Cb Defense

Cb Predictive Security Cloud

Release Notes
September 2018

General Notes

Starting the second week in September 2018, Cb Defense customers will receive an automatic upgrade to the Cb Defense Management Console. This document describes usability and performance improvements and bug fixes in the September release.

Features

LiveOps

What is LiveOps?

A new offering on the PSC including a unique set of capabilities allowing a user to ask questions of their endpoints and then take action. Live Query will have two paths: run a query from our list of recommended options, or hand write a query using SQL. Why SQL? The LiveOps query capability is tied to the open source project OSquery version 3.2.6, which allows for SQL-based queries to be run. This robust project is well supported by an active community and provides a long list of query options. After a query runs, and results return, users can narrow down their matches to get a clear vision of the answer to their question. **Windows sensor version 3.3+ is required to use LiveOps.** *Please contact your account representative to get LiveOps for your team.*

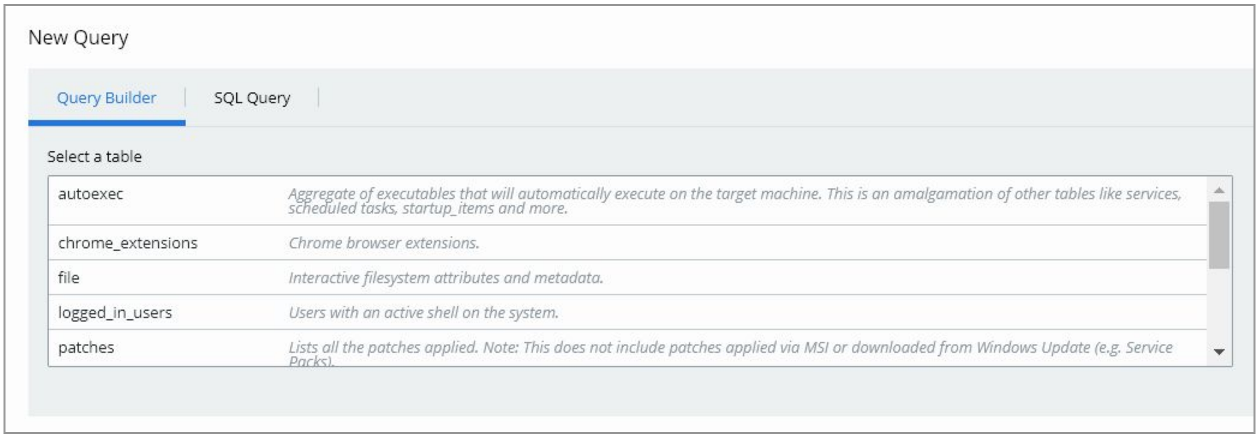
Why use LiveOps?

Security and IT Operations teams must assess the current state of their endpoints to further minimize risk and operational cost, and then efficiently remediate. LiveOps, in combination with our traditional EDR services on our Predictive Security Cloud, provides security analysts with full visibility through recorded and currently active data. It also bridges the gap between security and IT for a true collaborative approach to Security Operations: one tool for compliance, IT hygiene, and investigations.

Use cases for LiveOps

The **LiveOps** page supports following use cases:

