



Getting Started with Audit and Remediation

Audit and Remediation empowers teams to inspect endpoint status and trends and identify areas that require proactive action.



Carbon Black.

Complete the Carbon Black Cloud setup tasks

Before getting started with Audit and Remediation, add console administrators and deploy sensors

Sign in to the Carbon Black Cloud console and follow the **Getting Started** widget to complete these tasks.

Getting Started

Complete the fundamental tasks to set up your organization

Carbon Black Cloud setup	 Add console administrators	1 added
Prevent with policies	 Send sensor installation requests	0 sent
Additional resources	 View deployed sensors	0 active

If you don't see the **Getting Started** widget on your dashboard, click **Configure Dashboard** to add it.

Live Query



Ask questions of endpoints to see which need updates or patches, are displaying suspicious activity, and more

Live Query is powered by [Osquery](#), an open source project that uses a SQLite interface.

Use Live Query to:

- Run pre-built **recommended queries** from security experts
- Create your own **SQL query**

Query devices from Live Query or from Endpoints by clicking **Take Action** and then clicking **Query endpoints**.

[Live Query access is dependent on user role authorization.](#)

1 Run a Recommended Query



Recommended queries are created by security experts

1. View recommended queries by selecting a category.
2. Use the search and OS filter to further refine the list.
3. Choose whether to be notified when a query is ready.
4. Select a policy or endpoints. The default selection is all endpoints.
5. Click **Schedule** to run the query daily, weekly, or monthly.
6. Click **Run** to start a one-time query.

View the query status and results on the **Query Results** page.

The screenshot shows the 'NEW QUERY' interface. At the top, it says 'Run a recommended query or create your own with custom SQL. Learn more'. Below this are two tabs: 'Recommended' (selected) and 'SQL Query'. A link 'Visit the Query Exchange' is on the right. There are five category buttons: 'All (64)', 'IT Hygiene (21)', 'Vulnerability Mgmt (11)', 'Threat Hunting (14)', and 'Compliance (18)'. Below the buttons is a search bar with a magnifying glass icon and a 'Clear search' link. To the right of the search bar is an 'OS' dropdown menu. Below the search bar is a checkbox labeled 'Email me a summary of query results'. A note states: 'Queries run against all endpoints by default. However, you can select a specific policy or endpoints.' Below this is a section for 'COMPLIANCE' with a sub-section 'Authorized SSH Keys' (indicated by a calendar icon). This section has 'Schedule' and 'Run' buttons. The description reads: 'The Authorized_keys file for SSH is a critical file that controls which users can log into which systems.' The results are: 'Lists all relevant information about the authorized keys on the target systems.' There is a small icon of a person and a plus sign. At the bottom right, it says 'Carbon Black recommends that you run this query daily'.

1 Run a SQL Query



If you're familiar with SQL, create more granular queries in SQL Query

1. Choose whether to be notified when a query is ready.
2. Select policies or endpoints. The default selection is all endpoints.
3. Type or paste your SQL query into the text box.
4. Select **Schedule** to run the query daily, weekly, or monthly.
5. Name your query.
6. Click **Run** to start a one-time query or **Schedule** to save the schedule.

View the query status and results on the **Query Results** page.

For assistance writing valid SQL, view **Intro to SQL**, Osquery **Tables**, or **Visit the Query Exchange**.

NEW QUERY

Run a recommended query or create your own with custom SQL. [Learn more](#)

Recommended | **SQL Query** [Visit the Query Exchange](#)

Email me a summary of query results

Queries run against all endpoints by default. However, you can select a specific [policy](#) or [endpoints](#). [Clear](#)

osquery: [Intro to SQL](#) | [Tables](#)

Schedule query

Frequency

Daily Weekly Monthly

* Mo Tu We Th Fr Sa Su

Start time 9:00:00 AM (GMT-05:00) America/New York

Query name

Schedule Clear

2 One-time queries



One-time queries display the query start time, name, status, device response, and the user who started the query.

Click the symbol next to the query name for additional details.

To view results, click the query name.

QUERY RESULTS
View the status and results of past, running, and scheduled queries.

One-Time | Scheduled

Clear search

Q

TIME	QUERY	STATUS	DEVICE RESPONSE	USER	ACTIONS
10:46:16am Nov 27, 2019	Authorized SSH Keys	COMPLETE	<div style="width: 100%; height: 10px; background-color: green;"></div> 4/4	[REDACTED]	⌵
5:54:32pm Nov 26, 2019	select g;	COMPLETE	<div style="width: 100%; height: 10px; background-color: green;"></div> 5/5	[REDACTED]	⌵
5:43:02pm Nov 26, 2019	select *;	COMPLETE	<div style="width: 100%; height: 10px; background-color: green;"></div> 5/5	[REDACTED]	⌵

2 Scheduled queries



Scheduled queries display the name, frequency, policy/endpoints, last run date/time, and the user who scheduled the query. Click the symbol next to the query name for additional details.

To view scheduled queries that are still in progress or completed, click the caret to the left of the query name.

