Our December 2018 release of the PSC includes the following:

- CB Defense: Contextual User Guide
- CB Defense: Open Beta New Default Roles
- CB Defense: Fixed in this Release and Known Issues
- CB ThreatHunter: Fixed in this Release and Known Issues
- CB LiveOps: Target Specific Devices

We'll start rolling out these changes the third week in December 2018.

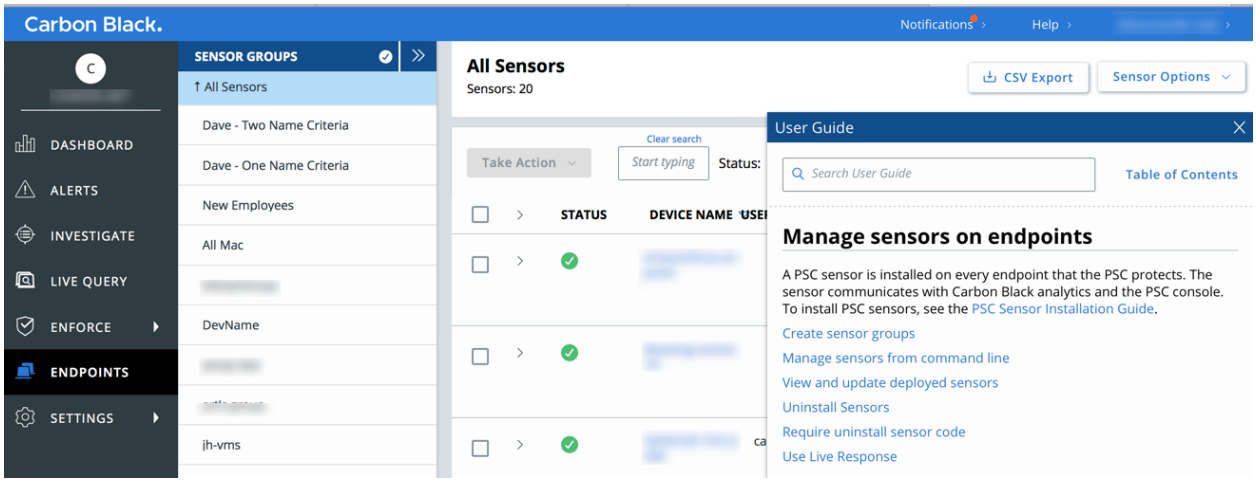
CB Defense

Features

Contextual User Guide

We've moved the User Guide into HTML in CB Defense. You can quickly find relevant information to the task at hand without having to exit CB Defense. You can access the User Guide from the top navigation bar **Help** menu.

The User Guide automatically displays results that are related to the current page in the PSC console.

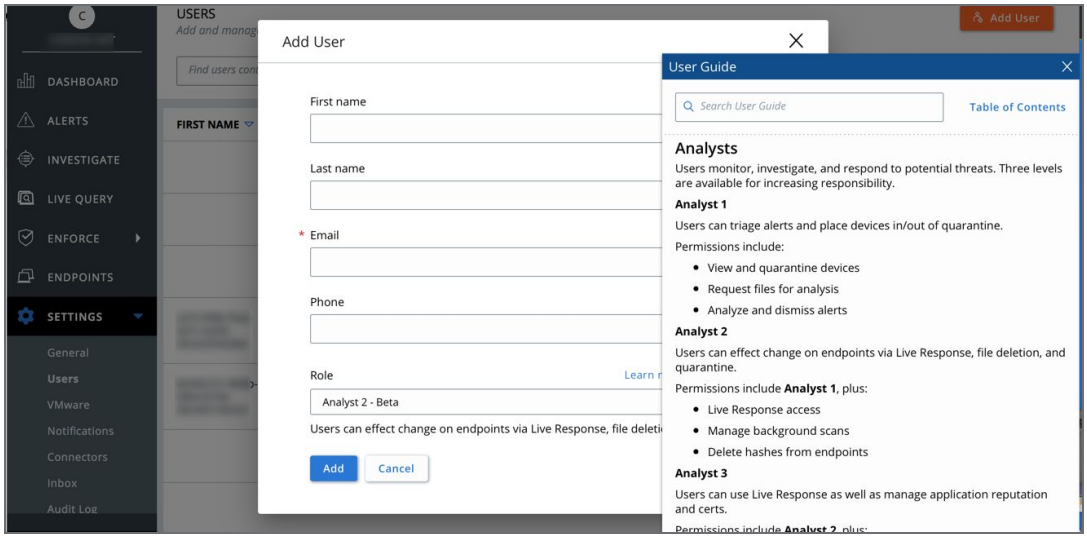


Open Beta: New Default Roles

With six new beta roles, you can give users access to just the functionality they need. Creating connectors, modifying policies, using Live Response, and other powerful actions can be restricted to only the appropriate users. The new roles are:

- Super Admin
- System Admin
- Analyst III
- Analyst II
- Analyst I
- View Only

For more information, see the User Guide.



Fixed in this release

Issue ID	Description
DSER-5763	Fixed an issue where quarantined devices were not reflected in the CSV download for the **Endpoints Health** dashboard results.
DSER-10343	Fixed an issue where some items with the reputation “Known Malware” did not show up on the **Malware Removal** page.
DSER-8725	Resolved an issue where the sensor download email invite resulted in **Token invalid** message when clicking the link.