Run a Query



New Query

Query Builder | SQL Query

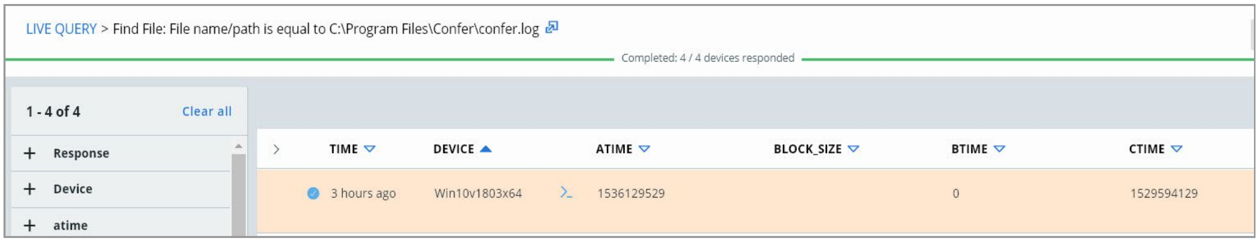
Select a table

autoexec	Aggregate of executables that will automatically execute on the target machine. This is an amalgamation of other tables like services, scheduled tasks, startup_items and more.
chrome_extensions	Chrome browser extensions.
file	Interactive filesystem attributes and metadata.
logged_in_users	Users with an active shell on the system.
patches	Lists all the patches applied. Note: This does not include patches applied via MSI or downloaded from Windows Update (e.g. Service Packs).

- Admins can create a query from the Query Builder using 10 available osquery tables:
  - Autoexec
  - Chrome_extensions
  - File
  - Logged_in_users
  - Patches
  - Process_open_sockets
  - Processes
  - Programs
  - Registry
  - Scheduled_tasks

- Admins can create a more customized query using the SQL Query Builder against all osquery schema tables.

Take action on LiveOps results



LIVE QUERY > Find File: File name/path is equal to C:\Program Files\Confer\confer.log

Completed: 4 / 4 devices responded

1 - 4 of 4 Clear all

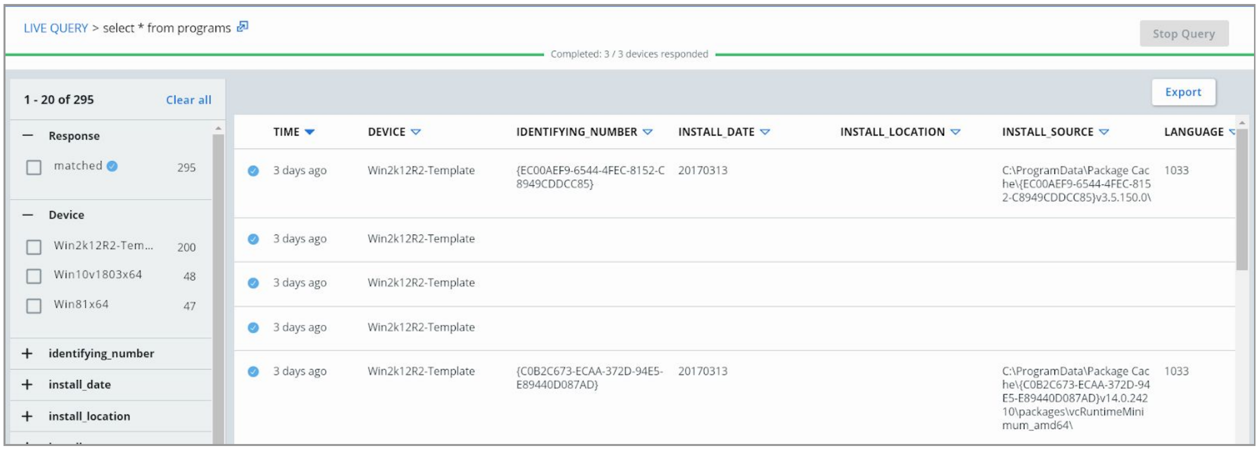
+ Response
+ Device
+ atime

TIME	DEVICE	ATIME	BLOCK_SIZE	BTIME	CTIME
3 hours ago	Win10v1803x64	1536129529		0	1529594129

(Click this icon to initiate a Live Response session. It is located next to the device name and appears if Live Response is enabled for the device.)

- Admins can initiate Live Response directly into the endpoint from the results page to investigate further.

Digest Results



LIVE QUERY > select * from programs

Completed: 3 / 3 devices responded

1 - 20 of 295

Response	
□ matched	295
Device	
□ Win2k12R2-Tem...	200
□ Win10v1803x64	48
□ Win81x64	47
+ identifying_number	
+ install_date	
+ install_location	

TIME	DEVICE	IDENTIFYING_NUMBER	INSTALL_DATE	INSTALL_LOCATION	INSTALL_SOURCE	LANGUAGE
3 days ago	Win2k12R2-Template	{EC00AEF9-6544-4FEC-8152-C8949CDDCC85}	20170313		C:\ProgramData\Package Cache\{EC00AEF9-6544-4FEC-8152-C8949CDDCC85}v3.5.150.0\	1033
3 days ago	Win2k12R2-Template					
3 days ago	Win2k12R2-Template					
3 days ago	Win2k12R2-Template					
3 days ago	Win2k12R2-Template	{C0B2C673-ECAA-372D-94E5-E89440D087AD}	20170313		C:\ProgramData\Package Cache\{C0B2C673-ECAA-372D-94E5-E89440D087AD}v14.0.24210\packages\vcRuntimeMinimum_amd64\	1033

- Admins can filter on data to narrow their results.
- Admins can track progress of the query via the progress bar at the top of the results page.
- Admins can sort the columns to better understand the result set.
- Admins can export the result set to CSV format to perform a deeper analysis.

Permissions

- Live Response administrators can use LiveOps.

Notes about LiveOps

LiveOps is implemented using Osquery open source project. LiveOps currently does not support daemon mode (evented tables) in Osquery. LiveOps operates within the same limitations as Osquery. Some examples of limitations are:

1. On Windows, file names containing multibyte characters over U+00FF, will not be found by osquery (No error given; they simply won't appear in the results of a file search).
2. ENDPOINT: shell app (osqueryi.exe) does not set %ERRORLEVEL% (last error). We must rely on the existence of any stderr to inform us that an error occurred during the query.
3. You cannot match recursively inside a path. For example /Users/%%/Configuration.conf is not a valid wildcard.
4. You cannot wildcard the drive letter when searching for a file. You must provide a drive letter, or if the path starts with a slash, the system drive is assumed. For example "path like '%%';" or "path like '%\%%';" results in nothing being found (and no error from osquery). Instead, if you use "path like '\%%';" the system drive (usually C: on Windows) is searched recursively in this example.
5. You can not find a file given its SHA256 hash.
6. When querying the hash table, a file size limit of 52428800 (50 MB) is enforced.

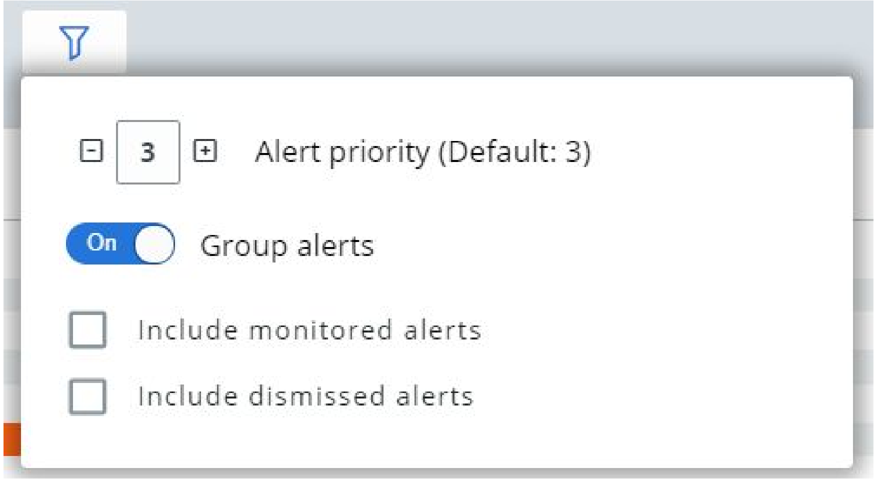
For additional details please visit: https://osquery.io/.

