Carbon Black
Version 5.1.0 Patch 2
Release Notes

Carbon Black v 5.1.0.150914.1400
21 October 2015

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

Introduction

The *Carbon Black Version 5.1.0 Patch 2 Release Notes* document provides information for users upgrading from previous versions as well as users new to the product. It consists of the following major sections:

- **Before you begin**: This section describes preparations you should make before beginning the installation process for Carbon Black Server.
- **Carbon Black 5.1.0 new and modified features**: This section provides a quick reference to changes in Carbon Black since version 5.0.0 Patch 3.
- **Corrective content:** This section describes issues resolved by this release as well as more general improvements in performance or behavior.
- **Known issues and limitations:** This section describes known issues or anomalies in Carbon Black version 5.1.0 that you should be aware of.
- **Contacting Bit9 support:** This section describes ways to contact Bit9 Technical Support and the information to have prepared to troubleshoot a problem.

This document is a supplement to the main Carbon Black Product documentation.

Important information

We recommend that you review these release notes carefully, especially the *New and modified features* and *Known issues and limitations* sections.

Purpose of this release

This release contains *major new feature functionality* as well as quality and performance improvements.

Documentation

The standard user documentation for Carbon Black includes:

- **Carbon Black User Guide:** Describes Carbon Black feature functionality in detail.
- **Carbon Black - Enterprise Server Sizing Guide:** Provides details on infrastructure sizing for Carbon Black.
- **Carbon Black API**: Documentation for the Carbon Black API is located at https://github.com/carbonblack/cbapi.

Additional documentation for special tasks and situations is available on the Carbon Black customer support portal.

Before you begin

This section describes preparations you should make before beginning the installation process for the Carbon Black server. These include actions you should take before installing the Carbon Black server, preparations you should make for configuring the server after installation, and general information you should know about the server and sensor. It contains information that applies to upgrades and new installations.

YUM URL:

Please use caution when pointing to the YUM repository. Different versions of the product are available on different branches as shown below:

The current 5.1.0 version is available on Carbon Black YUM, pointed to by the following base URL:

baseurl=https://yum.carbonblack.com/enterprise/stable/x86_64/

The current 4.2.7 version is available on Carbon Black YUM, pointed to by the following base URL:

baseurl=https://yum.carbonblack.com/enterprise/release/x86_64/

System requirements

The document *Carbon Black - Enterprise Server Sizing Guide describes* the hardware and software platform requirements for the Carbon Black Server and provides the current requirements for systems running the sensor. Both are available in the customer support portal area of the Bit9 web site.

Both upgrade and new customers should be sure to meet the requirements specified in these documents before proceeding.

Carbon Black Server Installations and Upgrades

Carbon Black server upgrades are supported from the following Carbon Black server versions to this v5.1.0 version

- All 4.2.x versions
- All 5.0 versions, including earlier patch releases

For more detailed instructions for installing or upgrading the server, please refer to the *Carbon Black User Guide*. It is available on the Bit9 customer support portal. For upgrading from 4.1.x and earlier version, please call or e-mail Bit9 Technical Support.

Support for the upgrade process

Carbon Black Server and sensor upgrade support is covered under the Customer Maintenance Agreement. Bit9 recommends contacting Technical Support prior to performing the upgrade, for further details on the upgrade process and the latest information that supplements the information contained in this document. Technical Support is available to assist with the upgrade process to ensure a smooth and efficient upgrade installation.

Before running the server upgrade

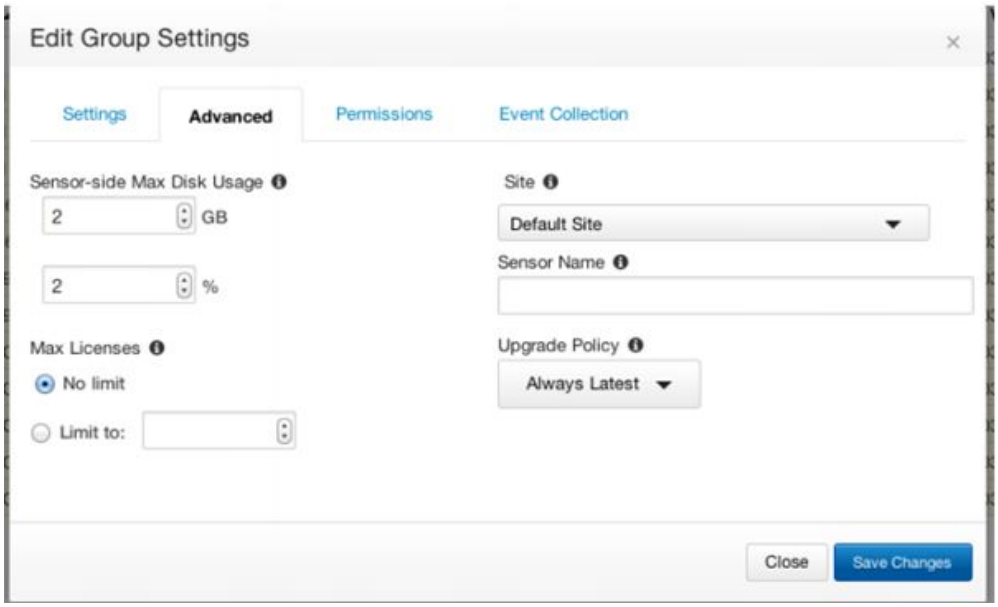
Carbon Black 5.1.0 comes with updated sensor versions. *Before* you run the Carbon Black Server upgrade program, you should determine if you would like to upgrade to the new sensor version. Servers and Sensors can be upgraded independently, and sensors can be upgraded by sensor groups, rather than all at once.

Decide if you would like to the new sensor to be deployed immediately to existing sensor installations, or if you want to install only the server updates first. Bit9 recommends a gradual upgrade of sensors to avoid any unacceptable impact on network and server performance.

Note: There is no expected degradation to sensor performance with Carbon Black 5.1.0.

Deployment of sensors can be configured via the web UI in the following manner:

1. Log in to the console, navigate to the 'Sensors' page, and edit the group settings for each active group:



2. Under the "Advanced" tab, find the "Upgrade Policy" setting. If this is set to "Always Latest", the server will automatically sensors to the latest sensor version.
   a. To keep the sensors at a specific version, select that version number from the dropdown prior to upgrade.
   b. To continue using whatever sensor versions are already installed, regardless of version, select "Manual".

Note: Automatic upgrade settings for Sensor Groups apply to Windows sensors only. To change OS X and Linux sensor upgrade settings please see the "Installing and Managing Sensors" chapter of the *Carbon Black User Guide*.

Server Upgrade Steps

If you are upgrading the server, please follow the steps in this section. These steps require SSH or console access to the server and minions with root privileges.

- **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.

- **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.

- **Note for Installations Using Single Sign On**

  Customers upgrading to *5.1.0 Patch 2* from earlier releases may need to edit their sso configuration file to ensure proper operation after upgrading. The following steps should be taken:

1. Verify the name of the current sso configuration file being used. This is defined in /etc/cb/cb.conf with the SSOConfig parameter, e.g.: SSOConfig=/etc/cb/sso/sso.conf
2. In the sso configuration file, find the entry for the assertion_consumer_service. It will look similar to the following:

```
"endpoints": {
        "assertion_consumer_service": [
          [
            "https://<IP Address>/api/saml/assertion",
           "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
          ]
        ]
 },
```

3. If the assertion_conumer_service is defined using square-bracket syntax as in the example above, change it to use curly-brace and replace the comma to a colon syntax, as follows:

```
        "endpoints": {
        "assertion_consumer_service": {
                "https://<IP Address>/api/saml/assertion":
               "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        }
},
```

Improvements of Carbon Black will occasionally require a utility called ‘cbupgrade’ to be used after *yum install cb-enterprise* to migrate the database schema or alliance feed data. Upgrading from previous stable version of Carbon Black to current release is not expected to require this step. However, running the utility is required when there are local changes to configuration files that have to be manually consolidated with the newer versions distributed by the release. 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.

Carbon Black v5.1: New and modified features

The following sections provide a quick reference to the new and modified features since v5.0.0 Patch 3:

Instant Attack Disruption & Threat Recovery with Custom Endpoint Threat Banning

With endpoint threat banning in Carbon Black, responders can now instantly stop, contain and disrupt advanced threats as well as block the future execution of similar attacks by banning binaries from being able to execute. This expands Carbon Black's ability to drive additional corrective action on impacted endpoints as a part of incident response efforts.

Improved Threat Detection & Kill Chain Analysis with Microsoft Enhanced Mitigation Experience Toolkit (EMET) Integration

Carbon Black 5.1 integrates with Microsoft's Enhanced Mitigation Experience Toolkit (EMET). This enables responders to correlate blocked exploitation attempts—from Microsoft EMET—with Carbon Black's collective intelligence to show key aspects of the attack both before and after the event. This empowers responders to optimize and improve their detection, investigations and patch management efforts by understanding the full kill chain of every exploitation attempt at the moment of compromise. SOC Personnel and incident responders can also have visibility into EMET configurations across an enterprise via this integration, to aid in their investigations and properly determine the appropriate response.

Searchable Threat Intelligence Reports

Providing new visibility and control into the threat intelligence feeds, Searchable Threat Reports allows visibility into the intelligence feeds. The visibility provided by the searchable reports includes insight into all indicators and queries contained within a feed. In addition, users can now suppress individual reports from triggering alerts to reduce false positive alerts for a feed.

Enriched Threat Intelligence with Damballa Integration, Domain Reputation, Geolocation & Icon Matching

Carbon Black now leverages enhancements made to the Bit9 + Carbon Black Threat Intelligence Cloud's services: Attack Classification, Reputation and Threat Indicator Services.

- **Attack Classification:** The Threat Intelligence Cloud's Attack Classification Service provides comprehensive attack context and attribution by integrating with a robust list of industry-leading third-party sources to assist enterprises in identifying the type of malware and threat actor group behind an attack. The Threat Intelligence Cloud now delivers unmatched network-to-endpoint attack classification through its integration with Damballa's leading threat intelligence on malicious destinations, advanced threat actor groups and command-and-control communications.
- **Reputation:** To optimize trust-based endpoint threat detection and response techniques, the Threat Intelligence Cloud now extends reputation to the network layer by delivering domain reputation—in addition to its already unmatched reputation regarding known-good, known-bad and unproven software.
- **Threat Indicators:** To identify spear phishing campaigns that actively deceive end users by masking malicious activities under the appearance of trusted applications, the Threat Intelligence Cloud now provides icon matching to help detect social engineering attacks.
    - The Threat Intelligence Cloud also now provides geolocation look up of inbound and outbound network connections.
    - In previous releases, Carbon Black tracked the destination port (the local port for inbound connections) and the remote IP address for network connections. In version 5.1, Carbon Black tracks Local IP for both ends of the connection. (Note that search functionality is limited to destination port and remote IP addresses.)

Note: Access to these enhanced threat intelligence features requires data sharing with the TIC.

Enhanced Threat Inspection, Analysis & Correlation with Cyphort Integration

Carbon Black now integrates with Cyphort for inspection, analysis and correlation of suspicious binaries discovered at the endpoint. Now Carbon Black can submit unknown or suspicious binaries to Cyphort Core—a secure threat analysis engine, which leverages Cyphort's multi-method behavioral detection technology and threat intelligence—to deliver threat scores used in Carbon Black to enhance detection, response and remediation efforts.

Resolving Alerts as False Positive and Ignoring Future Events

New in v5.1, you have the option to resolve Alerts as false positives and go one step further by preventing the feed from alerting you to the same conditions in the future.

Automatic Pruning of Inactive Sensors

In 5.1.0 Patch 1, we have added configuration to prune sensors that are dormant or inactive. This would include systems that are offline, uninstalled or otherwise have not communicated with the Carbon Black server for a given number of days. The following configuration has been added to the cb.conf to control pruning of such inactive sensors:

DeleteInactiveSensors=True
DeleteInactiveSensorsDays=10

By default the value is set to False.