To view results, click the query start-time.

QUERY RESULTS
View the status and results of past, running, and scheduled queries.

One-Time | **Scheduled**

Clear search

Q

QUERY ▾	POLICY/ENDPOINTS	FREQUENCY	LAST RUN ▾	USER ▾	ACTIONS
▾ SELECT * FROM users JOIN authorized_keys USING (UID);	All	Daily	11:00:00 am Nov 27, 2019	kpham+d1orion@carbonblack.co m	▾

TIME	STATUS	DEVICE RESPONSE	ACTIONS
11:00:00 am Nov 27, 2019	COMPLETE	 5/5	✕

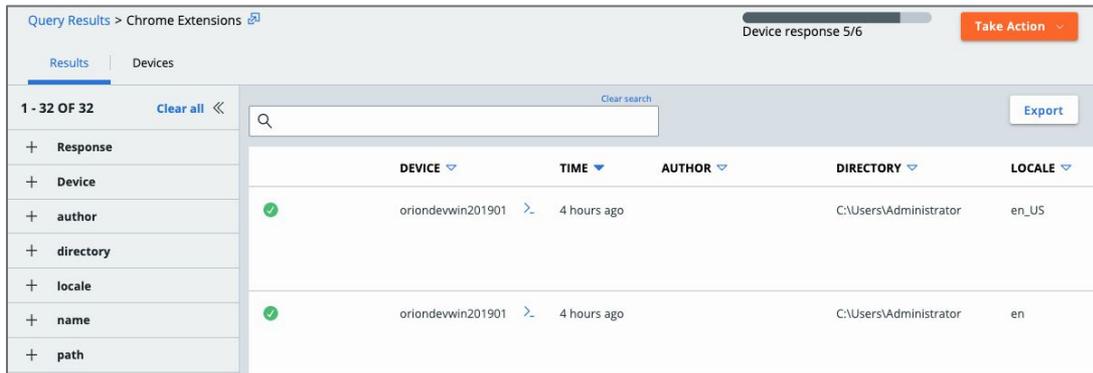
3 View query results



You can filter by **Results** or **Devices**. In each view, click the **Take Action** button to delete, stop (if applicable), rerun, or copy the query to SQL.

In the **Results** view, the **Response** and **Device** filters are always present. Other filters are generated based on your query. To download the data as a CSV file, click **Export**.

You can access **Live Response** to remediate threats by remotely accessing a user's machine. Click the **Live Response** icon () to get started.



	DEVICE	TIME	AUTHOR	DIRECTORY	LOCALE
✓	oriondevwin201901	4 hours ago		C:\Users\Administrator	en_US
✓	oriondevwin201901	4 hours ago		C:\Users\Administrator	en

In the **Devices** view, the **Device** and **Time** columns are always present. Other columns are generated based on your query.



	DEVICE	TIME	RESULTS	MEMORY	RESPONSE TIME	CPU USAGE	ACTIONS
✓	oriondevwin201901	4 hours ago	18	0.03%	421ms	0%	
✓	OrionDevMAC1013	4 hours ago	8	1.16%	446ms	0%	

4 Remediate with Live Response

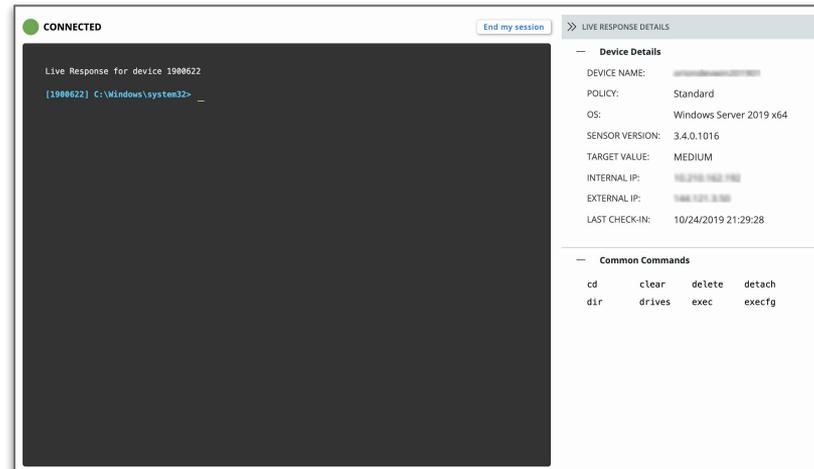


Use Live Response to perform investigations and remediate threats remotely

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

A black terminal screen appears once you're connected. To see a full list of available commands, type **help** or use the Live Response commands reference in the User Guide. To get help about a specific command, type **help commandname**.

Live Response access is dependent on user role authorization.



▶ Next Steps

Learn more about Audit and Remediation and the Carbon Black Cloud

Connect with the [Carbon Black User Exchange](#) for [the Query Hub](#) and additional resources, including [release notes](#), [knowledge base articles](#), [support](#), discussions, product news, updates, and more.

Take a [Carbon Black training course](#).