vmware Carbon Black

Getting Started with Audit and Remediation

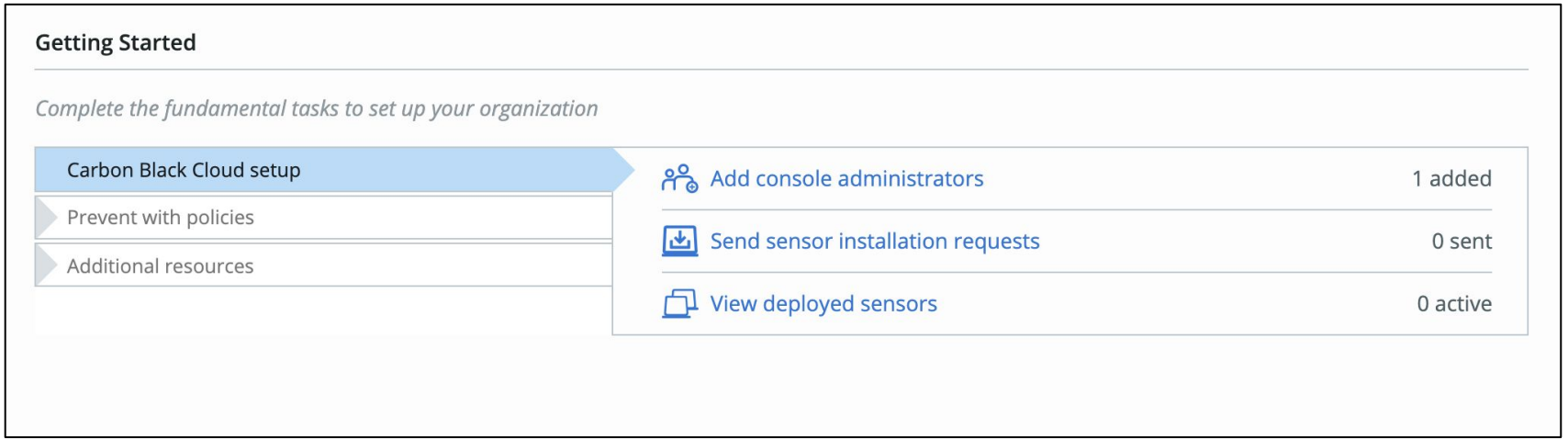
Audit and Remediation empowers teams to inspect endpoint status and trends and identify areas that require proactive action.

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.



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**

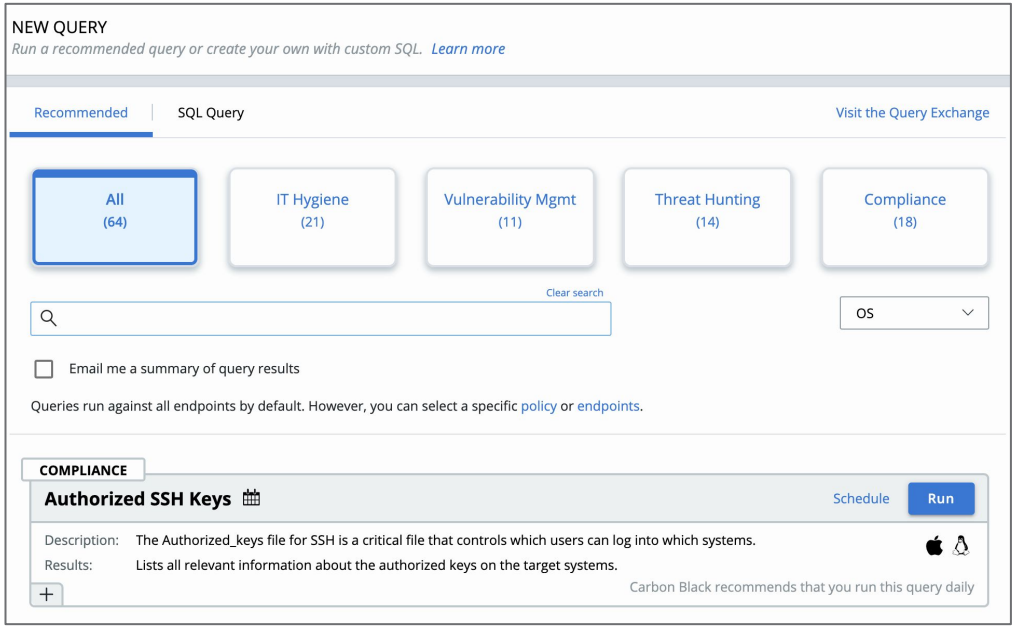
Query devices from Live Query or from Endpoints by clicking **Take Action** and then clicking **Query endpoints**.