Corrective Content

The following section provides the corrective content changes made for each release

Carbon Black v5.1.0 Patch 2:

Console and Server

1. Corrected a behavior where throttle_calc task in cb-enterprise progressively more CPU. (E-4698)
2. Fixed an issue with OS process document count in alliance statistics are broken in clustered deployments. (E-4688)
3. Updated nginx cb-multihome.conf to match nginx cb.conf in the product shipping with 5.1. (E-4669)
4. Corrected an issue with feed_searcher sending to syslog every time a md5 matches a feed to include VirustTotal (E-4652)
5. Added logic to rate-limit number of binary hash check HTTP calls to prevent self-inflicted denial of service on the cb-datastore. (E-4697)
6. Corrected an issue with cbdiag --post failing when post size is “too large” in some customer environments. (E-4668)
7. Corrected an issue with watchlist searcher throwing “Invalid Report ID” error causing current job to fail. (E-4677)
8. Fixed the system hang due to CbTools background task is running in the system cbcluster (E-4646)

Windows Sensor (5.1.0.150911.0926)

1. Fixed an issue with CB 5.1.0 sensor upgrades failing if service is renamed (obfuscation) but core driver is not. (WIN-346)
2. Fixed a potential memory leak in cbtdiflt connection close completion handling. (WIN-340)
3. Fixed a system crash issue when doing a live migration of a VM host. (WIN-329)

Linux Sensor (4.2.8.150908.0431)

1. Corrected a kernel panic in systems running Linux named service. (LNX-206)

Linux Sensor (4.2.9.151002.1507)

This is sensor adds support for Linux 6.7. It is not generally available. Please contact Bit9 + Carbon Black Technical Support team to get access.

Carbon Black v5.1.0 Patch 1:

Console and Server

1. CentOS 6.7 fails requesting to upgrade python-urllib3 library. This issue has been addressed in this release. (E-4612)

2. Addressed a failure when cb-enterprise services are started, due to cb-redis service no longer being able to create its own PID file. This is because SELinux policy in CentOS 6.7 has changes that restrict Redis process to where it is allowed to write PID and log files. (E-4653).

3. Several changes were made to increase the security of Carbon Black. (CBUI-1216)

4. Tagged processes could lose their highlighting in the console when they were later shown in search results. This issue has been fixed in the patch. (CBUI-1224)

5. URLs that directly referenced a console page would first open the login page and then display the Welcome Page instead of the page referenced in the URL. In this release, the user is directed to the correct page after authentication. (CBUI-1386)

6. Process or binary search boxes now accept a comma-separated list of query fields. (CBUI-1502)

7. Fixed an issue where the UI would occasionally display 504 errors, timeout errors or the license graph not being displayed after an upgrade from earlier releases to version 5.1.0. (ENT-4094)

8. Addressed an issue where the watchlist page was blank if a proxy was configured for the server. (ENT-4334)

9. Inactive sensors are now removed after 10 days of inactivity. (ENT-4409)

10. Corrected an issue where the EventPurgeEarliestTime date in cb_settings is being set in the future. This prevented deletion of files that should have been purged, which caused unnecessary disk usage. (ENT-4457)

11. Addressed performance issues, especially with backlog processing. (ENT-4506)

12. Corrected an issue where the binary downloads failed in clusters using a non-standard API port. (ENT-4508)

Windows Sensor

13. Fixed an issue where Chkdsk would not run on reboot when Carbon Black sensor was installed on certain Windows operating systems. (WIN-314)

Carbon Black v5.1.0:

Console and Server

1. Administration/Sensors page takes a long time to load on Servers with large number of sensors [CBUI-1236]

2. Addressed some non-functioning CBLR Commands on FireFox [CBUI-1285]

3. UI does not allow non-global-admin administrator of a group to edit group settings, the issue has been addressed in this release [CBUI-1307]

4. Fixed the Binary Preview hyperlink search it was not returning any results [CBUI-1385]

5. If you click on the notification boxes in a threat intelligence feed (the available boxes are "create alert" and "log to syslog"), the boxes will remain checked for the user who checked them, but they will not appear checked for other users. This issue has been addressed. [CBUI-1437]

6. Fixed the Watchlist Email Me option as when changed by 1 user, it affected other users [CBUI-1448]

7. When performing a process search by date, CB 5.0 will return search results for the prior day's data. The issue has been addressed. [CBUI-1402]

8. Address the issue where the server was reaching maximum number of DB connection in a clustered environments [E-3835]

9. After an alert has been resolved from the alerts page's default query, and the page is reloaded the alert shows unresolved again. This issue has been fixed. [E-3838]

10. Server dashboard does not display on occasion due to a product issue. The displayed error was: "unable to add db connection back to pool". This issue has been fixed. [E-3852]

11. The cbcluster startup performance issue has been addressed for this release. This issue appears after upgrading to 5.0.0 Patch 2. [E-4002]

12. Server scripts are displaying the following error <gevent.dns.DNSError'>: [Errno 67] request timed out) [E-4190]

13. If an exception is thrown during a full feed sync via the command line, all work appears to stop. The issue has been fixed. [E-4200]

14. Observing constant stream of HTTP 500 errors in the NGINX. The issue has been addressed by the server having a background health check task that monitors activity and log any time there is a SQL transaction that runs for a long time. [E-4210]

15. The purge process is not processing all appropriate files, which causing excessive disk usage. This issue has been addressed. [E-4235]

16. Triage alert is getting triggered repeatedly for the same file from the same endpoint even after it was acknowledge. The issue has been addressed in this release. [E-4290]

17. CSV generation from the process analyze view results in empty filemods.csv and regmods.csv. This is even if the result on the console shows entries for filemods and regmods events. The issue has been addressed in this release. [E-4382]

18. SSO setting is not redirecting with the specified port [E-4388]

Windows Sensor

1. CB Live Response “kill” command now works correctly on Windows 8+ machines when attempting to kill a process not running in the same session as cb.exe (typically session 0) [WIN-304]

2. Upgrade failure messages are now correctly sent to the server when upgrades failed [WIN-144]

3. Improved accuracy of binary storefile backlog reporting [WIN-199]

4. Modload event collection now can be correctly disabled [WIN-235]

5. Fixed an issue with false positive tamper events sent related to sensor’s own activity on startup and shutdown [WIN-300]

6. Fixed a race condition where persisted events may have been lost if another application on the system happened to have the file open when the sensor tried to send the events [WIN-297]

7. Fixed an issue with operation of CB Live Response that prevented it to start after clean install of sensor [WIN-296]

8. Reduced the likelihood of CB sensor’s hashing and binary inspection to cause sharing violations with other applications’ binaries [WIN-290]

9. Fixed an issue with sensor uninstaller not removing the “HKLM\software\wow6432node\carbonblack” registry key on 64-bit systems [WIN-297]

10. Improved reporting of delayed writes that occurred after a process has exited [WIN-279]

11. Fixed an issue on Windows 7+ machines that led to cb.exe to have high CPU utilization [WIN-277]

12. Improved agents debouncing logic to avoid sending duplicate module info events to the server [WIN-276]

13. Corrected reporting of cross-process events on Windows XP and 2003 systems when one process successfully performed a CreateRemoteThread operation [WIN-274]

14. Fixed a small race condition on driver unload that could lead to memory leak or in rare cases a system crash [WIN-265]
15. Fixed an issue with very long registry paths causing system to crash [WIN-264]
16. Improved accuracy of byte counts of outstanding uploads that is reported to the server [WIN-262]
17. Fixed an issue that causes events that were in queue to be lost when the sensor service was stopped [WIN-259]
18. Fixed an issue that caused sensor to report multiple ntoskrnl.exe (SYSTEM) processes for the same boot session with slightly different process creation times [WIN-250]
19. Fixed an issue that caused binary information of running processes to not be collected If binary info collection is disabled and then re-enabled [WIN-248]

OS X Sensor (4.2.7.50624)

1. A race condition in the daemon would occasionally cause it to crash. This has been corrected. [OSX-209].

Linux Sensor (4.2.7.50624)

