Carbon Black.

Cb Defense

February 2018 Update

Release Notes

February 2018

Carbon Black, Inc.

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

Email: support@carbonblack.com

Web: http://www.carbonblack.com

Carbon Black.

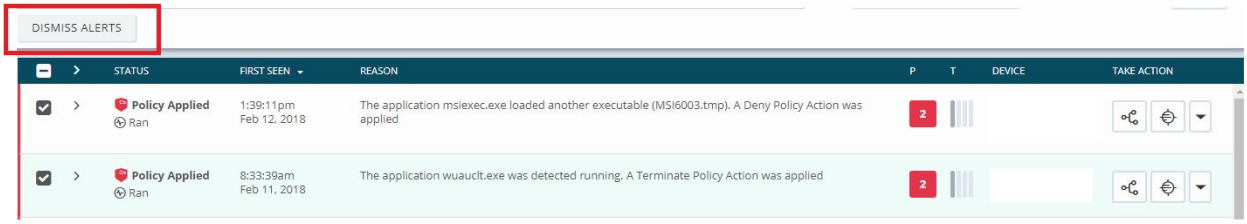
General Notes

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

Features

Bulk Alert Dismissal

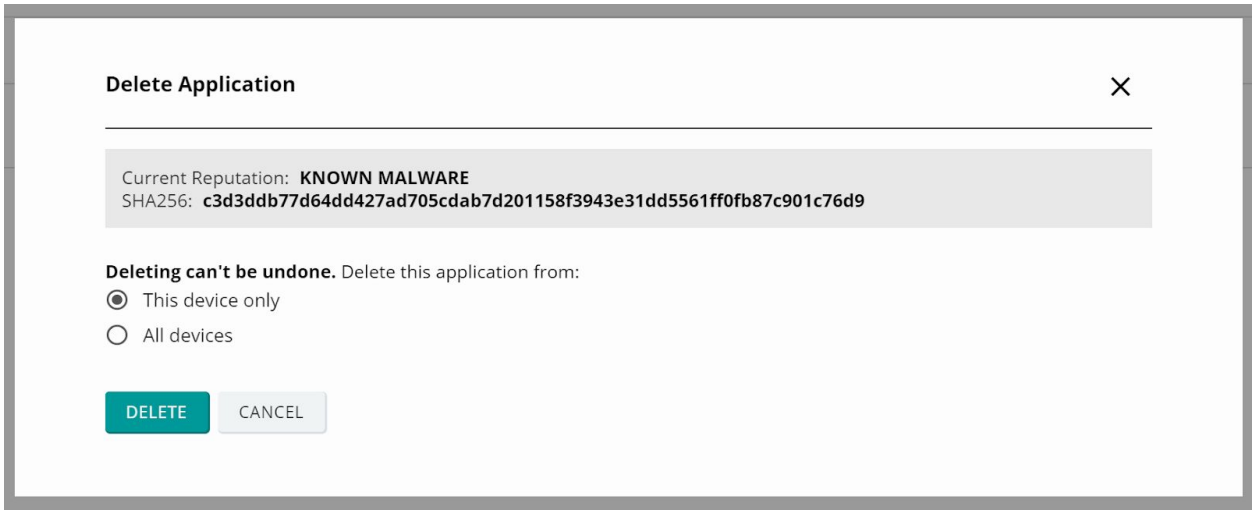
The **Alerts List** page now lets you select and dismiss multiple alerts. A checkbox at each row in the Alerts table lets you select multiple alerts. You can then click a button to dismiss all selected alerts. This action results in an audit log entry that summarizes both the bulk dismissal as well as an individual entry for each alert that was dismissed.



Bulk Delete Applications

Previously, to delete applications across all devices, you had to delete each application one at a time. Now, you can delete an application across all devices in a single action. This updated modal can be found on the **Alerts List**, **Alerts Triage**, and **Investigate** pages.

Important: Delete actions cannot be undone, so always consider the implications of deleting an application.



New and Improved Policies Page

Cb Defense has overhauled the **Policies** page so that you can more efficiently manage policy rules. The new page reduces complexity, improves usability, and addresses five idea requests from UeX. Major changes to the page include the following:

- **Combined rule sets** Similar policy rules that contain the same operation attempts and actions (Deny, Terminate, Bypass, Allow, and Allow & Log) are combined into rule sets instead of being separated into individual lines. Rule sets take up much less vertical page space, require less scrolling, and are much easier to read.

- **Edit mode** Click the **Pencil** icon in a rule set to enter Edit mode. In Edit mode, you can select action checkboxes that correspond to operation attempts.