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.

Carbon Black.

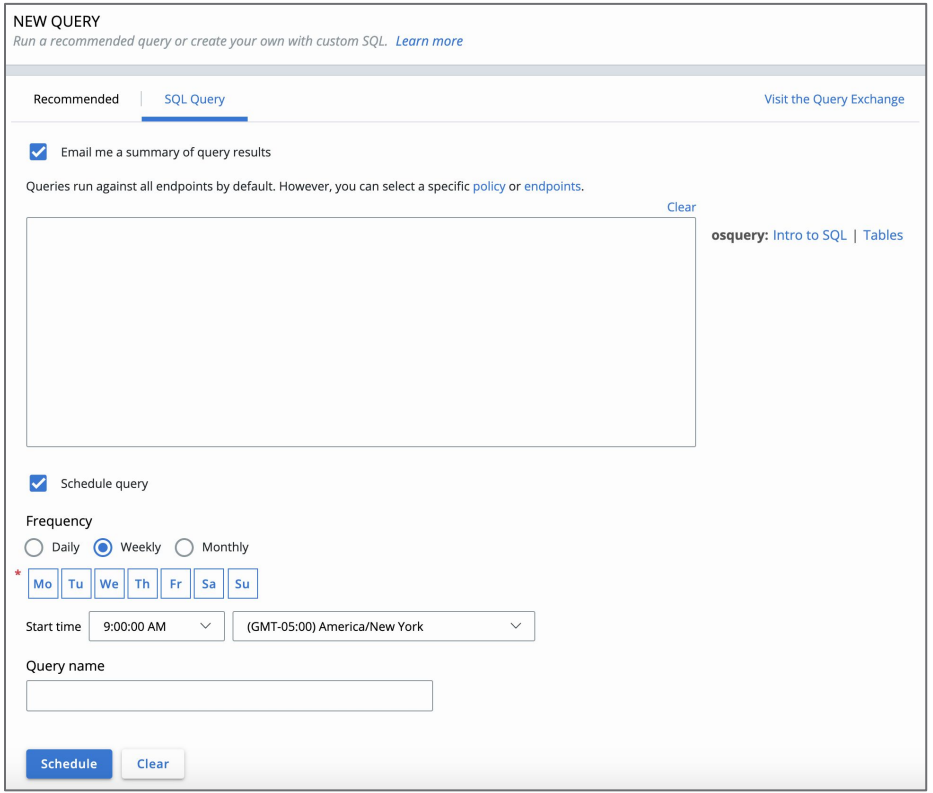
1 Run a SQL Query

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**.



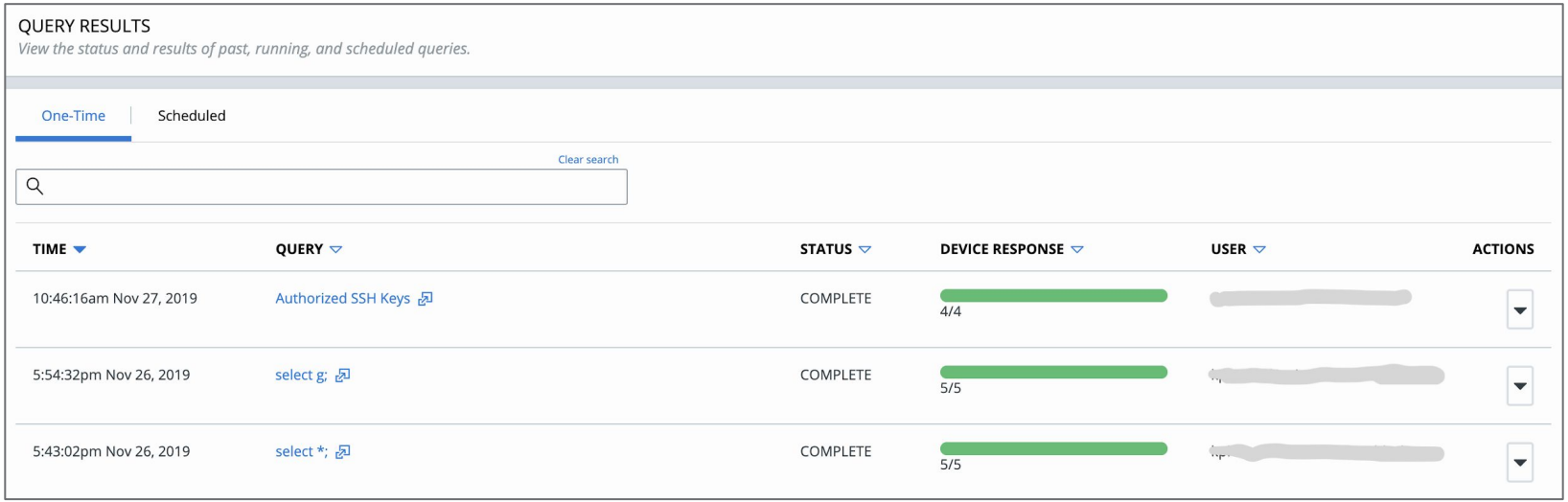
Carbon Black.

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.



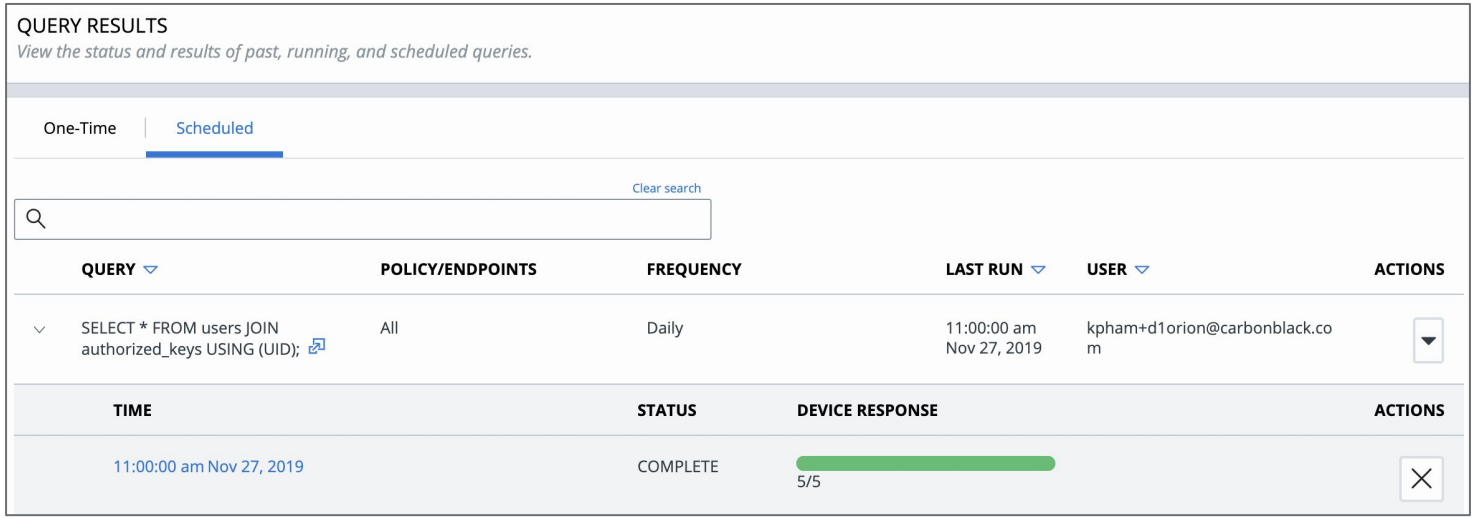
Carbon Black.