1. The Linux sensor now gracefully handles DNS timeouts. [LNX-98].
2. An issue was fixed involving RPM name collision of the Linux sensor installer package installed on the cb-enterprise server. [LNX-137].
3. Support for Redhat/Centos 7.1 has been added. [LNX-144].
4. The Linux sensor will now ignore its own operations. [LNX-152].
5. The subsystem start/shutdown sequence was adjusted to avoid a potential race

Carbon Black v5.1.0: OS Support

Server / Console:

- CentOS 6.4-6.7, (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.4-6.7 (64-bit)

Installation and testing is done on default installs using the 'minimal' distribution and the distribution's official package repositories. Customized Linux installations must be individually evaluated.

Sensor OSes (endpoints + servers)

- **Windows**: XP SP3 - 10. / Server 2003 - 2012R2, x86 and x64
  - Windows embedded OSes are individually evaluated
- **Mac**: OS X 10.7 through 10.10, x64 on Intel
- **Linux:** RHEL & CentOS 6.4-6.6, 7.0, 7.1 x64 – standard kernel versions (2.6.32-358.el6, 2.6.32-431.el6, 2.6.32-504.el6, 3.10.0.el7.x86_64) and the standard minor/ maintenance releases. Non RHEL/CentOS distributions or Modified RHEL/CentOS environments (those built on the RHEL platform) are not supported.
  For RHEL & CentOS 6.7 support, please contact Bit9 + Carbon Black Technical Support team to get access to the supported sensor.
  Note: Major releases of 6.7 and 7.2 will require moving to the next patch of the sensor.

The Linux sensor now supports Redhat/CentOS 6.4, 6.5, 6.6, 7.0, 7.1 without the need for a patch.
For Linux sensor for RedHat/CentOS 6.7, please contact Bit9 + Carbon Black Technical Support team to get access to the installation.

Known Issues and Limitations

1. The current implementation of sensor purging has a known issue. If a sensor has been purged prior to its process data being purged, the Process Analysis page will return a 404 error for that sensors processes. All searching capabilities and process events are still present, searchable, and will be alerted. To reduce the chances of this scenario if you choose to enable DeleteInactiveSensors, we recommend setting your DeleteInactiveSensorsDays equal to or greater than your desired storage retention period until fix in a later release.

2. Right after installation or upgrade of the sensor Tamper events are not reported to the server.Restarting the cb service and driver seems to fix the issue. [WIN-330]
3. If a sensor's system clock is wrong and in the future, the start time for processes from that sensor is not displayed correctly in the Carbon Black console. [CBUI-1102]
4. On the Carbon Black server, when a sensor is moved out of a group with a user on a team that has only "Viewer" access to that particular group, results for that group are still searchable for the time period it was in that group, but the process details page links get 405 errors. If the sensor is put back into the group, the 405 errors for those processes go away. [E-3788]
5. The Reshard tool can fail with "File Not Found" exception, in turn causing a corrupt index. If a re-shard is necessary please contact support for a potential work around. [E-3493]
6. The power state of a Linux sensor is not displayed correctly on the Host Details page. When a Linux sensor is powered off, the icon next to the Computer Name does not change to the correct state. [LNX-53]
7. The OS X sensor does not report on "First File Write" events. [OSX-208]
8. Under high volume event generation and resource constraint systems, the OS X sensor can cause a kernel panic in some instances. [OSX-217]
9. In order for sensor upgrades to work properly, McAfee EPO may need to be configured to exclude c:\windows\carbonblack\cb.exe from its "Prevent creation of new executable files in the Windows folder" option. [WIN-303]
10. On endpoints running the Windows 8.1 32-bit platform, banning may fail when processes are executed using gitbash (sh.exe). [WIN-307]
11. Fixed an issue that caused the sensor to lose connectivity with the server when Network Isolation was enabled. [LNX-158]

Contacting Bit9 Support

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

Technical Support Contact Options
Web: www.bit9.com

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

Reporting Problems

When you call or e-mail Bit9 Technical Support, please provide the following information to the support representative:

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