.

Process Metadata

Details about the process execution metadata display in the panel on the upper right side of the Process Analysis page:



The following information displays:

Table 13: Process Analysis: Process Metadata

Field	Description
<process executable file name>	Shows the name of the process executable file.
Company	Shows the name of the company that created the process executable file.
Product	Shows the product for which the process executable file was created.
Description	Shows a text description of the product .
Signed	Shows if the process or module that was executed or loaded has been signed by the publisher.
Publisher	Shows the official publisher of the process executable file.

Alliance Feeds

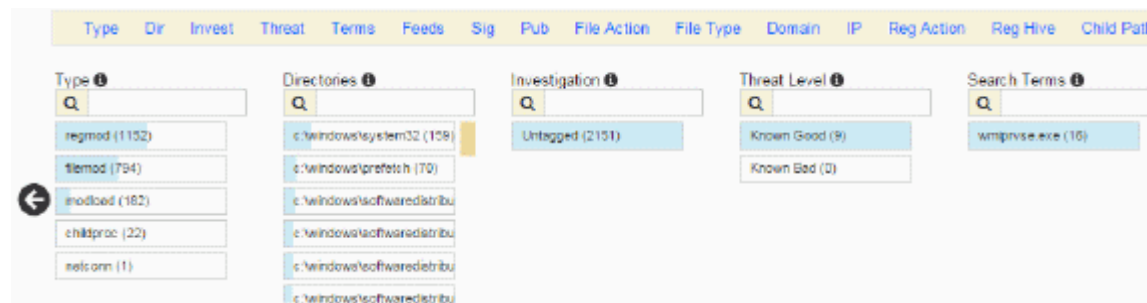
This section shows if the process event details had any hits from threat intelligence feeds:

Alliance Feeds 6 hit(s) in 6 report(s)	
ThreatConnect Connector	1 report(s)
ThreatConnect 2-16-2014 Score: 100 ❗ 8D6F9D5EC35884A06DEA1AD4A10FF118	
Fidelis XPS Connector	1 report(s)
Fidelis MD5 2-16-2014 Score: 100 ❗ 8D6F9D5EC35884A06DEA1AD4A10FF118	
ThreatConnect Carbon Black Community	1 report(s)
ThreatConnect MD5 2-16-2014 Score: 100	

If there are any hits, the results display below Alliance Feeds in rows that are expanded by default. Each row shows the source of the feed, a link to information about the threat that was detected, the date and score of the hit, and the MD5 hash value of the binary that caused the hit. Click on the MD5 hash value to go directly to the process event row for that binary.

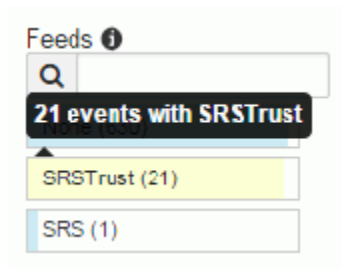
Process Event Details

There are several facets that provide a high-level summary of events in the process executable file.



You can access the facets by clicking the facet name in the facet menu bar or by clicking the arrows on the left and right of the facets panel. Hover over the information icons in the facet titles for more information.

You can also hover over facet rows to see the number of events that were affected, for example:



The following table provides a description of each facet. The name in parentheses is the name of the facet as shown in the menu bar.

Table 14: Process Analysis: Facet Descriptions

Facet	Menu Bar Name	Description
Type	Type	Shows the type of process event. The values are: <ul style="list-style-type: none"> filemod (file modifications) modload (number of modules loaded) regmod (registry modifications) netconn (number of network connections enabled) childproc (child processes) crossproc (cross processes)
Directories	Dir	Shows the directories used in this process.
Investigation	Invest	Shows the tagged status for events in this process for any investigations.
Threat Level	Threat	Shows report scores for events associated with threat intelligence feed hits in this process.

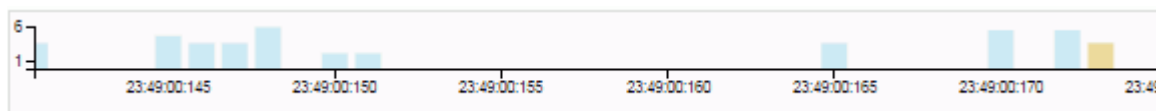
Table 14: Process Analysis: Facet Descriptions (continued)

Facet	Menu Bar Name	Description
Search Terms	Terms	Shows matching query terms used in searching for processes.
Feeds	Feeds	Shows threat intelligence feed hits found in this process.
Signature	Sig	Shows the signature status types of all modules that were loaded by this process (for example, signed, unsigned, or expired).
Publisher	Pub	Shows the publishers of all the modules that were loaded by this process.
FileMod action	File Action	Shows the types of file modifications that occurred during the execution of this process (create, delete, first write, last write), and the number of times those actions occurred.
FileMod fileType	File Type	Shows the types of the files that were modified.
Domain	Domain	Shows the domain (DNS) names associated with network connections that were made by this process.
IP address	IP	Shows the IP addresses associated with network connections that were made by this process.
RegMod action	Reg Action	Shows the type of registry modification (created, deleted key, deleted value, first write, last write).
RegMod hive	Reg Hive	Shows the location of the registry that is associated with registry modification events.
Childproc filepaths	Child Path	Shows paths to child processes that were created by this process.
Childproc md5s	Child MD5	Shows MD5 files of child processes that were created by this process.

On the far right of the facet menu bar, you can click the **Reset** button to reset all of the facets to their original state. For example, if you have been filtering or searching in any of the facets, you can reset them to their original state.

Time Range Bar Graph

The time range bar graph is useful for investigating Indicators of Compromise (IOCs) if you want to view events that occurred at a specific time. Below the row of facets, a bar graph displays that shows the times during which the selected process was executed.












You can hover over the bars in the graph to show the number of times the process was executed during a specific time period.

As you scroll down to view the rows in the process event details list, the time range bar graph is pinned to the top of the page and is updated with information for the rows that are currently viewable. The bars change color from blue to gold when the rows that display are in the time range that the bars represent. For example, if the rows on the page fall between 1:00 pm and 2:00 pm, events after 2:00 pm in the bar graph will display as blue and not gold.

Process Event Details

The events view for a selected process displays as a table with several rows at the bottom of the Process Analysis page:

			Time ^	Type	Description		Search
			2014-11-30 23:49:00.193 GMT	childproc	PID 11940 ended c:\program files (x86)\google\update\googleupdate.exe Signed (506708142bc63dabaf)		
	<input checked="" type="checkbox"/>		2014-11-30 23:49:00.137 GMT	modload	Loaded c:\windows\system32\apphelp.dll Signed (90499f3163a9f815cf196a205ea3cd5d)		
			2014-11-30 23:49:00.135 GMT	childproc	PID 11940 started c:\program files (x86)\google\update\googleupdate.exe Signed (506708142bc63dabaf)		
	<input checked="" type="checkbox"/>		2014-11-30 23:49:00.134 GMT	modload	Loaded c:\windows\system32\wmilite.dll Signed (6f8048f3d343e4b186ab5a9e302b7e16)		
			2014-11-30 23:49:00.131 GMT	regmod	First wrote to registry\machine\software\microsoft\windows nt\currentversion\schedule\{e8f47e68-547c-4e68-b8d1-8e8f47e68547}\data		

The process events rows show the following details:

Table 15: Process Event Details: Row Descriptions



Heading	Description
Tag 	Shows if an event is tagged for an investigation. You can click the tag icon to select this event for future investigation. After you select the tag icon, it turns blue to indicate that it is now included in an investigation.
Trusted Events <input checked="" type="checkbox"/>	Shows if the event is trusted. When you click on the row, the trust information displays with a link to the source.
Threat Intelligence Feed Hits 	Shows if this event has matched a threat intelligence feed.
Time	Shows the time that the event occurred.

Table 15: Process Event Details: Row Descriptions (continued)

Heading	Description
Type	Shows the type of process event. The values are: <ul style="list-style-type: none"> • filemod (file modification - displays with a light green bar) • modload (number of modules loaded - displays with a dark green bar) • regmod (registry modification - displays with a blue bar) • netconn (number of network connections enabled - displays with a purple bar) • childproc (child process - displays with an orange bar) • crossproc (cross process - displays with a red bar)
Description	Shows the operation that the Type event performed. For example: <ul style="list-style-type: none"> • filemod could display “Deleted” or “Created” and then provide the path to the file that was modified. • modload could display the module that was loaded by the process. Modload descriptions could also include the path of the module that was loaded, if the module was signed or unsigned by the publisher, and the unique MD5 hash. • regmod could display the Windows registry key that was created or modified. • netconn could display the connection made, including the IP address (including hostname), port, and protocol. • childproc could display the child process start time, end time, and PID of the selected parent process. • crossproc could display the action it performed, for example, opening a handle or starting or ending processes.
Search	Allows you to reduce the number the events that display and focus the results based on terms entered into the Search box. For example, entering “Microsoft” into the Search box would display only Microsoft events.

You can expand an event in the results table by clicking the down arrow on the right. Details about the event display. This example shows details for an event with the type modload:

The screenshot shows a process event detail view for a modload event. The event occurred on 2015-01-15 at 14:12:14.599 GMT. The event type is modload, and it shows a file being loaded from c:\windows\system32\dpapi.dll. The file is signed with the MD5 hash 92abf534e992c61730c24f003bbe192a. Below the event details, there is a summary of search results: 2 computer(s) have seen this md5 in 484 processes: computername, id-dc01. The event details are divided into two sections: Binary Info and Alliance Information. Binary Info includes: Company: Microsoft Corporation, Product: Microsoft® Windows® Operating System, Description: Data Protection API, Signature Status: Signed, and Publisher: Microsoft Corporation. Alliance Information includes: Bit9 Software Reputation Service Trust, SRS report for 92abf534e992c61730c24f003bbe192a, Score: 80, and a checkmark next to the MD5 hash 92ABF534E992C61730C24F003BBE192A.

Different types of details display for each type of event, as shown in the following table.

Table 16: Process Analysis: Event Type Details

Event Type	Details
filemod	Shows the number of computers that have seen this file modification, and the number of processes in which the file modification occurred on those computers.
modload	Shows the following information: <ul style="list-style-type: none"> • The number of computers that have seen the MD5 hash for the module that was loaded, and the number of processes the MD5 appears in on those computers. • Binary information: company name, product name, a description of the binary, signature status, and publisher • Alliance information: the source of the threat intelligence feed, a link to the report for the MD5 hash, the MD5 score, and the MD5 trust status
regmod	Shows the number of computers that have seen a modification of a registry key, and the number of processes in which the registry modification occurred on those computers.
netconn	Shows the number of network connections that the execution of this process either attempted or established.
childproc	Shows the following information: <ul style="list-style-type: none"> • The number of computers that have seen the MD5 in the description, and the number of processes in which this MD5 was observed. Lists the names of the processes. • Process metadata: length of time for which the process was active, and when the process execution occurred (for example, "about one month ago"), username of the user executing the process, MD5 hash name, and the command line of the process executable file. • Binary information: company name, product name, product description, signature status, and publisher.
crossproc	Shows the following information: <ul style="list-style-type: none"> • Description of the OpenProcess API call for the cross process. Carbon Black records all OpenProcess API calls that request <code>PROCESS_CREATE_THREAD</code>, <code>PROCESS_DUP_HANDLE</code>, <code>PROCESS_SUSPEND_RESUME</code>, <code>PROCESS_VM_OPERATION</code>, or <code>PROCESS_VM_WRITE</code> access rights. These access rights allow this process to change the behavior of the target process. • Process metadata: length of time the cross process was active, user name of the user who executed the process, MD5 hash name, and the command line of the process executable file. • Binary metadata: company name, product name, product description, signature status, and publisher.

Chapter 8

Binary Search and Analysis

This chapter describes investigating binary metadata.

Sections

Topic	Page
Overview	116
Entering Search Criteria	117
High-level Result Summaries	119
Related Metadata	120
Binary Preview	122
Binary Analysis	124

Overview

You can use Binary Search to explore the metadata of a binary. Carbon Black sensors begin tracking binaries at the moment that they are executed by a process, and displays the file information in binary search results.

To search for binaries, click **Respond > Binary Search**.

Search Binaries

Contains text... Search Reset search terms

+ Add Criteria

Digital Signature Publisher Company Name Product Name File Version File paths Groups Hostnames

Digital Signature (5) Publisher (27) Company Name (96) Product Name (200)

Signed (85.3%) Unsigned (14.7%) Invalid Chain (0.0%) Bad Signature (0.0%)

Microsoft Corporation (90.9%) Google Inc (1.6%) VMware, Inc. (1.5%) Oracle America, Inc. (1.1%)

Microsoft Corporation (88.4%) VMware, Inc. (1.4%) Adobe Systems Incorporated (1.0%) Oracle Corporation (0.9%)

Microsoft Windows Operating System... Microsoft .NET Framework (12.9%) Microsoft Office 2013 (3.3%) Microsoft (R) Windows (R) Operating Sys...

Sign Time Host Count First Seen Cb Alliance: VirusTotal Hit Counts

Showing 10 of 8,960 matching binaries Sort by First seen time

Binary Icon	Hash	Signature	Company	Seen as	Size	Actions
	8D466919CD6E9E76219136A1FE069C2	Signed	Microsoft Corporation	discan.dll about 11 days ago	183.5 KB	
	EE3ED9FF4BE5D79556EB8CC1BC869A74	Signed	Microsoft Corporation	security.dll about 18 days ago	5 KB	
	2A0CABDD9B4584538A1D0022A4D8FD3F	Signed	Google Inc.	delegate_execute.exe about 24 days ago	1.96 MB	
	AC13A4FE6396E08B46C7E270BC6CC22C	Signed	Microsoft Corporation	ping.exe about 24 days ago	20.5 KB	
	FC0B4A626881D7C5980D757214DB2D25	Signed	Microsoft Corporation	cmd.exe about 24 days ago	347.5 KB	

Entering Search Criteria

You can enter keyword searches or pre-defined search criteria in the **Search** box at the top of the page. While you type in criteria, the correct syntax displays. However, on the Binary Search page, the search not only auto-completes your criteria, but estimates results as well. If you do not enter any search criteria, the system runs a search with `*.*`, which includes every binary that has executed in your environment. The results display with a single instance of every binary and its metadata. Each binary is identified by its MD5 hash value.

To perform a binary search:

1. From the console menu, choose **Respond > Binary Search**. The Search Binaries page displays.
2. Enter search criteria:
 - In the **Search** box, type a search string and click **Search**, or
 - Click **Add Criteria**. A list of predefined search criteria displays:

Primary Criteria	File Metadata	Carbon Black Alliance	Bulk search
<input type="checkbox"/> First seen at	<input type="checkbox"/> File Description	<input type="checkbox"/> VirusTotal Updated	<input type="checkbox"/> IOCs
<input type="checkbox"/> Filename	<input type="checkbox"/> Company Name	<input type="checkbox"/> VirusTotal Score	Digital Signature Information
<input type="checkbox"/> MD5	<input type="checkbox"/> Product Name	<input type="checkbox"/> iSIGHT Partners feed Score	<input type="checkbox"/> Signature Status
<input type="checkbox"/> Size	<input type="checkbox"/> File Version	<input type="checkbox"/> National Vulnerability Database Score	<input type="checkbox"/> Publisher
<input type="checkbox"/> Watchlist Hit	<input type="checkbox"/> Comments	<input type="checkbox"/> abuse.ch Malware Domains Score	<input type="checkbox"/> Program Name
<input type="checkbox"/> Architecture	<input type="checkbox"/> Legal Trademark	<input type="checkbox"/> Bit9 + CB Advanced Threats Feed Score	<input type="checkbox"/> Issuer
<input type="checkbox"/> Binary Type	<input type="checkbox"/> Legal Copyright	<input type="checkbox"/> Bit9 + CB Early Access Indicators Feed Score	<input type="checkbox"/> Subject
<input type="checkbox"/> Hostname	<input type="checkbox"/> Internal Name	<input type="checkbox"/> Bit9 + CB Endpoint Suspicious Indicators Feed Score	<input type="checkbox"/> Sign Time
<input type="checkbox"/> Groups	<input type="checkbox"/> Metadata Filename	<input type="checkbox"/> Bit9 + CB Endpoint Visibility Feed Score	
<input type="checkbox"/> OS Type	<input type="checkbox"/> Product Description	<input type="checkbox"/> Carbon Black Endpoint Tamper Detection Score	
	<input type="checkbox"/> Product Version	<input type="checkbox"/> Malware Domain List Score	
	<input type="checkbox"/> Private Build	<input type="checkbox"/> ThreatConnect Carbon Black Community Score	
	<input type="checkbox"/> Special Build	<input type="checkbox"/> Tor Exit Nodes Score	

Select the check box of a field. A dialog box displays with options to specify the criteria for the field. Repeat to use more than one field for the search.

Note

The search box and the individual criteria fields can be used independently from one another, or they can be used in combination. When used in combination, the system combines them using an `AND` operator.

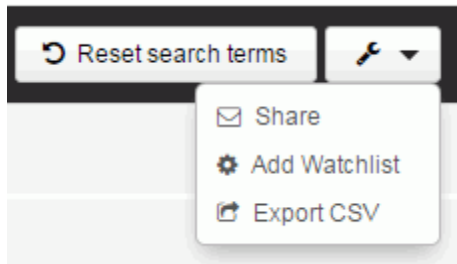
Click **Search**. The search results display in high-level groupings of binary metadata that contain fields with data that matches your search criteria.

Note

For detailed information about using queries in Carbon Black, see [Chapter 9, “Advanced Search Queries.”](#)

Additional Search Page Features

In the right top corner of the screen, the **Actions** button provides several options:



- **Share:** Use this option share query strings with other people. You can e-mail the URL of the Carbon Black Enterprise server with a query string to another Carbon Black user. That user can then use that string to view the same results in their own Carbon Black user interface.
- **Add Watchlist:** Use this option to create a watchlist that is based on the current query string. A watchlist is a saved search that you can use to track specific Indicators of Compromise (IOCs).
- **Export CSV:** Use this option to export the first 1000 binary search results to a .csv file in a comma separated value format for reporting, retention, or compliance. In addition to the data in the results, each row will contain the URL to the details of each result on the table.

Note

To export more than 1000 rows, you must configure API functionality to capture and save the data. For information about configuring APIs, see [Appendix D, “Carbon Black APIs.”](#)

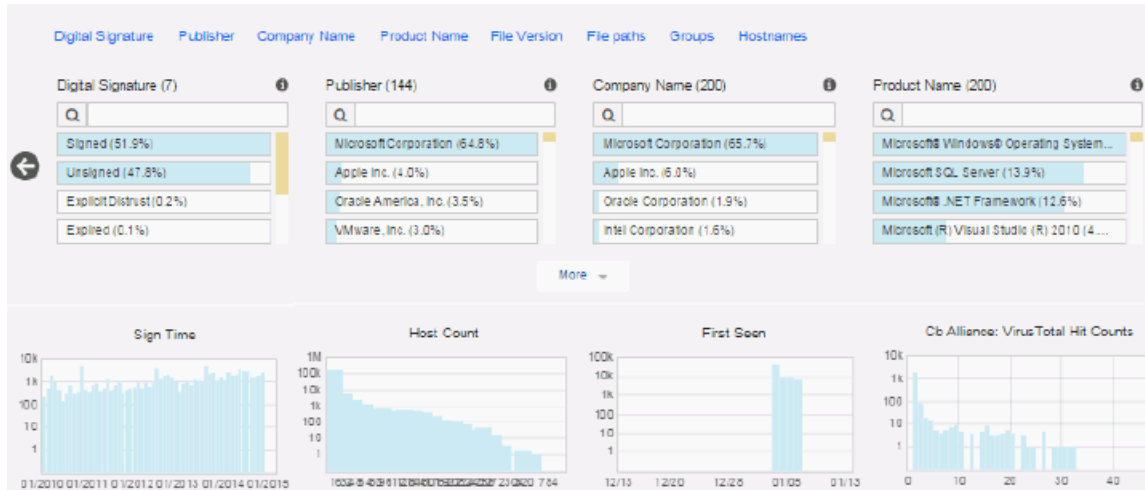
The **Reset search terms** button removes all search criteria and restores the default view using *.* as criteria.

High-level Result Summaries

When you click **Search**, the Search Binaries page updates the results data with information that is specific to the search criteria that you used. The results display in a variety of formats.

A summary of the results displays in facets (small tables and graphs that provide high-level result data). Each process that matches your search criteria displays in a row below the facets.

The following screen capture shows two rows of facets:



Facets provide a high-level summary of your current search results. Click the information icons to learn more.

There are two rows of facets. The top row of facets displays the following information about binaries in the results:

- **Digital Signature:** Shows the percentages of signed, unsigned, explicit distrust, and expired binaries.
- **Publisher:** Shows a list of binary publishers, and the percentage of binaries that have those publishers.
- **Company Name:** Shows a list of binary publisher companies and the percentage of binaries with those company names.
- **Product Name:** Shows the binary's product name.
- **File Version:** Shows the binary's file version.
- **File Paths:** Shows a list of file paths where files matching the current binary search have been seen.
- **Groups:** Shows a list of the sensor groups that have identified binaries.
- **Hostnames:** Shows a list of host names for computers on which binaries have been identified.

The second row of facets are graphs that display the following information about binaries in the results:

- **Sign Time:** Shows the number of binaries that were signed on a particular date.
- **Host Count:** Shows the number of binaries that were seen by Carbon Black on a host or a number of hosts.
- **First Seen:** Shows the number of binaries that were first detected on a particular date.
- **Cb Alliance: VirusTotal Hit Counts:** Graph that shows the number of binaries with VirusTotal hits and the VirusTotal value of the hits.

Related Metadata

Below the facets and to the left of the table of process search results, the Related Metadata panel displays:

Related Metadata
NOTEPAD.EXE
C:\Windows\system32\notepad.exe
c:\windows\syswow64\notepad.exe
c:\windows\system32\notepad.exe

The related metadata that displays in the illustration above reflect search results using notepad.exe for search criteria.

If you hover over an item in Related Metadata, rows that correspond with the selected common elements are highlighted, as shown in the following example:

Related Metadata	Showing <input type="text" value="10"/> of 4 matching binaries
NOTEPAD.EXE	 24DA05ADE2A978E199875DA0D859E7EB Seen as: notepad.exe abt Signature: Signed Company: Microsoft Corporation
C:\Windows\system32\notepad.exe	 D378BFFB70923139D6A4F546864AA61C Seen as: notepad.exe abt Signature: Signed Company: Microsoft Corporation
c:\windows\syswow64\notepad.exe	 F2C7BB8ACC97F92E987A2D4087D021B1 Seen as: notepad.exe abt Signature: Signed Company: Microsoft Corporation
c:\windows\system32\notepad.exe	 E30299799C4ECE3B53F4A7B8897A35B6 Seen as: notepad.exe abt Signature: Signed Company: Microsoft Corporation

Binary Search Results Table

At the bottom of the page, to the right of Related Metadata, the results table displays. Each row provides details about binary metadata that matches the search criteria.



Showing <input type="text" value="10"/> of 8,960 matching binaries		Sort by <input type="text" value="First seen time"/>	
	55A9A5D9F8EC7512B8F1153657BEDF92 Seen as: msfeeds.dll about 1 months ago Size: 614 KB Signature: Signed Company: Microsoft Corporation		 
	2689A9E9EF189534DC2FF5F870E26067 Seen as: mshtml.dll about 1 months ago Size: 22.46 MB Signature: Signed Company: Microsoft Corporation		 
	E6CCE5FA61801AA47891654747ADB924 Seen as: inetcp.cpl about 1 months ago Size: 1.95 MB Signature: Signed Company: Microsoft Corporation		 
	74C6B3109A607B88B1A3171A3D54C8D8 Seen as: cryptui.dll about 1 months ago Size: 584.5 KB Signature: Signed Company: Microsoft Corporation		 
	439A00B0F73BD7B6C1C08F4A760BEC07 Seen as: leadvpack.dll about 1 months ago Size: 128 KB Signature: Signed Company: Microsoft Corporation		 
	8A50547F54A3BD5BE9A1E151E15D3F92 Seen as: profext.dll about 1 months ago Size: 52.5 KB Signature: Signed Company: Microsoft Corporation		 
	C500954647E81A00700D3767C2B3CC4B Seen as: setupapi.dll about 1 months ago Size: 1.69 MB Signature: Signed Company: Microsoft Corporation		 

Above the search results you can see how many binaries match the search criteria and the filters you selected. The **Sort by** menu provides the following options:

- None
- First seen time (default)
- Cb Alliance: VirusTotal Hits
- Sign time
- File size
- Company name
- MD5

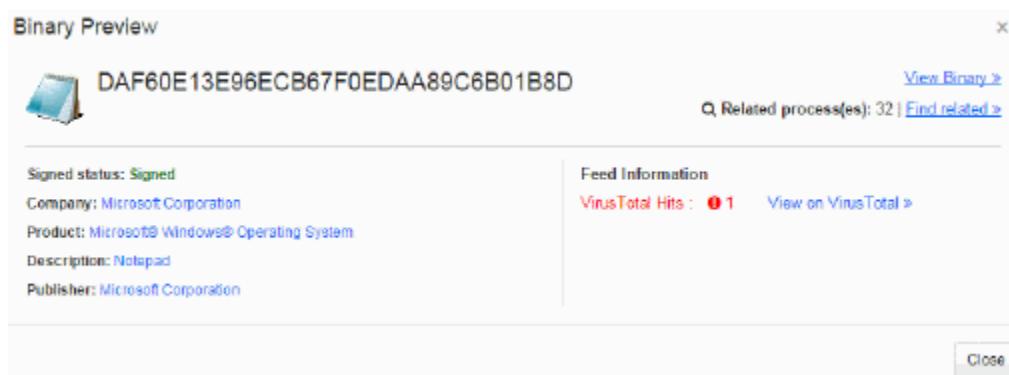
Table 17 shows the information displayed in each binary search results row.

Table 17: Binary Search Results Table Row details

Title	Description
Icon	Shows the icon of the file in which the binary was detected.
Binary Hash	Shows the MD5 hash value of the binary.
Execution Time	Shows the last time that the file in which the binary was identified was loaded.
Size	Shows the size of the file that contains the binary.
Signature	Shows whether the binary file is signed or unsigned.
Company	Shows the binary file's company name
	Shows if the binary was identified by an existing watchlist. If the icon is gray, the binary was not identified by a watchlist. If the icon is green, the binary was identified by a watchlist. Click on the icon to open the watchlist.
	Shows the Binary Preview page, which provides a more detailed summary of information about the binary than the information in this table, but less information than the Binary Details page. For more information, see Binary Preview .
>	Shows the Binary Analysis page with details about the binary file. For more information about process analysis, see " Binary Analysis " on page 124.

Binary Preview

If you click the magnifying glass icon in a row in the results table, the Binary Preview page displays:



At the top of the screen the MD5 hash value of the binary displays. The file name(s) that the binary has used are listed beneath the hash value.

This page provides a quick overview of the following details:

- **Metadata:**
 - **Signed status:** Shows if the binary file is signed by the publisher.
 - **Company:** Shows the company name identified in the metadata of the binary file.
 - **Product:** Shows the product name identified in the metadata for the binary file.
 - **Description:** Shows a text description of the binary file.
 - **Publisher:** Shows the official publisher of the binary file.
- **Feed information:** shows a list of threat intelligence feed scan results. You can click on the links to go to the source of the results.


At the top right of the page, the following options display:

- **View Binary:** Click to view the detailed analysis page for the binary. For more information about binary analysis, see [“Binary Analysis”](#) on page 124.
- **Find related:** Click to open the Process Search page, with a pre-defined query for the MD5 hash value of this binary. The number of related processes displays to the left of the **Find related** link.

Binary Analysis

Use the Binary Analysis page to investigate a binary more deeply. You can access the page from the **View Binary** link on the Binary Details page, or from clicking the > icon in a binary result row from the Search Binaries page.

D378BFFB70923139D6A4F546864AA61C
 Seen as: notepad.exe
 First seen at: 2014-10-04T15:25:24.597Z (about 3 months ago)
 Status: **Signed**
 Publisher Name: Microsoft Corporation



File writer(s): 0 | [Find writers >](#)
 Related process(es): 4252 | [Find related >](#)

Search the web: [Google >](#)

Frequency Data

280 computers have seen this md5 in 1614 processes.

Feed Information

✔ SRS Trust Score: **100** | [View on SRS Trust >](#)
❗ VirusTotal Hits: **1** | [View on VirusTotal >](#)

General Info

OS Type	Windows
Architecture	32 bit
Binary Type	Shared Resource
Size	175.5 KB Download

File Version Metadata

File Description	Notepad
File Version	6.1.7600.16385 (win7_rtm.090713-1255)
Original Filename	NOTEPAD.EXE.MUI
Internal Name	Notepad
Company Name	Microsoft Corporation
Product Name	Microsoft® Windows® Operating System
Product Version	6.1.7600.16385
Legal Copyright	© Microsoft Corporation. All rights reserved.

Digital Signature Metadata

Result	Signed
Publisher	Microsoft Corporation
Signed Time	2009-07-14T07:34:00Z
Result Code	0x0

Observed Paths

Observed Path	C:\Windows\system32\notepad.exe
Observed Path	c:\windows\system32\notepad.exe
Observed Path	C:\Windows\system64\notepad.exe
Observed Path	c:\windows\system64\notepad.exe

Observed Paths

Observed Path	C:\Windows\system32\notepad.exe
Observed Path	c:\windows\system32\notepad.exe
Observed Path	C:\Windows\system64\notepad.exe
Observed Path	c:\windows\system64\notepad.exe

Recently Observed Hosts (20+) ⓘ

Hostname	test1-1
Hostname	test1-100
Hostname	test1-101
Hostname	test1-102
Hostname	test1-103
Hostname	test1-106
Hostname	test1-107

This page contains the following elements to help you investigate more deeply into the details of the binary. Each item is described in the sections that follow.

- Binary Overview
- Frequency Data
- Feed Information
- General Info
- File Version Metadata
- Digital Signature Metadata
- Observed Paths
- Recently Observed Hosts

Binary Overview

The overview section contains the following information:

D378BFFB70923139D6A4F546864AA61C
 Seen as: notepad.exe
 First seen at: 2014-10-04T15:25:24.597Z (about 3 months ago)
 Status: **Signed**
 Publisher Name: Microsoft Corporation

 Q File writer(s): 0 | [Find writers »](#)
 Q Related process(es): 4252 | [Find related »](#)

Search the web: [Google »](#)

Table 18: Binary Analysis Overview Section

Heading	Description
MD5 Hash Value	Shows the MD5 hash value for the binary.
Seen as	Shows the filenames that were seen for binaries that match this MD5 hash value.
First seen at	Shows the full time stamp of the time that this binary was last observed by currently installed sensors.
Status	Shows the signature status - either Signed or Unsigned.
Publisher Name	Shows the binary's publisher name.
File writer(s)	Shows the number of files that this binary has written to, and the names of those files.
Related Process(es)	Shows the number of processes that have used this binary.
Search the web	Provides a Google search string that contains the binary's MD5 hash value so that you can see whether there is any other information or discussion about this binary.

Frequency Data

This section shows how many hosts have observed the binary with this MD5 hash value.

Frequency Data

280 computers have seen this md5 in 1614 processes.

Feed Information

This section shows scan results for this binary from Threat Intelligence Feeds. You can click the links to see the results.

Feed Information

✔ **SRS Trust Score:** 100
🔍 [View on SRS Trust »](#)

❗ **VirusTotal Hits:** 1
🔍 [View on VirusTotal »](#)

General Info

This section shows the following details about the binary.

General Info

OS Type	Windows
Architecture	32 bit
Binary Type	Shared Resource
Size	175.5 KB 📄 Download

Table 19: Binary Analysis General Info Section

Heading	Description
OS Type	Shows the operating system that the binary uses.
Architecture	Shows whether this binary uses 32-bit or 64-bit architecture.
Binary Type	Shows the resource type of the binary: either Standalone or Shared.
Size	Shows the size of the binary. Also provides a link to download the physical binary.

File Version Metadata

This section shows the file version metadata of the binary.

File Version Metadata	
File Description	Notepad
File Version	6.1.7600.16385 (win7_rtm.090713-1255)
Original Filename	NOTEPAD.EXE.MUI
Internal Name	Notepad
Company Name	Microsoft Corporation
Product Name	Microsoft® Windows® Operating System
Product Version	6.1.7600.16385
Legal Copyright	© Microsoft Corporation. All rights reserved.

Table 20: Binary Analysis File Version Metadata Section

Heading	Description
File Description	Shows the name of the binary (from the publisher).
File Version	Shows the version of the binary.
Original Filename	Shows the filename of the binary.
Internal Name	Shows the internal name of the binary
Company Name	Shows the company name of the binary.
Product Name	Shows the product name of the binary.
Product Version	Shows the product version of the binary file.
Legal Copyright	Shows the copyright details for the file, including its publisher.

Digital Signature Metadata

This section shows the binary file signature metadata.

Digital Signature Metadata	
Result	Signed
Publisher	Microsoft Corporation
Signed Time	2009-07-14T07:34:00Z
Result Code	0x0

Table 21: Binary Analysis File Digital Signature Metadata Section

Heading	Description
Result	Shows the status of the binary signature: either Signed or Unsigned.
Publisher	Shows the name of the publisher of the binary.
Signed Time	Shows the time that the binary was signed.
Result Code	Shows the result or exit code that followed the execution of the binary.


Observed Paths

This section shows the full physical paths from which the binary was loaded.

Observed Paths	
Observed Path	C:\Windows\system32\notepad.exe
Observed Path	c:\windows\system32\notepad.exe
Observed Path	C:\Windows\syswow64\notepad.exe
Observed Path	c:\windows\syswow64\notepad.exe

Observed Hosts

This section shows the names of all the hosts on which this binary has been observed.

Recently Observed Hosts (20+) 	
Hostname	test1-1
Hostname	test1-100
Hostname	test1-101
Hostname	test1-102
Hostname	test1-103
Hostname	test1-106
Hostname	test1-107
Hostname	test1-11

You can select the icon:



to download the entire list of hosts that used this binary.

Chapter 9

Advanced Search Queries

This appendix describes details about using queries to search for processes and binaries.

Sections

Topic	Page
Query Criteria Details	132
Query Syntax Details	132
Fields	134
Datatypes	138
Example Searches	141

Query Criteria Details

Carbon Black supports multiple types of query criteria. The following list shows a high-level summary of the supported criteria.

- Full Boolean support with AND, OR, and -
- Nested Boolean support with parenthesis, for example `(foo or bar) baz`
- Wildcard searches with *, for example, `process_name:*.exe`
- Force-phrase searches with double-quotes: `"foo\bar"` or `"foo bar"`

Searches are generally case-insensitive.

Query Syntax Details

Terms, phrases and operators

A term is a single keyword (without whitespace) that is searched in the Carbon Black process or binary data store, for example:

`foo`

Terms can be combined by logical operators and nested to form more complex queries, for example:

- and, AND, or whitespace: Boolean AND operator: `foo bar`, `foo and bar`
- or, OR: Boolean OR operator: `foo or bar`
- -: Boolean NOT operator: `-foo`
- nesting using parenthesis: `(foo or bar) baz`

Terms can be limited to a single field with `field:term`-style syntax, for example:

`process_name:svchost.exe`

Multiple terms are connected with AND if not otherwise specified. Terms without fields are expanded to search all default fields.

Because terms are whitespace delimited, use double-quotes or escape whitespaces when required, for example:

`filemod:"c:\program files\"` or `filemod:c:\program\ files\`

Terms can be combined to form phrases. A phrase is a set of terms separated by whitespace and enclosed in quotes. Whitespace between the terms of a phrase is not treated as a logical AND operator; rather a phrase is searched as a single keyword, for example: `"foo bar"`

Phrases can be combined and nested with other phrases and terms using logical operators, for example: `"foo bar" or baz`

Restrictions on Terms

Whitespace

Whitespace is the default delimiter. A query with whitespace would be parsed as multiple terms, for example:

Input: `c:\program files\windows`

Becomes: `c:\program` and `files\windows`

You can use a phrase query to avoid automatic parsing, for example:

Input: `"c:\program files\windows"`

Becomes: `"c:\program files\windows"`

Alternatively, whitespaces can be escaped using the backslash (\):

Input: `c:\program\ files\windows`

Output `c:\program files\windows`

Parenthesis

Parenthesis is used as a delimiter for nested queries. A query with parenthesis is parsed as a nested query, and if a proper nesting cannot be found, a syntax error is returned, for example:

Input: `c:\program files (x86)\windows`

Becomes: `c:\program` and `files` and `x86` and `\windows`

You can use a phrase query to avoid automatic nesting, for example:

Input: `"c:\program files (x86)\windows"`

Becomes: `"c:\program files (x86)\windows"`

Alternatively, whitespaces can be escaped using backslash (\) as the escape character, for example:

Input: `c:\program\ files\ \ (x86\)\windows`

Becomes: `c:\program files (x86)\windows`

Negative sign

The negative sign is used as logical NOT operator. Queries that begin with a negative sign are negated in the submitted query, for example:

Input: `-system.exe`

Becomes: `not system.exe`

You can use a phrase query to avoid automatic negation, for example:

Input: `"-system.exe"`

Becomes: `"-system.exe"`

Double Quotes

Double quotes are used as a delimiter for phrase queries. A query with double quotes must be escaped using backslash (\), for example:

cmdline: `"\"c:\program files \ (x86\)\google\update\googleupdate.exe\" /svc"`

Fields

This section contains a complete list of fields that are searchable in Carbon Black. Fields are valid in either process searches or binary searches. Some fields are valid in both. Any binary-related field used in the process search searches the executable file backing the process.

If no field is specified for a term, the search is executed on all default fields. Default fields are indicated by (def).

Table 22: Searchable Fields in Carbon Black

Field	Process Search	Binary Search	Field Type	Description
md5	x (def)	-	md5	MD5 of the process, the parent, a child process, a loaded module, or a written file.
domain	x (def)	-	domain	Network connection to this domain.
ipaddr	x	-	ipaddr	Network connection to or from this IP address.
modload	x (def)	-	path	Path of module loaded into this process.
filemod	x	-	path	Path of a file modified by this process.
regmod	x (def)	-	path	Path of a registry key modified by this process.
path	x (def)	-	path	Full path to the executable backing this process.
process_name	x (def)	-	keyword	Filename of the executable backing this process.
parent_name	x (def)	-	keyword	Filename of the parent process executable.
childproc_name	x (def)	-	keyword	Filename of the child process executables.
cmdline	x (def)	-	cmdline	Full command line for this process.
hostname	x (def)	-	keyword	Hostname of the computer on which the process was executed.
host_type	x (def)	-	keyword	Type of the computer: workstation, server, or domain controller.

Table 22: Searchable Fields in Carbon Black (continued)

Field	Process Search	Binary Search	Field Type	Description
group	x (def)	-	keyword	Sensor group this sensor was assigned to at the time of process execution.
username	x (def)	-	keyword	User context with which the process was executed.
process_md5	x (def)	-	md5	MD5 of the executable backing this process.
parent_md5	x (def)	-	md5	MD5 of the executable backing the parent process.
filewrite_md5	x (def)	-	md5	MD5 of a file written by this process.
childproc_md5	x (def)	-	md5	MD5 of the executable backing the created child processes.
modload_count	x	-	count	Total count of module loads by this process.
filemod_count	x	-	count	Total count of file modifications by this process.
regmod_count	x	-	count	Total count of registry modifications by this process.
netconn_count	x	-	count	Total count of network connections by this process.
childproc_count	x	-	count	Total count of child processes created by this process.
start	x	-	datetime	Start time of this process in the computer's local time.
last_update	x	-	datetime	Last activity in this process in the computer's local time.
last_server_update	x	-	datetime	Last activity in this process in the server's local time.
process_id	x	-	long	The internal Carbon Black process guid for the process.
parent_id	x	-	long	The internal Carbon Black process guid for the parent process.
sensor_id	x	-	long	The internal Carbon Black sensor guid of the computer on which this process was executed.

Table 22: Searchable Fields in Carbon Black (continued)

Field	Process Search	Binary Search	Field Type	Description
watchlist_<id>	x	x	datetime	The time that this process or binary matched the watchlist query with <id>.
os_type	x	x	keyword	Type of the operating system: Windows, OSX or Linux.
md5	-	x	md5	The binary's MD5 hash value.
orig_mod_len	x	x	count	Size in bytes of the binary at time of collection.
copied_mod_len	x	x	count	Number of bytes collected.
is_executable_image	x	x	bool	True if the binary is an EXE (versus DLL or SYS)
is_64bit	x	x	bool	True if architecture is x64.
observed_filename	x	x (def)	path	Full path of the binary at the time of collection.
digsig_publisher	x	x (def)	text	If digitally signed, the publisher.
digsig_issuer	x	x (def)	text	If digitally signed, the issuer.
digsig_subject	x	x (def)	text	If digitally signed, the subject.
digsig_prog_name	x	x (def)	text	If digitally signed, the program name.
digsig_result	x	x (def)	sign	If digitally signed, the result.
digsig_sign_time	x	x	datetime	If digitally signed, the time of signing.
product_version	x	x (def)	text	Product version string from FILEVERSIONINFO
file_version	x	x (def)	text	File version string from FILEVERSIONINFO
product_name	x	x (def)	text	Product name string from FILEVERSIONINFO
company_name	x	x (def)	text	Company name string from FILEVERSIONINFO
internal_name	x	x (def)	text	Internal name string from FILEVERSIONINFO
original_filename	x	x (def)	text	Original name string from FILEVERSIONINFO

Table 22: Searchable Fields in Carbon Black (continued)

Field	Process Search	Binary Search	Field Type	Description
file_desc	x	x (def)	text	File description string from FILEVERSIONINFO
product_desc	x	x (def)	text	Product description string from FILEVERSIONINFO
comments	-	x (def)	text	Comment string from FILEVERSIONINFO
legal_copyright	x	x (def)	text	Legal copyright string from FILEVERSIONINFO
legal_trademark	x	x (def)	text	Legal trademark string from FILEVERSIONINFO
private_build	x	x (def)	text	Private build string from FILEVERSIONINFO
special_build	x	x (def)	text	Special build string from FILEVERSIONINFO
server_added_timestamp	-	x	datetime	The time this binary was first seen by the server.
crossproc_count	x	x	count	Total number of cross process events by this process.
crossproc_type	x	x	remote_thread process_open	A remote thread is open, or a process handle is open
crossproc_md5	-	x	md5	MD5 hash value of the process with which an actor process had a cross-process event.
crossproc_name	x	x	text	Name of the process with which an actor process had a cross-process event.
tampered	x	x	bool	Values are True or False - indicates if the event has been tampered with.

Datatypes

domain

Domains are split into labels. Separator characters (.) are maintained to enable position-dependent searches. A search with leading or trailing .'s is position-dependent. Searches with inner .'s are phrase searches. Searches without .'s will match any domain with that label anywhere in the domain name. The following table provides examples of domain searches.

Table 23: Domain Datatype

Search	foo.com	foo.com.au
domain:com	match	match
domain:.com	match	no match
domain:.com.	no match	match
domain:com.	no match	no match
domain:foo.	match	match
domain:foo.com	match	no match

ipaddr

IP addresses are searched with CIDR notation:

```
(ip) / (netmask)
```

If the netmask is omitted, it is presumed to be 32, for example:

```
ipaddr:192.168.0.0/16 or ipaddr:10.0.1.1
```

text

Text fields are tokenized on whitespace and punctuation. Searches are case-insensitive.

The string from the `product_name` field, for example:

```
Microsoft Visual Studio2010
```

will be split into the terms `microsoft`, `visual`, `studio` and `2010`.

Searches for any one of these strings will match on the binary. Phrase queries for any two consecutive terms will also match on the binary, for example:

```
product_name: "visual studio"
```

count

An integer value. If it exists, values from 0 to `MAXINT`. Supports two types of search syntaxes:

- `X`: Matches all fields with precisely `X`, for example, `modload_count:34` for processes with exactly 34 modloads.
- `[X TO Y]`: Matches all fields with counts $\geq X$ and $\leq Y$, for example, `modload_count:[1 TO 10]` for processes with 1 to 10 modloads.

In both cases, either `X` or `Y` can be replaced the wildcard `*`. for example, `netconn_count:*` for any process where the `netconn_count` field exists. `netconn_count:[10 TO *]` for any process with more than 10 network connections.

datetime

Datetime fields have five types of search syntaxes:

- `YYYY-MM-DD` matches all entries on this day, for example, `start:2013-12-01` for all processes started on Dec 1, 2013.
- `YYYY-MM-DDThh:mm:ss` matches all entries within the next 24 hours from this date and time, for example, `start:2013-12-01T22:15:00` for all processes started between Dec 1, 2013 at 22:15:00 to Dec 2, 2013 at 22:14:59.
- `[YYYY-MM-DD TO YYYY-MM-DD]` matches all entries between, for example, `start:[2013-12-01 TO 2013-12-31]` for all processes started in Dec 2013.
- `[YYYY-MM-DDThh:mm:ss TO YYYY-MM-DDThh:mm:ss]` matches all entries between, for example, `start:[2013-12-01T22:15:00 TO 2013-12-01:23:14:59]` for all processes started in Dec 1, 2013 within the given time frame.
- `-Xh` relative time calculations matches all entries with a time between `NOW-10h` and `NOW`. Support units supported are `h`: hours, `m`: minutes, `s`: seconds as observed on the host, for example, `start:-24h` for all processes started in the last 24 hours.

As with counts, `YYYYMMDD` can be replaced the wildcard `*`. for example, `start:[2013-01-01 TO *]` for any process started after 1 Jan 2013.

keyword

Keywords are `text` fields with no tokenization. The term that is searched for must exactly match the value in the field, for example, `process_name:svchost.exe`. Queries containing wildcards can be submitted with keyword queries, for example, `process_name:*.exe`

md5

MD5 fields are keyword fields with an md5 hash value. The term searched for must exactly match the value in the field, for example, `process_md5:6d7c8a951af6ad6835c029b3cb88d333`

path

Path fields are special text fields. They are tokenized according to path hierarchy, for example, `path:c:\windows`.

For a given path, all subpaths are tokenized. For example:

```
c:\windows\system32\boot\winload.exe
```

is tokenized as:

```
c:\windows\system32\boot\winload.exe
```

```
\windows\system32\boot\winload.exe
```

```
system32\boot\winload.exe
```

```
boot\winload.exe
```

```
winload.exe
```

For queries involving path segments that are not tokenized, wildcard queries can be submitted, for example, `path:system*`, for any path that has `system` as sub-path in it.

bool

Boolean fields have only two possible values, the string `true` or `false`. Searches are case-insensitive.

sign

Signature fields can be one of the eight possible values: `Signed`, `Unsigned`, `Bad Signature`, `Invalid Signature`, `Expired`, `Invalid Chain`, `Untrusted Root`, `Explicit Distrust`. Values with whitespace must be enclosed in quotes, for example, `digsig_result:Signed` or `digsig_result:"Invalid Chain"`

cmdline

Command line strings that contain parenthesis or double quotes must be escaped using a backslash. If the string also contains whitespaces, enclose it in double quotes or use escape for the whitespaces, for example: `cmdline:"\"c:\program files\x86\google\update\googleupdate.exe\" /svc"` or `cmdline:\"c:\program\ files\ \x86\google\update\googleupdate.exe\" /svc`

Example Searches

Process Search Examples

Table 24: Process Search Query String Examples

Example Query Strings	Result
domain:www.carbonblack.com	Returns all processes with network connections to or from domains matching the given FQDN.
domain:.com	Returns all processes with network connections to or from domains matching *.com
domain:.com.	Returns all processes with network connections to or from domains matching the form *.com.*
domain:www.	Returns all processes with network connections to or from domains matching the form www.*
domain:microsoft	Returns all processes with network connections to or from domains matching *.microsoft OR *.microsoft.* OR microsoft.*
ipaddr:127.0.0.1	Returns all processes with network connections to or from IP address 127.0.0.1
ipaddr:192.168.1.0/24	Returns all processes with network connections to or from IP addresses in the network subnet 192.168.1.0/24
modload:kernel32.dll	Returns all processes that loaded a module kernel32.dll (accepts path hierarchies).
modload:c:\windows\system32\sxs.dll	Returns all processes that loaded a module matching path and file sxs.dll (accepts path hierarchies).
path:c:\windows\system32\notepad.exe	Also returns all processes with the matching path (accepts path hierarchies).
regmod:\registry\machine\system\controlset001\control\deviceclasses*	Returns all processes that modified a registry entry with the matching path (accepts path hierarchies).
path:excel.exe	Returns all processes with the matching path (accepts path hierarchies).
cmdline:backup	Returns all processes with matching command line arguments.
hostname:win-5ikqdnf9go1	Returns all processes executed on the host with matching hostname.
group:"default group"	Returns all processes executed on hosts with matching group name (use of quotes are required when submitting two-word group names).
host_type:workstation	Returns all processes executed on hosts with matching type (use of quotes are required when submitting two-word host types).

Table 24: Process Search Query String Examples (continued)

Example Query Strings	Result
username:system	Returns all processes executed with the matching user context.
process_name:java.exe	Returns all processes with matching names.
parent_name:explorer.exe	Returns all processes executed by a parent process with matching names.
childproc_name:cmd.exe	Returns all processes that executed a child process with matching names.
md5:5a18f00ab9330ac7539675f3f326cf11	Returns all processes, modified files, or loaded modules with matching MD5 hash values.
process_md5:5a18f00ab9330ac7539675f3f326cf11	Returns all processes with matching MD5 hash values.
parent_md5:5a18f00ab9330ac7539675f3f326cf11	Returns all processes that have a parent process with the given MD5 hash value.
filewrite_md5:5a18f00ab9330ac7539675f3f326cf11	Returns all processes that modified a file or module with matching MD5 hash values.
childproc_md5:5a18f00ab9330ac7539675f3f326cf11	Returns all processes that executed a child process with matching MD5 hash values.
<type>_count:*	Returns all processes that have xxx_count field > 0, where type is one of modload, filemod, regmod, netconn, or childproc.
<type>_count:10	Returns all processes that have xxx_count field = 10, where type is one of modload, filemod, regmod, netconn, or childproc.
<type>_count:[10 TO 20]	Returns all processes that have xxx_count field >= 10 and <= 20, where type is one of modload, filemod, regmod, netconn, or childproc.
<type>_count:[10 TO *]	Returns all processes that have xxx_count field >= 10, where type is one of modload, filemod, regmod, netconn, or childproc.
<type>_count:[* TO 10]	Returns all processes that have xxx_count field < 10, where type is one of modload, filemod, regmod, netconn, or childproc.
start:2011-12-31	Returns all processes with a start date of 2011-12-31 (as observed on the host).
start:[* TO 2011-12-31]	Returns all processes with a start date earlier than or equal to 2011-12-31 (as observed on the host).
start:[* TO 2011-12-31T22:15:00]	Returns all processes with a start date earlier than or equal to 2011-12-31 at 22:15:00 (as observed on the host).

Table 24: Process Search Query String Examples (continued)

Example Query Strings	Result
start:[2011-12-31 TO *]	Returns all processes with a start date later than or equal to 2011-12-31 (as observed on the host).
start:[2011-12-31T09:45:00 TO *]	Returns all processes with a start date later than or equal to 2011-12-31 at 09:45:00 (as observed on the host).
start:*	Returns processes with any start date (as observed on the host).
start:[* TO *]	Returns processes with any start date (as observed on the host).
start:-10h	Returns all processes with a start time between NOW-10h and NOW. Units supported are, h: hours, m: minutes, s: seconds (as observed on the host).
last_update:2011-12-31	Returns all processes last updated on date 2011-12-31 (as observed on the host).
last_update:[* TO 2011-12-31]	Returns all processes last updated on a date earlier than or equal to 2011-12-31 (as observed on the host).
last_update:[* TO 2011-12-31T22:15:00]	Returns all processes last updated on a date earlier than or equal to 2011-12-31 at 22:15:00 (as observed on the host).
last_update:[2011-12-31 TO *]	Returns all processes last updated on a date later than or equal to 2011-12-31 (as observed on the host).
last_server_update:[2011-12-31T09:45:00 TO *]	Returns all processes last updated on a date later than or equal to 2011-12-31 at 09:45:00 (as observed at the server).
last_server_update:*	Returns processes with any update date (as observed on the server).
last_server_update:[* TO *]	Returns processes with any update date (as observed on the server) within the range provided.
last_server_update:-10h	Returns all processes last updated between NOW-10h and NOW. Units supported are h: hours, m: minutes, s: seconds (as observed on the server).
process_id:<guid>	Returns the process with the given process id, where <guid> is a signed 64-bit integer.
parent_id:<guid>	Returns the process with the given parent process id, where <guid> is a signed 64-bit integer.
sensor_id:<guid>	Returns processes executed on host with given sensor id, where <guid> is an unsigned 64-bit integer.

Binary Search Examples

Table 25: Binary Search Query String Examples

Example Query Strings	Result
md5:5a18f00ab9330ac7539675f326cf11	Returns all binaries with matching MD5 hash values.
digsig_publisher:Oracle	Returns all binaries with a digital signature publisher field with a matching name.
digsig_issues:VeriSign	Returns all binaries with a digital signature issuer field with a matching name.
digsig_subject:Oracle	Returns all binaries with a digital signature subject field with a matching name.
digsig_prog_name:Java	Returns all binaries with a digital signature program name field with a matching name.
digsig_result:"<status>"	Returns all binaries with a digital signature status of <status>.
digsig_sign_time:2011-12-31	Returns all binaries with a digital signature date of 2011-12-31.
digsig_sign_time:[* TO 2011-12-31]	Returns all binaries with a digital signature date earlier than or equal to 2011-12-31.
digsig_sign_time:[2011-12-31 TO *]	Returns all binaries with a digital signature date later than or equal to 2011-12-31.
digsig_sign_time:*	Returns binaries with any digital signature date.
digsig_sign_time:[* TO *]	Returns binaries with any digital signature date within the range provided.
digsig_sign_time:-10h	Returns all binaries with a start time between NOW-10h and NOW. Units supported are h: hours, m: minutes, s: seconds.
<type>_version:7.0.170.2	Returns all binaries with matching version, where <type> is product or file.
product_name:Java	Returns all binaries with matching product name.
company_name:Oracle	Returns all binaries with matching company name.
internal_name:java	Returns all binaries with matching internal name.
original_filename:mtxoci.dll	Returns all binaries with matching filename.
observed_filename:c:\windows\system32\mtxoci.dll	Returns all binaries that have been observed to run on or were loaded with the given path.
<type>_mod_len:[* TO 10]	Returns all binaries that have <type>_mod_len (module length in bytes) field < 4096, where type is original or copied.

Table 25: Binary Search Query String Examples (continued)

Example Query Strings	Result
<type>_desc:"database support"	Returns all binaries that have <type>_desc field with matching text, where type is file or product.
legal_<type>:Microsoft	Returns all binaries with matching legal_<type> field text, where type is trademark or copyright.
<type>_build:"Public version"	Returns all binaries with matching <type>_build field text, where type is special or private.
is_executable_image:True or False	Boolean search (case insensitive) returning all binaries that are executable or not executable.
is_64bit_:True or False	Boolean search (case insensitive) returning all binaries that are 64-bit or not 64-bit.

Threat Intelligence (Alliance) Search Examples

Any document matching a threat intelligence feed is tagged with an alliance_score_<feed> field, where the value is a score from 1 to 100. <feed> is the “short name” of the threat intelligence feed, such as “nvd”, “isight”, or “virustotal.” For any threat intelligence feed, you can click the **View Hits** button to discover the feed’s short name.

Table 26: Threat Intelligence Search Examples

Example Query Strings	Result
alliance_score_<feed>:*	Returns all binaries that have <feed> score > 0.
alliance_score_<feed>:10	Returns all binaries that have <feed> score = 10.
alliance_score_<feed>:[10 TO 20]	Returns all binaries that have <feed> score >= 10 and <= 20.
alliance_score_<feed>:[10 TO *]	Returns all binaries that have <feed> score >= 10.
alliance_score_<feed>:[* TO 10]	Returns all binaries that have <feed> score < 10.

Chapter 10

Threat Intelligence Feeds

This chapter describes Threat Intelligence Feeds that may be enabled on a Carbon Black server to enhance the verification, detection, visibility and analysis of threats on your endpoints.

Sections

Topic	Page
Overview	148
The Threat Intelligence Feeds Page	149
Checking for New Alliance Feeds	151
Syncing Alliance Feeds	151
Feeds and Data Sharing Settings	152
Enabling, Disabling, and Configuring a Feed	155
Creating and Adding New Feeds	157

Overview

Threat Intelligence Feeds are streams of reports about Indicators of Compromise (IOCs) found in the wild by a variety of services and products. One or more feeds may be integrated into the Carbon Black server and console to enhance the verification, detection, visibility and analysis of threats on your endpoints.

The source of a feed may be a third-party Carbon Black Alliance partner or it may be from the information and analysis collected by the Bit9 Software Reputation Service, Bit9 Platform threat detection tools and shared data collected from Carbon Black and Bit9 customer enterprises. You can even create and add a new feed if you choose. Some feeds do not require data collection from your server while others require that you share information from your enterprise back to the feed provider to improve community intelligence data.

Available feeds appear on the Threat Intelligence Feed page. You can enable or disable any feed you see on that page. The Carbon Black server supports the following types of IOCs:

- Binary MD5s
- IPv4 addresses
- DNS names
- Query-based feeds using the Carbon Black process/binary search syntax to define an IOC

When a feed is enabled and IOCs from it are received, the following information and capabilities are added in Carbon Black:

- **Feed Results Added to Sensor-Reported Process and Binary Records** – If an IOC from a feed report matches processes or binaries reported by sensors on your endpoints are added to the records for those processes or binaries in Carbon Black. You can search and filter for processes or binaries using the existence or score of a feed report, for example creating a table of all processes whose National Vulnerability Database score is greater than 4.
- **Feed-based Watchlists** – You can create a Carbon Black Watchlist that tags a process or binary found on one of your endpoints when the score from a specified feed matches a specified score or falls within a score range.
- **Feed-based Alerts** – You can configure a console and/or email alert to be sent any time a process or binary found on one of your endpoints is the subject of a report from a specified feed.
- **Links to Feed Sources** – You can link back to the source of a feed for more information, which can range from a general description of the feed to specific details about an IOC reported by that feed.

Note

You may also integrate the Carbon Black server with local or cloud-based devices that provide threat intelligence. See [Appendix C, “Network Integrations for Feeds,”](#) for a list of supported integrations and pointers to documents about these integrations on the Carbon Black customer portal.

The Threat Intelligence Feeds Page

On the Threat Intelligence Feeds page, you can:

- View the available feeds and get more information about them
- Enable or disable feeds
- Configure alerts and logging for feeds
- Change the rating used to calculate the severity assigned to IOCs from a feed
- Sync one or all feeds
- Check for new feeds
- Add a new feed
- Delete user-defined feeds

Note

Feeds that Carbon Black makes available from Bit9 + Carbon Black sources and third-party partners are **Carbon Black Alliance** feeds. They may be enabled and in some cases disabled but may not be deleted from the page.












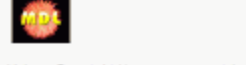

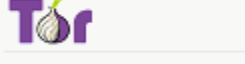
To view the Threat Intelligence Feeds page:

- On the console menu, choose **Detect > Threat Intelligence**. The Threat Intelligence Feeds page appears.

The following page shows an example of the Threat Intelligence Feeds page and the feeds that might appear on it. Note that feeds may be added or removed, so what appears here should not be taken to indicate that all pictured feeds are available.

Threat Intelligence Feeds

+ Add New Feed

 <p>VirusTotal harnesses the power of over forty-five Anti-Virus vendors to identify suspicious binaries.</p> <p>It is necessary to share MD5s of observed binaries with the Carbon Black Alliance to use this feed. ...</p> <p>More Info</p> <p>★★★★☆</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>	 <p>The Bit9 Software Reputation Service (SRS) Trust feed provides a level of confidence that software is good.</p> <p>It is necessary to share MD5s of observed binaries with the Carbon Black Alliance to use this feed. ...</p> <p>More Info</p> <p>★★★★☆</p> <p><input type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>	 <p>The Bit9 Software Reputation Service (SRS) Threat feed provides an assessment of the risk associated with software.</p> <p>It is necessary to share MD5s of observed binaries with the Carbon Black Alliance to use this feed. ...</p> <p>More Info</p> <p>★★★★☆</p> <p><input type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>	 <p>iSIGHT Partners provides a cyber intelligence feed.</p> <p>There are no requirements to share any data with Carbon Black to receive this feed. The underlying IOC data is provided by iSIGHT Partners ...</p> <p>More Info</p> <p>★★★★☆</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>
 <p>NVD is the U.S. government repository of standards based vulnerability management data. This feed will flag all executed applications vulnerable to one or more CVEs.</p> <p>There are no requirements to share any d...</p> <p>More Info</p> <p>★★★★☆</p> <p><input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>	 <p>abuse.ch tracks C&C servers for Zeus, SpyEye and Palevo malware. This feed combines the three domain names blocklists.</p> <p>There are no requirements to share any data to receive this feed. ...</p> <p>More Info</p> <p>★★★★☆</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>	 <p>This feed is a list of high-confidence threat indicators, updated periodically. Generally, hits on this feed should be suitable for generating alerts.</p> <p>There are no requirements to share any data to receive this feed. ...</p> <p>More Info</p> <p>★★★★☆</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>	 <p>This feed is a list of beta queries that have not been fully tested and validated. Queries in this feed may generate many false positives, but should also be useful in identifying malicious activity. As these queries are beta, this feed may generate a large volume of hits and it is not...</p> <p>More Info</p> <p>★★★★☆</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>
 <p>This feed is a list of queries designed to identify suspicious activities on endpoints. Hits on this feed may or may not be indicative of malicious activity, but are generally more suspicious in nature. As this feed may generate a large volume of hits, it is not recommended to be used for alert...</p> <p>More Info</p> <p>★★★★☆</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>	 <p>This feed is a list of queries designed to give further visibility into endpoint behavior. Hits on this feed may or may not be indicative of malicious activity. As this feed may generate a large volume of hits, it is not recommended to be used for alert generation.</p> <p>More Info</p> <p>★★★★☆</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>	 <p>This feed reports on actions potentially indicative of sensor tampering. Alerts indicate changes to the Carbon Black configuration, attempted changes to the running sensor process or unloading Cb drivers.</p> <p>More Info</p> <p>★★★★☆</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>	 <p>Malware Domain List is a non-commercial community project to track domains used by malware. This feed contains the most recent 100 days of entries.</p> <p>There are no requirements to share any data to receive this feed. ...</p> <p>More Info</p> <p>★★★★☆</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>
 <p>Threat intelligence data provided by ThreatConnect to the Carbon Black Community.</p> <p>There are no requirements to share any data to receive this feed.</p> <p>More Info</p> <p>★★★★☆</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>	 <p>This feed is a list of Tor Node IP addresses, updated every 30 minutes.</p> <p>There are no requirements to share any data to receive this feed.</p> <p>More Info</p> <p>★★★★☆</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Email Me On Hit</p> <p>Notifications</p> <p>Process Matches Binary Matches Actions</p>		

Each available feed is represented by a panel on this page. There are also controls on the page that check for new feeds available from the Carbon Black Alliance, synchronize all feeds on the page, and add user-defined feeds.

The Bit9 Tamper Protection feed, which alerts on endpoint activity that is indicative of tampering with CB sensor activity, is enabled by default. If you opt in to alliance sharing (see [“Feeds and Data Sharing Settings”](#) on page 152), the VirusTotal feed is also enabled by default. You must enable other feeds you want to use. See [“Enabling, Disabling, and Configuring a Feed”](#) on page 155 for more on enabling and configuring a feed.

See [“Creating and Adding New Feeds”](#) on page 157 for information on adding user-defined feeds.

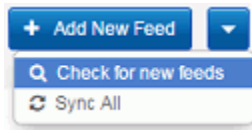
Checking for New Alliance Feeds

Carbon Black works with a variety of partners to provide threat intelligence feeds for the Carbon Black server. New partners and feeds may be added after you install the server at your site. So that you can take advantage of the latest available feeds, the Threat Intelligence Feeds page includes the ability to check for new feeds. You may want to do this before deciding which feeds to enable, and also check for new feeds periodically.

This command also removes feeds if the feed source no longer provides them, although any existing reports and tagged processes and binaries will still identify the feed.

To check for new Alliance feeds:

- On the Threat Intelligence Feeds page, choose **Check for new feeds** on the action (down-arrow) menu in the top right corner of the page. If new feeds are available, they are added to the page.

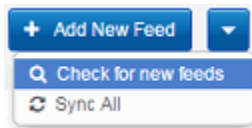


Syncing Alliance Feeds

Alliance feeds are updated periodically by the feed sources. If you want to make certain that all feeds are up-to-date with the latest information from their source, you can use the Sync All command.

To sync all Alliance feeds on the page:

- On the Threat Intelligence Feeds page, choose **Sync All** on the action (down-arrow) menu in the top right corner of the page.



Note

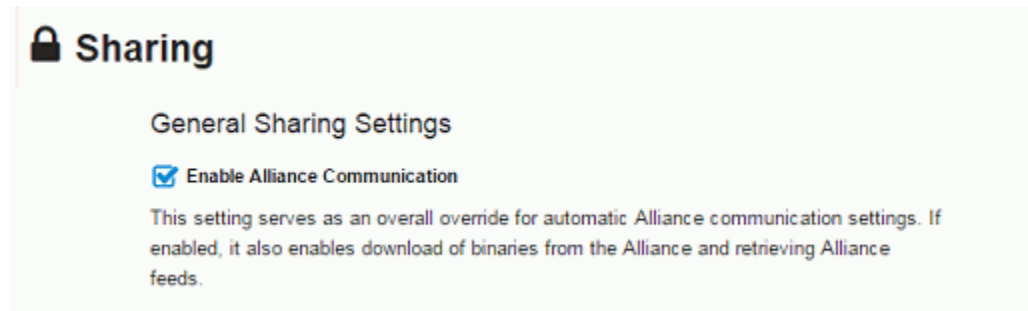
You can sync feeds individually if you choose rather than all at one time. Sync commands for individual feeds on on the Action menu in the feed panel. See [Table 27](#) on page 156 for a description of these options.

Feeds and Data Sharing Settings

Most Alliance feed partners provide a list of all of the IOCs they track. Other than the Bit9 Tamper Protection feed, all feeds require that you enable communication on the Sharing Settings page. Some feeds require that you also enable data sharing.

To enable communication with Carbon Black Alliance feed partners:

1. On the console menu, choose **Administration > Sharing Settings**. The Sharing page appears.



2. On the Sharing page, under General Sharing Settings, make sure the **Enable Alliance Communication** box is checked.

If Enable Alliance Communication is enabled for the first time (or after being disabled), a full Sync with the available feeds is done in the background.

Some feeds, for example VirusTotal or most Bit9 feeds, only include reports on MD5s that are observed in your enterprise. For these, you must Enable Alliance Communication, but you must also enable feed-specific sharing. If you enable sharing for these feeds, Carbon Black pushes MD5s that are observed by your sensors and binaries originating from your enterprise to the servers for each of the feeds you enable. These are compared to data that Bit9 and other third parties have on those binaries. If there is a corresponding report or record, the feed is updated to include that information.

Important

Be sure to read and understand the descriptions of the options you choose on the Sharing page. These settings can send MD5 data about all of the binaries discovered on your endpoints, or even the binaries themselves, to Carbon Black or a third-party feed provider. Make sure you are comfortable with this and that this data sharing is in compliance with your organization's policies.

To enable data sharing with Carbon Black Alliance feed partners:

1. On the console menu, choose **Administration > Sharing Settings**.
2. Scroll to the Endpoint Activity Sharing section at the bottom of the Sharing page

Endpoint Activity Sharing

Some threat intelligence resources require your server to send endpoint activity to Bit9 or our Alliance Partners. The threat intelligence databases may be too large or too dynamic to be hosted locally, analysis may be computationally intense or analysis may be dependent on external data sources. The activity sent varies with each dataset and terms of use with each partner. Complete details are available below.

	Bit9 & Alliance Partners	VirusTotal
Binary Hashes & Metadata	DISABLED	DISABLED
Complete Binaries	DISABLED	DISABLED

3. In the Binary Hashes & Metadata row for each of the feeds you want to enable, if the setting is **Disabled**, click on that setting. This opens the *Share binary hashes* page. This page describes the data that will be shared with the source and provides a privacy statement for you to review. Please review all of the sharing and privacy information carefully before making sharing choices.
4. If you are willing to share the data as described, you have two options:
 - a. Click **Enable** to share data from endpoints in all Sensor Groups.
 - b. Click **Partial** to share data from endpoints in some Sensor Groups, and use the arrow between the SHARE FROM and DO NOT SHARE FROM windows to choose which groups you will allow to share data.

Share binary hashes with Bit9 ×

Summary
Use Bit9's Software Reputation Service and confirm trust level by hash for all executed binaries. By sharing hashes with Bit9, hashes can be checked with Bit9's catalog of trusted files.

Data Shared

For every binary executed in the groups below, the following information is sent to Bit9 if you so elect:

- Filename
- File md5 hash
- File metadata (Company Name, Product Name, etc)
- Digital signature information
- File writer name and hash

```
{
  'md5': 'a3d53b9706919538f4a40c9f8d01a3e1',
  'file_description': 'Windows Update client proxy stub',
  'company_name': 'Microsoft Corporation',
  'product_name': 'Microsoft® Windows® Operating System',
  'file_version': '7.8.9200.16384 (win8_rtm.120725-1247)',
  'comments': '',
  'legal_copyright': '© Microsoft Corporation. All right',
  'legal_trademark': '',
  'internal_name': 'wups.dll',
  'original_filename': 'wups.dll',
  'product_description': '',
  'product_version': '7.8.9200.16384'.
}
```

Privacy

Data shared with Bit9 is:

- securely transmitted and stored in our secure cloud infrastructure
- never publicly shared unless elected, anonymized, and aggregated

A checked box designates you are "opting in" and thereby electing to share this information with Bit9 and its threat intelligence "Alliance" partners in the manner described. All information is anonymized to the extent reasonably practicable before being shared with Alliance partners. The applicable terms and conditions are set forth in and subject to your Bit9 License Agreement. DATA COLLECTION: In the event that You opt in through the Software, then, notwithstanding anything to the contrary set forth herein, Bit9 may collect and use (a) but not distribute externally, technical information about Your devices. files. networks. systems. software.

ENABLE (Share from ALL Groups)
 DISABLE (Do Not Share from ANY Groups)
 PARTIAL (Share from SOME Groups)

SHARE FROM

DO NOT SHARE FROM

Default Group
Test123

Close Share

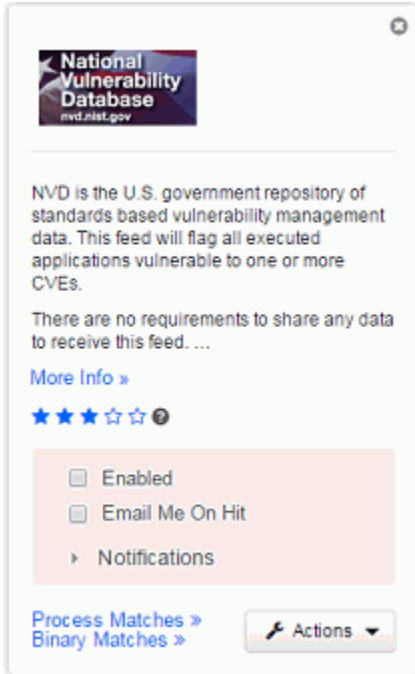
5. Click the **Share** button when you have chosen the sharing configuration for this feed.
6. Repeat for any other feed you want to enable on the Endpoint Activity Sharing panel.

Note

If you disable the main Enable Alliance Communication setting, you also lose access to any feeds you configured in the Endpoint Activity Sharing interface.

Enabling, Disabling, and Configuring a Feed

Each feed available on a Carbon Black server is represented by a panel on the Threat Intelligence Feeds page. The panel provides information about the feed and allows you to enable and configure it.



To enable a Threat Intelligence Feed:

1. On the console menu, choose **Detect > Threat Intelligence**. The Threat Intelligence Feeds page appears.
2. Choose a feed that you would like to enable, and on that panel, check the **Enabled** box to enable the feed.
3. Set any of the configuration options you would like to change. See [Table 27](#) for details.

To disable a Threat Intelligence Feed:

1. On the console menu, choose **Detect > Threat Intelligence**. The Threat Intelligence Feeds page appears.
2. Choose the feed that you would like to disable, and on that panel, *uncheck* the **Enabled** box to disable the feed.

If you disable a feed, its reports remain on the server and any data coming in will be tagged against locally existing IOCs it reported. However, new reports from these feeds about IOCs will not be downloaded for scanning, and for feeds that require data to be sent to them, new binary MD5s from your sensors will not be sent.

Table 27: Configuration and Action Options for a Threat Intelligence Feed

Field/Menu	Description
More info	This link goes to a URL at the feed provider. It may provide technical information about the feed or general information about the provider and its products.
★ ★ ★ ☆ ☆ (Rating)	By default, the field showing five stars indicates the rating of this field by the community of Carbon Black users. The default for all ratings is three (filled) stars. You can click on a star to modify the rating of this feed on your server. The rating affects the severity assigned to alerts coming from this feed, which in turn can affect order of alerts if sorted by severity.
Enabled	If this box is checked, the feed is enabled if available. If it is not checked, the feed is not enabled. Note: Most feeds also require that Enable Alliance Communication be enabled on the Sharing Settings page. In addition, feeds that upload data from your server require that you opt into hash sharing with that specific feed. See “Feeds and Data Sharing Settings” on page 152.
Email Me on Hit	If this box is checked, IOCs from this feed that reference a process or binary recorded on this Carbon Black server cause an email alert to be sent to the logged in console user. See “Enabling Email Alerts” on page 189 for more on email alerts.
Notifications menu	This menu provides additional notification options: <ul style="list-style-type: none"> • Create Alert – If this box is checked, IOCs from this feed that reference a process or binary recorded on this Carbon Black server cause a console alert. See “Enabling Console Alerts” on page 176 for more on email alerts. • Log to Syslog – If this box is checked, IOCs from this feed that reference a process or binary recorded on this Carbon Black server are included in Syslog output from this Carbon Black server. See the <i>Syslog User Guide</i> and related documents on the Carbon Black customer site for more on how Carbon Black events can be accessed via Syslog.
Process Matches	Clicking this link opens the Process Search page with the results of a search that shows each process that matches IOCs from this feed. See Chapter 7, “Process Search and Analysis,” for information on process searches.
Binary Matches	Clicking this link opens the Binary Search page with the results of a search that shows each binary that matches IOCs from this feed. See Chapter 8, “Binary Search and Analysis,” for information on binary searches.
Actions menu	The Action menu includes the following commands: <ul style="list-style-type: none"> • Create Watchlist – Create a Watchlist, which is a saved search whose results will be processes or binaries matching IOCs reported by this feed. • Incremental Sync – This option adds report data from this feed that has been observed since the previous synchronization. • Full Sync – This option rewrites all of the report data from this feed.

Creating and Adding New Feeds

You can create and add new Threat Intelligence Feeds to a Carbon Black server. A feed can be created in any language that allows for building JSON, or even built by hand. One way to build a feed is to use the Carbon Black Feeds API (CBFAPI), which is found on github at:

<https://github.com/carbonblack/cbfeeds>

The CBFAPI is a collection of documentation, example scripts, and a helper library to help create and validate Carbon Black feeds.

Regardless of how a feed is created, the feed file itself must match the feed structure, or schema, defined in the "Feed Structure" section of the Carbon Black Feeds API documentation referenced above.

There are several options for the amount of specification you provide when adding a new feed to a Carbon Black server. The minimum requirement is that you provide a URL to the feed.

To add a new Threat Intelligence Feed to the Carbon Black server:

1. Confirm that the feed you have created follows the Feed Structure instructions in the Carbon Black Feeds API documentation on github.
2. On the console menu, choose **Detect > Threat Intelligence**.
3. On the Threat Intelligence Feeds page, click the **Add New Feeds** button in the upper right. The Edit Alliance Feed dialog appears. The **Add from URL** tab is the default tab on this dialog.
4. Choose either Add from URL or Add Manually, and provide the information for the feed as described in Table 28. If you are entering authentication information, click the **Show Feed Server Authentication Options** link.
5. When you have finished entering the settings for this feed, click the **Save** button at the bottom of the dialog. If the settings you entered provide access to a feed server, the new feed appears on the Threat Intelligence Feeds page. Error messages will indicate failure to add the feed, for example, if the URL does not point to a feed server.

Table 28: Settings for New Feeds

Field	Add from URL	Add Manually	Description
Feed URL	Required	Required	The URL for the feed itself that will be providing IOC reports
Use Proxy	Optional	Optional	Check this box to use a proxy for the Feed URL. The configuration for this proxy is entered in the cb.conf file, which is documented on the Carbon Black customer portal.
Validate Server Cert	Optional	Optional	Check this box to require a validation check on the feed server's certificate.
Provider URL	N/A	Required	The URL to the page that will open when the user clicks More Info on the feed panel.

Table 28: Settings for New Feeds (continued)

Field	Add from URL	Add Manually	Description
Summary	N/A	Required	The text that will appear in the panel to describe this feed.
Server Authentication Options	Optional	Optional	<p>If the server providing the feed requires authentication, click the Show Server Authentication Options link and provide the following authentication information:</p> <ul style="list-style-type: none"> • Username • Password • Private Cert • Public Key

Chapter 11

Creating and Using Investigations

This chapter describes how to work with investigations. Investigations provide a way to group data for reporting, compliance, or retention purposes.

Sections

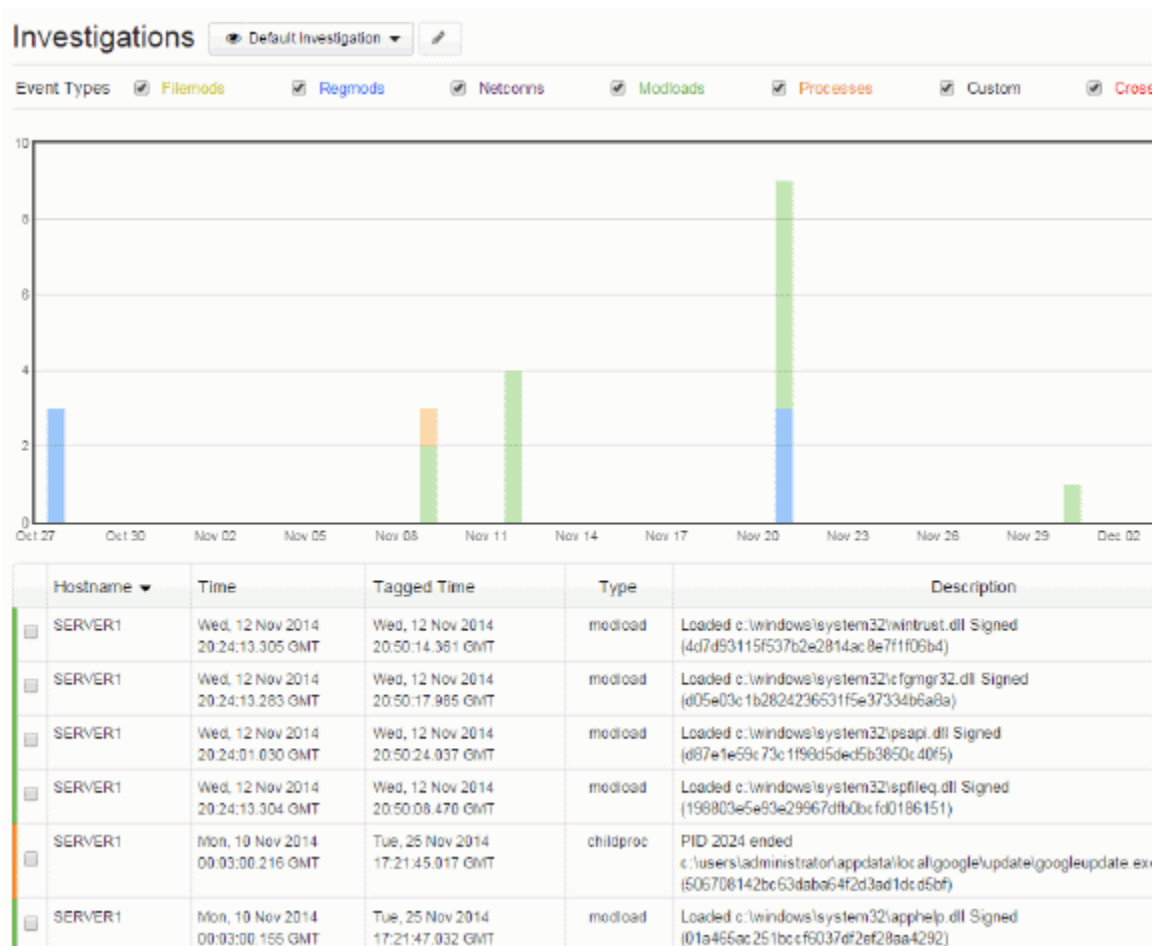
Topic	Page
Overview	160
Creating Investigations	162
Adding Events to Investigations	163
Removing Events from Investigations	164
Adding Custom Events to Investigations	164
Deleting Investigations	165

Overview

Investigations are collections of process events that share a common focus. Investigations can include details and notes, and provide a way to group data for reporting, compliance, or retention purposes. Investigations are not particular to any user, so every investigation is available to every Carbon Black administrator.

It is a best practice to start an investigation whenever you begin any type of search, for example, after you discover a suspicious indicator and you start searching to find related process activity on your hosts. You could create an investigation to keep an ongoing record of the scope and effects of the threat so that you can stop it before it causes damage to your systems. There is no cost to creating an investigation, and if you tag process events during your search, you have a built-in record of the steps that provided the end result.

A default investigation comes with the server installation and is always available to collect any data that you tag. The default investigation cannot be deleted, so it is best used as a repository for data that interest you but do not warrant a dedicated investigation of their own. The first time that you open the Investigations page, the default investigation displays. To open an investigation, from the menu bar, click **Respond > Investigations**. The following illustration shows an example of a default investigation:



On the Investigations page, the following information displays:

Investigations menu bar:

- Dropdown list of investigations (Default Investigation is the default)
- Edit button (provides the option to rename the investigation)
- Actions menu with the following options:
 - Remove Events (see [“Removing Events from Investigations”](#) on page 164)
 - Add Custom Event (see [“Adding Custom Events to Investigations”](#) on page 164)
 - Add Investigation (see [“Creating Investigations”](#) on page 162)
 - Delete Investigation (see [“Deleting Investigations”](#) on page 165)
 - Export timeline to PNG (exports data from the graph to a .png file and downloads it to your computer)
 - Export events to CSV (exports data from the rows at the bottom of the page to a .csv file and downloads it to your computer)

Event Types: Select or deselect the checkboxes next to the event types to sort the events that display in the timeline and table. (Only selected events display.)

- **Filemods** (the number of files that were modified by process executions, displays in light green)
- **Regmods** (the number of Windows registry modifications that were made by processes executions, displays in blue)
- **Netconns** (the number of network connections that process executions either attempted or established, displays in purple)
- **Modloads** (the number of modules that were loaded by process executions, displays in green)
- **Processes** (the number of child processes that were generated from process executions, displays in orange)
- **Custom** (a custom event that you can create using the Add Custom Event option in the Actions menu, displays in black)
- **Cross Processes** (a process that crosses the security boundary of another process, displays in red)

Bar graph with a timeline of the events that are tagged for the investigation. The events display in color-coded bars (according to the event types). Events appear stacked when they occur at the same time. The color coding indicates which events happen at which times. Hovering over the color indicators on the timeline produces pop-up text which explains what that block of color represents.

Events table that shows the events contained in the investigations. A colored bar displays on the left border of each row to indicate the type of event. The following table describes the information that displays:

Table 29: Investigations Events Table Description

Column	Description
Hostname	The name of the host on which the event occurred.
Time	The date and time that the event occurred.
Tagged Time	The time that the event was tagged for this investigation.
Type	The event type (filemod, regmod, netconn, modload, process, custom, crossproc).
Description	Description of the event, for example, paths to files and registry elements that were modified, signature status, and MD5 hash values.
Search	Opens the event in the Search Processes page.
Analyze	Opens the event in the Process Analysis page.

When you hover over the description in each row, a pencil icon displays that you can use to edit the description. You can use this to add context to the technical description, or to add insights to share with the rest of your investigative team. Edits made to a description are visible within the investigation, but do not display in the process execution data when viewed outside of the Investigation page.

Rows that represent child processes contain a magnifying glass icon. This option displays a preview of what you would see if you opted to open the Process Analysis page for the child process.

You can use the Investigation icon:



to open an investigation, which displays over any page that you currently have open. The investigation consists of events that are tagged in processes from search results. Click **View** at the top right of the page to open the Investigations page with the current investigation open. Click the icon again to close the smaller investigation window.

Creating Investigations

There are two options for creating investigations.

To create an investigation from the Respond menu:

1. From the menu bar, click **Respond > Investigations**. The default investigation displays.
2. Click **Actions > Add Investigation**. The Add Investigation dialog box displays.
3. In the **Name** field, type a name for the investigation and click **Save**. The name must be alpha-numeric – special characters are not allowed.

- The new investigation displays in the Investigations window. It is empty.

To create an investigation using the Investigation icon:

- Click the **Investigation** icon:



An investigation window opens.

- Expand the Investigation menu. A list of all investigations displays. At the bottom of the list, select **Create New Investigation**. The Add Investigation dialog box displays.
- In the **Name** field, type a name for the investigation and click **Save**. The name must be alpha-numeric – special characters are not allowed. After providing a name, your new investigation becomes the currently open investigation. Any newly-tagged items are added to the open investigation.

Adding Events to Investigations

While you are performing searches for process executions or binary files, you can use the Investigation icon to have an investigation continually open. Events that you tag in your search results are added to this investigation.

To add events to investigations:

- Use the **Investigation** icon to open an investigation.

Host Name	Process Name	Description
COMPUTERNAME	conhost.exe	Opened handle with change access rights to c:\windows\system32\cmd.exe (fc0b4a626881d7c5960d757214
COMPUTERNAME	conhost.exe	Opened handle with change access rights to c:\windows\system32\ping.exe (ac13a4fe5396e05b46c7e270bc
COMPUTERNAME	conhost.exe	Opened handle with change access rights to c:\windows\system32\ping.exe (ac13a4fe5396e05b46c7e270bc
COMPUTERNAME	conhost.exe	Opened handle with change access rights to c:\windows\system32\ping.exe (ac13a4fe5396e05b46c7e270bc
COMPUTERNAME	conhost.exe	Opened handle with change access rights to c:\windows\system32\ping.exe (ac13a4fe5396e05b46c7e270bc

- Select a process from the Search Processes page and open the Process Analysis page.
- Click the tag icon in an event row that you would like to add to the investigation (the tag changes from gray to blue). The events are automatically added to the investigation that you have open.

Removing Events from Investigations

When you remove an event from an investigation, it continues to exist in the system, but is no longer included in the investigation. There are two ways to remove an event from an investigation. You can use the full investigation page (accessed by Respond > Investigation) or the smaller version of the page that is accessed by the Investigation icon.

To remove an event from an investigation from the Respond menu:

1. From the menu bar, click **Respond > Investigations**. The default investigation displays. Select the investigation from which to remove an event.
2. Click **Actions > Remove Events**. The event is removed from the list at the bottom of the page.

To remove an event using the Investigation icon:

1. Click the **Investigation** icon:



An investigation window opens.

2. Expand the Investigation menu. A list of all investigations displays. Select the investigation that contains the event to remove.
3. At the far right of the event row to remove, click the delete icon. A confirmation dialog box opens. Click **OK**. The event row is removed from the list.

Adding Custom Events to Investigations

You can create a custom event that you can use to add a new event type to the system, or to add a note that displays on its own line in the rows at the bottom of the Investigations page. You can specify time parameters for the event so that it displays where you want it to in the timeline.

To create custom events:

1. From the menu bar, click **Respond > Investigations**.
2. Click **Actions > Add Custom Event**.
3. In the **Description** field, type a description for the event.
4. In **Start Time**, enter the date and time for the event.
5. Click **Save**.

Deleting Investigations

When you delete an investigation, only the grouping, tagging, and edited descriptions are deleted. It has no other effect on the process executions that were a part of the investigation, or how those processes display in other pages.

To delete investigations:

1. From the menu bar, click **Respond > Investigations**.
2. In the dropdown menu of investigations, select the investigation to delete. The investigation opens.
3. Click **Actions > Delete Investigation**. A confirmation dialog box opens. Click **OK**. The investigation is removed.

Chapter 12

Watchlists

This chapter describes creating and using watchlists. Watchlists are saved searches that are visible to all users.

Sections

Topic	Page
Overview	168
Viewing and Searching Watchlists	168
Creating Watchlists	170
Editing Watchlists	173
Deleting Watchlists	173

Overview

Watchlists are saved searches, visible to all users. They can be either Process Searches or Binary Searches. You can create and use watchlists in the Process Search, Binary Search, and Threat Intelligence Feeds pages. For many watchlists that are based on threat intelligence feeds, you can factor scoring into a saved search.

For information about how watchlists are used, see the following chapters:

- [Chapter 6, ‘Incident Response on Endpoints’](#)
- [Chapter 7, ‘Process Search and Analysis’](#)
- [Chapter 8, ‘Binary Search and Analysis’](#)
- [Chapter 10, ‘Threat Intelligence Feeds’](#)
- [Chapter 13, ‘Console and Email Alerts’](#)

Viewing and Searching Watchlists

The Watchlist page enables you to quickly see items that as a first responder, you might find interesting. For example, using one of the default watchlists (Newly Executed Applications), if there were known recent issues with any new applications, you can see a list of process and binary execution results from those applications and scan them to find potential problems.

In the **Detect > Watchlists** menu, all watchlists can be seen by all users. The following illustration is a watchlist for newly executed applications (one of the default watchlists).

The screenshot displays the Carbon Black Watchlists interface. On the left, there is a sidebar with a search bar and filter options (All, Binaries, Processes). The main content area shows the configuration for the 'Newly Executed Applications' watchlist. It includes a 'Hit Count Over Time' bar chart showing a single hit. Below the chart, there are options to 'Enable Watchlist' and 'On Hit' actions (Email Me, Log to Syslog, Create Alert). The bottom section shows a list of matching binaries, including details like signature, company, and when the binary was last seen.

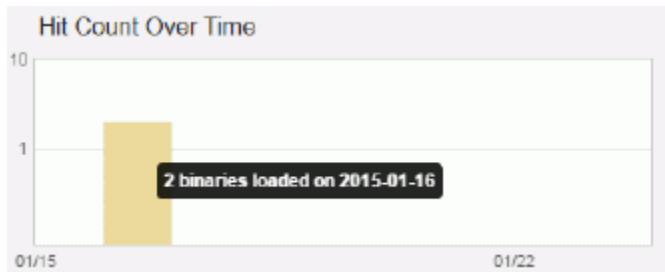
Binary ID	Signature	Company	Seen as	Time
A23FCE5B6D0B316A8C7327A6AAF3E6C	Signed	Google Inc.	setup.exe	about 6 days ago
BA7DC0C9141BE7292CA7E744B6F19F26	Signed	Publisher: Google Inc	39.0.2171.99_39.0.2171.96_chrome_up...	
8D466919CD6E9E976219136A1FE069C2	Signed	Microsoft Corporation	discan.dll	about 21 days ago
EE3ED9FF4BE5D79556EB8CC1BC889A74	Signed	Microsoft Corporation	security.dll	about 29 days ago
2A0CABDD9B4584538A1DD022A4D8FD3F			delegate_execute.exe	about 1 months ...

Names of all the existing watchlists display in a list on the left of the screen. If you click the name of a watchlist, the results for the search specified in the watchlist display on the right side of the page. Above the list of watchlists on the left, you can use the **Search** box to search for watchlists by name.

With the results displayed, you can use the **Search** button in the upper right corner of the screen to either the full Process Search or Binary Search (using the query that created the watchlist).

Above the results table, summary information displays on the left, and a bar graph displays on the right.

The bar graph displays the number of processes on the Y axis, and the date on the X-Axis. You can hover over the bar graph to see these details:



There are several default watchlists:

- Newly Executed Applications
- Newly Loaded Modules
- USB drive usage
- Non-System Filemods to system
- Netconns to .cn or .ru
- Autoruns
- Newly Installed Applications
- Filemods to Webroot

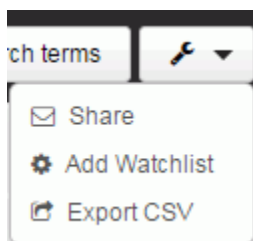
If the default watchlists do not meet your needs, you can create your own customized watchlists following the steps in [“Creating Watchlists”](#) on page 170.