Known issues

ID	Description
DSER-5437	Additional markup is added to events that are forwarded via the event forwarder.
DSER-9144	When copying out of the **Investigate** page, additional line breaks are included. Pasting this directly into the search bar does not return any results.
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** on the **Alerts** page returns Non-Malware results.
DSER-10667	After whitelisting a file, the reputation on the **Application** tab of the **Investigate** page erroneously displays as NOT_LISTED.
DSER-10679	The date/time format in the device API output changed in the September release to a new format.
DSER-10714	The API URLs presented under **Settings -> Connectors -> Download** are incorrect.

DSER-10790	IT Tool whitelist upload removes backslash and the next character.
DSER-10961	On non-current sensor versions, the request to delete PSC sensor files from the backend succeeds, which causes the sensor to stop functioning.
DSER-11370	When dismissing alerts, selecting a dismissal reason causes the alert to not dismiss properly.

CB ThreatHunter

Fixed in this release

Issue ID	Description
DSER-11434	Fixed an issue where the time range filter didn't match the passed-in URL parameters from hyperlinked queries.
DSER-11655	Fixed an issue where customer who did not opt in to ThreatHunter binary uploads will no longer be linked to the **Binary Details** page from the **Process Analysis** page.
DSER-12017	Fixed an issue where you could not delete created reports.
DSER-12048	Fixed an issue where the **Binary Details** page did not distinguish between "We have no data on that hash" versus "the requested hash is invalid".
DSER-12159	Fixed an issue where the **First seen** field is always reported "Unknown" on the **Binary Details** page.
DSER-12160	Fixed an issue where the **First seen as** field is always reported "Unknown" on the **Binary Details** page.
DSER-12161	Fixed an issue where **Reputation** is always reported "Unknown" on the **Binary Details** page.
DSER-12200	Fixed an issue where **Size** field was labelled in KB but was displaying the Bytes value on the **Binary Details** page.
DSER-12403	Fixed an issue where binaries with no resource section could not be uploaded to CB Unified Binary Store (UBS).

Known issues

ID	Description
	First seen as field on the **Binary Details** page (and from the API) does not return paths in prevalence order; therefore, it is not possible to guarantee the actual first seen instance.
UAV-640	childproc_reputation and childproc_effective_reputation are being misreported by the PSC sensor under certain conditions.
DSER-11760	User cannot edit IOCs created in their Organization.
DSER-11841	Navigating from **Alerts** page to **Investigate** page via hyperlink sometimes throws "The query is invalid" due to undefined device_id.
DSER-12162	**Binary type** field is always reported "Unknown" on **Binary Details** page.
DSER-12355	IPv6 addresses are not properly formatted on the **Process Analysis** page.
DSER-12424	Data access events from from the PSC sensor feature don't show up in ThreatHunter **Investigate** page results.
DSER-12463	**Investigate** page searches that have regex statements are flagged by the UI as invalid, but are accepted if you submit the search anyway.
DSER-12493	Search exclusion for device_os does not eliminate "Hit" search results.
DSER-12540	Exclusion filters aren't excluding processes in search results on **Investigate** page.

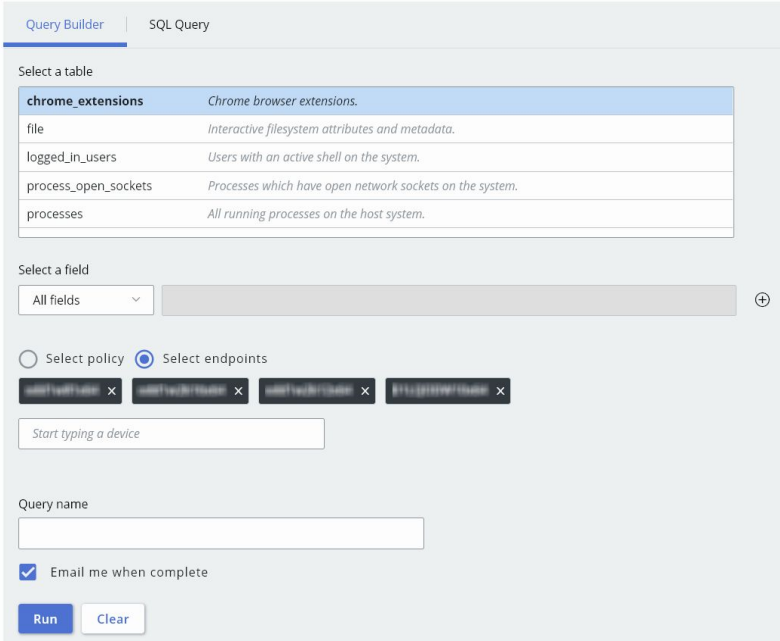
CB LiveOps

LiveOps: Target Specific Devices

You can now query specific devices in CB LiveOps. This enables you to run your query on a targeted set of devices rather than on all endpoints in your organization. You can select which devices you would like to run the query on from the **Live Query** page (**Query Builder** and **SQL Builder**) or on the **Endpoints** page.

Please contact your account representative to get CB LiveOps for your team.

Select endpoints on the **LiveOps** page:



Select endpoints on the **Endpoints** page: