CrowdStrike APIs

12/10/2025

CrowdStrike OAuth2-Based APIs

Learn CrowdStrike API fundamentals, including OAuth 2.0 authentication, API clients and scopes, token management, rate limits, and more.

Overview

The CrowdStrike API is a set of REST-based API endpoints that allow you to perform actions programmatically instead of by using the Falcon console. This article provides a general overview of common API tasks, as well as example requests and responses.

Before you begin

The CrowdStrike API uses OAuth2 for authentication.

OAuth2 enables you to do the following:

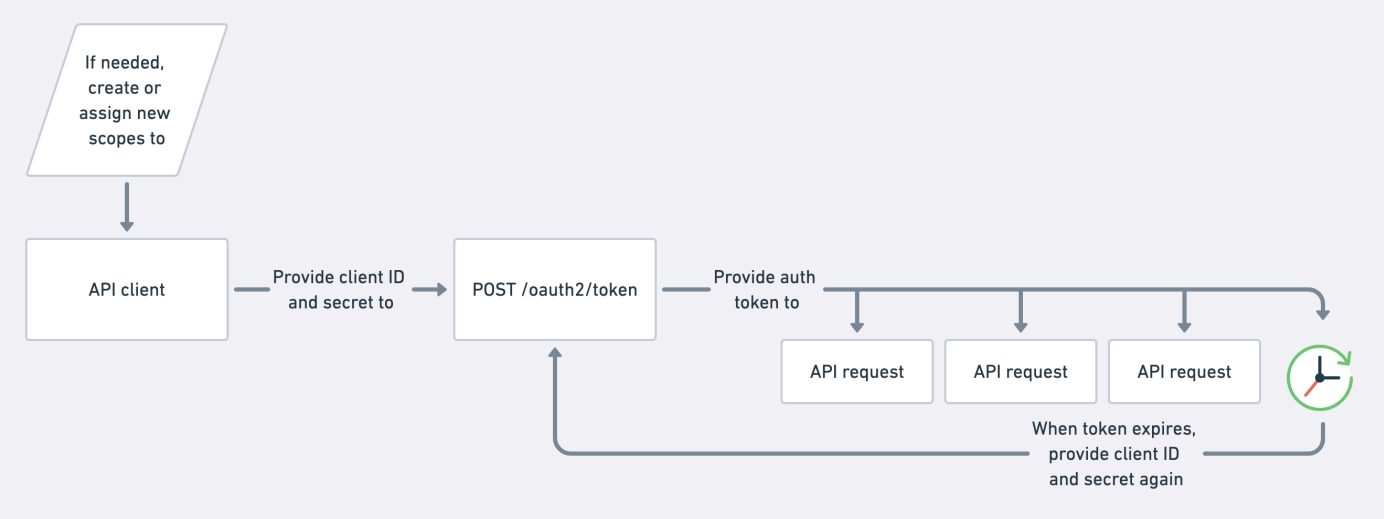
- Use access tokens to make API requests
- Manage multiple API clients within your organization
- Define limited scopes of permissions for API functionality

Key terms

Familiarize yourself with these key terms about APIs:

- **OAuth2**: An industry-standard specification for APIs. Get more info from the OAuth2 project.
  - **access token**: A limited-time authentication mechanism defined by the OAuth2 spec
  - **API client**: Represents an application or integration that accesses data from Falcon. Also used as a name for our newer authentication standard.
  - **API client ID**: One half of an API client's authentication credentials (similar to a username). API client IDs are case sensitive.
  - **API client secret**: The other half of an API client's authentication credentials (similar to a password). API client secrets are case sensitive.
  - **scope**: Defines what actions an API client can perform. Similar to permissions.
- **API endpoint**: An individual command that you can run using our API. For example, `/alerts/queries/alerts/v2` is an API endpoint that retrieves a list of alerts.
- **request**: An instance of you sending a command to Falcon using an API endpoint.
- **response**: An instance of receiving data after a request. In other words, Falcon replies to your request with a response.

Authenticating



1. Make a request to `POST /oauth2/token`, including an API client ID and API client secret.
   - `POST /oauth2/token` returns an access token to use in other requests.
   - Each access token is active for 30 minutes.

     Note: Don't request a new token for each API request. You'll be rate limited.
2. Make other requests to other API endpoints using your token.
3. When your token expires after 30 minutes, make a new request to `POST /oauth2/token`, then continue making requests to other API endpoints. Repeat this process for as long as you continue to make API requests.

Accessing the CrowdStrike API specification (Swagger)

See our CrowdStrike API specification outside of Falcon for full API reference info, including all available endpoints, parameters, and data models.

Note: You must be logged into the Falcon console in order to access the Swagger API specification.

Cloud environment	API reference info link
US-1	https://assets.falcon.crowdstrike.com/support/api/swagger.html
US-2	https://assets.falcon.us-2.crowdstrike.com/support/api/swagger-us2.html
EU-1	https://assets.falcon.eu-1.crowdstrike.com/support/api/swagger-eu.html
US-GOV-1	https://assets.falcon.laggar.gcw.crowdstrike.com/support/api/swagger-eagle.html
US-GOV-2	https://assets.falcon.us-gov-2.crowdstrike.mil/support/api/swagger.html

Base URLs

Each CrowdStrike cloud has a different base URL. When making requests to the CrowdStrike API, use the base URL that corresponds to the cloud where your integration is hosted.

- US-1: `https://api.crowdstrike.com`
- US-2: `https://api.us-2.crowdstrike.com`
- EU-1: `https://api.eu-1.crowdstrike.com`
- US-GOV-1: `https://api.laggar.gcw.crowdstrike.com`
- US-GOV-2: `https://api.us-gov-2.crowdstrike.mil`

Note: Unless otherwise indicated, the examples provided in CrowdStrike API documentation use the US-1 base URL. If necessary, be sure to modify example requests with the appropriate base URL for your cloud.

CrowdStrike domains and IP addresses to allow

For secure communication, access to the CrowdStrike API is restricted to certain domains and IP addresses. We recommend adding your cloud's designated domain name and the listed IP addresses (if applicable) to your network allowlist to avoid unintended access disruptions.

CrowdStrike API domains:

- US-1: `api.crowdstrike.com`
- US-2: `api.us-2.crowdstrike.com`
- EU-1: `api.eu-1.crowdstrike.com`
- US-GOV-1: `api.laggar.gcw.crowdstrike.com`
- US-GOV-2: `api.falcon.us-gov-2.crowdstrike.mil`

If you use CrowdStrike's US-1 cloud, you must also allow access for the following static IP addresses. All other clouds use dynamically assigned IPs that are subject to change.

US-1 API IP addresses:

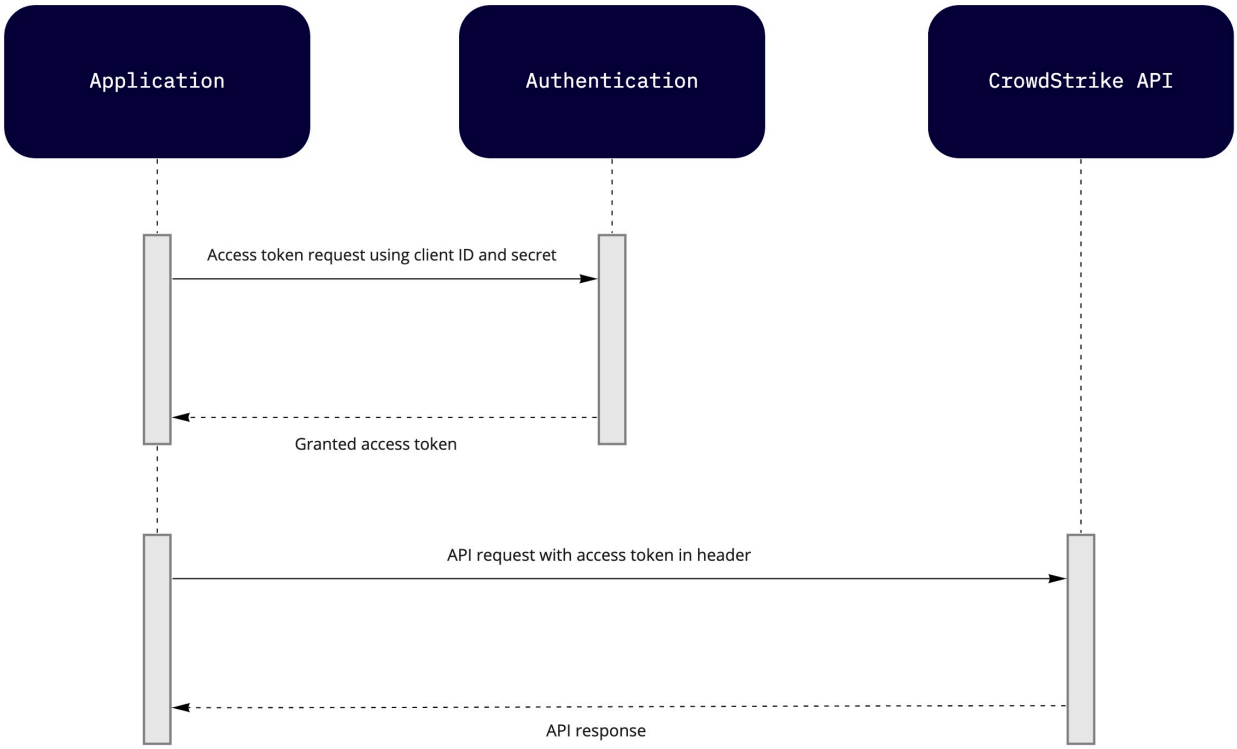
- 54.241.246.108
- 13.56.9.61

API clients

The OAuth 2.0 protocol provides secure access to the CrowdStrike API through scoped access tokens. To interact with any of our APIs, create an API client in the Falcon console and use the credentials to obtain an access token for making requests.

Understanding API clients

An API client is an identity mechanism that provides secure access to the CrowdStrike API. It contains credentials and scoped permissions to access specific API resources. You create an API client to generate your OAuth 2.0 client ID and secret credentials, which you exchange in the authentication flow for an access token that authorizes API requests.



Scopes

Each API client is assigned one or more API scopes. Scopes are permissions that specify the endpoints and methods an API client is allowed to access. When creating an API client you choose from read and write actions that can be executed on different groups of API endpoints. The scopes you set are applied to access tokens generated by the API client credentials and access is granted to only those endpoints authorized for use.

API client name and description

An API client has a name and optional description that you provide.

- **Name:** A unique, descriptive name up to 50 characters in length that identifies your API client in Falcon and in Action logs. The name can be anything you want and contain any combination of upper and lowercase letters, numbers, and special characters.
- **Description:** An optional description (up to 250 characters) can be provided to briefly define the API Client. We recommend stating the API client's intended purpose and any other information that your organization might want to track.

Client ID and secret

When an API client is created, a client ID and secret credential pair are generated. This information is used in the auth flow to identify and validate your integration.

- **Client ID:** The unique identifier of the API client. The client ID is visible from the API clients table in the Falcon console.
- **Secret:** A secret code for an API client, equivalent to a password. Keep the secret private and store it to a secure location for future reference. The secret is only visible to you at the time the API client is created. After that, it is not retrievable. If your client secret is ever lost, you can reset it to generate a new one.

Note: API Client IDs and secrets are case sensitive.

Access tokens

The API client ID and secret are exchanged in the authentication flow for an OAuth 2.0 access token that authorizes your API requests. Provide this token in each of your API requests using the HTTP authorization header. Tokens expire every half hour. They can't be refreshed but can be re-created as many times as necessary.

Best practices for API clients

- Create specialized API clients. It's easier to troubleshoot or audit API actions when each API client has a specific purpose.
- Follow the principle of least privilege: grant each API client only the scopes it needs to accomplish its task.

Managing your API clients

Users with the Falcon Administrator role can create new API clients from the API Clients and Keys page of the console.

Getting to your API clients

Access your API clients at Support and resources > Resources and tools > API clients and keys. From this page, you can perform these actions:

- View a list of current API clients
- Create new API clients
- Edit, delete, and reset the client secret of existing API clients
- Open the details panel of an API client to see:
    - Attributes such as description, client ID, date created, and last modified date
    - A sortable 90-day history of changes made to this API client
    - Which scopes are currently enabled on the API client
- View a log of API client activity.

Create an API client

Create API clients to grant various levels of API access for different purposes.

1. On the **API Clients and Keys** page (Support and resources > Resources and tools > API Clients and Keys), click **Create API client**.
2. Enter details to define your API client:
    - **Client Name** (required)
    - **Description** (optional)
    - API Scopes (required):
        - Select the **Read** and/or **Write** boxes next to a scope to enable access to its endpoints.
        - At least one scope must be assigned.
3. Click **Create** to save the API client and generate the client ID and secret.

Note: Record your API client secret somewhere safe. After the credential window is closed, the secret is no longer visible.

Reset an API client secret

If you lose your API client secret or suspect that it has been compromised, you can reset it from Support and resources > Resources and tools > API Clients and Keys in the Falcon console.

When you reset a client secret, the old secret no longer works and you must update your integration to use the new one. All access tokens issued before resetting the secret are immediately invalidated when the secret is reset.

1. Go to Support and resources > Resources and tools > API clients and keys.
2. On the right of the API client you want to update, click the three-dot menu ⋮ and select **Reset secret**.

   Note: You can also reset the secret from the three-dot menu ⋮ inside the details panel of a selected API client.
3. Click **Reset** on the confirmation prompt to permanently reset the API client secret.

   Note: Record your API client secret somewhere safe. After the credential window is closed, the secret is no longer visible.

Edit an API client

You can edit the name, description, and scopes of an existing API client in the Falcon console by going to Support and resources > Resources and tools > API clients and keys .

- API client name and description changes can take up to two minutes to appear.
- The Client ID cannot be changed.
- The API client secret cannot be customized, but it can be reset. For more info, see Reset an API client secret.

1. Go to Support and resources > Resources and tools > API clients and keys .
2. Next to the API client you want to update, click the **Open menu** ⋮ and select **Edit API client**.

   Note: You can also access the editor from the **Open menu** ⋮ inside the details panel of a selected API client.
3. Make changes to the **Client Name**, **Description**, or **API Scopes**, as needed.
4. Click **Update client details** to record your changes.

Delete an API client

Delete an API client you no longer need. Deleting an API client permanently removes it from the system, and it cannot be restored. Any access tokens issued to the deleted API client are immediately invalidated and no longer work.

1. On the **API clients and keys** page (Support and resources > Resources and tools > API clients and keys), click the three-dot menu ⋮ on the right of the API client you want to delete and select **Delete API client**.
2. Click **Delete** on the confirmation prompt.

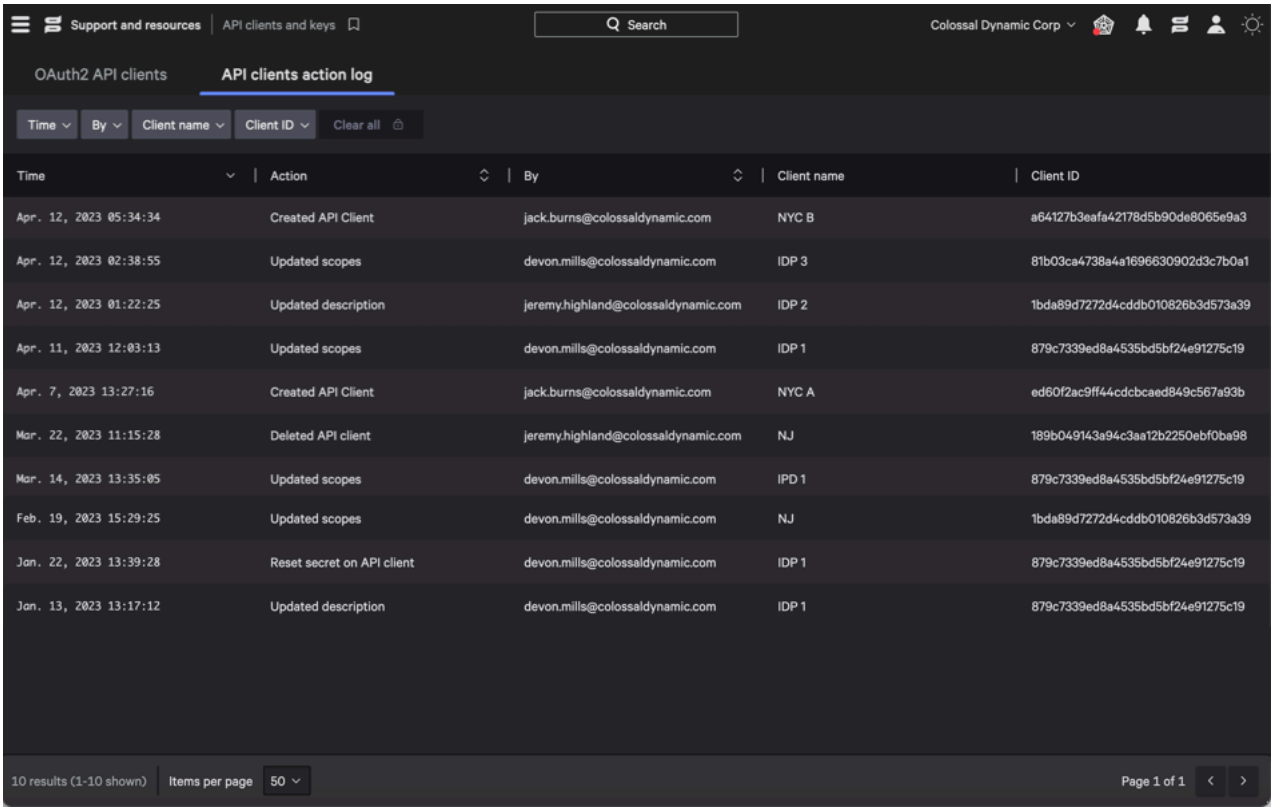
Reviewing the API client action log

The API clients action log provides a searchable 90-day history of recorded activity for the following actions:

- Creating API clients
- Deleting API clients
- Modifying an API client name or description
- Updating scopes
- Resetting the secret

To open the **Action log**, go to Support and resources > Resources and tools > API Clients and Keys and click the **API clients action log** tab.

The default view orders API Client actions by **Time**, with the most recent action displaying first. Use the filter menus to display only the actions you're interested in.



API scopes

API clients are granted one or more API scopes. Scopes allow access to specific CrowdStrike APIs and describe the actions that an API client can perform. Use scopes to fine-tune permissions of your API clients. OAuth 2.0 access tokens are scoped to the resources configured in the API client.

CrowdStrike supports the following API scopes. Not all scopes are available to all users. The scopes you see when creating an API client are determined by your subscribed products and the cloud where your account is hosted.

Scope name	API Swagger collection and path prefix	Capabilities and permissions	Product requirements
Actors (Falcon Intelligence)	intel /intel/	Search for data about adversaries that CrowdStrike is tracking. • **Read**: Get info about adversaries that match provided filters, retrieve specific adversaries using their adversary IDs, get adversary IDs that match provided filters. • **Write**: n/a	Falcon Intelligence or Falcon Intelligence Premium

Scope name	API Swagger collection and path prefix	Capabilities and permissions	Product requirements
Alerts	alerts /alerts/	View and manage detection information. In the CrowdStrike API, detections are stored as `alerts`. • **Read**: View information about a detection, such as its behavior, severity, associated host, timestamps, and more. • **Write**: Modify metadata about a detection, such as its status, assignee, and tags. This scope can't change core information about the detection (behavior, severity, associated host, timestamp, and so on).	Falcon Insight XDR or Falcon Prevent
Assets	discover, exposure management /discover/ (asset managment) /fem/ (external attack surface management)	Search for data about accounts, logins, applications, and managed, unmanaged, unsupported, and external assets. • **Read**: Get info about accounts, logins, applications, and assets that match provided filters, retrieve specific accounts, logins, applications, and assets using their IDs, get IDs that match provided filters. • **Write**: n/a	Falcon Exposure Management (asset management and external attack surface management) Falcon Discover (asset management only) Falcon Surface (external attack surface management only)
AWS accounts	cloud-connect-aws /cloud-connect-aws/	Allows access to your AWS resources. • **Read**: View information about your AWS resources. • **Write**: Create, modify, and delete Falcon information about your AWS resources.	Falcon Discover for Cloud and Containers
Cloud Security AWS Registration	/cloud-security-registration-aws/	Perform actions related to AWS accounts. • **Read**: View metadata for registered AWS accounts, such as features enabled, account name, and registration resources created. • **Write**: Register and remove AWS accounts and change the features enabled for AWS accounts.	Falcon Cloud Security
Cloud Security OCI Registration	/cloud-security-registration-oci//cloud-security-registration-oci/	Perform actions related to OCI tenancies. • **Read:** View metadata for registered OCI tenancies, such as features enabled, account name, and registration resources created. • **Write:** Register and remove OCI tenancies and change the features enabled for OCI tenancies.	Falcon Cloud Security
Configuration Assessment	/configuration-assessment/	Find and get detailed info about configuration assessments in your environment. • Read: Search for and get details about configuration assessments. • Write: n/a	Falcon Exposure Management
Content update policy	content-update-policies /policy/	Create and manage content update policies. • Read: View information about content update policies. • Write: Create, modify, and delete content update policies.	Falcon Insight XDR, Falcon Prevent
Correlation Rules	correlation-rules /correlation-rules/	Create and manage Next-Gen SIEM correlation rules. • Read: View details about correlation rules. • Write: Create, modify, and delete correlation rules.	Falcon Next-Gen SIEM or Falcon Next-Gen SIEM 10GB
CSPM registration	cspm-registration /cloud-connect-cspm-aws/, /settings/	Onboard and manage Azure accounts, Google Cloud (also known as Google Cloud Platform or GCP) accounts, and AWS accounts registered with legacy registration methods. • **Read**: View information about your AWS, Azure, and GCP resources, policies, and scan scheduling. • **Write**: Create, modify, and delete AWS, Azure, and GCP resources as well as update policy settings and scan schedule configurations.	Falcon Cloud Security

Scope name	API Swagger collection and path prefix	Capabilities and permissions	Product requirements
Custom IOA rules	custom-ioa /ioarules/	Add and manage custom indicators of attack (IOAs) to gain visibility into activity that isn't detected or prevented by Falcon. • **Read**: View details about your custom IOA rules and rule groups. • **Write**: Create, modify, or delete your custom IOA rules and rule groups, as well as assign rule groups to prevention policies. In addition, users with both Falcon Prevent and Falcon Insight XDR can enable Block and Kill actions.	Falcon Insight XDR
D4C registration	d4c-registration /cloud-connect-azure/, /cloud-connect-gcp/	Allows access to your GCP and Azure resources. • **Read**: View information about your GCP and Azure resources. • **Write**: Create and modify Falcon information about your GCP and Azure resources.	Falcon Discover for Cloud and Containers
Detections	detects /detects/	Allows access to detection information. • **Read**: View information about a detection, such as its behavior, severity, associated host, timestamps, and more. • **Write**: Modify metadata about a detection, such as its status, assignee, and description. This scope can't change core information about the detection (behavior, severity, associated host, timestamp, and so on).	Falcon Insight XDR or Falcon Prevent
Device control policies	device-control-policies /policy/	Create and manage USB device policies to gain visibility and control over USB devices in your environment. • **Read**: View information about your device control policies. • **Write**: Create, modify, and delete device control policies.	Falcon Device Control with either Falcon Prevent or Falcon Insight XDR
Event streams	streaming /sensors/	Connect to event streams (also called the streaming API). • **Read**: Find and connect to event streams. • **Write**: n/a Note: If your CrowdStrike cloud is US-GOV-1 or US-GOV-2 and your CID doesn't have event streams enabled, or if the status is unknown, contact Support for assistance.	Falcon Insight XDR, Falcon Prevent, or Falcon for Mobile
Falcon Complete Dashboard	...	The **Falcon Complete dashboard** scope describes an API client's access to Falcon Complete data. • **Read**: Get totals and aggregate information for Falcon Complete data. • **Write**: N/A	Falcon Complete
Falcon Container Image	falcon-container-image /falcon-container-image/	Allows access to scan your container images for vulnerabilities. • **Read**: View information and reports about image scanning. • **Write**: Push images to CrowdStrike for scanning.	Falcon Cloud Workload Protection
Falcon container registry	n/a	This scope is deprecated and should not be granted to clients.	n/a
Falcon Discover IoT	discover /discover/	Retrieve info on IT, operational technology (OT), Internet of Things (IoT), Internet of Medical Things (IoMT), and building management systems (BMS) assets in your environment. • Read: View aggregate or individual details for the managed, unmanaged, and unsupported assets in your environment. Endpoints support filters and sorting parameters. • Write: n/a	Falcon Discover for IoT
Falcon Images Download	falcon-container /container-security/	Allows access to the Linux User Mode Only Sensor (Lumos) • **Read**: Access API keys that enable pulling images from the CrowdStrike registry. • **Write**: n/a	Falcon Cloud Workload Protection
FileVantage	filevantage/filevantage/	Search for data about unauthorized changes in your environment.	Falcon FileVantage

Scope name	API Swagger collection and path prefix	Capabilities and permissions	Product requirements
		• **Read**: Get info about changes that match provided filters, retrieve specific changes using their change IDs, sort changes based on properties, get change IDs that match provided filters. • **Write**: n/a	
Firewall management	firewall-management, firewall-policies /fwmgr/ (firewall management) /policy/ (firewall policies)	Create and manage firewall policies using the firewall management and firewall policies APIs. • **Read**: View firewall policies, rules, rule groups, and activity. • **Write**: Create, modify, and delete firewall policies, rules, and rule groups.	Falcon Firewall Management with either Falcon Insight XDR or Falcon Prevent
Flight control	flight-control /mssp/	Manage CID groups, user groups, and role assignments in your Flight Control (MSSP) or multi-CID environments. • **Read**: View current CID groups, user groups, memberships, and role assignments • **Write**: Create, update, and delete CID groups, user groups, memberships, and role assignments	Falcon Flight Control
Host groups	host-group /devices/	Allows access to groups of hosts. You use host groups to assign policies. • **Read**: Search for groups, get hosts assigned to a group, and get other group details. • **Write**: Create groups, assign hosts to groups, and other actions.	Falcon Prevent or Falcon Insight XDR
Hosts	hosts /devices/, /devices/combined/devices/v1	Allows access to hosts.Note: Containing a host stops any network communications to locations other than the CrowdStrike cloud and IPs specified in your containment policy. For more info, see Network Containment. • **Read**: Search for hosts and get host details, using standard, scrolling pagination, or combined device endpoint. Details include OS type and version, sensor version, assigned policies, containment status, and more. • **Write**: Take action on hosts, including containing or lifting containment on a host.	Falcon Insight XDR or Falcon Prevent
Identity Protection Assessment	securityAssessment, riskFactors, riskByMembershipSummary, securityAssessmentGoals, securityAssessmentHistory /identity-protection/combined/graphql/v1	Retrieve security assessment and risk information. • **Read**: Search for domain-level security risk factors and risk factors for entities • **Write**: n/a **Note**: You must also enable the **Identity Protection GraphQL** *write* scope.	Falcon Identity Threat Detection or Falcon Identity Threat Protection
Identity Protection Detections	incident, incidents /identity-protection/combined/graphql/v1	Retrieve data about incidents • **Read**: Search incident data • **Write**: Change incident status **Note**: You must also enable the **Identity Protection GraphQL** *write* scope.	Falcon Identity Threat Detection or Falcon Identity Threat Protection
Identity Protection Enforcement	N/A	Used for integration with federation providers. • **Read**: View policy evaluation status and results, MFA UI state • **Write**: Provide external application access, advance MFA state	Falcon Identity Threat Detection or Falcon Identity Threat Protection
Identity Protection Entities	entities /identity-protection/combined/graphql/v1	Retrieve entity data. • **Read**: Search entity data • **Write**: Add/remove entity to watchlist, Mark/unmark entity **Note**: You must also enable the **Identity Protection GraphQL** *write* scope.	Falcon Identity Threat Detection or Falcon Identity Threat Protection

Scope name	API Swagger collection and path prefix	Capabilities and permissions	Product requirements
Identity Protection GraphQL	N/A	Enables access to the Identity Protection GraphQL APIs. • **Read**: n/a • **Write**: Allows usage of the Identity Protection GraphQL API	Falcon Identity Threat Detection or Falcon Identity Threat Protection
Identity Protection Health	N/A	Used for integration with federation providers. • **Read**: View Identity Protection cloud status • **Write**: n/a	Falcon Identity Threat Detection or Falcon Identity Threat Protection
Identity Protection on-premise enablement	N/A	Enables connections from the on-premises MFA enablement tool. • You must add both Read and Write.	Falcon Identity Threat Detection or Falcon Identity Threat Protection
Identity Protection Timeline	timeline /identity-protection/combined/graphql/v1	Retrieve data about timeline events and activities. • **Read**: Search timeline data • **Write**: n/a **Note**: You must also enable the **Identity Protection GraphQL** *write* scope.	Falcon Identity Threat Detection or Falcon Identity Threat Protection
Incidents	incidents /incidents/	Manage incidents and behaviors. • **Read**: Search and view details on incidents and behaviors. • **Write**: Perform actions on incidents, such as adding tags or comments or updating the incident name or description.	Falcon Insight XDR
Indicators (Falcon Intelligence)	intel /intel/	Look for various types of indicators. • **Read**: Find specific indicators and get info about indicators that match provided filter criteria. • **Write**: n/a	Falcon Intelligence or Falcon Intelligence Premium
Installation Tokens	installation-tokens /installation-tokens/	Create and manage installation tokens. Installation tokens are an opt-in security measure used when installing sensors in your environment. • **Read**: Find installation tokens and view token details. • **Write**: Create, modify, and delete installation tokens.	Falcon Prevent or Falcon Insight XDR
IOA Exclusions	ioa-exclusions /policy/	Create and manage exclusions that stop behavioral indicator of attack (IOA) detections and preventions. • **Read**: Search for and view the details about IOA exclusions. • **Write**: Create, modify, and delete IOA exclusions.	Falcon Prevent or Falcon Insight XDR
IOC Management	ioc-management /iocs/	Allows access to custom indicators of compromise (IOCs) in your customer account. • **Read**: Search your custom IOCs and view hosts that have observed your custom IOCs. **Note**: Falcon Prevent users can only search for IOCs that occurred under a certain detection tree. • **Write**: Create, modify, or delete your custom IOCs.	Falcon Insight XDR
Kubernetes Protection	kubernetes-protection /kubernetes-protection/	Allows you to view and manage visibility into your EKS, AKS and self-managed Kubernetes clusters. • **Read**: Visualize nodes, deployments, pods, and containers. • **Write**: Register AWS and AKS accounts for Kubernetes protection.	Falcon Cloud Workload Protection
Kubernetes Protection Agent	kubernetes-protection /kubernetes-protection/agent/	Allows you to extend runtime security to container workloads in Kubernetes clusters. • **Read**: n/a • **Write**: Register deployed Kubernetes Protection Agents.	Falcon Cloud Workload Protection

Scope name	API Swagger collection and path prefix	Capabilities and permissions	Product requirements
Machine Learning Exclusions	ml-exclusions /policy/	Create and manage machine learning (ML) exclusions. Use ML exclusions to stop all ML-based detections and preventions, or to prevent file uploads to the CrowdStrike cloud. • **Read**: Search for and view the details about ML exclusions. • **Write**: Create, modify, and delete ML exclusions.	Falcon Insight XDR or Falcon Prevent
MalQuery	malquery /malquery/	Query the contents of over a half-billion binary files, both clean and malicious, that are part of Falcon MalQuery's corpus. • **Read**: Retrieve metadata about files, get information about search and download quotas, check the status and results of YARA hunt requests, and list the monitor rules and their results. • **Write**: Perform YARA hunts, submit download requests, and create, edit, and delete monitoring rules.	MalQuery
Message Center	message-center /message-center/	The **Message Center** scope describes an API client's access to the Falcon Complete Message Center. • **Read**: See the Message Center. • **Write**: Read and write messages in the Message Center.	Falcon Complete
Message center for Falcon OverWatch	message-center /message-center/	The **Message Center for Falcon Overwatch** scope describes an API client's access to the Message Center for Falcon Overwatch. • **Read**: See the Message Center. • **Write**: Read and write messages in the Message Center.	Falcon Overwatch
Message Center for OverWatch Elite	message-center /message-center/	The **Message Center For Falcon Overwatch Elite** scope describes an API client's access to the Message Center for Falcon Overwatch Elite. • **Read**: See the Message Center. • **Write**: Read and write messages in the Message Center.	Falcon Overwatch Elite
Mobile Enrollment	mobile-enrollment /enrollments/	Generate email invitations to users when manually enrolling mobile devices. • Read: N/A • Write: Send email invitations to specified addresses.	Falcon for Mobile
On-demand scans (ODS)	ods /ods/	Run and view scans of PE files on Windows hosts, either immediately or according to a schedule. • Read: View data about upcoming or recent scans, and view scan results. • Write: Create, modify, and delete scans.	Falcon Prevent
OverWatch dashboard	...	The **OverWatch Dashboard** scope describes an API client's access to Falcon OverWatch data. • **Read**: Get totals and aggregate information for OverWatch data. • **Write**: N/A	Falcon OverWatch
Prevention policies	prevention-policies /policy/	Allows access to prevention policies.Policies are collections of settings that you assign to host groups. Prevention policies define how hosts detect and prevent activity. • **Read**: Search for prevention policies, get the state of prevention policy options for a prevention policy, and get other policy details. • **Write**: Create prevention policies, change prevention policy	Falcon Insight XDR or Falcon Prevent
Quick Scan (Falcon Intelligence)	quick-scan /scanner/	Submit uploaded files for analysis and receive verdicts. A verdict lets you know if a file is clean, potentially unwanted, or malware. • **Read**: Poll for the results of a scan and retrieve verdicts. • **Write**: Submit files for scanning.	QuickScan with either Falcon Intelligence or Falcon Intelligence Premium

Scope name	API Swagger collection and path prefix	Capabilities and permissions	Product requirements
Real time response	real-time-response /real-time-response/	Run Real Time Response commands equivalent to the RTR Read Only Analyst or RTR Active Responder user roles. For a list of commands by role, see Real Time Response. • **Read**: Run RTR commands that get information from a host, equivalent to the RTR Read Only Analyst role. • **Write**: Run RTR commands that send information to a host, equivalent to the RTR Active Responder role.	Falcon Insight XDR or Falcon Prevent with Control and Respond
Real time response (admin)	real-time-response-admin /real-time-response/	Run Real Time Response commands equivalent to the RTR Administrator user role. For a list of commands by role, see Real Time Response commands. • **Read**: n/a • **Write**: Run RTR commands equivalent to the RTR Administrator role.	Falcon Insight XDR or Falcon Prevent with Control and Respond
Real time response audit	real-time-response-audit /real-time-response-audit/	View an audit log of all Real Time Response actions (UI and API) equivalent to the Falcon Admin user role. For a list of commands by role, see Real Time Response. • **Read**: View an audit log of all RTR actions, across all users, run using the UI and API, equivalent to the Falcon Admin user role. • **Write**: n/a	Falcon Insight XDR or Falcon Prevent with Control and Respond
Reports (Falcon Intelligence)	intel /intel/	Query CrowdStrike intelligence publications. • **Read**: Get info about reports that match provided filters, return report PDF attachments, retrieve specific reports using their report IDs, and get report IDs that match provided filters. • **Write**: n/a	Falcon Intelligence Premium
Response policies	response-policies /policy/	Create and manage policies that define which Real Time Response commands can be executed on your hosts. • **Read**: Get info about your Real Time Response policies. • **Write**: Create, modify, and delete Real Time Response policies.	Falcon Insight XDR
Rules (Falcon Intelligence)	intel /intel/	Download packages of rules that intelligence publishes (such as Snort, Yara, Suricata, Common Event, and NetWitness). • **Read**: Search for rule IDs that match provided filter criteria, retrieve details for rule sets for the specified IDs, and download the latest and earlier rule sets. • **Write**: n/a	Falcon Intelligence Premium
Sample uploads	sample-uploads /archives/, /samples/	Upload files to CrowdStrike and retrieve uploaded files. • **Read**: Retrieve files associated with given IDs (SHA256). • **Write**: Upload files for further analysis and delete uploaded samples.	Falcon Intelligence or Falcon Intelligence Premium
Sandbox (Falcon Intelligence)	falconx-sandbox /falconx/, /samples/	Submit malware samples and download reports using Falcon Intelligence. • **Read**: Get summaries, reports, PCAP files, and other artifacts; search for uploaded samples or reports. • **Write**: Upload malware samples and submit samples for sandbox analysis.	Falcon Intelligence or Falcon Intelligence Premium
SaaS Security (Falcon Shield)	saas-security /saas-security/	Retrieve and manage SaaS security configuration and event data. • **Read**: View details about configured integrations, security checks, inventories and event information. • **Write**: Dismiss security checks and upload custom integration data sets.	Falcon Shield
Sensor Download	sensor-download /sensors/	Find and download sensor installers, as well as your customer ID with checksum (CCID).	Falcon Insight XDR or Falcon Prevent

Scope name	API Swagger collection and path prefix	Capabilities and permissions	Product requirements
		• **Read**: Search for sensor installers and get sensor installer details. Get your organization's customer ID with checksum (CCID). • **Write**: n/a	
Sensor update policies	sensor-update-policies /policy/	Allows access to sensor update policies, uninstall tokens, and bulk maintenance tokens. Policies are collections of settings that you assign to host groups. Sensor update policies manage automatic or manual upgrades to the Falcon sensor. • **Read**: Search for sensor update policies, get the state of sensor update policy options, get other policy details. • **Write**: Create sensor update policies, change sensor update policy options, and delete sensor update policies, reveal uninstall tokens, and retrieve maintenance tokens.	Falcon Insight XDR or Falcon Prevent
Sensor Visibility Exclusions	sensor-visibility-exclusions /policy/	Create and manage sensor visibility exclusion policies. These APIs enable you to exclude trusted file paths from sensor monitoring. • **Read**: Search for and get the details of sensor visibility exclusions. • **Write**: Create, modify, and delete sensor visibility exclusions.	Falcon Insight XDR or Falcon Prevent
Threatgraph	threatgraph /threatgraph/	Retrieve data from ThreatGraph. • **Read**: Get metadata and see relationships between entities such as indicators, process executions, image file loads, and IP addresses. Look up instances of indicators (such as hashes, domain names, and IP addresses) seen on hosts in your environment. • **Write**: N/A	Falcon Insight XDR or Falcon Prevent
User Management	user-management /user-roles/, /users/	Allows access to user and role information. Users represent the people who access the Falcon console to manage your Falcon environment. User roles are collections of permissions that govern which actions users can take in the Falcon console. For more info, see User Management. • **Read**: Find users and get information about users (such as user IDs, email addresses, and roles). • **Write**: Create users, change user information (such as first or last names), and assign or revoke roles.	Falcon Insight XDR or Falcon Prevent or Falcon Intelligence or Falcon Intelligence Premium or Malquery
Vulnerabilities	spotlight-vulnerabilities /spotlight/	Find and get detailed info about vulnerabilities in your environment. • **Read**: Search for and get details about vulnerabilities and remediations. • **Write**: n/a	Falcon Spotlight or Falcon Exposure Management
Workflow	workflows /workflows/	Manage Fusion SOAR workflows. • **Read:** Find and view workflow executions, execution results, and human input. Find, view and export workflow definitions. • **Write:** Execute workflows, run mock executions. Import, update, and delete workflow definitions.	Any subscription that can access Fusion SOAR workflows
Zero Trust Assessment	zero-trust-assessment/entities/	Retrieve Zero Trust Assessment data for one or more hosts. • **Read**: Get ZTA data about the security posture of one or more hosts that match the specified filters. • **Write**: n/a	Falcon Insight XDR

Rate limiting

All requests to the CrowdStrike API are subject to a rate limit.

- The default rate limit for requests containing a valid bearer token is 6,000 requests per minute per customer account. Each request in your customer account removes one request from that pool, regardless of which API endpoint or API client is used for the request. The rate limit is calculated on a sliding window.
- Requests with missing, malformed, or expired bearer tokens are rate limited at 300 requests per minute per source IP address (not per customer account). This includes requests to get an auth token, because by definition these requests do not include a bearer token. For more info, see Get an auth token.

If you exceed your rate limit, the response to any further request returns a **HTTP 429: Too Many Requests** error, along with current rate limit status as HTTP headers.

Rate limiting header	Type	Description	Included in responses
`X-RateLimit-Limit`	`int`	Maximum number of requests per minute that can be made by all API clients in your customer account (also called a "CID")	Every response
`X-RateLimit-Remaining`	`int`	Number of requests that remain in your customer account's rate limiting pool. Remember that making an API request removes one request from your customer account's API rate limiting pool; the pool automatically replenishes requests over time.	Every response
`X-RateLimit-RetryAfter`	Date/time (UTC epoch timestamp)	The next time when your customer account's rate limit pool will have at least one request available. This header is only included if you exceed your customer account's rate limit (in other words, after `X-RateLimit-Remaining` would go below `0`).	Only when rate limit is exceeded

Best practices for rate limiting

As a best practice, we recommend that you monitor the rate limiting headers that are returned with each request, then tune your API script or integration so that the rate limiting pool is restored more quickly than your requests deplete it.

Rate limited response

If you make a request when your rate limiting pool is empty, the response looks like this:

```
HTTP/2 429
content-type: application/json
x-content-type-options: nosniff
x-ratelimit-limit: 6000
x-ratelimit-remaining: 0
x-ratelimit-retryafter: 1555640820
content-length: 224
date: Fri, 19 Apr 2019 02:26:34 GMT


{
 "meta": {
  "query_time": 0.000875986,
  "powered_by": "crowdstrike-api-gateway",
  "trace_id": "7d1d6add-950d-4c45-89a3-5aa565d31e39"
 },
 "errors": [
  {
   "code": 429,
   "message": "API rate limit exceeded."
  }
 ]
```

Cross-cloud URL redirects

The CrowdStrike API supports automatic URL redirects between US-1, US-2, and EU-1 clouds to help ensure requests are sent to the correct environment. The cross-cloud redirect functionality identifies when a request is submitted to the wrong cloud and intelligently routes it to the correct cloud instead of returning an "invalid credentials" error.

Note: API redirect behavior is only provided between CrowdStrike US-1, US-2, and EU-1 clouds. Support for US-GOV-1 and US-GOV-2 is not currently available.

How cross-cloud redirection works

Incoming requests to CrowdStrike API are handled by first obtaining the right cloud location based on the ID of the API client. If the landing cloud of the request does not match the API client cloud, the request is automatically rerouted to the correct cloud. For example, a request that hits US-1 with US-2 credentials redirects to US-2 (and vice versa). All requests are authenticated prior to redirection. Redirected requests return an HTTP 308 (Permanent Redirect) status with the correct cloud URL provided in the Location header of the response.

Redirect handling

Your integration must handle 308 redirects. Many common programming languages and HTTP-related libraries follow the redirect instruction of HTTP 308. However, some might require special handling for redirects.

A 308 redirect provides a new URL in the Location header to resubmit the request. If you see an HTTP 308 response, follow the redirect by repeating the request at the new address with the same HTTP method and body used in the original request. In addition, some programming libraries do not forward the Authorization header to the redirected URL, which results in a 401 (Unauthorized) error. Your code should anticipate that the Authorization header might not be passed and add the header back before resending the call.

Redirects and rate limiting

Because the HTTP 308 requires an additional round trip, redirected requests are counted twice toward the rate limit. To avoid rate limit errors, we recommend caching the Location and making all subsequent requests directly to this URL.

Formatting requests

Your API requests should follow these general guidelines:

- JSON formatting: Requests and responses are formatted as JSON. Your requests must include `Content-Type` and `Accepts` headers with the value `application/json`.
- Time formatting: Requests and responses use UTC timestamps that conform to RFC 3339, such as: `2013-04-17T09:12:36-00:00`

Format of responses

All responses from the CrowdStrike API include these three sections:

- Meta: Metadata about the response, including paging information, query time, and a trace identifier for debugging
- Resources: Your actual data as an array of objects
- Errors: Any errors associated with your response.

Below is a sample response showing all three sections:

```
{
  "meta": {
    "query_time": 0.002,
    "trace_id": "96d0c5db",
  },
  "resources": [],
  "errors": []
}
```

Note: Data retention: Information included in API responses is subject to your data retention plan. CrowdStrike purges data for hosts if they haven't contacted the CrowdStrike cloud for 45 days.

Responses with partial successes

API endpoints that allow bulk operations can partially succeed, in which case successful operations are included in `resources` and failed operations are included in `errors`. This example includes a request about two domains; the first domain exists (`example1.com`) and the second does not (`example2.com`):

```
curl -X GET "https://api.crowdstrike.com/indicators/entities/iocs/v1?ids=domain:example1.com&ids=domain:example2.com"
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json' \
```

Note: Unless otherwise indicated, the examples provided in CrowdStrike API documentation use the US-1 base URL. If necessary, be sure to modify example requests with the appropriate base URL for your cloud. For more info, see Base URLs.

The associated response indicates partial success:

```
{
  "meta": {
    "query_time": 0.0032846000000000004,
    "trace_id": "503fde00-f1e8-4e96-9baf-633412ee1922"
  },
  "resources": [
    {
      "type": "domain",
      "value": "example1.com",
      "policy": "detect",
      "source": "source",
      "share_level": "red",
      "expiration_timestamp": "2016-06-16T00:00:00Z",
      "description": "here is my description",
      "created_timestamp": "2016-05-17T20:32:02Z",
      "created_by": "XXXXXXXXXXXXXXXXXXXXXX",
      "modified_timestamp": "2016-05-17T20:32:02Z",
      "modified_by": "XXXXXXXXXXXXXXXXXXXXX"
    }
  ],
  "errors": [
    {
      "code": 404,
      "message": "domain:example2.com - Resource Not Found"
    }
  ]
}
```

Auditing APIs in the Falcon console

Use the Falcon console to audit these items:

- Actions taken using the API
- Changes to your API clients

Auditing API actions

The Audit logs > Audit logs > API dashboard shows critical actions taken using OAuth2-based APIs in your Falcon environment. The dashboard shows these items:

- User changes, creations, or deletions
- Requests made to the API and their outcomes–excluding the request body and authorization headers
- Host group changes, creations or deletions
- Prevention policy changes, creations, or deletions
- Sensor update policy changes, creations, or deletions
- API client changes, creations, or deletions
- Applying or lifting containment on hosts
- Detection updates

Also, you can export the current view.

The dashboard offers these features:

- Configurable columns. Click **Configure table columns** to set the columns you see.
- Filters across the top of the dashboard to focus the view on what's most important.
- The **Add/remove filters** dropdown menu to adjust the filters.
- A detail panel to easily see the main info for any request. Click a row to show its detail panel. The panel content changes based on the row type clicked.

Note: The API audit dashboard shows actions taken using OAuth2-based APIs. It doesn't show actions taken using the Falcon console or our APIs that still use our legacy key-based authentication.

OAuth2 Auth Token APIs

Generate and manage OAuth 2.0 tokens required for accessing CrowdStrike APIs.

About CrowdStrike APIs

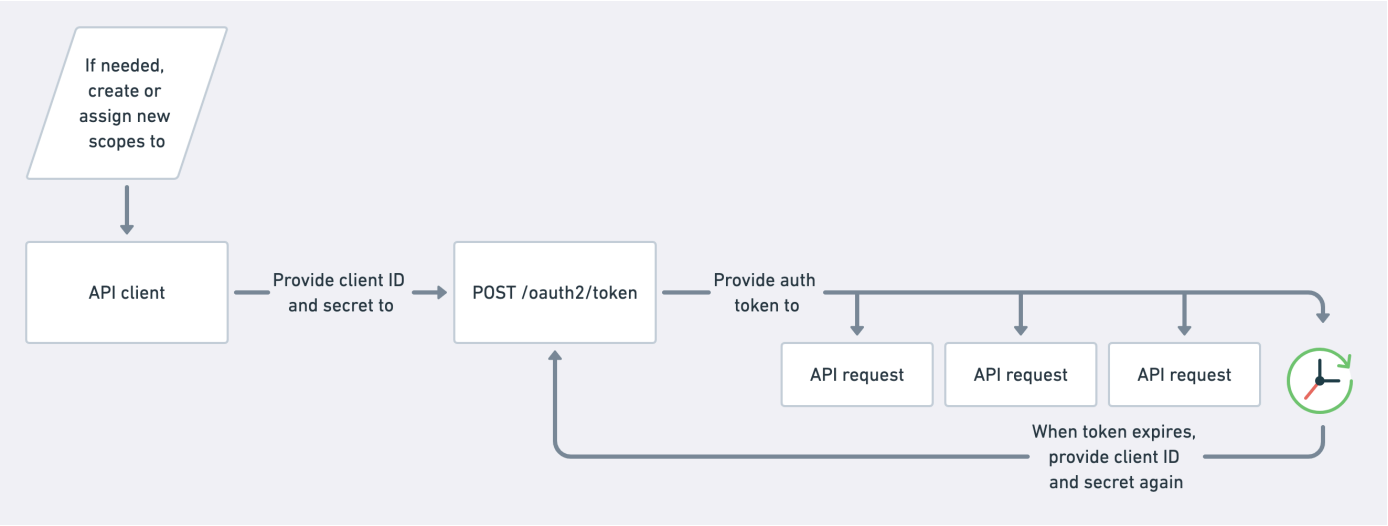
CrowdStrike provides use cases and example requests and responses for interacting with a specific set of our OAuth2-based APIs. For general info about CrowdStrike APIs, see CrowdStrike OAuth2-Based APIs, which covers these topics:

- Details on getting started, such as authentication and API scopes
- Domains used in base URLs by cloud
- Links to our Swagger API specification by cloud

Manage auth tokens

CrowdStrike API endpoints use OAuth2 token-based authentication. Basic authentication using a username and password is not supported.

The general flow for OAuth2-based API authentication looks like this:



You can use the CrowdStrike API to perform these common tasks related to auth tokens:

- Get an auth token
- Revoke an auth token

Get an auth token

Getting an auth token is a very common action because you must supply an auth token with each request to a CrowdStrike API endpoint.

Auth tokens expire 30 minutes after they're created. After that time, the API responds with an auth error. When this happens, your API integration should pause, get a new auth token, then resume its normal activity.

The rate limit for auth tokens is 300 requests per minute per source IP address (not per customer account). Our best practice recommendation is to request a new auth token only when the previous auth token's lifetime ends after 30 minutes. For more info, see Rate limiting.