Auto-Delete of Known Malware

The Auto-delete of Known Malware feature automatically deletes known malware from endpoints after a specific amount of time that you configure on the **Policy** page. When this feature is enabled, Known Malware appearing on the **Malware Removal** page is queued for deletion. This feature requires Windows sensors 3.2.1 and later, and Mac sensors 3.3.1 and later.

Dashboard Improvements

We've added an alerts filter button to the top of your dashboard page. You can use this button to have greater control over which alerts appear in your dashboard widgets. By default, only alerts with a score of 3 or higher are displayed. You can also control whether to group alerts, and whether to display monitored or dismissed alerts in your dashboard widgets.



⊟ 3 ⊞ Alert priority (Default: 3)

On Group alerts

□ Include monitored alerts

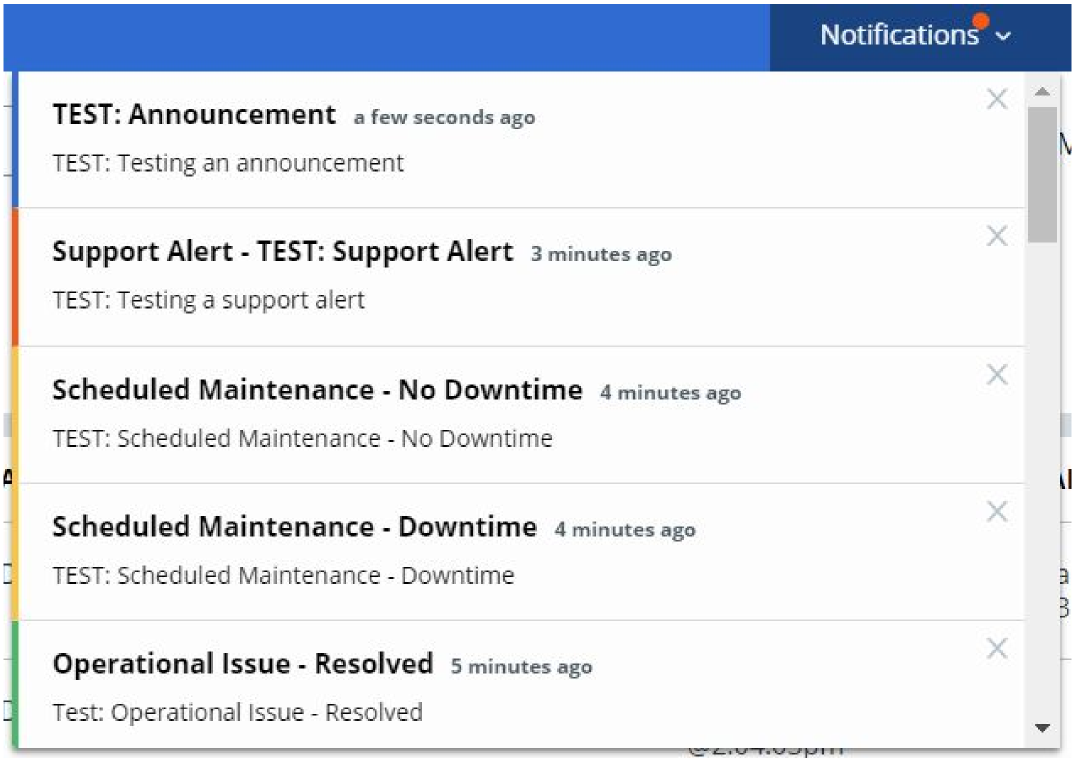
□ Include dismissed alerts

Notification Improvements

With this release, we've broken out these notifications into more specific categories and color-coordinated them to make it easier for your team to understand what the notification is about. The notification types are:

- Operational Issue - Monitoring (Orange)
- Operational Issue - Resolved (Green)
- Scheduled Maintenance - Downtime (Yellow)
- Scheduled Maintenance - No Downtime (Yellow)
- Support Alert (Orange)