Creating Watchlists

You can create watchlists from the Process Search or Binary Search pages. You can also create watchlists from the Threat Intelligence Feeds page, where you can create a watchlist that tags a process or binary found on one of your endpoints when the score from a specified feed matches a specified score or falls within a score range. The score is the rating used to calculate the severity assigned to Indicators of Compromise (IOCs) from a feed.

To create watchlists from process or binary searches:

1. From the **Respond** menu, select either **Process Search** or **Binary Search**. The appropriate search window opens.
2. Click the **Action** menu icon:



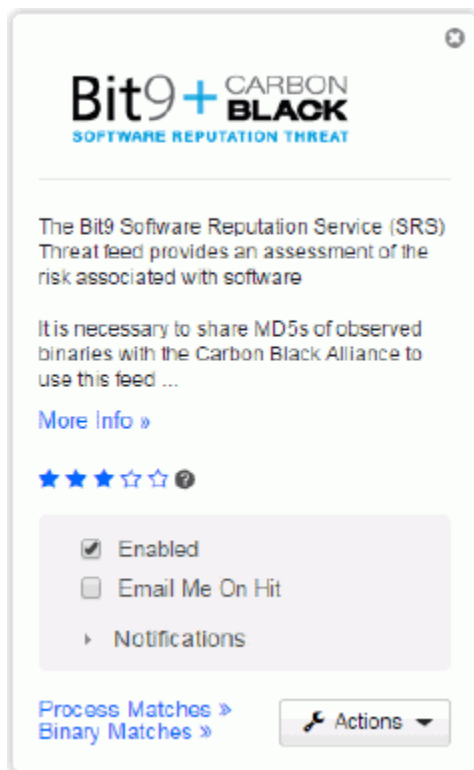
3. Select **Add Watchlist**. The Add Watchlist window opens.

4. In the **Name** field, type a name for the watchlist.
5. In the **Search Query** field, notice that the URL in the Search Query field is the query that is currently open. You cannot edit this field.
6. Select the **Email Me** check box to receive email notifications when there are hits that match your search.

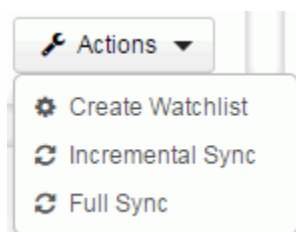
7. Select the **Create Alert** check box to send an alert when conditions matching the watchlist occur. Triggered alerts are reported in the Alert Dashboard page and the Triage Alerts page. For more information about alerts, see [Chapter 13, “Console and Email Alerts.”](#)
8. Select the **Log to Syslog** check box to log all hits that match the search in this watchlist to `syslog`, a repository for logs on the Carbon Black Enterprise server, with the program name prefix `cb-notifications-`.
9. Click **Save changes**.

To create watchlists from the Threat Intelligence Feeds page:

1. From the menu, choose **Detect > Threat Intelligence**. The Threat Intelligence Feeds page opens.
2. Select the feed for which you would like to create a watchlist, for example, the Bit9+Carbon Black Software Reputation Service (SRS) Threat feed.



3. Click the **Actions** button. Actions options display:



4. Select **Create Watchlist**. The Add Watchlist window opens:

The screenshot shows the 'Add Watchlist' dialog box. It features a title bar with the text 'Add Watchlist' and a close button (X). The main content area includes a 'Name' text input field. Below this is the 'Feed Score Criteria' section, which contains four radio button options: 'Greater than or Equal', 'Less than or Equal', 'Between', and 'Equals'. Each option is followed by a text input field. The 'Between' option has two text input fields. Below the 'Feed Score Criteria' section is a 'Type' dropdown menu currently set to 'Process'. At the bottom of the dialog are three checkboxes: 'Email Me', 'Create Alert', and 'Log to Syslog'. At the very bottom are 'Close' and 'Save changes' buttons.

5. In the **Name** field, type a name for the watchlist
6. In **Feed Score Criteria**, enter the score criteria for the severity of IOCs to track.
7. In **Type**, select either **Process** or **Binary**.
8. Select the **Email Me** check box to receive email notifications when there are hits that match your search.
9. Select the **Create Alert** check box to send an alert when conditions matching the watchlist occur. Triggered alerts are reported in the Alert Dashboard page and the Triage Alerts page. For more information about alerts, see [Chapter 13, “Console and Email Alerts.”](#)
10. Select the **Log to Syslog** check box to log all hits that match the search in this watchlist to `syslog`, a repository for logs on the Carbon Black Enterprise server, with the program name prefix `cb-notifications-`.
11. Click **Save changes**.

Editing Watchlists

You can edit some aspects of watchlists in the Watchlists page. However, you cannot edit the URL that is used as a basis for the watchlist search query.

To edit watchlists:

1. Open the Watchlists page by choosing **Detect > Watchlists** from the menu.
2. From the list of watchlists on the left, select the one to edit. The watchlist details display on the right.
3. You can edit the following attributes of the watchlist:
 - a. To change the name of the watchlist, click the pencil icon next to the name at the top of the page.
 - b. To enable the watchlist, select the checkbox next to **Enable Watchlist**. To disable the watchlist, deselect the checkbox.
 - c. To receive email notifications when there are hits that match your search, select the **Email Me** check box. Deselect the checkbox to stop receiving email notifications.
 - d. To send an alert when conditions matching the watchlist occur, select the **Create Alert** check box. Deselect the checkbox to stop sending alerts.
 - e. To log all hits that match the search in this watchlist to `syslog`, a repository for logs on the Carbon Black Enterprise server, with the program name prefix `cb-notifications-`, select the **Log to Syslog** check box. Deselect the checkbox to stop logging hits.

Deleting Watchlists

The only way that you can delete watchlists is by using the Watchlists page.

To delete watchlists:

1. Open the Watchlists page by choosing **Detect > Watchlists** from the menu.
2. From the list of watchlists on the left, select the watchlist to delete.
3. At the top right corner of the page, click the **Delete** button. A confirmation dialog box displays. Click **OK**. The watchlist is deleted.

Deleting a watchlist does not delete the query that it is based on, or any of the results that the query generates.

Chapter 13

Console and Email Alerts

This chapter describes the creation and management of Carbon Black alerts on the console. Alerts can be triggered due to watchlist or threat intelligence feed events. The chapter also provides details for enabling email reporting of these events.

Sections

Topic	Page
Overview	176
Enabling Console Alerts	176
Viewing Alert Activity using the Dashboard	178
Managing Alerts on the Triage Alerts Page	181
Enabling Email Alerts	189

Overview

You can create alerts that will indicate in the Carbon Black console when suspicious or malicious activity appears on your endpoints. Alerts are available for two types of events:

- **Watchlist hits** – Any Watchlist may be configured to send an alert when conditions matching the watchlist occur. See [Chapter 12, “Watchlists,”](#) for more information about Watchlists.
- **Threat Intelligence Feed hits** – Any Threat Intelligence Feed may be configured to send an alert when that feed reports an indicator of compromise that has been seen on sensor-managed computers reporting to your Carbon Black server. See [Chapter 10, “Threat Intelligence Feeds,”](#) for more information about Threat Intelligence Feeds.

Triggered alerts are reported in two locations in the Carbon Black console:

- **Dashboard page** – The (Alert) Dashboard is a summary page, showing the number unresolved alerts, the number of hosts with unresolved alerts, and other alert-related data, including the alerts for each host.
- **Triage Alerts page** – The Triage Alerts page includes more extensive details about alerts that have been triggered, and provides a filter and search interface to locate alerts matching different criteria. It also is the place in which you can manage the alert workflow, marking that status of each alert from the initial triggering through resolution.

In addition to alerts shown in the console, you can configure Watchlists and Threat Intelligence Feeds to send email alerts when there is a “hit” on data from a Carbon Black sensor that matches the watchlist or feed. These may be enabled in addition to or instead of the console-based alerts. See [“Enabling Email Alerts”](#) on page 189 for more details.

Enabling Console Alerts

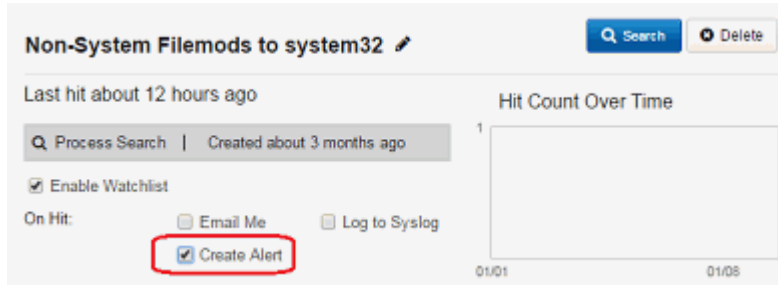
You can enable alerts for any Watchlist or Threat Intelligence Feed. Consider how many hits you are likely to receive when you enable an alert. Some Watchlists or feeds might generate too many hits to be useful, making location of significant alerts more difficult. Ideally, an alert should be getting your attention for something you need to follow up on. By default no alerts are enabled.

Watchlist Alerts

Watchlists are user-created custom saved searches based on a process or binary search, or on feed results. They can be used to monitor your computers for the appearance of indicators of compromise. Adding a console alert to the Watchlist lets you select which Watchlists are of highest importance for monitoring, and also to combine these high-importance Watchlist hits with high-importance feed hits on a single Alerts pages.

To enable console alerts for a Watchlist:

1. On the console menu, choose **Detect > Watchlists** and in the left menu click on the name of the Watchlist for which you want to create an alert. If the name is not visible or you are not sure of the name, use the Search box above the names.
2. With the Watchlist details showing, be sure the **Enable Watchlist** box is checked.



3. Check the **Create Alert** box in the On Hit area. The Watchlist should begin generating alerts when .

Threat Intelligence Feed Alerts

Threat Intelligence Feeds are information feeds to help identify malware and its sources. Carbon Black integrates with both third-party feeds and feeds from Bit9 + Carbon Black, including the Bit9 Software Reputation Service and the Bit9 Tamper Protection feed that identifies hosts on which attempts to tamper with Carbon Black occur. Adding a console alert to a feed lets you highlight hits matching reported malware from a particular source that you might find most useful, and also combine these feed hits with high-importance watchlist hits on a single Alerts pages.

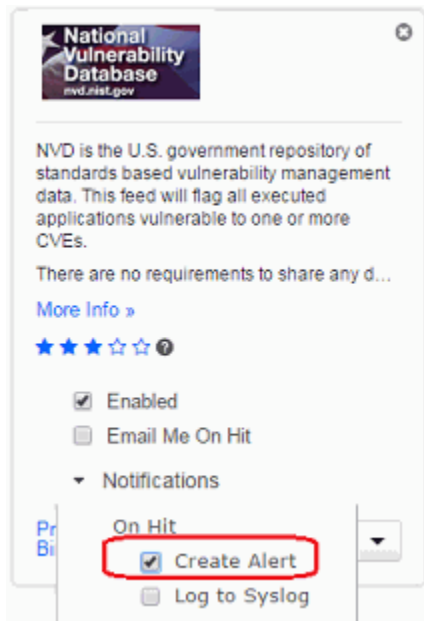
Be sure to understand the volume of reports you are likely to receive from any feed before enabling alerts for it. Among other things, read the description of a feed on the Threat Intelligence Feeds page. Some include a specific recommendation *not* to enable alerts because of the report volume or the percentage of false positives that can occur.

Note

You also have the option of creating a Watchlist for any feed, and then can create an alert for hits on that Watchlist.

To enable console alerts for a Threat Intelligence Feed:

1. On the console menu, choose **Detect > Threat Intelligence**.
2. For each feed for which you want to activate console alerts, click the **Notifications** link and then check the **Create Alert** box. Console alerts are now enabled for each feed you checked.



To disable console alerts for a Threat Intelligence Feed:

- On the Threat Intelligence Feeds page, for each feed for which you want to disable console alerts, click the **Notifications** link and then click to *uncheck* the **Create Alert** box. Console alerts are now disabled for each feed whose box you unchecked.

Viewing Alert Activity using the Dashboard

The Dashboard page provides a summary of alerts on hosts monitored by sensors reporting to your Carbon Black server. It is a quick reference view that includes charts, graphs, and tables for current alert status, trends, hosts and users with the most alerts, and related information. Links in some of these panes open the Triage Alerts page filtered for the item clicked on (for example, all alerts for a host that you clicked on).

Note

The Carbon Black console also has a *Server* Dashboard. That is not described in this section.

To view the alerts Dashboard:

- On the console menu, choose **Detect > Dashboard**.
The Dashboard page opens.

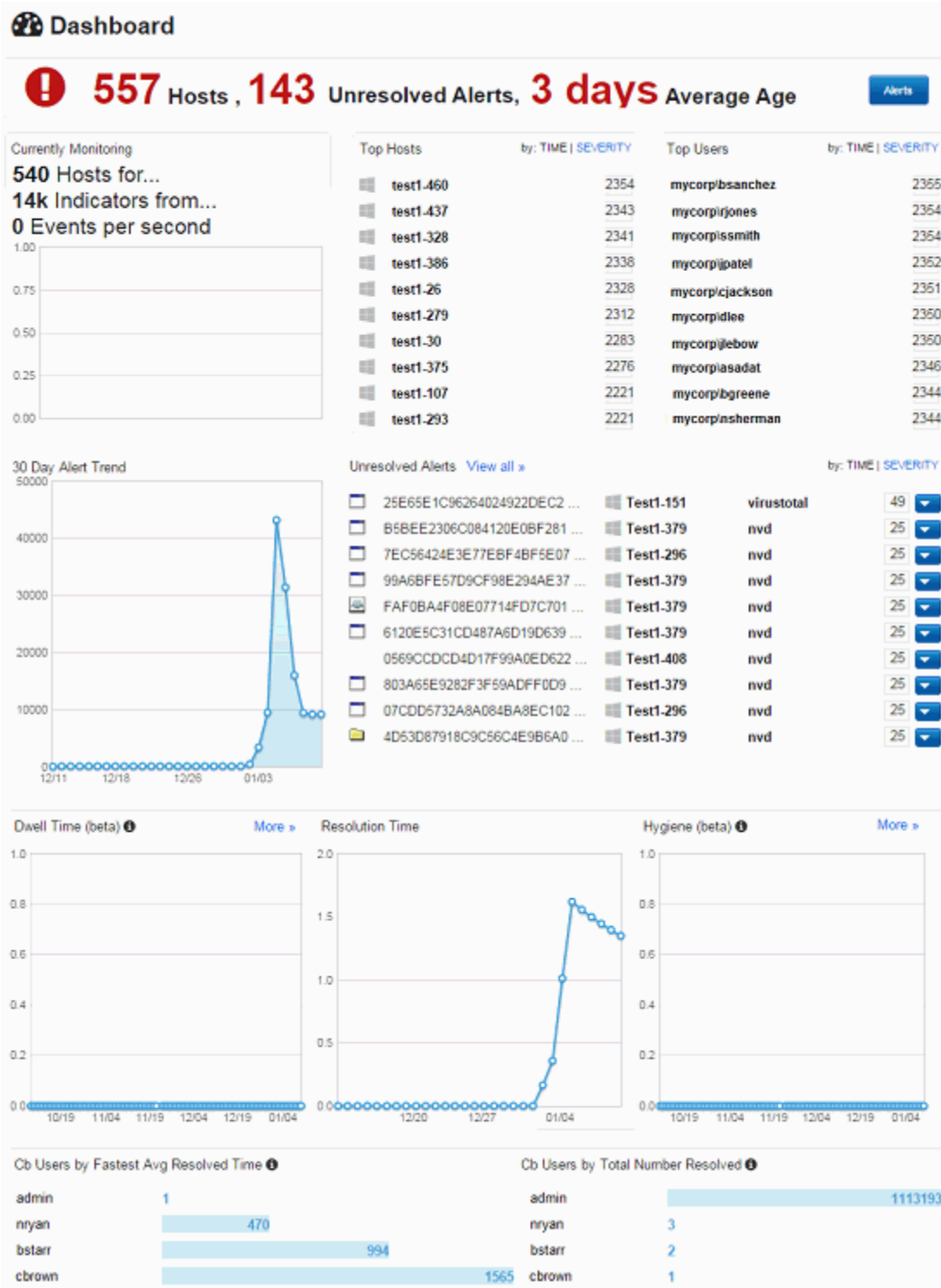


Table 30 describes the information and links available on the alerts Dashboard.

Table 30: Alerts Dashboard

Pane	Description
Summary Banner	<p>This shows a large-format summary of the number of hosts reporting alerts to this server, the number of unresolved alerts, and the average age of the unresolved alerts.</p> <p>Clicking the Alerts button here opens the Triage Alerts page.</p>
Currently Monitoring	<p>This shows the number of hosts with sensors currently reporting to the server, the number of indicators of compromise, and how many alert events are arriving on this server per second.</p>
Top Hosts	<p>This table shows the 10 hosts with the highest average alert ages (i.e., time during which the alert has been unresolved). You also can choose to display the top 10 hosts reporting alerts with the highest severity.</p> <p>Clicking on any host name opens the Triage Alerts page filtered for alerts from that host.</p>
Top Users	<p>This table shows the 10 users running processes that triggered alerts with the highest average alert ages (i.e., time during which the alert has been unresolved). You also can choose to display the top 10 users running processes that triggered alerts with the highest severity.</p> <p>Clicking on any user name opens the Triage Alerts page filtered for alerts from hosts on which that user is logged in.</p>
30 Day Alert Trend	<p>This graph shows the number of currently unresolved alerts for alerts reported on each of the most recent 30 days. Each day is represented by a circular node, and moving the mouse over a node displays a tooltip that gives the date and the number of unresolved alerts on that day</p>
Unresolved Alerts	<p>This table the top 10 unresolved alerts. By default it shows the most recent alerts. You also can choose to show the top 10 alerts by severity. Clicking on a hostname in this table opens the Triage Alerts page filtered for that host. Similarly, clicking on the alert source opens the Triage Alerts page filtered for that source.</p> <p>Clicking the View All link opens the Triage Alerts page to shown all unresolved alerts in order of age.</p>
Dwell Time (beta)	<p>This graph shows the daily average for how long malware “dwells” on hosts reporting to this server over a 30-day period. This is based on the duration between when an undesirable binary first appears on one of the hosts and when it is no longer reported on any hosts.</p> <p>You must enable Sharing Hashes with VirusTotal for dwell time to be calculated. Otherwise there will be no data for this graph. Note that this is a beta feature and is subject to change.</p> <p>Clicking on More in this pane provides additional discussion of Dwell Time.</p>

Table 30: Alerts Dashboard (continued)

Pane	Description
Resolution Time	This graph shows the average amount of time (in hours) between reporting and resolution of alerts on each day over a 30-day period. Each day is represented by a circular node, and moving the mouse over a node displays a tooltip that gives the date and the average amount of time to resolve alerts on that day.
Hygiene (beta)	<p>This graph shows the daily percentage of hosts reporting suspect processes over a 30-day period. This is based on two values recorded by Carbon Black: the total number of active hosts in the network and number of hosts with one or more 'bad' processes.</p> <p>You must enable Sharing Hashes with VirusTotal for hygiene to be calculated. Otherwise there will be no data for this graph. Note that this is a beta feature and is subject to change.</p> <p>Clicking on More in this pane provides additional discussion of Hygiene.</p>
Cb Users by Fastest Avg Resolved Time	This graph shows the top Carbon Black console users ranked by how quickly they resolve alerts.
Cb Users by Total Number Resolved	This graph shows the top Carbon Black console users ranked by how many alerts they resolve.

Managing Alerts on the Triage Alerts Page

When an alert is received indicating suspicious or malicious activity on one or more of your endpoints, incident responders need to determine the seriousness of the alert, and if the alert indicates a sufficiently severe threat, find a way to resolve the threat. This might involve using Carbon Black features such as Endpoint Isolation and Live Response, or it might require use of other tools. Given the high volume of threat reports in the current environment, it is critical to be able to prioritize, investigate, and keep track of the status of alerts. Once an alert is resolved, it should be removed from the list of threats requiring attention so that ongoing threats may be addressed.

The Triage Alerts page provides features for alert management. It includes search and filtering capabilities for locating specific alerts or types of alerts. It also allows you change the status of alerts.

To open the Triage Alerts page:

- In the console menu, choose **Detect > Triage Alerts**.
The Triage Alerts page is displayed.

Note

You also can navigate to the Triage Alerts page from the alerts Dashboard. See [“Viewing Alert Activity using the Dashboard”](#) on page 178 for more details.

The Triage Alerts page is divided into three major sections:

- The top section includes the main Search box, Search Criteria dialog, and an Action menu that applies to the whole page.
- The middle section contains a series of “facets” that are category-specific lists (Alert Status, Username, etc.) showing the percentage of alerts matching different values in each category and allowing you to filter the view to show alerts matching one or more values.
- The bottom section is the Alerts table, showing details for alerts matching the search or filtering entered in the first two sections.

The Triage Alerts page presents alert data in formats similar to the presentation of other data in the Carbon Black console. See [Chapter 2, “Using the Carbon Black Console,”](#) for a description of “facets” and tables in the Carbon Black user interface. See [Chapter 7, “Process Search and Analysis,”](#) and [Chapter 9, “Advanced Search Queries,”](#) for more on query rules and syntax.