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.



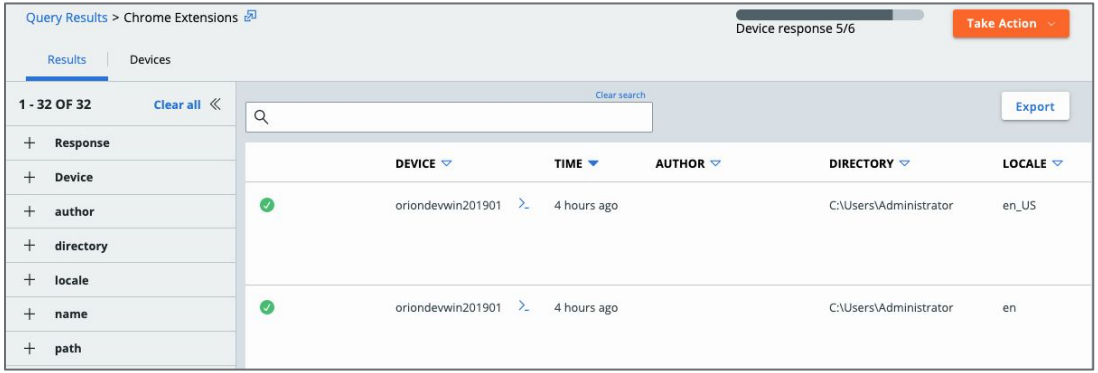
Carbon Black.

3 View query results

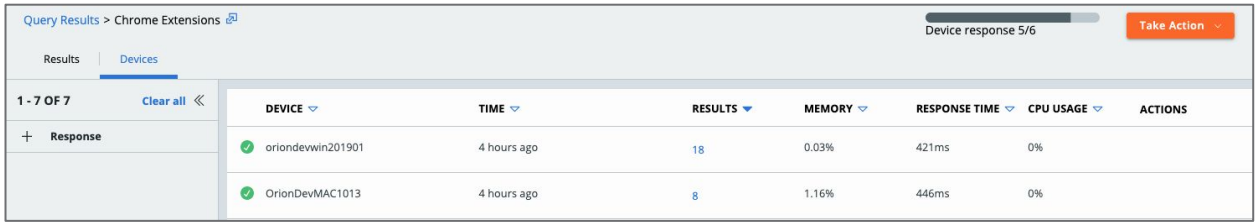
You can filter by **Results** or **Devices**. In each view, click the **Take Action** button to delete, stop (if applicable), rerun, or copy the query to SQL.

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.



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



Carbon Black.

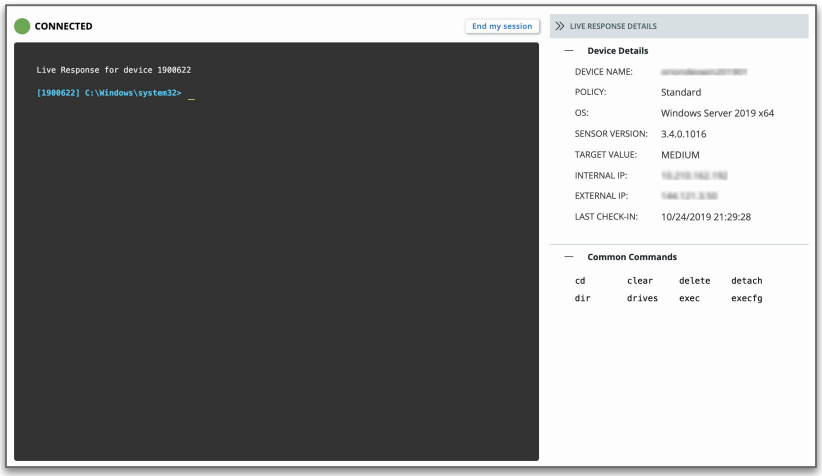
4 Remediate with Live Response

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.



Carbon Black.

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.