- Announcement (Blue)



TEST: Announcement a few seconds ago
TEST: Testing an announcement

Support Alert - TEST: Support Alert 3 minutes ago
TEST: Testing a support alert

Scheduled Maintenance - No Downtime 4 minutes ago
TEST: Scheduled Maintenance - No Downtime

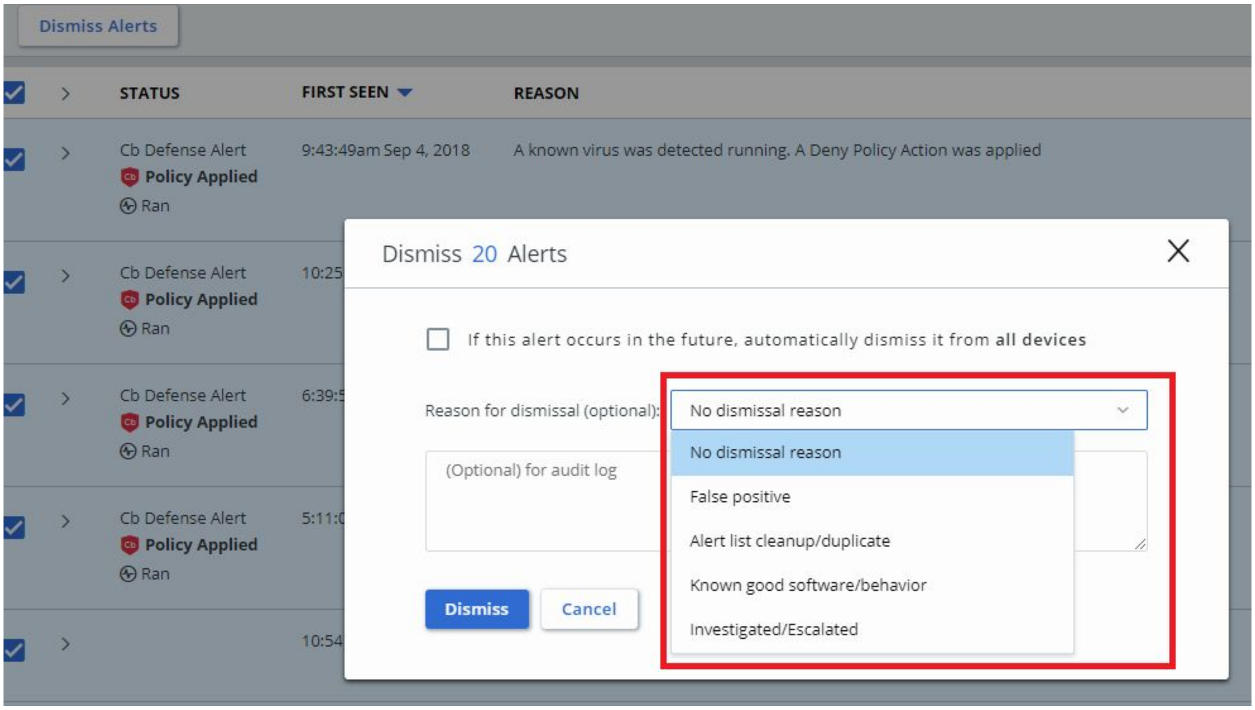
Scheduled Maintenance - Downtime 4 minutes ago
TEST: Scheduled Maintenance - Downtime

Operational Issue - Resolved 5 minutes ago
Test: Operational Issue - Resolved

Alert Dismissal Reasons

To make it easier for teams to track and audit the reasons that specific alerts were dismissed, we've added a list of reasons to choose from when you dismiss an alert.
We can use this anonymized feedback to improve user experience within the product, as it relates to things like duplicated alerts or false positives. The reasons include:

- False Positive
- Alert List Cleanup/Duplicate
- Known Good Software/Behavior
- Investigated/Escalated