Triage Alerts 1k Unresolved

Search: Search Reset search terms

+ Add Criteria

Facets:

- Status (3)**: unresolved (12.0%), resolved (88.0%), false positive (0.0%)
- Username (50+)**: dragon (25.9%), system (12.3%), root (11.9%), cbrown (4.4%)
- Hostname (50+)**: test1-319 (15.6%), test1-149 (10.7%), test1-222 (4.5%), test1-379 (3.8%)
- Feed (8)**: nvd (76.7%), my watchlists (11.2%), cbtamper (0.6%), virusotal (1.8%)

Show 10 of 1,986 | Sort by Severity

DESCRIPTION	ACTIVITY	ALERT DATA	ACTION
<p>38ECEA81F9B4722522DB05CB1F6ADF15</p> <p>Test-43 mdkitadapter.dll (2 more)</p> <p>LAPTOP-44</p> <p>5.0.0 Sensors with Tamper Windows</p>	<p>29</p>	<p>38ec ea81f9b4722522db05c b1f6adf15</p> <p>CVE-2013-3351 acrobat_reader (cvss_sco ... nvd</p> <p>AlertCbServiceStopped</p> <p>Carbon Black sensor process has been t ... Tamper Detection</p>	<p>68</p> <p>feed rating: ██████████</p> <p>report score: ██████████</p> <p>confidence: ██████████</p> <p>orality: ██████████</p>
<p>chrome.exe</p> <p>ABC123 c:\program files (x86)\google\chrome\application\chrome.exe</p>	<p>about 22 days ago</p>	<p>146.185.183.13</p> <p>146.185.183.13 has been a TOR exit nod ... tor</p>	<p>22</p> <p>feed rating: ████████</p> <p>report score: ██████████</p> <p>confidence: ██████████</p> <p>orality: ██████████</p>

Table 31: Triage Alerts Page

Pane	Description
Unresolved Count	The red Unresolved count shown in the top right area of the page shows the number of unresolved alerts in the current search and filter results.
Search Box and Criteria Dialog	<p>You can customize the search criteria by clicking + Add Criteria button below the search box.</p> <p>The Reset search terms button to the right of the search box restores the default view.</p> <p>See Chapter 7, “Process Search and Analysis,” and Chapter 9, “Advanced Search Queries,” for more on search query rules and syntax.</p>
Main Action (wrench) Menu	<p>The Action (wrench) menu in the top right of the Triage Alerts page contains commands that apply to the page as a whole:</p> <ul style="list-style-type: none"> • Share – Opens your default email client with a message prepopulated with the URL of the Carbon Black Enterprise server and the query string for the currently displayed page. Use this to share information about alerts with other users. • Export CSV – Exports the first 1000 rows in the alerts table to a .csv file for reporting, retention, or compliance. Each row contains the data displayed on the page for that alert and the URL to the details of each result on the table. • Mark all as Resolved – Mark the status of all alerts in the current search results as Resolved. • Mark all as Unresolved – Mark the status of all alerts in the current search results as Unresolved. • Mark all as In-Progress – Mark the status of all alerts in the current search results as In-Progress. • Mark all as Resolved False Positive – Mark the status of all alerts in the current search results as Resolved False Positive. <p>When you choose any of the Mark All commands, a message appears in the menu bar at the top of the page indicating how many alerts were changed.</p> <p>Note: Be sure you want to change the status of alerts before confirming any of the “Mark all” commands. See “Managing Alert Status” on page 187 for more information on alert status.</p>

Table 31: Triage Alerts Page (continued)

Pane	Description
Criteria-Specific Search Results Summaries	<p>In the panel below the search box, there is a series of criteria-specific lists (“facets”) that show the percentage of alerts matching different values within the criteria. Clicking on a row in a list filters the view based on that row.</p> <ul style="list-style-type: none"> • Status – This shows the percentage of alerts in each of the status categories for the alerts in this view. • Username – This shows the percentage of process-related alerts associated with specific usernames running the process in this view. • Hostname – This shows the percentage of alerts for activity on specific hosts. • Feed – This shows the percentage of alerts triggered because of reports from each available feed. Any alerts triggered by a watchlist are combined in Feed category labeled <i>My Watchlists</i>. • Report – This shows the percentage of alerts associated with each Watchlist or report from a Feed. • IOC – This shows the percentage of alerts associated with each Indicator of Compromise (MD5, IP address, or query). • Assigned To – This shows the most recent user to change their status. <p>See Chapter 2, “Using the Carbon Black Console,” for more on “facets”.</p>
Alerts Table	<p>The Alerts table includes a description and data for each alert matching the search criteria on the page (by default, all unresolved alerts, if no other criteria were provided). See “Reviewing Alerts” for complete information about the description and data provided.</p>

Reviewing Alerts

Each row in the Alerts table shows the description and data for an individual alert. The description and data that appears can vary depending upon a variety of factors, including the source and type of the alert, whether the binary for a process has been signed, and whether a binary for which an alert has been reported is considered “Trusted” by the Carbon Black Alliance.

The screenshot displays a table of alerts with the following columns: DESCRIPTION, ACTIVITY, ALERT DATA, and ACTION. The table shows two alert entries:

DESCRIPTION	ACTIVITY	ALERT DATA	ACTION
<p>38ECEA81F9B4722522DB05CB1F6ADF15</p> <p>Test-43 mdkitadapter.dll (2 more)</p> <p>about 3 days ago Signed</p>	29	<p>38ecea81f9b4722522db05cb1f6adf15</p> <p>CVE-2013-3351 acrobat_reader (cvss_sco ... nvd</p>	<p>68</p> <p>feed rating: ██████████ report score: ██████████ confidence: ██████████ criticality: ██████████</p>
<p>chrome.exe</p> <p>ABC123 c:\program files (x86)\google\chrome\application\chrome.exe</p> <p>about 22 days ago</p>		<p>146.185.183.13</p> <p>146.185.183.13 has been a TOR exit nod ... tor</p>	<p>22</p> <p>feed rating: ██████████ report score: ██████████ confidence: ██████████ criticality: ██████████</p>

The Alerts table has several tools for adjusting the table display:

- **Alerts per page** – You can choose the number of alerts to show per page by changing the number in the **Show** box at the top left of the table.
- **Sort order** – You can choose to sort the table differently by choosing Severity (the default) or Most Recent on the **Sort by** menu at the top right of the table.
- **Page navigator** – At the bottom right of the table, there is a page navigation bar for moving between pages in table views that do not fit on a single page.

Activity That Triggered the Alert: Description and Chart

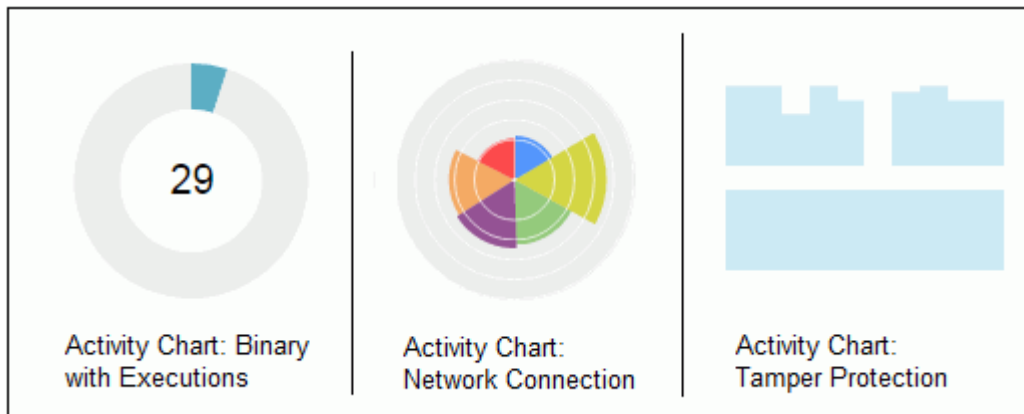
The row for each alert in the table is divided into columns. The Description column, which includes a variety of information including an Activity chart, is on the left. Some of the information in this column varies depending upon the type of alert represented.



The Alert Description column shows some or all of the following information (varying by the type of threat):

- **Threat Source** – For an alert that is triggered by a report of a malicious or suspicious binary, the MD5 hash of that binary is shown. For an alert triggered by network connections, this field is a filename. For a tamper protection alert, this field is a hostname. Clicking on the MD5 or filename opens the Process Analysis page for that binary. Clicking on the hostname opens the sensor details page for this host.
- **Threat File Icon** – This is the icon representing the binary that caused the threat, if available. If there is no special icon for this binary, a generic file icon is used. Not used for tamper alerts.
- **Host Where Alert Triggered** – This shows the host on which this alert was triggered. Clicking on its name opens its sensor details page. If the threat source field shows a hostname, it is not repeated here.
- **Platform Icon** – This icon represents the operating platform (Windows, Mac, Linux) for the host on which the alert issue appeared.
- **Threat Filename** –
- **Age, Certificate, Trust** – This block of fields shows different information depending on what is available and the type of alert. For all alerts, the age of the alert is shown; for example, it might indicate that the alert was triggered “about 3 days ago”. For binary alerts, an indicator shows whether or not the binary was signed. If the binary is trusted by feed sources, another indicator shows that.

The Activity chart in an alert description varies depending upon whether the alert is based on a binary or a network connection.



There are three formats for the activity chart:

- For alerts triggered by a reported binary that has executed on one or more hosts, a doughnut chart is shown, with the blue section representing hosts that executed the binary, the grey section representing hosts that have not, and the number of hosts that executed the binary in the center of the doughnut. Moving the mouse over either section shows the number of hosts in each category.
- For alerts involving network access, pie chart showing the number of actions related to this alert, by category. For each pie slice, tooltips show the exact categories and number of actions in each category:
 - **File modifications** – The yellow-green slice shows the file modifications due to the threat reported in this alert.
 - **Modloads** – The green slice shows the modules loaded due to the threat reported in this alert.
 - **Network connections** – The purple slice shows the network connections due to the threat reported in this alert.
 - **Processes** – The orange slice shows the processes run due to the threat reported in this alert.
 - **Registry modifications** – The blue slice shows the registry modifications due to the threat reported in this alert.
- For tamper protection alerts, a bar graph design is shown.

Alert Data

Most of the right half of an alert row displays the Alert Data column, which describes the threat intelligence that triggered the alert. Information in this column varies depending upon the source of alert represented, which can be a watchlist, feed, or a host tamper alert.



The Alert Data column shows the following information:

- **IOC Value** – IP Address if a network connection; MD5 if binary; alert name if this is a tamper event without binary information.
- **Report Title** – IP address and reason it alerted if this is a network connection alert; MD5 for a binary if this is a file/process-related alert; Description of tamper suspicious activity if this is a tamper protection alert. Clicking on this field links to the source of the alert. Note that if the alert is external to Carbon Black, you may need a login name and account to access the source information.
- **Alert Source** – The source of the alert, which is either a feed or watchlist name.
- **Alert Severity** – Numeric rating (1-100) for the threat, highest number indicating highest threat, with color indicator (yellow through red).
- **Contributing Factors** – Indicator (1-5) of the factors contributing to the severity:
 - **Feed rating** -- A floating point number from 1 to 5 based on the rating given to this feed on the Threat Intelligence Feeds page by the current user. Defaults to 3.
 - **Report Score** -- The score given by the feed provider, normalized to a scale of 0 to 100. Default is 100.
 - **Criticality** -- An attribute of sensor groups that can specify that IOCs on hosts in that group should have high, medium, or low criticality (converted to numeric ratings of 1, 2 or 3, respectively). Default is 2.
 - **Confidence** -- Not currently implemented.





Managing Alert Status

You can change the status of individual alerts or all alerts in the current view. Changing alert status is strictly for alert management purposes, to let you know which alerts need attention and which are being investigated or have been resolved. Change status to indicate what you are doing or have done based on your review of an alert. Alert status has no effect on the actual issue that caused the alert.

In the Alerts table, the far right column includes an icon representing the current alert status and a menu for changing that status.

[Table 32](#) describes the alert status options and shows their icons.

Table 32: Alert Status

Status	Icon	Description
Unresolved		This is the initial status. If you changed the status of this alert but cannot resolve the issue at this time, choose this status.
In-Progress		Choose this status if you have begun work on investigating and remediating the issue that caused this alert.
Resolved		Choose this status if you have addressed the issue that caused the alert. (If you are reading this on a black-and-white print, note that this checkmark is green.)
Resolved False Positive		Choose this status if you have determined that the report that triggered this alert does not indicate an actual threat. (If you are reading this on a black-and-white print, note that this checkmark is yellow.)

To change the status of all alerts matching a search and/or filter:

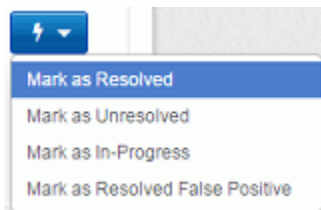
1. On the Triage Alerts page, enter the search string and/or filter criteria for the alerts whose status you want to change.
2. On the action (wrench) menu at the top right of the page, choose the “Mark all as ...” menu command for the status you want to assign.
3. On the confirmation dialog, if you are certain you want to change the status of all of these alerts, click **OK**.

Note

When using the “Mark all” commands, be certain you want to change all of the alerts matching the current filter and search, including those on other pages. Once you change status, there is no “undo” command. Be especially careful of changing status when the view is unfiltered (i.e., showing all alerts).

To change the status of one alert:

1. In the Alerts table, locate the alert whose status you want to change.
2. In the Action column at the far right of the row for that alert, click on the button for the Status menu (lightning bolt), and choose the status for this alert.



Keep in mind that alerts whose status you change will disappear from the current view if you have filtered the page for a different status.

Enabling Email Alerts

You can enable email reporting of the same type of events that trigger alerts – Watchlists and Threat Intelligence Feeds – either with or without console alerts enabled. With email enabled, you will be informed of events of interest even when you are not logged into the Carbon Black console, and if an event is significant enough, you can then go to the console to investigate and resolve it.

Email reporting of Watchlist and Threat Intelligence Feed hits is enabled on a per-console-user basis.

Configuring an Email Server

Before you begin enabling email reporting for specific Watchlists or feeds, you should decide what mail server you will be using. You have the option of using your own mail server, using the Carbon Black External Mail Server, or opting out of any email alerts. If you use the Carbon Black External Mail Server, your server ID, the time of the email, and the name of the Watchlist or Feed are that triggered the hit are sent through the server and kept by Carbon Black.

Important

For this release, Carbon Black strongly recommends that you use your own server because mail sent through the Carbon Black External Mail Server is sent over the internet in clear text.

To configure an email server for alerts:

1. On the console menu, choose **Administration > Settings**.
2. On the Settings page, click **Email** in the left menu. The Alerting via Email page appears.

The screenshot shows the 'Alerting via Email' configuration page in the Carbon Black console. On the left, a navigation menu includes 'Sites', 'E-Mail' (highlighted), 'License', 'Server Nodes', and 'Bit9 Platform Server Settings'. The main area is titled 'Alerting via Email' and contains the following options:

- Use Carbon Black External Mail Server (Secure HTTPS POST to api.alliance.carbonblack.com)
- Use My Own Mail Server

Fields for 'Use My Own Mail Server' include:

- SMTP Server:
- Port:
- Username:
- Password:

Under 'Connection Type':

- Secure Connection using TLS
- Secure Connection using SSL
- Plaintext Connection (insecure)

At the bottom, there is an option to opt out: I do not want to receive email alerts from Carbon Black, and a blue 'Save Changes' button.

3. Click on the **Use My Own Mail Server** radio button.

4. Provide the following information for the mail server you want to use:
 - a. **SMTP Server** – The address of the SMTP server you will use
 - b. **Port** – The port for email service
 - c. **Username** – The login account required to login to the server
 - d. **Password** – The password needed to login as the specified user
 - e. **Connection Type** – The security protocol to use for this connection, or Plaintext Connection if you do not want the mail to be secure.
5. When you have finished entering server configuration settings, click the **Save Changes** button.

All email alerts for all console users will now be routed through this server.

Enabling Specific Email Alerts

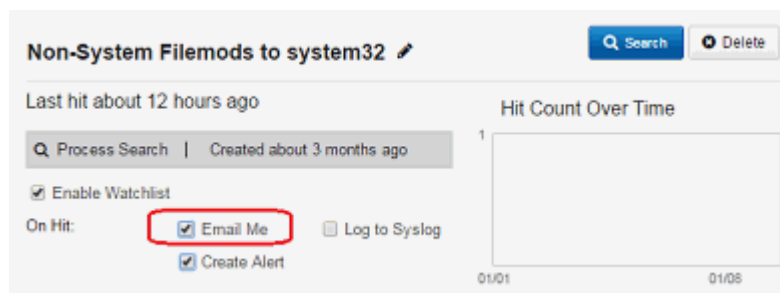
Once you have an email server configured, any Watchlist or Feed in the Carbon Black console can be configured to send email when it gets a hit on a Carbon Black sensor. Email alerts may be turned on and off for individual Watchlists and Feeds as needed, for example, if you find that one of them is creating too much email traffic. Keep in mind that email alerts for any specific watchlist or feed are enabled on a per user basis.

Note

If you have upgraded from a previous release of Carbon Black, any email alerts you had enabled for a Watchlist will remain enabled after upgrade.

To enable email alerts for a Watchlist:

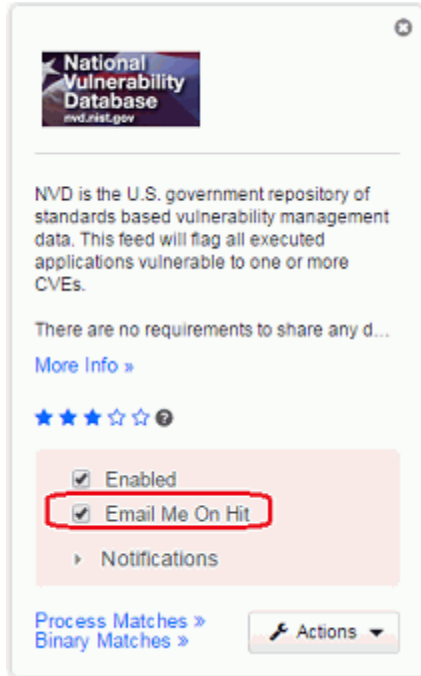
1. On the console menu, choose **Detect > Watchlists** and in the left menu click on the name of the Watchlist for which you want email alerts enabled. If the name is not visible or you are not sure of the name, use the Search box above the names.
2. With the Watchlist details showing, if you want to begin receiving alerts immediately, be sure the **Enable Watchlist** box is checked.



3. Check the **Email me** box in the On Hit area. Email alerts are now enabled for this Watchlist for the current console user.

To enable email alerts for a Threat Intelligence Feed:

1. On the console menu, choose **Detect > Threat Intelligence**.
2. For each feed for which you want to activate email alerts, check the Email Me On Hit box. Email alerts are now enabled for each feed you checked.



Appendix A

Installing the Carbon Black Enterprise Server**Sections**

Topic	Page
Overview	194
Installing a New Carbon Black Enterprise Server	195
Initialization and Configuration Dialog (cbinit)	198
Upgrading a Carbon Black Enterprise Server	203
Server Troubleshooting	204

Overview

This appendix describes the steps for installing the Carbon Black Enterprise Server. Both new installations and server upgrades are covered. The entire process can be completed in about ten minutes, assuming reasonable download speed.

The separate *Carbon Black - Enterprise Server Sizing Guide* document provides guidelines for hardware and software required for the Carbon Black Enterprise Server. You must have an environment meeting these requirements before you begin the procedures described in this document.

Carbon Black Enterprise Server installation consists of three primary steps:

1. Get and install a RPM from Carbon Black. This RPM does not install the enterprise server. It does set up a yum repo and installs a SSL client certificate that allows the full enterprise server to be downloaded and installed.
2. Download the enterprise server using the yum repo that was set up in step 1.
3. Install the enterprise server. This is a two-step process that involves both "yum install" and running a simple configuration script.

You can automate server installation using a script named `cbinit`. This might be desirable in situations requiring multiple installations, for example, in a test environment. See the separate document *Cbinit Automation* on the Carbon Black customer portal at <https://bit9.com/customer-portal>.

In addition to the automation document, the customer portal includes other documents related to server installation and management that may be of interest to you.

When you have installed the server, you can then install sensors on the endpoints you intend to monitor. Instructions for installing and upgrading sensors can be found in [Chapter 5, "Installing and Managing Sensors."](#)

Firewall and Connectivity Requirements

Internet connectivity via outbound TCP is required on the Enterprise Server system for the scenarios described in [Table 33](#).

Table 33: Connectivity Requirements for Server Installation and Operation

Scenario	Description	Address
Carbon Black Yum Repository	The RPM installer sets up a yum repository.	yum.carbonblack.com:443
Carbon Black Alliance Server	The Alliance Server provides threat intelligence and can also enable further analysis of files on endpoints via alliance partners.	api.alliance.carbonblack.com:443
CentOS Yum Repository	The standard CentOS Yum repository server used during Carbon Black Enterprise Server installation to download standard packages	mirror.centos.org:80

Installing a New Carbon Black Enterprise Server

This section describes the procedure for installing a new Carbon Black Enterprise Server..

Important

The steps in this section are for a new installation only. If you already have the Enterprise Server installed, **do not** perform these steps. Instead, see the "Server Upgrade" section later in this document. Use of the new installation procedure on an existing server will likely result in the loss of all data, including configuration and event data collected from sensors

To install and initialize a new server:

1. Verify the server you intend to install Carbon Black Enterprise Server on meets the hardware and software requirements specified in the *Carbon Black - Enterprise Server Sizing Guide* document you received from your Carbon Black representative.
2. Verify that the server has Internet connectivity as specified in "[Firewall and Connectivity Requirements](#)" on page 194.
3. Procure an installation RPM from Carbon Black. This requires interaction, by e-mail, with Carbon Black.
4. Install the RPM:
 - a. Verify you are running with root access
 - b. Install the RPM using the following command:
rpm -Uvh carbon-black-release-1.0.0-1.el6.x86_64.rpm

```
[root@MyCbServer yum.repos.d]# rpm -Uvh carbon-black-release-1.0.0-1.el6.x86_64.rpm
[root@MyCbServer yum.repos.d]# pwd
/etc/yum.repos.d
[root@MyCbServer yum.repos.d]# cat CarbonBlack.repo
[cb]
name=cb
baseurl=https://yum.carbonblack.com/enterprise/stable/x86_64/
repodata
gpgcheck=0
enabled=1
[root@MyCbServer yum.repos.d]#
```

- c. (Optional) Verify that the Carbon Black [cb] yum repository was set up in `/etc/yum.repos.d/CarbonBlack.repo`
- d. (Optional) Verify that the Carbon Black SSL client certificate was installed in `/etc/cb/certs/carbonblack-alliance-client.key`

5. Install the Carbon Black Enterprise Server:
 - a. Verify that your computer's date and time settings are accurate. Incorrect date/time settings can result to failures in SSL negotiation, which is required for yum downloads.
 - b. Run the following command using sudo:
sudo yum install cb-enterprise

```
[bsmith@localhost yum.repos.d]$ sudo yum install cb-enterprise
```

- c. Install the CentOS GPG key if you are prompted to do so.
 - d. If your environment requires that outbound firewall exceptions be made, ensure that the exceptions documented in [“Firewall and Connectivity Requirements”](#) on page 194 are followed. You will also have to update `/etc/yum.repos.d/CentOS-Base.repo` to enable the baseurl of `http://mirror.centos.org`.

Note: Yum supports the use of web proxies. However, Carbon Black is not aware of a way to use yum with NTLM-authenticated web proxies.
6. When the installation completes, initialize and configure the Carbon Black Enterprise Server -- see [“Initialization and Configuration Dialog \(cbinit\)”](#) on page 198 for a sample dialog so that you are prepared to respond to the prompts in this script:
 - a. Run the following command and respond to the prompts:
sudo /usr/share/cb/cbinit

```
[bsmith@localhost yum.repos.d]$ sudo /usr/share/cb/cbinit  
[sudo] password for bsmith:
```

- b. When viewing the license agreement, use **q** to exit the editor.
 - c. Back up the SSL certificate generated to protect sensor-to-server communications, as prompted by cbinit.

7. Configure your firewall if you have not already done so:
 - a. Open port 443 if you did not allow the cbinit script to automatically do that for you.

```
[bsmith@localhost yum.repos.d]$ sudo vim /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
# New additions to the IPTABLES for carbon black
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
COMMIT
```

- b. (Optional) Open port 80 to allow use of web UI and sensor communications via unsecured channel. This is not required and only recommended for exploration or troubleshooting.
8. Log in to the Carbon Black Enterprise Server web user interface.
 - a. <https://<your server address>/>
 - b. Use the username and password set up in the cbinit script.

Note

Google Chrome is the only supported browser for this release. Although not supported, internal testing indicates that Firefox, Opera and IE10 or higher should work. Note, however, that IE browsers must not be in compatibility mode, and servers in the same subnet as the browser are automatically connected in this mode.

When the Carbon Black Enterprise Server is installed, configured, and initialized, it should be accessible via the web UI, on port 443 with a self-signed certificate. If you have opened port 80, the web UI is also accessible via HTTP on port 80.