Relevant API endpoints

- POST /oauth2/token

1. Supply your API client ID and API client secret to `/oauth2/token`

Example request

Make a request to `POST /oauth2/token`, including your API client's client ID and client secret.

```
curl -X POST "https://api.crowdstrike.com/oauth2/token" \
 -H "accept: application/json" \
 -H "Content-Type: application/x-www-form-urlencoded" \
 -d "client_id=a1b2c3d4e5f6&client_secret=QWE987RTY654UIOP321"
```

Example response


```
{
    "access_token":
"RmFsY29ucyAoL8uIZsmSbGvJmW4sIMuIZsmUy5BsLSwgy4hmw6ZsLS8pIGFyZSBiaXJkcyBvZiBwcmV5IGluIHRoZSBnZW51cyBGYWxjbywgd2hpY2ggaW5jbHVkZXMgYWJvdXQgNDAgc3BlY2llcy4gRmFsY29uc
yBhcmUgd2lkZWx5IGRpc3RyaWJ1dGVkIG9uIGFsbCBjb250aW5lbnRzIG9mIHRoZSB3b3JsZCBleGNlcHQgQW50YXJjdGljYSwgdGhvdWdoIGNsb3NlbHkgcmVsYXRlZCByYXB0b3JzIGRpZCBvY2N1ciB0aGVyZSB
pbiB0aGUgRW9jZW5lLlsxXQ==RmFsY29ucyAoL8uIZsmSbGvJmW4sIMuIZsmUy5BsLSwgy4hmw6ZsLS8pIGFyZSBiaXJkcyBvZiBwcmV5IGluIHRoZSBnZW51cyBGYWxjbywgd2hpY2ggaW5jbHVkZXMgYWJvdXQgN
DAgc3BlY2llcy4gRmFsY29ucyBhcmUgd2lkZWx5IGRpc3RyaWJ1dGVkIG9uIGFsbCBjb250aW5lbnRzIG9mIHRoZSB3b3JsZCBleGNlcHQgQW50YXJjdGljYSwgdGhvdWdoIGNsb3NlbHkgcmVsYXRlZCByYXB0b3J
zIGRpZCBvY2N1ciB0aGVyZSBpbiB0aGUgRW9jZW5lLlsxXQ==RmFsY29ucyAoL8uIZsmSbGvJmW4sIMuIZsmUy5BsLSwgy4hmw6ZsLS8pIGFyZSBiaXJkcyBvZiBwcmV5IGluIHRoZSBnZW51cyBGYWxjbywgd2hpY
2ggaW5jbHVkZXMgYWJvdXQgNDAgc3BlY2llcy4gRmFsY29ucyBhcmUgd2lkZWx5IGRpc3RyaWJ1dGVkIG9uIGFsbCBjb250aW5lbnRzIG9mIHRoZSB3b3JsZCBleGNlcHQgQW50YXJjdGljYSwgdGhvdWdoIGNsb3N
lbHkgcmVsYXRlZCByYXB0b3JzIGRpZCBvY2N1ciB0aGVyZSBpbiB0aGUgRW9jZW5lLlsxXQ==",
    "token_type": "bearer",
    "expires_in": 1799
}
```


Revoke an auth token

Revoke an auth token to cancel it before the end of its normal 30-minute lifespan. Revoking a token is not required for normal API activity. In most cases, revoke a token only for an immediate concern, such as a token accidentally being shared online.

Relevant API endpoints

- POST /oauth2/revoke

Steps

1. Base-64 encode your API client ID and secret into a single string, using this format:

   `clientID:clientSecret`

2. Make a request to `POST /oauth2/revoke`, including the token to revoke and your base-64 encoded client ID and secret

Example request

```
curl -X POST "https://api.crowdstrike.com/oauth2/revoke" \
 -H 'Accept: application/json' \
 -H 'Authorization: Basic bXlfYXBpX2NsaWVudF9pZDpteV9hcGlfY2xpZW50X3NlY3JldA' \
 -H 'Content-Type: application/x-www-form-urlencoded' \
 -d
'token=RmFsY29ucyAoL8uIZsmSbGvJmW4sIMuIZsmUy5BsLSwgy4hmw6ZsLS8pIGFyZSBiaXJkcyBvZiBwcmV5IGluIHRoZSBnZW51cyBGYWxjbywgd2hpY2ggaW5jbHVkZXMgYWJvdXQgNDAgc3BlY2llcy4gRmF
sY29ucyBhcmUgd2lkZWx5IGRpc3RyaWJ1dGVkIG9uIGFsbCBjb250aW5lbnRzIG9mIHRoZSB3b3JsZCBleGNlcHQgQW50YXJjdGljYSwgdGhvdWdoIGNsb3NlbHkgcmVsYXRlZCByYXB0b3JzIGRpZCBvY2N1ciB0a
GVyZSBpbiB0aGUgRW9jZW5lLlsxXQ==RmFsY29ucyAoL8uIZsmSbGvJmW4sIMuIZsmUy5BsLSwgy4hmw6ZsLS8pIGFyZSBiaXJkcyBvZiBwcmV5IGluIHRoZSBnZW51cyBGYWxjbywgd2hpY2ggaW5jbHVkZXMgYWJ
vdXQgNDAgc3BlY2llcy4gRmFsY29ucyBhcmUgd2lkZWx5IGRpc3RyaWJ1dGVkIG9uIGFsbCBjb250aW5lbnRzIG9mIHRoZSB3b3JsZCBleGNlcHQgQW50YXJjdGljYSwgdGhvdWdoIGNsb3NlbHkgcmVsYXRlZCByY
XB0b3JzIGRpZCBvY2N1ciB0aGVyZSBpbiB0aGUgRW9jZW5lLlsxXQ==RmFsY29ucyAoL8uIZsmSbGvJmW4sIMuIZsmUy5BsLSwgy4hmw6ZsLS8pIGFyZSBiaXJkcyBvZiBwcmV5IGluIHRoZSBnZW51cyBGYWxjbyw
gd2hpY2ggaW5jbHVkZXMgYWJvdXQgNDAgc3BlY2llcy4gRmFsY29ucyBhcmUgd2lkZWx5IGRpc3RyaWJ1dGVkIG9uIGFsbCBjb250aW5lbnRzIG9mIHRoZSB3b3JsZCBleGNlcHQgQW50YXJjdGljYSwgdGhvdWdoI
GNsb3NlbHkgcmVsYXRlZCByYXB0b3JzIGRpZCBvY2N1ciB0aGVyZSBpbiB0aGUgRW9jZW5lLlsxXQ=='
```

Retrieving a list of available sensor versions

Get a list of the available sensor build versions that you can use in your policies.

Each build version value can include this info:

- Build number: All builds, fixed or automatic, include a build number
- Build stage: For automatic builds only
    - `early_adopter`: Auto - Early Adopter
    - `n`: Auto - Latest
    - `n-1`: Auto - N-1
    - `n-2`: Auto - N-2
- `tagged | <number>`: For automatic builds only, CrowdStrike internal identifier for a tag type, platform, and cloud environment.

For example:

```
"build": "16410|n|tagged|11",
```

Endpoint

```
GET /policy/combined/sensor-update-builds/v1
```

Parameters

Name	In	Description
`platform` *optional*	query	Limit the response to builds on the specified platform. One of: • `windows` • `linux` • `mac` Enter as shown, in lowercase. If the `platform` parameter is not specified, builds for all platforms are returned.
`stage` *optional*	query	Limit the response to builds in a specific stage. One of: • `prod` • `early_adopter` Enter as shown, in lowercase. The default value is prod. If the `stage` parameter is not specified, only builds in the `prod` stage are returned.

Note: You can see kernel support info for specific versions of Falcon sensor for Linux using the `/policy/combined/sensor-update-kernels/v1` endpoint. For more info, see Retrieving kernel support info.

Example request

```
curl --request GET \
--header 'accept: application/json' \
--header 'Authorization: Bearer eyJh....H8Y' \
'https://api.crowdstrike.com/policy/combined/sensor-update-builds/v1?platform=windows&stage=early_adopter&stage=prod'
```

Example response


```
{
  "meta": {
    "query_time": 0.011198251,
    "trace_id": "b1836dc1-c083-4200-ba16-69963ba34407"
  },
  "errors": [],
  "resources": [
   {
     "build": "16303|n-1|tagged|1",
     "sensor_version": "6.49.16303",
     "platform": "Windows",
     "stage": "prod"
   },
   {
     "build": "16207|n-2|tagged|2",
     "sensor_version": "6.48.16207",
     "platform": "Windows",
     "stage": "prod"
   },
   {
     "build": "16410|n|tagged|11",
     "sensor_version": "6.50.16410",
     "platform": "Windows",
```

```
    "stage": "prod"
   },
   {
    "build": "16411|early_adopter|tagged|16",
    "sensor_version": "6.50.16411",
    "platform": "Windows",
    "stage": "early_adopter"
   }
  ]
}
```

Sensor Usage APIs

Retrieve weekly and hourly sensor usage metrics by category across your environment.

Overview

Retrieve average weekly or hourly sensor usage data for your customer ID (CID), broken down by sensor category. The Sensor Usage API retrieves the same data provided through the Sensor usage dashboard (Dashboards and reports > Billing > Sensor Usage) in the Falcon console. For more info, see View usage with the Sensor usage dashboard. For info about getting started with CrowdStrike APIs, see CrowdStrike OAuth2-Based APIs.

Requirements

- CrowdStrike clouds: Sensor usage APIs are not available in the US-GOV-1 or US-GOV-2 CrowdStrike clouds.
- API client scope: To use the Sensor usage APIs, your API client must be assigned the Sensor usage scope with read permissions. For more info, see API clients.
- Feature flags: To get aggregated usage data in multi-CID (non-Flight Control) accounts, the access-account-billing-data feature flag must be enabled. Contact your account team to enable feature flags.

  Note: Falcon Flight Control parent CIDs automatically receive aggregated child CID data and do not require this feature flag.

Endpoints

The Sensor Usage API includes these endpoints:

Operation	Endpoint
Get hourly sensor usage data	`GET /billing-dashboards-usage/aggregates/hourly-average/v1`
Get weekly sensor usage data	`GET /billing-dashboards-usage/aggregates/weekly-average/v1`

Rate limiting

The Sensor Usage API allows up to 60 requests per minute for each endpoint. If you exceed the limit, a `429 Too Many Requests` error is returned with a `Retry-After` header specifying how long to wait before attempting another request.

Falcon Flight Control and multi-CID support

- In Falcon Flight Control deployments, aggregated child CID sensor usage data is automatically returned in requests made from the parent CID.
- In non-Flight Control multi-CID accounts, requests made from a CID with the access-account-billing-data feature flag return aggregated usage for all CIDs in the environment.
- Multi-CID accounts with the access-account-billing-data feature flag and Flight Control parent CIDs can get sensor usage data for specific CIDs in their deployment using the Falcon Query Language (FQL) `selected_cids` filter. See Appendix A: FQL filters for info.

Usage categories

API responses return usage data by category. These categories differ in name from the names used in the Falcon console Sensor usage dashboard. The following table lists the response field category names and their corresponding Sensor usage dashboard category, along with the endpoint and workload types included in each category.

Response field	Relative Sensor usage dashboard category name	Included endpoint and workload types
`chrome_os`	Not currently available in the Falcon console Sensor usage dashboard.	
`containers`	Container hosts	This field value represents a combined total of `public_cloud_with_containers` and `servers_with_containers`
`lumos`	Managed containers	LUMOS

`mobile`	Mobile devices	Android and iOS devices
`public_cloud_with_containers`	Container hosts	Public clouds with containers and servers with containers
`public_cloud_without_containers`	Cloud virtual machines	Non-container-basedAWS, Azure, Oracle (OCI) and Google Cloud public clouds
`servers_with_containers`	Container hosts	Public clouds with containers and servers with containers
`servers_without_containers`	Servers	Non-container-based Windows servers, Linux servers, Domain Controllers, private clouds, and public clouds other than AWS, Azure, OCI, and Google Cloud
`workstations`	Workstations	Windows and macOS desktop and laptop machines

Sensor Usage API examples

The following examples demonstrate how to use the Sensor Usage API endpoints to accomplish various tasks.

Get hourly sensor usage

Get a daily breakdown of your CID's average hourly sensor usage by sensor category. Successful requests return an HTTP 200 code and an array of objects with hourly usage data. Each object in the response shows the average number of unique hosts seen per hour for the previous 28 days. By default, 28 days of data is returned, ending on the current date minus 2 days. You can provide FQL filters in your request to retrieve data for a specific period of time. For more info, see Appendix A: FQL filters.

Note:

- Your CID must have the **ui-billing-dashboards-v3-hourly** feature flag enabled to get hourly sensor data.
- While the API returns hourly data for all usage categories, the **Sensor usage dashboard** in the Falcon console only displays hourly data for usage categories that support hourly billing (**Cloud virtual machines**, **Container hosts**, and **Managed containers**).

Endpoint

```
GET /billing-dashboards-usage/aggregates/hourly-average/v1
```

Parameters

Name	In	Type	Description
`filter` *optional*	query	string	An FQL filter expression used to limit the result set. For available options, see Appendix A: FQL filters.