Dismiss Alerts

☑	STATUS	FIRST SEEN	REASON
☑	Cb Defense Alert Policy Applied Ran	9:43:49am Sep 4, 2018	A known virus was detected running. A Deny Policy Action was applied
☑	Cb Defense Alert Policy Applied Ran	10:25	
☑	Cb Defense Alert Policy Applied Ran	6:39:5	
☑	Cb Defense Alert Policy Applied Ran	5:11:0	
☑		10:54	

Dismiss 20 Alerts

□ If this alert occurs in the future, automatically dismiss it from **all devices**

Reason for dismissal (optional): No dismissal reason

- No dismissal reason
- False positive
- Alert list cleanup/duplicate
- Known good software/behavior
- Investigated/Escalated

(Optional) for audit log

Dismiss Cancel

Usability Improvements

- Added Getting Started Guide - We've added a getting started guide to the Help menu to make it easier for our users to get up and running as they begin using the PSC.
- Alert URL from Investigate - Upon navigating to the **Investigate** page within an alert context, you can now click on the Alert ID to navigate back to the **Alerts** page with that alert selected.
- Exportable **Reputation** page - The **Reputation** page is now exportable. Click the **Export** button at the top right of the table to view the data in CSV format.
- Dashboard Export Timezone Improvements - Formatting improvements were made to the data that is exported from the Cb Defense dashboard widgets. All data exported from the dashboard now includes the timezone stamp.
- Easy Search Stickiness - Previously this feature had to be turned on or off during each new browser session. We have made this setting sticky, so your preferences are remembered across user sessions.

Browsers Supported

- On Windows - Firefox, Chrome, and Edge
- On Mac - Safari, Firefox, and Chrome

Note that IE11 is not a supported browser.

Issues Resolved in September

ID	Description
EA-12560, DSER-9023	Resolved an issue that led to dismiss for future to work incorrectly in some instances.
DSER-9263	Resolved an issue where default policy rules included “Ransomware” + “deny” rather than “Ransomware” + “terminate.”
DSER-9387	Resolved an issue where selecting a policy to filter on the dashboard led to inconsistent results in the endpoint health widget.
EA-12205 EA-12766 EA-12518	Resolved an issue where, on the **Endpoints** page, sensors were occasionally appearing to revert to a previously assigned policy and, at other times, did actually revert. All policy assignments now persist on the endpoint, as expected.
DSER-8511	Removed unsupported Android sensor-related TTPs from the UI.
DSER-9672	Resolved an issue that prevented “\” from being used in the search field on the **Investigate** page.
EA-12281 DSER-8962	In some instances, incomplete information was being presented on the **Malware Removal** page. This has been fixed in this release.

Known Issues and Caveats

The following section lists known issues in this version of the Cb Defense backend/UI.

ID	Description
DSER-2951	Using Live Response to get or put a file greater than 2MB might be slow or not occur.
DSER-10270	When using **Live Response**, if the browser times out, there may be unexpected behavior. A workaround for this issue is disconnecting and reconnecting the **Live Response** session.
DSER-5437	Additional markup is added to events forwarded via the event forwarder.

DSER-7403	When exporting large data sets from the UI, if the export takes longer than 60 seconds, no data is returned.
DSER-8725	Emailed sensor download invite results in **Token invalid** message when clicking the link.
DSER-9664	Occasionally, clicking the link an an emailed alert notification results in the Alert Triage page not rendering correctly.
DSER-9670	Searching for “threat category:Malware” will occasionally return Non-Malware results.
DSER-9812	Last check in time for a sensor is not updated properly, resulting in out-of-date last check-in times.
DSER-10296	Live Response large file retrievals may fail in some cases.
DSER-10275	Live Response sessions may take up to 30 seconds to initiate.
DSER-10312	“Dismiss alerts for future occurrences” may not be respected in some cases.
DSER-10352	Bulk upload of hash reputation may fail in some cases.