- **Action Checkboxes** Action selections on the policy page are displayed in checkboxes instead of dropdown selections. These action checkboxes visually indicate which rule combinations can be created and which cannot, and they increase rule validation by eliminating the creation of duplicate rules.

- **Helper Tips** When you are in Edit mode, you can click **Show Tips**, which displays information about processes, operation attempts, actions, path rules, and wildcards. These tips can be toggled on or off, and are hidden when you exit edit mode.

- **Floating Save bar** After you have made and confirmed changes to policy rules, those changes appear in teal. To ensure that all of your changes are saved, click the **Save** button in the floating Save bar. (As you scroll through the page, the Save bar persists at the bottom of the browser.

- **Copy Rules** You can click the new **Copy** button in the bottom-left corner of each rule set to copy the entire rule set to another policy group. You can search for specific policies to copy the rule set to, or you can copy the rule set to all policies. If

the rule set conflicts with any existing rules in the target policy, a modal window notifies you of the rule conflicts. You can to replace the existing rule set, skip the copy action to the target policy group that contains the existing rule, or cancel the copy process.

- **Collapsible panels** Each panel (**General**, **Permissions**, **Blocking and Isolation**, and **Uploads**) of the **Policies** page can be collapsed or expanded. This lets you focus on a specific area of the page. Click the arrow/carat to expand or collapse each panel.

- **Predictive policy search** When you are creating new policy rules, you can use a predictive policy search to determine the events that a new rule would block. Click the **Investigate** icon to the right of an **Operation Attempt** column to open the **Investigate** page in a new browser tab, and run a query that corresponds to the process and operation that you selected on the **Policies** page. For example, click the **Investigate** icon next to **Known malware** and **Communicates over the network** to open the following query on the **Investigate** page: "Operation:Communicates over the network AND all.reputation:KNOWN_MALWARE." The returned search results list the events that would be blocked if you create a "Known malware... communicates over the network..." deny or terminate rule on the **Policies** page.

Support Button

Click the new **Support** button (headset icon) on the Navigation bar to open the Support page in UeX (https://community.carbonblack.com/community/resources/support). Here, you can open a support case and find helpful resources such as product docs and downloads, knowledge base articles, product updates, and training and certification.

Usability Improvements

Search Improvements

We've implemented several high priority search enhancements, including the following:

- **Operation keys** New keys utilize key-value search pairs that map to the operation attempts that correspond to policy rules. These keys are used in the new predictive policy search feature, which is part of the new **Policies** page.

- **Suggested Search Improvements** The suggested searches that appear when you put your cursor in the **Investigate** page search bar have been reformatted. They no longer appear as unformatted fields and are therefore easier to read.

- **Copy button** A **Copy** button at the far right of the search bar on the **Investigate** and **Alerts List** pages copies the contents of the search bar.

- **Boolean operators** The following additional boolean operators have been added: OR, AND, OR NOT, AND NOT. You can type those boolean operators to create more complex queries, or use your mouse to focus on and select an operator. You can also use the tab or arrow keys to navigate through your search terms and select or change boolean operators.

- **Additional TTPs** The following TTP keys have been added: Attempted_Server, Hollow_Process, Kernel_Access, Process_Image_Replaced.

Named Browser Tabs

For users who open multiple browser tabs while performing an investigation, we've added page names to each tab to help you select the correct tab. In addition to the page name, alert IDs and policy names appear in the browser tab.

Live Response

We have added a new command titled 'execfg'. This command allows the users to execute a remote command on the device a receive the results of the command directly in the console. This provides increased usability for command that typical write output to a traditional console window such as 'netstat' or 'ipconfig'.

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 February

ID	Description
EA-11257	Provided the ability to export up to 100k devices using the APIs.
EA-11139	Changed the API connector to handle 0.0.0.0/0 as an IP whitelist.
EA-11049	Fixed an issue using a colon (:) to start a search with a single saved search.
EA-10866	Fixed QUARANTINE_DEVICE state to be the result of a logical OR of sensor action and policy state, where the quarantined is given preference over not quarantined
EA-10401	Fixed Notifications page missing relation between TTPs when building a notifier.
	Resolved an issue preventing the display of the sliding time window on the Investigate page.

Known Issues and Caveats

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

ID	Description
EA-7903 EA-7882	Automatic update of sensors from the cloud is currently disabled due to network bandwidth concerns. Manual push from the cloud is supported for 100 sensors at a time.
DSER-2951	Using Live Response to get or put a file greater than 2MB might be slow or not occur.
	The **Allow Uploads for Scan** setting on the policy configuration page is currently disabled while we transition this service to the Carbon Black Collective Defense Cloud.