Example 1: Get the average hourly sensor usage for 5 days, ending on June 15, 2024

Example 1 request

```
curl -X GET  'https://api.crowdstrike.com/billing-dashboards-usage/aggregates/hourly-average/v1?filter=event_date:\''2024-06-15'\'',period:'\''5'\''' \
-H 'Accept: application/json' \
-H 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example 1 response


```
{
 "meta": {
  "query_time": 0.002471624,
  "trace_id": "9fa7eba4-ca44-44b3-b09f-837ce3ab41e7"
 },
 "resources": [
  {
   "containers": 0.6339285714285714,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 3.8110119047619047,
   "servers_with_containers": 0.6339285714285714,
   "servers_without_containers": 0.4330357142857143,
   "workstations": 0.24851190476190474,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-06-15"
  },
  {
   "containers": 0.5982142857142857,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 3.8110119047619047,
   "servers_with_containers": 0.5982142857142857,
   "servers_without_containers": 0.46130952380952384,
   "workstations": 0.24553571428571427,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-06-14"
```

```
  },
  {
   "containers": 0.5982142857142857,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 3.8110119047619047,
   "servers_with_containers": 0.5982142857142857,
   "servers_without_containers": 0.4449404761904762,
   "workstations": 0.2589285714285714,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-06-13"
  },
  {
   "containers": 0.5625,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 3.8110119047619047,
   "servers_with_containers": 0.5625,
   "servers_without_containers": 0.4702380952380953,
   "workstations": 0.26041666666666663,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-06-12"
  },
  {
   "containers": 0.5267857142857143,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 3.775297619047619,
   "servers_with_containers": 0.5267857142857143,
   "servers_without_containers": 0.5044642857142857,
   "workstations": 0.24553571428571427,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-06-11"
  }
 ]
}
```


Example 2: (Flight Control/multi-CID environments) Get the 3 most recent days of available weekly usage for CID IDs abc123, def456, and ghi789

Example request

```
curl -X GET  'https://api.crowdstrike.com/billing-dashboards/usage/aggregates/hourly-average/v1?filter=selected_cids:'\''abc123,def456,ghi789'\'',period:'\''3'\'''
\' \
-H 'Accept: application/json' \
-H 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response


```
{
 "meta": {
  "query_time": 0.004270267,
  "trace_id": "bf6873a4-2a57-4227-8497-251a99b17e61"
 },
 "resources": [
  {
   "containers": 0,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 5.977678571428572,
   "servers_with_containers": 0,
   "servers_without_containers": 10.944940476190476,
   "workstations": 9.593749999999998,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-10-01"
  },
  {
   "containers": 0,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 6.038690476190476,
   "servers_with_containers": 0,
   "servers_without_containers": 10.933035714285714,
   "workstations": 9.516369047619047,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-09-30"
  },
  {
   "containers": 0,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 6.026785714285715,
   "servers_with_containers": 0,
   "servers_without_containers": 10.90922619047619,
   "workstations": 9.492559523809522,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-09-29"
```

```
  }
 ]
}
```

Get weekly sensor usage

Get a daily breakdown of your CID's average weekly sensor usage by sensor category. Successful requests return an HTTP 200 code and an array of objects with weekly sensor usage data. Each object in the response represents a specific day and shows the average number of unique hosts seen each week over the previous four weeks. By default, 28 days of data is returned, ending on the current date minus 2 days. You can provide FQL filters in your request to retrieve data for a specific period of time. For more info, see Appendix A: FQL filters.

Endpoint

```
GET /billing-dashboards-usage/aggregates/weekly-average/v1
```

Parameters

Name	In	Type	Description
`filter` *optional*	query	string	An FQL filter expression used to limit the result set. For available options, see Appendix A: FQL filters.

Example 1: Get the average weekly sensor usage for 7 days ending on July 10, 2024

Example 1 request

```
curl -X GET  'https://api.crowdstrike.com/billing-dashboards/usage/aggregates/weekly-average/v1?filter=event_date:\''2024-07-10'\'',period:\''7'\''' \' \
-H 'Accept: application/json' \
-H 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example 1 response

```
{
 "meta": {
  "query_time": 0.001333371,
  "trace_id": "a8c84673-a3f8-4e71-844d-63ee70d55219"
 },
 "resources": [
  {
   "containers": 1,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 4.25,
   "servers_with_containers": 1,
   "servers_without_containers": 2,
   "workstations": 4.5,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-07-10"
  },
  {
   "containers": 0.75,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 4,
   "servers_with_containers": 0.75,
   "servers_without_containers": 1.75,
   "workstations": 4.5,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-07-09"
  },
  {
   "containers": 0.75,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 4,
   "servers_with_containers": 0.75,
   "servers_without_containers": 2.25,
   "workstations": 5,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-07-08"
  },
  {
   "containers": 0.5,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 3,
   "servers_with_containers": 0.5,
   "servers_without_containers": 1.75,
   "workstations": 3.75,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
```

```
   "date": "2024-07-07"
  },
  {
   "containers": 0.75,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 4,
   "servers_with_containers": 0.75,
   "servers_without_containers": 2,
   "workstations": 4.75,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-07-06"
  },
  {
   "containers": 1,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 4,
   "servers_with_containers": 1,
   "servers_without_containers": 2,
   "workstations": 4.5,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-07-05"
  },
  {
   "containers": 1,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 4,
   "servers_with_containers": 1,
   "servers_without_containers": 1.75,
   "workstations": 4.5,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-07-04"
  }
 ]
}
```


Example 2: (Flight Control/multi-CID environments) Get the 5 most recent available days of weekly usage for CID IDs abc123 and def456

Example request

```
curl -X GET  'https://api.crowdstrike.com/billing-dashboards/usage/aggregates/weekly-average/v1?filter=selected_cids:'\''abc123,def456'\'',period:'\''5'\''' \' \
-H 'Accept: application/json' \
-H 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response


```
{
 "meta": {
  "query_time": 0.005605158,
  "trace_id": "62a3671b-08ac-4eec-bb1d-ac46e819dd5e"
 },
 "resources": [
  {
   "containers": 0,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 3,
   "servers_with_containers": 0,
   "servers_without_containers": 10,
   "workstations": 11,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-10-01"
  },
  {
   "containers": 0,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 3,
   "servers_with_containers": 0,
   "servers_without_containers": 10,
   "workstations": 9.75,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-09-30"
  },
  {
   "containers": 0,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 3,
   "servers_with_containers": 0,
   "servers_without_containers": 10,
   "workstations": 9.5,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-09-29"
```

```
  },
  {
   "containers": 0,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 3,
   "servers_with_containers": 0,
   "servers_without_containers": 10,
   "workstations": 9.5,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-09-28"
  },
  {
   "containers": 0,
   "public_cloud_with_containers": 0,
   "public_cloud_without_containers": 3,
   "servers_with_containers": 0,
   "servers_without_containers": 10,
   "workstations": 9.5,
   "mobile": 0,
   "lumos": 0,
   "chrome_os": 0,
   "date": "2024-09-27"
  }
 ]
}
```


Appendix A: FQL filters

The Sensor usage API supports the following FQL filters. You can use these filters to retrieve data for specific dates and CIDs. For more info about how filtering works, see Falcon Query Language (FQL).

Name	Type	Description	Example
`event_date`	date	The final date of the results to be returned in ISO 8601 format (YYYY-MM-DD). Data is available for retrieval starting with the current date minus 2 days and going back 395 days. Data is not available for the current date or the current date minus 1 day. Requests sent with an `event_date` more recent than the current date minus 2 days return an HTTP 400 error with the message `"Invalid date, date occurs after the latest valid date: YYYY-MM-DD."` If an `event_date` is provided without a `period`, the default `period` (28 days) is returned, ending on the specified `event_date`. Default: the current date minus 2 days	`filter=event_date:'2024-06-11'`
`period`	integer	The number of days of data to return. If a `period` is provided without an `event_date`, the default `event_date` (the current date minus 2 days) is used. Minimum: 1 Maximum: 395 Default: 28	`filter=period:'30'`
`selected_cids`	string	A comma-separated list of up to 100 CID IDs to return data for. This filter is available to Falcon Flight Control parent CIDs and to CIDs in multi-CID deployments with the access-account-billing-data feature flag enabled. Note: This field is case-sensitive and requires the correct input of capital and lowercase letters.	`filter=selected_cids:'cid_1,cid_2,cid_3'`

Falcon Platform Administration APIs

Control and configure Falcon platform administrative functions, including Flight Control, user and role assignments, scheduled reporting, host group management, event streams, and SOAR workflow automation.

Host and Host Group Management APIs

Create, manage, and retrieve information about hosts and host groups in your environment.

About CrowdStrike APIs

CrowdStrike provides use cases and example requests and responses for interacting with a specific set of our OAuth2-based APIs. For general info about CrowdStrike APIs, see CrowdStrike OAuth2-Based APIs, which covers these topics:

- Details on getting started, such as authentication and API scopes
- Domains used in base URLs by cloud
- Links to our Swagger API specification by cloud

Managing hosts

Hosts are endpoints that run the Falcon sensor.

Use the CrowdStrike hosts API to get host details, contain or lift containment on hosts, and delete or restore hosts.

List host IDs

Get a list of host IDs. You can send optional FQL filters in your requests to find host IDs based on specific attributes, such as platform, hostname, or IP. Successful requests return an HTTP 200 code and an array of host IDs that match the query criteria.

Requests to this endpoint allow a maximum of 150,000 results for customers in CrowdStrike's US-1 cloud, or 10,000 results for US-2, US-GOV-1, and EU-1 cloud customers. See the Falcon Console User Guide for info on determining your host cloud. This limit applies to the total response size, regardless of pagination options set in the offset and limit parameters. CrowdStrike returns an HTML 500 response for result sets that exceed the allowed limit. You can use filters to refine your search and reduce the number of results. See Appendix A: Device filters for the list of available filters.

Falcon Flight Control support

Child CID host IDs are automatically returned in the response of requests made from the parent CID. You can get hidden hosts for a specific child CID using the `cid` filter.

Tip: Use the resulting IDs to get detailed information about specific hosts in `POST` or `GET ``/devices/entities/devices/v2`.

Endpoint

```
GET /devices/queries/devices/v1
```

Required API client scope

Hosts: read

Parameters

Name	In	Type	Description
`filter` *optional*	query	string	The filter expression used to limit the result set. See Appendix A: Device filters for available options.
`offset` *optional*	query	integer	The zero-based position of the first record to return. Default value: 0
`limit` *optional*	query	integer	The maximum number of records to return. [1-5000] Default value: 100
`sort` *optional*	query	string	The attribute and direction to order the results.

Example: Finding Falcon hosts that match a given AWS instance ID

Example request

```
curl -X GET "https://api.crowdstrike.com/devices/queries/devices/v1?filter=instance_id:'i-0d8dxxxxxx6fd6'" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response


```
{
 "meta": {
  "query_time": 0.005413855,
  "pagination": {
   "offset": 1,
   "limit": 100,
   "total": 1
  },
  "powered_by": "device-api",
  "trace_id": "b76d4abb-2722-4fa8-b364-da48517c7c97"
 },
 "resources": [
  "6b48a2xxxxxxxx1c3a7f"
 ],
 "errors": []
}
```


Example: Finding all Windows hosts

Example request

```
curl -X GET  "https://api.crowdstrike.com/devices/queries/devices/v1?filter=platform_name:'Windows'" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response


```
{
 "meta": {
  "query_time": 0.006987649,
  "pagination": {
   "offset": 100,
   "limit": 100,
   "total": 200
  },
  "powered_by": "device-api",
  "trace_id": "ef5ec400-f17a-48a3-8347-e31c0dc293ae"
 },
 "resources": [
  "061a51xxxxxxxx44624a",
  "2bcb52xxxxxxxx447d64",
  ...
  "9148a2xxxxxxxx4c7975",
  "61be33xxxxxxxx42f6af"
 ],
 "errors": []
}
```


Example: Finding workstations based on multiple query criteria

Example request

Search for hosts that are:

- Windows or Mac hosts
- Have a containment status of normal (are not currently contained)
- Were last seen on or after July 4, 2020

```
curl -X GET "https://api.crowdstrike.com/devices/queries/devices/v1" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json' \
 -H 'Content-Type: application/json' \
 --data-urlencode "filter=product_type_desc:'Workstation'+status:'normal'+platform_name:['Windows','Mac']+last_seen:>='2020-07-04'"
```

Example response


```
{
 "meta": {
  "query_time": 0.006911112,
  "pagination": {
   "offset": 100,
   "limit": 100,
   "total": 1141
  },
  "powered_by": "device-api",
  "trace_id": "dee561e5-f4ba-45f7-8f28-57610323d26e"
 },
 "resources": [
  "061a51xxxxxxxx44624a",
  "2bcb52xxxxxxxx447d64",
```

```
  ...
  "9148a2xxxxxxxx4c7975",
  "61be33xxxxxxxx42f6af"
 ],
 "errors": []
}
```

List host IDs with continuous pagination

If your query is too large to list host IDs with `GET /devices/queries/devices/v1`, use continuous pagination to find hosts. This endpoint allows a response set of any size to be returned. Pagination is continuous based on an offset pointer so there is no maximum limit. Offset pointers expire after two minutes. Like `GET /devices/queries/devices/v1`, you can apply filters to reduce the number of results. (See Appendix A: Device filters for the list of available filters.) Successful requests return an HTTP 200 code and an array of host IDs that match the query criteria.

You can optionally specify a limit in the initial GET request to limit the number of returned items in each response.

1. Search for hosts with GET /devices/queries/devices-scroll/v1

   Note: To limit the number of returned items, use GET /devices/queries/devices-scroll/v1?limit={limit}

2. Retrieve the next set of items using the unique offset provided by the response with GET /devices/queries/devices-scroll/v1?offset={offset}

Continue returning results using the provided offsets to effectively scroll through results. Offset values expire after two minutes.