The next step, especially in a test environment, is to download a sensor installer and install one or more sensors to begin collecting data. Sensor installation is described in [Chapter 5, “Installing and Managing Sensors.”](#)

Initialization and Configuration Dialog (cbinit)

The following text shows the dialog presented when you run **cbinit** to initialize and configure the Carbon Black Enterprise Server. The responses are samples -- your responses should reflect your environment, although it is strongly recommended that you back up the SSL certificate when prompted.

```
-----  
CARBON BLACK ENTERPRISE SERVER - INITIALIZATION  
-----
```

```
Thank you for installing Carbon Black Enterprise Server. This tool will  
guide you through a few setup steps which are necessary in order to finalize  
the installation of the server.
```

```
-----  
END USER LICENSE AGREEMENT  
-----
```

```
Please, review and accept the End User License Agreement before proceeding  
with the server setup
```

```
Hit 'return' to open the agreement and 'q' when you're done reading it:
```

```
<AGREEMENT>
```

```
Do you accept the license agreement [yes/no]: yes
```

```
-----  
STORAGE LOCATION  
-----
```

```
Please choose a data storage location with as much space as possible. If  
needed, refer to the Carbon Black Data Storage Guidelines document.
```

```
Enter path for data storage location [/var/cb/data]: (Pressed enter)
```

```
You picked: /var/cb/data
```

```
-----  
ADMINISTRATOR ACCOUNT  
-----
```

```
Here you configure your GLOBAL ADMINISTRATOR account.  
This account is the most powerful account on the server.
```

```
Be sure to put a valid e-mail address if you want to take full advantage  
of Carbon Black's notification system.
```

```
Verify Account Information...
```

```
Username: bsmith  
First Name: Bill  
Last Name: Smith  
E-Mail: bsmitht@my.org  
Password:  
Confirm password:
```

Appendix A: Installing the Carbon Black Enterprise Server

Verify Account Information:

Username: bsmith
First Name: Bill
Last Name: Smith
E-Mail: bsmith@my.org
Is this correct [Y/n]: y

SENSOR COMMUNICATIONS

You need to configure the address that the sensors will talk to. This needs to be an ip-address or domain name that is reachable by the sensor machines.

This can be different per sensor-group and can be changed later, but it is easiest if you put in the valid address now.

Default sensor group server URL: https://192.123.45.123:443

Would you like to keep the default [Y/n]:

HELP IMPROVE YOUR CARBON BLACK EXPERIENCE

We are constantly looking for ways to make the Carbon Black user experience better. Please help us achieve this goal by allowing automatic reporting of usage, resource, and sensor statistics to our technology and support teams.

You can later change your mind, too, by going here:

>>> Administration -> Sharing Settings

Do you want your Cb Server to submit statistics and feedback information back to Bit9? [Y/n]:

BIT9 ALLIANCE

Be notified of any binary flagged by VirusTotal. Information such as the filename, MD5 hash and parent process will be shared with the Bit9 Alliance partners, including VirusTotal.

All information is anonymized to the extent reasonably practicable before being shared with Bit9 Alliance partners. The applicable terms and conditions are set forth in and subject to your Bit9 License Agreement. For further information on what information is collected and shared by the Bit9 Alliance Server, please visit <http://carbonblack.com/collaboration>.

You can change this setting at any time in the Carbon Black web console:

>>> Administration -> Sensors -> Edit Settings (for a particular group)

Carbon Black User Guide

If you enable this, you will then be prompted to either enable or disable the uploading of unknown binaries.

Do you want the default sensor group to have Bit9 Alliance connectivity enabled? [Y/n]:

Detect new variants of known malware by sharing the full binary content of unknown executable files. Binaries will be uploaded and shared with the Bit9 Alliance partners, including VirusTotal. Any binary submitted to the Bit9 Alliance is deleted on the local Carbon Black server, saving disk space.

All information is anonymized to the extent reasonably practicable before being shared with Bit9 Alliance partners. The applicable terms and conditions are set forth in and subject to your Bit9 License Agreement. For further information on what information is collected and shared by the Bit9 Alliance server, please visit <http://carbonblack.com/collaboration>.

You can change this setting at any time in the Carbon Black web console:

```
>>> Administration -> Sensors -> Edit Settings (for a particular group)
```

Do you want the default sensor group to submit unknown binaries to the Bit9 Alliance? [y/N]: y

Please confirm that you want to scan unknown binaries with VirusTotal [y/N]: y

```
-----  
SECURITY - SSL CERTIFICATE GENERATION  
-----
```

Generating self-signed HTTPS Server certificate...

Generating self-signed HTTPS Sensor CA certificate...

Carbon Black Enterprise Server uses a SSL certificate to establish secure communications between sensors and the server.

Should the certificate and/or its private key be lost, sensors will no longer be able to communicate with the Enterprise Server.

We recommend backing up the SSL certificate files at this time by running:

```
/usr/share/cb/cbssl backup --out <backup_file_name>
```

IMPORTANT: Backup file must be securely stored. Anyone with access to the information contained in that file will be able to compromise the security of sensor-server communications and potentially compromise the security of the computers on which the sensors run.

Continue [return]:

SECURITY - IPTABLES CONFIGURATION

Carbon Black Enterprise Server listens on a number of TCP/IP ports. If iptables firewall is running on the host machine, iptables must be configured to allow incoming connections on these ports.

To get a list iptables rules that need to be added to current host configuration, you can run `"/usr/share/cb/cbcheck iptables -l"` at any time and apply the rules manually. Alternatively, Carbon Black Server setup and configuration tools can take over management of iptables configuration and apply updates whenever they are needed.

Would you like Carbon Black Server to manage iptables [Y/n]:

Applying iptables rules:

```
-I INPUT 5 -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
```

iptables: Saving firewall rules to /etc/sysconfig/iptables:[OK]

SETTING UP POSTGRESQL DATABASE

Initializing Carbon Black Server PostgreSQL Instance...

The files belonging to this database system will be owned by user "cb". This user must also own the server process.

The database cluster will be initialized with locale "en_US.UTF-8". The default text search configuration will be set to "english".

Data page checksums are disabled.

```
creating directory /var/cb/data/pgsql ... ok
creating subdirectories ... ok
selecting default max_connections ... 100
selecting default shared_buffers ... 128MB
creating configuration files ... ok
creating template1 database in /var/cb/data/pgsql/base/1 ... ok
initializing pg_authid ... ok
setting password ... ok
initializing dependencies ... ok
creating system views ... ok
loading system objects' descriptions ... ok
creating collations ... ok
creating conversions ... ok
creating dictionaries ... ok
setting privileges on built-in objects ... ok
creating information schema ... ok
loading PL/pgSQL server-side language ... ok
vacuuming database template1 ... ok
copying template1 to template0 ... ok
copying template1 to postgres ... ok
syncing data to disk ... ok
```

Carbon Black User Guide

Success. You can now start the database server using:

```
/usr/pgsql-9.3/bin/postgres -D /var/cb/data/pgsql  
or  
/usr/pgsql-9.3/bin/pg_ctl -D /var/cb/data/pgsql -l logfile start
```

```
waiting for server to start.... done  
server started  
Creating core model DB schema...  
Creating alliance model DB schema...  
waiting for server to shut down.... done  
server stopped
```

```
-----  
SETUP COMPLETE!  
-----
```

Server setup has COMPLETED successfully.

Do you want to start the services [Y/n]:

Upgrading a Carbon Black Enterprise Server

If you are upgrading the server, the procedure varies depending upon whether you are upgrading a standalone server or a clustered server, and whether the database schema or alliance feed data must be migrated after the new server version is installed.

To upgrade a standalone server:

1. On the server, stop the Carbon Black services:
service cb-enterprise stop
2. Update the Carbon Black services:
yum update cb-enterprise
3. Restart the Carbon Black services:
service cb-enterprise start

To upgrade a clustered server:

1. On the Master server, navigate to the cb install directory (defaults to /usr/share/cb) and stop the Carbon Black services:
cbcluster stop
2. Update the Carbon Black services on all nodes:
yum update cb-enterprise
3. Restart the Carbon Black services:
cbcluster start

Improvements of Carbon Black will occasionally require a utility called `cbupgrade` to be used after `yum update cb-enterprise` to migrate the database schema or alliance feed data. The operator will be notified of this requirement when attempting to start the `cb-enterprise` services. In a clustered Server configuration, this utility will need to be run on all nodes before restarting the cluster. When running this utility in a clustered environment, be sure to answer 'NO' when asked to start the CB services, the administrator will need to use `cbcluster` to start the clustered server.

Server Upgrades and New Sensor Versions

A new server version might include a new sensor version. Please check the Release Notes or contact support@bit9.com if there are any questions about this.

If a new sensor version is included, you will need to decide whether you want the new sensor to be deployed immediately to existing sensor installations, or if you want to install only server updates. See [Chapter 5, “Installing and Managing Sensors,”](#) for platform-specific sensor upgrade instructions.

Server Troubleshooting

Server logs are found at `/var/log/cb`. Logs are organized into subdirectories by component, as described in [Table 34](#).

Table 34: Carbon Black Server Logs

Component	Description
allianceclient	The Alliance Client communicates with the Carbon Black Alliance server, and allows for notifications of VirusTotal alerts among other capabilities.
cbfs-http	The core event data processing component. This component manages incoming event data from the sensors, indexes, and stores the data.
coreservices	Provides access to functionality via web APIs to both the web UI and to sensors. Nearly all UI issues should result in log entries for coreservices.
job-runner	The Carbon Black server uses cron jobs to provide various scheduled maintenance, data trimming, and similar tasks.
pgsql	The Carbon Black server uses Postgres SQL to store administrative data. Event data gathered from the sensors is not stored in Posgres.

[Table 35](#) shows troubleshooting scripts found in `/usr/share/cb`.

Table 35: Carbon Black Diagnostic Scripts

Script	Description
cbdiag	Dumps verbose troubleshooting information, including logs and configuration, to a gzip archive. This file can be analyzed offline or provided to Carbon Black with support requests.
sensor_report	Generates a log of all registered sensors, with an emphasis of calling out error conditions.
cbpasswd	Resets a user's password. Can only be run as root.

Appendix B

Integrating Carbon Black with a Bit9 Server

This chapter describes the procedure for integrating a Carbon Black Enterprise Server with a Bit9 Platform Server. It also describes the features available when this integration is active, and general features that contribute to the coexistence of the Carbon Black Sensor and the Bit9 Agent on the same computer.

Sections

Topic	Page
Overview	206
Activating Carbon Black-Bit9 Server Integration	207
Creating a Carbon Black User for Integration	207
Configuring and Activating the Integration	209
Viewing Integration Settings in Carbon Black	212
Server Integration Features in the Bit9 Console	213
Correlation of Exported Data	218

Overview

Carbon Black provides powerful features for endpoint threat detection and response. The Bit9 Platform provides its own powerful features for endpoint threat protection.. Both solutions have been engineered to allow you to take advantage of the their complementary features by installing both the Carbon Black Sensor and the Bit9 Agent on your endpoints and adding Carbon Black features inside the Bit9 Platform to improve your security posture..

Note

In addition to integrating with each other, both Carbon Black and the Bit9 Platform can take advantage of the Bit9 Threat Intelligence Cloud, which provides reputation information, threat indicators, and attack classification intelligence. See [Chapter 10, “Threat Intelligence Feeds,”](#) for more information on the Threat Intelligence Cloud.

Built-in Compatibility Features

The Bit9 Agent recognizes the Carbon Black Sensor and reports its presence to the Bit9 Server. The server has many optimizations to allow efficient operation of both the Bit9 Agent and the Carbon Black Sensor on the same endpoint. These include:

- **Performance Optimizations** – Internal performance optimizations nearly eliminate any performance impact on either product from having the other product’s agent or sensor installed.
- **Trust for Sensor Updates** – An Updater rule allow seamless installation and upgrades of Carbon Black sensors that would otherwise have been blocked by a Bit9 Agent in Medium and High enforcement modes. See “Approving by Updater” in the Bit9 Console help for more information about updater rules.
- **Publisher Trust for Carbon Black** – A Publisher rule in Bit9 trusts by default files that are identified as being from the publisher “Carbon Black, Inc.”. See “Approving or Banning by Publisher” in the Bit9 Console help for more information about publisher rules.
- **Server Integration Interface** – The Licensing tab on the Bit9 System Configuration page includes a Carbon Black tab that can be used to activate integration with a specific Carbon Black server. Step-by-step instructions are detailed in [“Activating Carbon Black-Bit9 Server Integration”](#) on page 207. The features associated with this integration are listed in the following section.

Features when Servers are Integrated

Additional Bit9-Carbon Black integration features become available when you explicitly configure the two servers to work with each other. The majority of these features involve making information from and about Carbon Black available in the Bit9 Console:

- **Carbon Black Sensor Details in Bit9 Console** – Pages displaying details about a computer running the Bit9 Agent will show whether the Carbon Black Sensor is installed, and if so, the version and status of the sensor.
- **Carbon Black File Statistics in Bit9 Console** –Pages displaying details about a file found on a computer running the Bit9 Agent will show Carbon Black statistics about

the file, such as how many watchlists it is on, the number of computers and processes in which the file has been seen, and the number of network connections.

- **Links to the Carbon Black server in Bit9 Console** – Menu and inline links from the Bit9 Console events table, computer details and files details pages connect to the Carbon Black data for the object being viewed.
- **Bit9 Agent Status in Carbon Black Console** – In the Carbon Black console, the Host Information page for each Windows computer running a sensor reports whether a Bit9 Agent is installed.
- **Process Data Correlation** – A globally unique process identifier called a *Process Key* makes it possible to know when events on a Carbon Black server and a Bit9 Server are referencing the same process. It uniquely identifies an individual instance of this process running. This identifier is available in Syslog output as well as data exported for third-party analysis tools such as Splunk.

See “[Server Integration Features in the Bit9 Console](#)” on page 213 for more details on integration features.

Activating Carbon Black-Bit9 Server Integration

The configuration settings for a Carbon Black-Bit9 Server integration appear in both the Carbon Black console and the Bit9 Console. The configuration must be done on the System Configuration page/Licensing tab on the Bit9 Server. Configuration may be *viewed* on the Carbon Black server once the integration has been set up.

Creating a Carbon Black User for Integration

If you do not already have a user that you plan to use for Bit9 Platform integration, follow the procedure below. Note that this user must have Global administrator privileges.

To create a Bit9 Integration user and API Token:

1. In the Carbon Black console main menu, choose **Administration > Users**.
2. On the Users page, click the **Add User** button. The Add user page appears.

3. On the Add user dialog, define the user you will use for the integration:
 - a. In the Username field, enter **bit9integration** or some similar name that clearly indicates the purpose of the account.
 - b. Use the First Name and Last Name fields to provide a useful display name; this will appear in the Carbon Black console for this user. For example, you could use **Bit9** as the first name and **Integration** as the Last name.
 - c. Provide an email account for the user. An email account is required for Carbon Black console users. For this account, however, the account can be fictitious since it is not going to be used as it would be for a normal user.
 - d. Enter and confirm a password for the user. Have this password available for logging in as the new user.
 - e. In the *Assign to* panel, check the **Administrators** box to assign this user to the Administrators team.
 - f. Check the **Global administrator** box below the *Assign to* panel.
 - g. When you have entered all the required information, click the **Save changes** button.
4. Log out of the Carbon Black console.

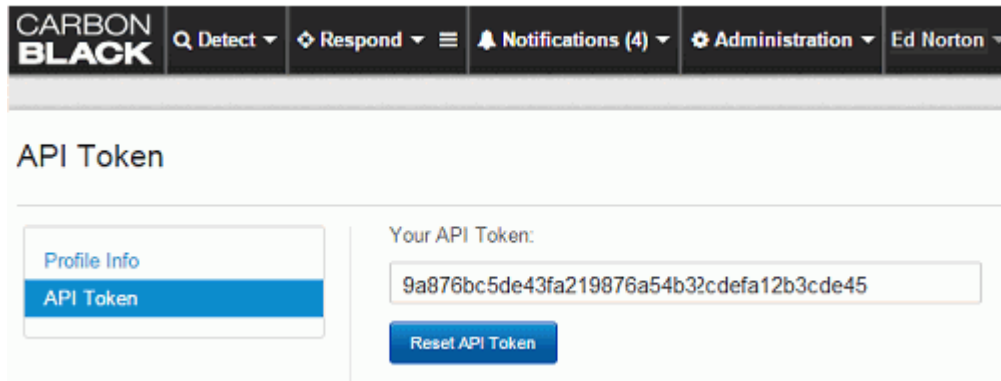
Configuring and Activating the Integration

Review the information in [Table 36](#) to prepare for setting up the integration on the Bit9 Server. This is the information you will need to provide.

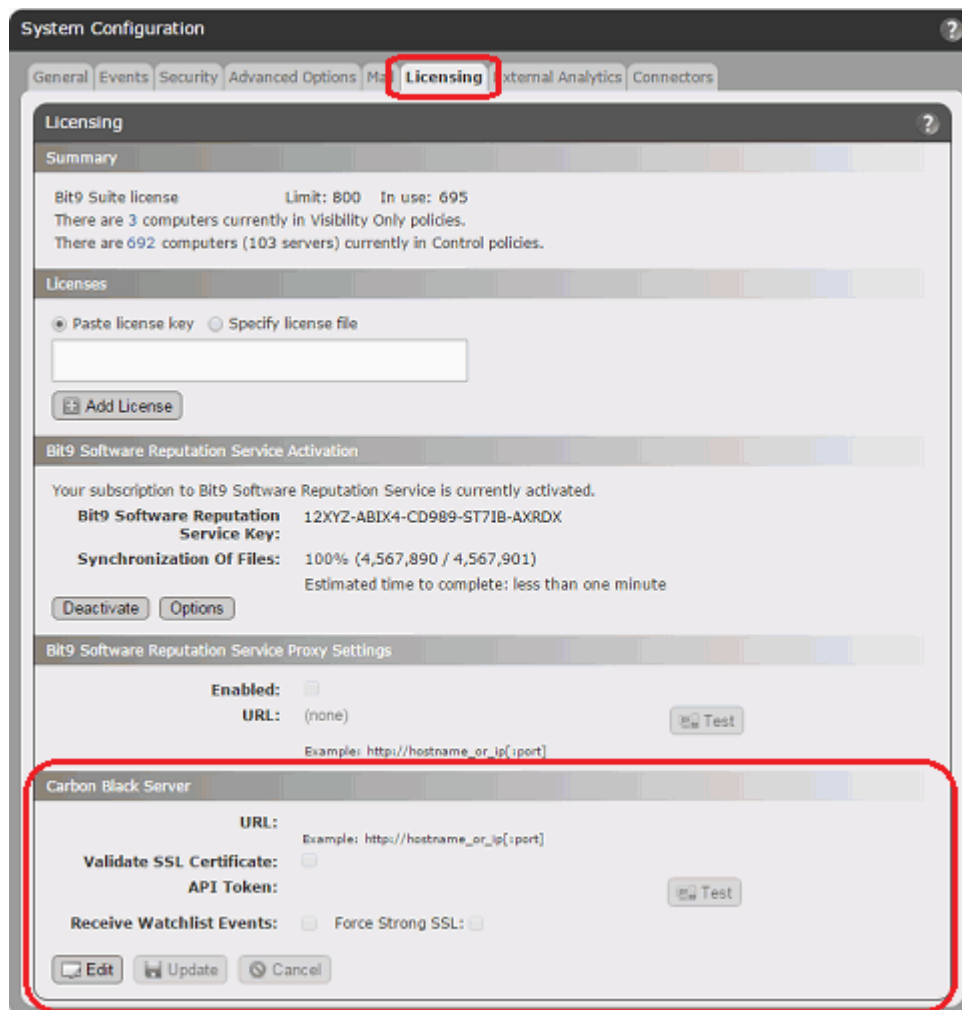
The following procedure describes using two browsers. You also could copy information out of the Carbon Black configuration into a text editor in preparation for pasting it into the Bit9 Console.

To activate Carbon Black-Bit9 Platform Server integration:

1. On the Carbon Black console, log in with the integration user account.
2. When you are logged in, in the Carbon Black Console menu, choose *username* > **Profile info**.
3. On the My Account page, choose **API Token** on the left menu.



4. On the API Token page, copy the string in the **Your API Token** box.
5. Open another browser and log into the Bit Console using an account with Administrator privileges.
6. In the Bit9 Console menu, choose **Administration > System Configuration**.
7. On the System Configuration page, click the **Licensing** tab. The Carbon Black server panel is at the bottom of page when the Licensing tab is displayed.



8. Enter the Carbon Black configuration settings as shown in [Table 36](#).

Table 36: Settings on the Bit9 Server for Carbon Black Integration

Field/Button	Description
URL	The URL of the Carbon Black server you want to link to the Bit9 Server. Port is only necessary if you do not use standard ports on the Carbon Black server (80 for HTTP and 443 for HTTPS). You can copy the base URL (without any page-specific additions) from the Carbon Black browser and paste it into the relevant section of the Bit9 configuration page – for example, <i>https://cbserver.mycompany.local</i> .
Validate SSL Certificate	Checking this box causes a validity check on the Carbon Black server certificate. This should be checked only if the Carbon Black server certificate is issued by a trusted certificate authority. Without manual configuration, Carbon Black uses a self-signed certificate and so this generally should not be checked.

Table 36: Settings on the Bit9 Server for Carbon Black Integration (continued)

Field/Button	Description
API Token	You enter the Carbon Black server API Token here by copying it from the Carbon Black console. Click the Test button to confirm that the server is accessible and the key works. The test returns one of the following values: <ul style="list-style-type: none"> • Success, version: <Carbon Black product version> • Invalid API Token • Server not accessible.
Receive Watchlist Events	Checking this box activates delivery of Carbon Black watch list events from the configured server to the Bit9 Server.
Force Strong SSL	Checking this box causes the Carbon Black server to check the Bit9 Server certificate before sending events. This should not be checked if your server uses a self-signed Bit9 certificate on IIS.

9. Click the **Test** button to determine whether the servers are able to communicate. Possible causes of failure their troubleshooting steps are:
- **Invalid API Token** -- Make sure that the API token for the Bit9 user is has been copied correctly from the Carbon Black console and pasted into the configuration page on the Bit9 console. Also make sure that this user is an administrator and has global administrator privileges.
 - **Server not accessible** -- Confirm that the correct URL and port number (if needed) has been entered in the configuration page on the Bit9 console, and that the Validate SSL certificate box was not checked when you are using a self-signed certificate. Also make sure that access to the Carbon Black server is not blocked by the network firewall.
 - **Force Strong SSL** -- Checking this box causes the Carbon Black server to check the Bit9 Server certificate before sending watchlist events. This should be checked only if the Bit9 console certificate is issued by a trusted authority (e.g. not self-signed).

If you are unable to create a successful connection, contact Bit9 Technical Support.

10. When you have entered and successfully tested the Carbon Black server settings in the Bit9 Console, click **Update** on the System Configuration/Licensing page. The configuration should be complete and your servers should be integrated.

Viewing Integration Settings in Carbon Black

In the Carbon Black Console, you can view the current Bit9 Platform integration settings on the Bit9 Platform Server page.

To view Bit9 Platform integration settings in the Carbon Black console:

1. In the Carbon Black console menu, choose **Administration > Settings**.
2. In the left menu, choose **Bit9 Platform Server Settings**.
The Bit9 Platform Server settings page appears, showing the current integration settings (if any).

Note

You may change the Watchlist and SSL settings in the Carbon Black Console, but although the fields appear editable, you may not change the URL or API Token parameters here. If these need to be modified, use the Bit9 Console.