Falcon Flight Control support

Child CID host IDs are automatically returned in the response of requests made from the parent CID. You can get hidden hosts for a specific child CID using the `cid` filter.

Endpoint

```
GET /devices/queries/devices-scroll/v1
```

Required API client scope

Hosts: read

Parameters

Name	In	Type	Description
`filter` *optional*	query	string	The filter expression used to limit the result set. See Appendix A: Device filters for available options.
`offset` *optional*	query	string	The offset to page from, for the next result set.
`limit` *optional*	query	integer	The maximum number of records to return. [1-5000] Default value: 100
`sort` *optional*	query	string	The attribute and direction to order the results.

Example: Retrieving a list of the first 100 devices in your environment

Example request

```
curl -X GET "https://api.crowdstrike.com/devices/queries/devices-scroll/v1?limit=100" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response

```
{
 "meta": {
  "query_time": 0.01997684,
  "pagination": {
   "total": 1157,
   "offset": "DnF1ZXJ5VGhlbkZldGNoAgAAAAAASLtuFk12b09QQXZMVC1HS2ZfSnFMNWs3MVEAAAAALi6ZphZFT2l1em1JNVFYZUE0bUxCTjlfWmh3",
```

```
   "expires_at": 1602009890150715194
  },
  "powered_by": "device-api",
  "trace_id": "240a961c-3a0d-4131-80ff-b44fa409e3df"
 },
 "resources": [
  "d89bxxxxxxxx54db",
  "a1f8xxxxxxxxaeef",
  ...
  "3478xxxxxxxx69b5",
  "0b4exxxxxxxxb64a"
 ],
 "errors": []
}
```


Example: Retrieving the next 100 devices

Example request

Use the offset provided in the previous response.

```
curl -X GET "https://api.crowdstrike.com/devices/queries/devices-scroll/v1?
offset=DnF1ZXJ5VGhlbkZldGNoAgAAAAAASLtuFk12b09QQXZMVC1HS2ZfSnFMNWs3MVEAAAAALi6ZphZFT2l1em1JNVFYZUE0bUxCTjlfWmh3" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response


```
{
 "meta": {
  "query_time": 0.124431583,
  "pagination": {
   "total": 1157,
   "offset": "DnF1ZXJ5VGhlbkZldGNoAgAAAAAASLtuFk12b09QQXZMVC1HS2ZfSnFMNWs3MVEAAAAALi6ZphZFT2l1em1JNVFYZUE0bUxCTjlfWmh3",
   "expires_at": 1602010079240922237
  },
  "powered_by": "device-api",
  "trace_id": "ff1c261c-37e1-4ed4-8350-756ad40f94e8"
 },
 "resources": [
  "061a51xxxxxxxx44624a",
  "2bcb52xxxxxxxx447d64",
  ...
  "9148a2xxxxxxxx4c7975",
  "61be33xxxxxxxx42f6af"
 ],
 "errors": []
}
```


List host IDs with combined devices endpoint

The combined device endpoint is an alternative to the continuous pagination method for large queries. This endpoint allows a response of any size to be returned, limited to 10,000 items per page. Use this endpoint if you're seeing errors or partial results when you use the `/devices/queries/devices-scroll/v1` endpoint. The combined device endpoint is continuous based on an offset pointer so there is no maximum limit. Offset pointers don't expire. Devices can be changed, added, or deleted while you're querying this endpoint.

Successful requests return an HTTP 200 code and the entire device records that match the query criteria. You can use filters to limit what's returned. For example, if you want your query to only return device IDs, use `fields=device_id`. For a list of available filters, see Appendix A: Device filters.

You can optionally use a limit in the initial GET request to limit the number of returned items in each response.

1. Search for hosts with GET `/devices/combined/devices/v1`
2. To limit the number of returned items, use GET `/devices/combined/devices/v1?limit={limit}`
3. Retrieve the next set of items using the unique offset provided by the response with GET `/devices/combined/devices/v1?offset={next}`

Continue returning results using the provided offsets to effectively scroll through results.

Note: The `device_id` field is always returned by this endpoint.

Falcon Flight Control support

Child CID host IDs are automatically returned in the response of requests made from the parent CID. The combined devices endpoint does not return hidden hosts. For that, use `/combined/devices-hidden/v1`.

Endpoint

```
GET /devices/combined/devices/v1
```

Required API client scope

Hosts: read

Parameters

Name	In	Type	Description
`fields` *optional*	query	string	The list of fields to be returned, comma-delimited.
`filter` *optional*	query	string	The filter expression used to limit the result set. For available options, see Appendix A: Device filters.
`limit` *optional*	query	integer	The maximum number of records to return. [1-10000] Default value: 100
`offset` *optional*	query	string	The offset to page from, for the next result set.
`sort` *optional*	query	string	The attribute and direction to order the results.

Example: Retrieving a list of the first 100 devices in your environment

Example request

```
curl -X GET "https://api.crowdstrike.com/devices/combined/devices/v1?limit=100" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response

```
{
  "meta": {
    "query_time": 0.053728824,
    "pagination": {
      "total": 19399,
      "limit": 100,
      "next": "1DyRbIjAwMjAwMjk2M2Q4NzRlMDE4YzI0MzVkZWNkM2U4MzFmIl0"
    },
    "powered_by": "device-api",
    "trace_id": "58xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx00"
  },
  "resources": [
    {
      "device_id": "0cc5bxxxxxx942e7b",
      "config_id_base": "65994765",
      "config_id_build": "10701",
      ...
    }
  ]
}
```

Example: Setting a higher limit and getting the first page

Example request

```
curl -X GET "https://api.crowdstrike.com/devices/combined/devices/v1?limit=1000" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response

```
{
  "meta": {
    "query_time": 0.219126071,
    "pagination": {
      "total": 19387,
      "limit": 1000,
      "next": "1DyRbIjBjYzU0Zjk5YWQyNDQyNTZhMWUyMDgxZDY5ZTY5ZjkwIl0"
    },
    "powered_by": "device-api",
    "trace_id": "81xxxxxx-xxxx-xxxx-xxxx-xxxxxxf8"
```

```
  },
  "resources": [
    {
      "device_id": "0cc7e7xxxxxxabc614",
      "agent_load_flags": "3",
      "agent_local_time": "2016-04-28T14:33:47.302Z",
      ...
    }
  ]
}
```

Example: Using the next value as the offset to get the next page

Example request

```
curl -X GET "https://api.crowdstrike.com/devices/combined/devices/v1?limit=1000&offset=1DyRbIjBjYzU0Zjk5YWQyNDQyNTZhMWUyMDgxZDY5ZTY5ZjkwIl0" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response

```
{
  "meta": {
    "query_time": 0.25839668,
    "pagination": {
      "total": 19387,
      "limit": 1000,
      "next": "1DyRbIjFhMGFkN2M2NjZhMjQ4ZTZiNTZmMzg1ZmI5YjFmYWZlIl0",
      "previous": "1DyRbIjBjYzU0Zjk5YWQyNDQyNTZhMWUyMDgxZDY5ZTY5ZjkwIl0"
    },
    "powered_by": "device-api",
    "trace_id": "2bxxxxxx-xxxx-xxxx-xxxx-xxxxxx4c"
  },
  "resources": [
    {
      "device_id": "0cc8d8xxxxxx8a6f01",
      "agent_load_flags": "3",
      "agent_local_time": "2016-04-28T14:33:47.302Z",
      ...
    }
  ]
}
```

You're done paging through your results when `next` is missing, is an empty string, or the number of results is less than the limit.

Example: Sorting your results by host name

Example request

```
curl -X GET "https://api.crowdstrike.com/devices/combined/devices/v1?sort=hostname.desc" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response

```
{
  "meta": {
     "query_time": 0.096354153,
    "pagination": {
      "total": 19387,
      "limit": 100,
      "next": "1D1dbImZhbHNpdGgtV2luZG93cy02NmIyN2UzOGI2NTI0MjBkYTgzZmY3YWUxYmIxZmI2MSIsIjY2YjI3ZTM4YjY1MjQyMGRhODNmZjdhZTFiYjFmYjYxIl0"
    },
    "powered_by": "device-api",
    "trace_id": "49xxxxxx-xxxx-xxxx-xxxx-xxxxxx22"
  },
  "resources": [
    {
      "device_id": "fc417fxxxxxx4ab50a",
      "hostname": "myhost123"
      ...
    },
    {
      "device_id": "4ab50axxxxxxfc417f",
      "hostname": "zabesthost123"
      ...
    }
  ]
}
```

Example: Filtering results with a specific hostname

Example request

```
curl -X GET "https://api.crowdstrike.com/devices/combined/devices/v1?filter=hostname:'myhost'" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response

```
{
  "meta": {
    "query_time": 0.053728824,
    "pagination": {
      "total": 19399,
      "limit": 100,
      "next": "1DyRbIjAwMjAwMjk2M2Q4NzRlMDE4YzI0MzVkZWNkM2U4MzFmIl0"
    },
    "powered_by": "device-api",
    "trace_id": "58xxxxxx-xxxx-xxxx-xxxx-xxxxxx00"
  },
  "resources": [
    {
      "device_id": "fc417fxxxxxx4ab50a",
      "hostname": "myhost"
      ...
    }
  ]
}
```

Example: Restricting fields returned in the response

Example request

```
curl -X GET "https://api.crowdstrike.com/devices/combined/devices/v1?fields=device_id" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response

```
{
  "meta": {
    "query_time": 0.538033425,
    "pagination": {
      "total": 19387,
      "limit": 100,
      "next": "1DyRbIjAxMjc1ZDI4ZjRjMDRjZTU5OWFmYjU5MjExODllMWRkIl0"
    },
    "powered_by": "device-api",
    "trace_id": "e8xxxxxx-xxxx-xxxx-xxxx-xxxxxxf8"
  },
  "resources": [
    {
      "device_id": "0001dxxxxxx400452"
    },
    {
      "device_id": "000270xxxxxx4d54e8"
    },
    {
      "device_id": "00045exxxxxx1e35aa"
    },
    ...
  ]
}
```

Example: Returning host and sensor version

Example request

```
curl -X GET "https://api.crowdstrike.com/devices/combined/devices/v1?fields=hostname,agent_version" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response

```
{
  "meta": {
    "query_time": 0.097610025,
    "pagination": {
      "total": 19387,
      "limit": 100,
```

```
      "offset": "",
      "next": "1DyRbIjAxMjc1ZDI4ZjRjMDRjZTU5OWFmYjU5MjExODllMWRkIl0"
    },
    "powered_by": "device-api",
    "trace_id": "29xxxxxx-xxxx-xxxx-xxxx-xxxxxx2b"
  },
  "resources": [
    {
      "device_id": "002483xxxxxx10c436",
      "agent_version": "5.25.10601.0",
      "hostname": "myhost1"
    },
    {
      "device_id": "002673xxxxxx47c6e2",
      "agent_version": "5.25.10701.0",
      "hostname": "myhost2"
    },
    {
      "device_id": "003002xxxxxx7f83d6",
      "agent_version": "5.25.11701.0",
      "hostname": "myhost3"
    },
    ...
  ]
}
```


Get host details

Retrieve detailed information for one or more host IDs. Successful requests return an HTTP 200 code and a host object for each specified host ID in the request.

You can use the API to get the following host information:

- Software information, such as platform, OS version, kernel version, and OS build ID (OS build ID available for Windows and macOS only)
- Network information, such as its IP address and MAC address
- Sensor information, such as its version
- Status information, such as its last connection time to the CrowdStrike cloud or its network containment status
- Configuration information, such as the active prevention policies in effect on this host

Falcon Flight Control support

Falcon Flight Control customers can get child CID host details from the parent CID. When making requests from the parent CID, specify the child CID host IDs you want to get details for.

Tip: You can get host IDs with the `GET /devices/queries/devices/v1` endpoint, from the Falcon console, or using the Streaming API.

Endpoint

`/devices/entities/devices/v2`

This endpoint uses POST and GET methods to support different request sizes.

Method	Details
`POST`	Send up to 5000 ids in the request body.
`GET`	Send up to 100 ids in the query string.

Required API client scope

Hosts: read

Parameters

Name	In	Type	Description
`ids` *required*	body (`POST` requests) query (`GET` requests)	string	The unique ID of the host. Multiple IDs are supported in a single request as described below. In `POST` requests, send one or more (5000 max) host IDs as a comma-separated array in the request body. In `GET` requests, send one or more (100 max) host IDs in the query string. Send multiple IDs as parameter=value clauses, separated by & (`ids={a}&ids={b}`).

Example: Get the details of a host with the ID abcd1234wxyz56.

Example GET request

```
curl -X GET "https://api.crowdstrike.com/devices/entities/devices/v2?ids= abcd1234wxyz56" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example POST request

```
curl -X POST  'https://api.crowdstrike.com/devices/entities/devices/v2' \
-H 'Content-Type: application/json' \
-H 'Accept: application/json' \
-H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
-d
'{"ids":["abcd1234wxyz56"]}'
```