To view Bit9 Platform integration status in the Carbon Black console:

1. In the Carbon Black console menu, choose **Administration > Server Dashboard**.
The status of the Bit9 Platform Server connection is shown in the Server Communication Status panel, in the upper right of the page.
2. There are three possible statuses. You may need to take additional steps depending upon the status:
 - a. **Bit9 Platform Server is connected** – This status indicates that the integration has been configured and the connection is currently functioning properly.
 - b. **Bit9 Platform Server not configured** – If the Bit9 Server connection has not been configured, a **Settings** button appears in the status line for the connection. Do not use this button. Keep in mind that you cannot configure the API Token or URL on this page – they must be entered in the Bit9 Console itself.
 - c. **Unable to connect to Bit9 Platform Server** – This status may indicate network or firewall problems, bad URL or port configuration. It can also occur if Force Strong SSL was chosen on the Bit9 console System Configuration page for Carbon Black when a self-signed certificate is being used on the Bit9 console.

Regenerating the Authorization ID for Server Communication

The Bit9 Server creates a hidden token that the Carbon Black server uses to send back Watchlist hits. This token is not visible in the console of either product, but can be retrieved from the database. It can also be entered manually on Carbon Black side for diagnostic purposes. If you believe this token was compromised, or if your configuration stops working -- for example, because the Carbon Black server lost the token due to a reinstall or a manual token change -- you can regenerate a new key.

To regenerate the authorization key for server communications:

1. In the Bit9 Console, choose **Administration > System Configuration** and click the **Licensing** tab.
2. In the Carbon Black Server panel, uncheck the **Receive Watchlist Events** box and click the **Update** button.
3. Check the **Receive Watchlist Events** box and click the **Update** button. A new key is generated.
4. Verify on both servers that there is a successful connection between the Bit9 Server and the Carbon Black server.

Server Integration Features in the Bit9 Console

Sensor Information

If you integrate the Bit9 Server with the Carbon Black Enterprise Server, Bit9 Console pages that show computer information include Carbon Black Sensor details when available.

To view a table of Bit9-managed computers also running a Carbon Black Sensor:

1. In the console menu, choose **Assets > Computers**. The Computers page appears.
2. On the Saved Views menu, choose **Carbon Black Deployments** to see computers grouped by whether they have had a Carbon Black Sensor installed on them. This table also shows the Carbon Black Sensor version and its current status.

You also can click the View Details button for any computer in this view to see more Carbon Black Sensor details on the Computer Details page for any computer. The Carbon Black panel on this page reports the presence, version and status, and other details of any Carbon Black Sensor found on a computer running the Bit9 Agent. If a Carbon Black server is not configured or the computer is not running a Carbon Black sensor, this tab shows only a status of *Not installed*. By default, the Bit9 Server checks Carbon Black status every 30 minutes.

The Carbon Black panel of the Computer Details page also provides a **More information** link to the Sensors page of the Carbon Black Console. You also can use the **Carbon Black Details** link in the Related Views menu to go to the Carbon Black Console.

Bit9 Platform Console: Computer Details Page with Carbon Black Tab

The screenshot shows the 'Computer Details' page in the Bit9 Platform Console. The page is divided into several sections:

- General:**
 - Computer Name: MYCORP\Server-4
 - IP Address: fe20::8cc:9ccc:3120:2812
 - Connection Status: Connected
 - Health Check: Passed
 - Platform: Windows
 - Description: [Empty text box]
 - Computer Tag: [Empty text box]
- Policy:**
 - Policy: Medium
 - Policy Mode: Control
 - Connected Enforcement: Medium (Prompt Unapproved)
 - Disconnected Enforcement: Medium (Prompt Unapproved)
- Navigation Tabs:** Bit9 Agent, Connection History, Policy Override, System Details, AD Details, **Carbon Black** (selected)
- Carbon Black Tab Content:**
 - Sensor Version: 4.2.0.40325
 - Last Status: Running
 - Uptime: 118 minutes(s)
 - Computer Status: Online
 - Registration Time: Apr 07 2014 02:18:48 PM
 - Last Checkin: Apr 07 2014 04:16:49 PM
 - Next Checkin: Apr 07 2014 04:17:19 PM
 - [More information](#)
- Related Views (Right Sidebar):**
 - Recent Events
 - Health Check Events
 - Files on this Computer
 - Carbon Black Details
- Actions (Right Sidebar):**
 - Change Policy [Dropdown]
 - Delete Computer
 - Prioritize Updates
 - Add Files to Snapshot [Dropdown]
- Advanced (Right Sidebar):**
 - Convert to Template
 - Set Debug Level [Dropdown]
 - Configure Agent Dumps [Dropdown]
 - Reset CLI Password
 - Disable Tamper Protection
 - Change Local State [Dropdown]
 - Perform Cache Consistency Check [Dropdown]
 - Other Actions [Dropdown]

Table 37 describes the information available on the Carbon Black tab for Bit9 File Details pages.

Table 37: Fields on the Carbon Black tab of the Bit9 Computer Details page

Field	Description
Sensor Version (Carbon Black Version in table)	The version of the Carbon Black sensor installed on this computer.
Carbon Black Status (in table) Last Status (on Details page)	<p>This field shows the last Carbon Black sensor status for this computer, as reported by the Bit9 Agent to the Bit9 Server. The Bit9 Server checks Carbon Black status every 30 minutes, and so status changes may be out of sync for up to that amount of time.</p> <p>The possible values for Carbon Black Status in the table are:</p> <ul style="list-style-type: none"> • Unknown • Installed, initializing – sensor is installed but not fully initialized • Installed, running • Installed, not running • Not installed • Stopped <p>On the Details page, the Last Status field on the Carbon Black tab is similar to Carbon Black Status in the table. However, it does not appear if sensor status is Unknown. Its possible values are:</p> <ul style="list-style-type: none"> • Running • Service not running • Kernel not running • Stopped <p>Notes: In addition to up to a 30-minute gap between sensor installation and Bit9 polling of Carbon Black status, status will continue to report as <i>Not installed</i> until the Carbon Black sensor connects to the Carbon Black server and receives a sensor id. Also, if the Bit9 Agent is offline or uninstalled from a computer, the last Carbon Black sensor status reported by the agent is displayed in the Bit9 Console, even if sensor status changes.</p>
Uptime	Number of minutes and hours that the Carbon Black sensor has been running since it was last started.
Computer Status	The status of this computer as reported by the Carbon Black server.
Registration Time	The date and time the Carbon Black sensor on this computer registered with its server.
Last Checkin	The date and time the Carbon Black sensor on this computer last checked in with its server.
Next Checkin	The date and time of the next scheduled server checkin for the Carbon Black sensor on this computer.
More Information	<p>Connects to the login page of the Carbon Black server configured on the System Configuration page Licensing tab. Logging in takes you to the Sensors page in Carbon Black so you can view additional details about this computer.</p> <p>Note: You must have valid login credentials for the Carbon Black server to successfully open the Carbon Black console.</p>

File and Process Information

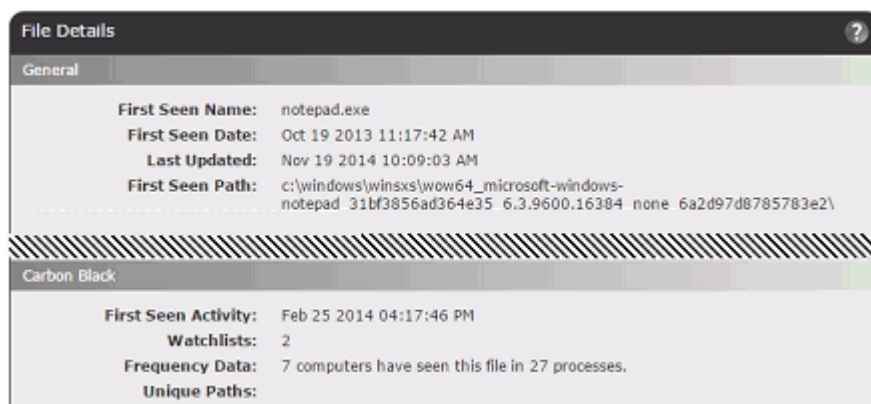
On Bit9 Console pages that show file details, Carbon Black statistics about the file, such as how many watchlists it is on and the number of computers and processes in which the file has been seen, are shown if available.

Note

Carbon Black process information is available to the Bit9 Platform from Windows sensors only. It is not be available in Bit9 from the Carbon Black OSX and Linux sensors.

To view a details for a file found on a Bit9-managed computer:

1. In the console menu, choose **Assets > Files**. The Files page appears.
2. On the Files page, click the **File Catalog** tab to view a table of unique files discovered on computers managed by this Bit9 Server. Note that you can also choose Files on Computers if you prefer to view a table of all file instances.
3. When you find the file whose details you want to view, click the View Details icon (file and pencil) on the left of that files row. The File Details page opens.



Bit9 Platform File Details Page: Carbon Black Panel

Table 38: Carbon Black fields on Bit9 File/File Instance Details pages

Field	Description
First Seen Activity	The date and time when activity involving this file was first reported to the Carbon Black server
Watchlists	The number of Carbon Black watchlists on which this file appears. This appears if Watchlist export is configured on the Bit9 System Configuration page for Carbon Black.
Frequency Data	The frequency of the file is the number of endpoints that have this file associated with a process. The number of processes is the count of all processes that have been associated with this file.
Unique Paths	The number of unique paths in which this file has been seen

Table 38: Carbon Black fields on Bit9 File/File Instance Details pages (continued)

Field	Description
VirusTotal Score	If available, the VirusTotal score for this file and the date and time of the analysis
Network Connections	Whether there have been any network connections associated with this file, and if so, on how many computers.
Registry Modifications	Whether there have been any registry modifications associated with this file, and if so, on how many computers.
File Icon	The icon for this file (if any)
More information	Link to the Carbon Black Console page showing more information about this file (from the File Details page) or a particular instance of this file on a particular computer (from the File Instance Details page). See “Links to the Carbon Black Console” on page 218.

Event Information

The Bit9 Console Events page can display two different Carbon Black-related event subtypes: *Carbon black sensor status* and *Carbon black watchlist*. Carbon Black events may be seen in unfiltered views of the events table, but there is also a Saved View for Carbon Black events.

To view Carbon Black-related events in the Bit9 Console:

1. In the console menu, choose **Reports > Events**. The Events page appears.
2. On the Saved Views menu, choose **Carbon Black**. The illustration below shows this view with its filters displayed.

The screenshot shows the Bit9 Console Events page. At the top, there is a 'Saved Views' section with a dropdown menu set to 'Carbon Black' and an 'Add' button. To the right, there is a 'Group By' section with a dropdown menu set to '(none)' and a 'Ascending' dropdown. Below these are links for 'Show/Hide Filter', 'Show/Hide Columns', 'Export to CSV', 'Access Event Archives', and 'Refresh Page'. A 'Filters' section is visible, showing 'Add filter' and two active filters: 'Subtype is Carbon Black watchlist' and 'Carbon Black sensor status'. There are 'Apply', 'Cancel', and 'Reset' buttons. Below the filters is an 'Action' dropdown and a table of events. The table has columns for 'Timestamp', 'Priority', and 'Description'. The events listed are:

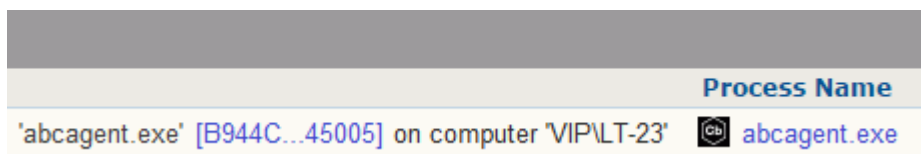
Timestamp	Priority	Description
Dec 15 2014 09:19:24 PM	Notice	Carbon Black process watchlist 'Non-System Filemods to system32' hit for process 'dpir
Dec 15 2014 09:18:39 PM	Notice	Carbon Black process watchlist 'Non-System Filemods to system32' hit for process 'pari
Dec 15 2014 09:17:22 PM	Notice	Carbon Black process watchlist 'Non-System Filemods to system32' hit for process 'pari
Dec 15 2014 09:14:34 PM	Notice	Carbon Black binary watchlist 'Newly Loaded Modules' detected file 'c:\windows\syswow
Dec 15 2014 09:14:34 PM	Notice	Carbon Black binary watchlist 'Newly Loaded Modules' detected file 'c:\windows\syswow
Dec 15 2014 09:14:04 PM	Notice	Carbon Black binary watchlist 'Newly Executed Applications' detected file 'c:\program fi
Dec 15 2014 03:42:48 PM	Info	Carbon Black Sensor Version '5.0.0.41211' installed and 'Running'.
Dec 15 2014 03:45:16 PM	Info	Carbon Black Sensor Version '5.0.0.41211' installed and 'Running'.

Both process and binary watchlist event are exported to Bit9 from Carbon Black (when export is activated). For process watchlist events, you can add a column to display the unique Process Key ID that correlates process information between Bit9 and Carbon Black. See [“Correlation of Exported Data”](#) on page 218 for more information.

When Carbon Black watchlist hits appear in the Bit9 Platform Events table, the watchlist name appears in the Rule Name and Description fields of the table.

Links to the Carbon Black Console

Where Carbon Black information is displayed in the Bit9 Console, there is often a link back to the relevant location in the Carbon Black Console. The link is identified with the Carbon Black logo and uses the server URL provided in the Carbon Black server section of the Bit9 System Configuration page. The following example from the Events page shows how such a link appears.



In other cases, there may be a menu link on a page to [“Carbon Black Details”](#).

When a user clicks one of these links, the Carbon Black login screen is displayed first, and the user must provide a Carbon Black login account and password there. Once the login information is provided, the linked page is displayed. If this browser remains open, the login credentials stay active for 90 minutes, and so any subsequent use of links during this period will go directly to the relevant page.

Correlation of Exported Data

[“File and Process Information”](#) on page 216 describes how file and process data correlation is used inside the Bit9 Console. Both the Carbon Black Enterprise Server and the Bit9 Server also make event data available for external use. Users with both Carbon Black and the Bit9 Platform may want to correlate or analyze data from both sources.

To facilitate this, events that include process data have a “Process Key”, a unique identifier for each process. The process key is available in the following locations and ways:

- Syslog output from the Carbon Black server (See [Appendix E, “Syslog Output for Carbon Black Events.”](#))
- Syslog output from the Bit9 Server
- Carbon Black API queries (See [Appendix D, “Carbon Black APIs.”](#))
- Bit9 Live Inventory SDK/Public API queries
- Data exported specifically for Splunk from the Bit9 Server
- External event exports and event archives from the Bit9 Server
- Carbon Black email alerts ([“Enabling Email Alerts”](#) on page 189)

See the Bit9 console online help or *Using the Bit9 Security Platform* for information about the Bit9 features listed above.

Appendix C

Network Integrations for Feeds

Indicators of compromise are reported to the Carbon Black server on the Threat Intelligence Feeds page and added to endpoint file and process data. These feeds may be added to the Carbon Black server several different ways:

- **Alliance Feeds/Threat Intelligence Cloud** -- Feeds from Bit9 and third-party partners in the Carbon Black Alliance are provided to the Carbon Black server through the Bit9 + Carbon Black Threat Intelligence Cloud. See [Chapter 10, “Threat Intelligence Feeds,”](#) for instructions on enabling these feeds.
- **Manually Added Feeds** -- You can create a feed and manually add it on the Threat Intelligence Feeds page by providing a URL and configuration information. See <https://github.com/carbonblack/cbfeeds> for instructions on creating a feed.
- **Network Integrations** -- You can add a feed based on a network integration to a local or cloud-based third-party device. Integrations use a separately installed, out-of-band bridge provided by Carbon Black to push IOCs as a feed to the Carbon Black server.

Feeds from network integrations report IOCs based on the capabilities of their devices. For example, one integration might report suspicious network traffic activity while another one reports the results of binary detonations. Some integrations also send metadata from the Carbon Black server back to the connected device or service.

Integration Documents on the Customer Portal

For this release, documentation about the Carbon Black third-party integrations is available on the Bit9 + Carbon Black customer portal at <https://bit9.com/customer-portal>.

The available documents are:

- **Network Integration Checkpoint** ([network_integration_checkpoint.pdf](#)) -- This document describes Carbon Black integration with an on-premise Check Point device for correlating Check Point alerts with Carbon Black collected data.
- **Network Integration Fidelis** ([network_integration_fidelis.pdf](#)) -- This document describes the bi-directional Carbon Black integration with an on-premise Fidelis device for correlating Fidelis alerts in the Carbon Black enterprise server and returning Carbon Black metadata to Fidelis.
- **Network Integration FireEye** ([network_integration_fireeye.pdf](#)) -- This document describes Carbon Black integration with an on-premise FireEye device for correlating FireEye alerts with Carbon Black collected data.
- **Network Integration LastLine** ([network_integration_lastline.pdf](#)) -- This document describes Carbon Black integration with the Lastline service for checking the reputation of certain binary files.
- **Network Integration Palo Alto WildFire** ([network_integration_paloalto_wildfire.pdf](#)) -- This document describes Carbon Black integration with the Palo Alto Wildfire cloud service for checking the reputation of certain binary files.
- **Threatconnect Connector** ([threatconnect_connector.pdf](#)) -- This document describes Carbon Black integration with ThreatConnect for retrieving indicators of compromise (IOCs) from specified communities.

Appendix D

Carbon Black APIs

Carbon Black includes extensive support for programmatic access to the underlying data and configuration via APIs. Documentation, example scripts, and a helper library for each of these libraries is available at:

<https://github.com/carbonblack/cbapi>

There are three primary APIs:

- **Carbon Black Client API (CBCAPI)** – The CBCAPI is a collection of documentation, example scripts, and a helper library to allow for querying the backend data store and getting and setting configuration. This is the same API that the Carbon Black web console uses to interface with the Carbon Black server. The specific URL for this API is:
https://github.com/carbonblack/cbapi/tree/master/client_apis
- **Carbon Black Server API (CBSAPI)** – The CBSAPI is a collection of documentation, example scripts, and a helper library to help subscribe to Carbon Black server notifications, parse and understand the contents of those notifications, and demonstrate common business logic uses of those notifications. The specific URL for this API is:
https://github.com/carbonblack/cbapi/tree/master/server_apis
- **Carbon Black Feed API (CBFAPI)** – The CBFAPI is a collection of documentation, example scripts, and a helper library to help build and validate Carbon Black feeds. The specific URL for this API is:
<https://github.com/carbonblack/cbfeeds>

The Carbon Black API is versioned. A new API revision is released with each release of the Carbon Black Enterprise Server. Previous version documentation can be found using git tags.

Appendix E

Syslog Output for Carbon Black Events

Carbon Black logs the following events to syslog:

- **Watchlist hits** -- This event occurs when activity or binaries found on one of your endpoints matches a query in a Watchlist. See [Chapter 12, “Watchlists,”](#) for more information.
- **Feed hits** -- This event occurs when activity or binaries found on one of your endpoints matches an IOC reported by a Threat Intelligence Feed. See [Chapter 10, “Threat Intelligence Feeds,”](#) for more information.
- **Binary Information events** -- This event occurs when a process execution adds a binary to the Carbon Black database.

The program name prefix is `cb-notifications-`. By default, these events are written to log files at `/var/log/cb/notifications` on the Carbon Black server (based on the syslog configuration at `/etc/rsyslog.d/cb-coreservices`).

There is one file for all hits, one file for each watchlist and each feed. Per-file watchlists include the watchlist id in the program name and log file name, while per-file feeds include the feed id in the program name and log file name. Binary information events are logged in a separate file.

For example, the directory listing below contains four log files: one for all watchlist and feed hits, another for just hits to watchlist id 10, another for just hits to feed id 8, and a fourth one for all binary information events:

```
[root@localhost coreservices]# ll /var/log/cb/notifications/*.log
-rw-----. Jun 9 15:30 /var/log/cb/notifications/cb-all-
notifications.log
-rw-----. Jun 9 15:30 /var/log/cb/notifications/cb-
notifications-watchlist-10.log
-rw-----. Jun 9 18:02 /var/log/cb/notifications/cb-
notifications-feed-8.log
-rw-----. Jun 9 18:04 /var/log/cb/notifications/cb-
notifications-binaryinfo.log
```

Syslog Documentation on the Customer Portal

For this release, documentation about the Carbon Black syslog implementation is available on the Bit9 + Carbon Black customer portal. The URL for this site is:

<https://bit9.com/customer-portal>

The available documents are:

- **Syslog User Guide** (`syslog_cef_user_guide.pdf`)-- Describes how Carbon Black events can be accessed via syslog. In addition to information about where the files are written and how they are named, it provides syslog formats for Carbon Black output.
- **Syslog Integration Guide** (`Carbon Black HowTo - Carbon Black Syslog Integration.pdf`)-- Describes how to set up the Carbon Black server to send all or selected data to another device and how to set up the remote device to receive Carbon Black syslog output.

- ***Syslog Templates Developer Guide*** (syslog_templates_developer_guide.pdf) -- Describes how to use Carbon Black syslog templates to build custom-formatted syslog notifications on Watchlist and Feed hits and Binary Information events.
- ***Syslog CEF User Guide*** (syslog_user_guide.pdf) -- Describes how Carbon Black syslog output for Watchlists can be modified to match the ArcSight Common Event Format (CEF).

Appendix F

Additional Administration Documents

This appendix lists separate documents on the Bit9 + Carbon Black customer portal that address Carbon Black server and sensor administration topics. The URL for this site is:

<https://bit9.com/customer-portal>

Server Administration

- ***Cbinit Automation*** (cbinit_automation.pdf) -- This document describes how the Carbon Black Enterprise Server installation can be automated through the use of an 'answer file' for cbinit.
- ***Server Overview*** (server_overview.pdf) -- This document describes the Carbon Black technology stack, daemons, configuration and logs.
- ***Cb.Conf*** (cb.conf.pdf) -- This document describes the file /etc/cb/cb.conf, which is the primary server configuration file. Although there should normally be no need to modify this file, the configuration options listed here could be helpful when troubleshooting the server or tailoring the configuration for local integration.
- ***Server Changelog*** (server_changelog.pdf) -- This document describes the significant changes introduced in each release of the Carbon Black server.
- ***Server SSL*** (server_ssl.pdf) -- This document describes the use of SSL Certificates for authentication and confidentiality between the Carbon Black server and components used with it, including the yum repository, Alliance server, sensors, and the browser displaying the console. It includes the location and configuration of each certificate and some Frequently Asked Questions on certificate management.
- ***Server VDI Support*** (server_vdi_support.pdf) -- This document describes Carbon Black support for Virtual Desktop Infrastructure (VDI) environments. It includes information about keeping the same sensor ID for a Carbon Black sensor despite frequent re-imaging so that client event history is maintained.
- ***Single Sign On Integration*** (single_sign_on_integration.pdf) -- This document provides a summary of supported capabilities and steps needed to be taken in order to configure and troubleshoot Single-Sign-On integration with an external SAML 2.0-compliant identity provider.
- ***Server Predefined Watchlists*** (server_predefined_watchlists.pdf) -- This document describes how to add custom watchlists at server setup time.

Sensor Administration

- ***Sensor Changelog*** (sensor_changelog.pdf) -- This document describes the significant changes introduced in each release of the Carbon Black sensor.
- ***Sensor Troubleshooting*** (sensor_troubleshooting.pdf) -- This document includes several suggestions for troubleshooting the Carbon Black sensor.