Example response


```
{
    "meta": {
        "query_time": 0.017458709,
        "powered_by": "device-api",
        "trace_id": "7aea2f44-9891-4892-b633-bf0544830e55"
    },
    "resources": [
        {
            "device_id": "abcd1234wxyz56",
            "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV",
            "agent_load_flags": "1",
            "agent_local_time": "2017-09-15T06:13:15.223Z",
            "agent_version": "3.5.5606.0",
            "bios_manufacturer": "Phoenix Technologies LTD",
            "bios_version": "6.00",
            "config_id_base": "65994753",
            "config_id_build": "5606",
            "config_id_platform": "3",
            "external_ip": "24.16.20.181",
            "mac_address": "00-50-56-8c-17-81",
            "hostname": "example_host",
            "first_seen": "2017-07-19T02:08:24Z",
            "last_seen": "2017-09-25T23:45:55Z",
            "local_ip": "192.0.2.100",
            "machine_domain": "example.com",
            "major_version": "6",
            "minor_version": "1",
            "os_version": "Windows 7",
            "os_build": "19H1323",
            "platform_id": "0",
            "platform_name": "Windows",
            "policies": [
                {
                    "policy_type": "prevention",
                    "policy_id": "aaabbbdddcccddd",
                    "applied": true,
                    "settings_hash": "ed4a7460",
                    "assigned_date": "2017-09-14T13:03:33.038805882Z",
                    "applied_date": "2017-09-14T13:03:45.823683755Z"
                }
            ],
            "device_policies": {
                "prevention": {
                    "policy_type": "prevention",
                    "policy_id": "aaabbbdddcccddd",
                    "applied": true,
                    "settings_hash": "ed4a7460",
                    "assigned_date": "2017-09-14T13:03:33.038805882Z",
                    "applied_date": "2017-09-14T13:03:45.823683755Z"
                },
                "sensor_update": {
                    "policy_type": "sensor-update",
                    "policy_id": "aaabbbdddcccddd",
                    "applied": true,
                    "settings_hash": "65994753|3|2|automatic",
                    "assigned_date": "2017-09-14T05:15:40.878196578Z",
                    "applied_date": "2017-09-14T05:16:20.847887649Z"
                }
            },
            "product_type": "1",
            "product_type_desc": "Workstation",
            "site_name": "Default-First-Site-Name",
            "status": "normal",
            "system_manufacturer": "VMware, Inc.",
            "system_product_name": "VMware Virtual Platform",
            "modified_timestamp": "2017-09-25T23:46:06Z",
            "meta": {
                "version": "49662"
            },
    "kernel_version": "6.1.7601.17592"
```

```
  }
    ],
    "errors": []
}
```

Get host content update states

View content package states for hosts in your environment, including the timestamp for when a specific host was last updated with content for each category.

These endpoints are available:

Endpoint	Description
`GET /device-content/queries/states/v1`	Get host IDs for hosts that meet your filter criteria, such as all hosts that have received a content update for sensor operations content in the last 24 hours.
`GET /device-content/entities/states/v1`	Get content update information for one or more hosts. Use the `ids` parameter to specify up to 100 host IDs.

Content update states required scope

This API client scope is required for content update states endpoints:

`Device Content: read`

Get host IDs for content update states

Get host IDs for hosts that meet your filter criteria, such as all hosts that have received a content update for sensor operations content in the last 24 hours or all hosts currently in RFM.

To get a list of host IDs:

- `GET /device-content/queries/states/v1`

Parameters

The `/device-content/queries/states/v1` endpoint accepts these parameters to filter a list of host IDs that can be used to get content update information.

Parameter	In	Type	Description
`limit` optional	query	integer	Limit the maximum number of records returned. The acceptable range of this value is between 1 and 10,000.
`offset` optional	query	integer	Offset the records in the response. For example, an offset value of 50 specifies that the first 50 records aren't included in the response.

`filter`
optional
	query	expression	Specify an FQL filter. Hosts that meet this filter are included. These fields are available:
			`device_id`
			`cid`
			`hostname`
			`platform_name`
			`last_seen`
			`reduced_functionality_mode`
			`groups`
			`rapid_response_content.last_update`
			`sensor_operations.last_update`
			`system_critical.last_update`
			`vulnerability_management.last_update`

`sort`
optional
	query	string	Specify a sort order for the response. These sort values are available:
			`device_id.asc`
			`device_id.desc`
			`cid.asc`
			`cid.desc`
			`hostname.asc`

			hostname.desc platform_name.asc platform_name.desc last_seen.asc last_seen.desc reduced_functionality_mode.asc reduced_functionality_mode.desc groups.asc groups.desc rapid_response_content.last_update.asc rapid_response_content.last_update.desc sensor_operations.last_update.asc sensor_operations.last_update.desc system_critical.last_update.asc system_critical.last_update.desc vulnerability_management.last_update.asc vulnerability_management.last_update.desc

Example request

This example uses the filter parameter to get host IDs for hosts that are currently in RFM, sorted by sensor operations updates to show hosts that have gone the longest without an update at the top of the list.

```
curl -X GET \ 'https://api.crowdstrike.com/device-content/queries/states/v1?filter=reduced_functionality_mode:'yes'&sort=sensor_operations.last_update.asc'\
-H 'Content-Type: application/json' \
-H 'Accept: application/json' \
-H 'Authorization: Bearer <bearer_token>'
```

Example response


```
{
  "meta": {
    "query_time": 1.58e-7,
    "pagination": {
      "offset": 0,
      "limit": 0,
      "total": 10
    },
    "powered_by": "devicecontent",
    "trace_id": "ecbdf2xxxxx8d4a8ff"
  },
  "errors": [],
  "resources": [
    "5731a47xxxxxd7bd63",
    "368e9xxxxxxx945d4a",
    "db074dxxxxxx1eb4ee",
    "6f140bcxxxxxxxx6cb0",
    "e03b2xxxxxx1da626b",
    "413ad6fxxxxxd2835d",
    "df93a25bxxxxxe5573",
    "c17468cxxxxxdafdea",
    "bf7540xxxxxx91c4e4",
    "5f5ca9cxxxxx5265d1"
  ]
}
```


Get host content update information

To get content package update information for a list of host IDs:

- `GET /device-content/entities/states/v1?ids=<hostID>`

Parameters

The `/device-content/entities/states/v1` endpoint accepts these parameters to specify which hosts to get package update information for.

Parameter	In	Type	Description
`ids`	query	string	Specify one or more host IDs to query.

required			

Example request

This example gets host content update information for a list of host IDs included in the query.

```
curl -X POST \
'https://api.crowdstrike.com/device-content/entities/states/v1?
ids=67af3bxxxxx28b44&ids=18bddxxxxxd35170&ids=6f3eb9xxxxx86&ids=ddc77xxxxx992c7&ids=ad45e010xxxxx8714' \
 -H 'Accept: application/json' \
 -H 'Authorization: Bearer <bearer_token>' \
 -H 'Content-Type: application/json'
```

Example response

Note: Although overrides are applied to all categories of an entire content update policy, this API response shows an `override` field for each category. These fields display the override status for the entire policy.


```
{
 "meta": {
  "query_time": 5e-8,
  "powered_by": "devicecontent",
  "trace_id": "5d320eexxxxxx8f3bfd9"
 },
 "resources": [
  {
   "device_id": "67af3bxxxxx28b44",
   "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV-WX",
   "hostname": "hostexample1",
   "platform_name": "Mac",
   "last_seen": "2024-11-04T20:32:07Z",
   "reduced_functionality_mode": "no",
   "groups": [
    "6f140bcxxxxxxxx6cb0",
    "e03b2xxxxxx1da626b"
   ],
   "system_critical": {
        "last_update": "2025-01-16T20:46:50Z",
        "policy_setting": "ga_4h",
        "override": "None"
   },
   "rapid_response_content": {
        "last_update": "2025-01-16T22:24:47Z",
        "policy_setting": "ga",
        "override": "None"
   },
   "vulnerability_management": {
        "last_update": "2025-01-16T20:46:50Z",
        "policy_setting": "ga",
        "override": "None"
   },
   "sensor_operations": {
        "last_update": "2025-01-17T00:00:16Z",
        "policy_setting": "ga",
        "override": "None"
   },
   "content_update_policy_id": "8c60c62xxxxx4b7d8863",
   "content_update_policy_applied_date": "2024-12-16T20:28:19Z"
  },
  {
   "device_id": "18bddxxxxxd35170",
   "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV-WX",
   "hostname": "hostexample2",
   "platform_name": "Mac",
   "last_seen": "2024-11-04T20:35:13Z",
   "reduced_functionality_mode": "no",
   "groups": [
    "413ad6fxxxxxd2835d",
    "df93a25bxxxxxe5573"
   ],
   "rapid_response_content": {
        "last_update": "2024-11-01T00:28:50Z",
        "policy_setting": "ga",
        "override": "Pause all"
   },
   "sensor_operations": {
        "last_update": "2024-11-01T00:28:50Z",
        "policy_setting": "ga",
        "override": "Pause all"
   },
   "system_critical": {
        "last_update": "2024-11-01T00:28:50Z",
        "policy_setting": "ga",
        "override": "Pause all"
   },
   "vulnerability_management": {
        "last_update": "2024-11-01T00:28:50Z",
        "policy_setting": "ga",
```

```
      "override": "Pause all"
  }
 },
 {
  "device_id": "6f3eb9xxxxx86",
  "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV-WX",
  "hostname": "hostexample3",
  "platform_name": "Linux",
  "last_seen": "2024-11-04T20:36:56Z",
  "reduced_functionality_mode": "no",
  "groups": [],
  "system_critical": {
      "last_update": "2025-01-21T21:41:43Z",
      "policy_setting": "ga",
      "override": "Allow all"
  },
  "rapid_response_content": {
      "last_update": "2025-01-21T21:41:15Z",
      "policy_setting": "ga_1h",
      "override": "Allow all"
  },
  "vulnerability_management": {
      "last_update": "2025-01-21T21:42:11Z",
      "policy_setting": "ea",
      "override": "Allow all"
  },
  "sensor_operations": {
      "last_update": "2025-01-21T21:40:47Z",
      "policy_setting": "pause",
      "override": "Allow all"
  },
  "content_update_policy_id": "7ae06038xxxxx3d47c698b7",
  "content_update_policy_applied_date": "2025-01-21T21:40:40Z"
 },
 {
  "device_id": "ddc77xxxxx992c7",
  "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV-WX",
  "hostname": "hostexample4",
  "platform_name": "Linux",
  "last_seen": "2024-11-04T20:36:53Z",
  "reduced_functionality_mode": "no",
  "groups": [
   "c17468cxxxxxdafdea",
   "bf7540xxxxxx91c4e4"
  ],
  "system_critical": {
      "last_update": "2025-01-21T21:41:43Z",
      "policy_setting": "ga",
      "override": "None"
  },
  "rapid_response_content": {
      "last_update": "2025-01-21T21:41:15Z",
      "policy_setting": "ga_4h",
      "override": "None"
  },
  "vulnerability_management": {
      "last_update": "2025-01-21T21:42:11Z",
      "policy_setting": "ea",
      "override": "None"
  },
  "sensor_operations": {
      "last_update": "2025-01-21T21:40:47Z",
      "policy_setting": "pause",
      "override": "None"
  },
  "content_update_policy_id": "7ae06038xxxxx3d47c698b7",
  "content_update_policy_applied_date": "2025-01-21T21:40:40Z"
 },
 {
  "device_id": "ad45e010xxxxx8714",
  "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV-WX",
  "hostname": "hostexample5",
  "platform_name": "Linux",
  "last_seen": "2024-11-04T21:01:56Z",
  "reduced_functionality_mode": "no",
  "groups": [],
  "system_critical": {
      "last_update": "2025-01-16T20:46:50Z",
      "policy_setting": "ga_1h",
      "override": "None"
  },
  "rapid_response_content": {
      "last_update": "2025-01-16T22:24:47Z",
      "policy_setting": "ga",
      "override": "None"
  },
  "vulnerability_management": {
      "last_update": "2025-01-16T20:46:50Z",
      "policy_setting": "ga",
      "override": "None"
  },
  "sensor_operations": {
      "last_update": "2025-01-17T00:00:16Z",
      "policy_setting": "ga",
```

```
        "override": "None"
    },
    "content_update_policy_id": "8c60c62xxxxx4b7d8863",
    "content_update_policy_applied_date": "2024-12-16T20:28:19Z"
   }
  ],
  "errors": []
}
```


List hidden host IDs

Get a list of hidden host IDs. You can send optional filters in your requests to get hidden host IDs based on specific attributes. (See Appendix A: Device filters for the list of available filters.) Successful requests return an HTTP 200 code and an array of host IDs that match the query criteria.

Falcon Flight Control support

Child CID hidden host IDs are automatically returned in the response of requests made from the parent CID. You can get hidden hosts for a specific child CID using the `cid` filter.

Endpoint

```
GET /devices/queries/devices-hidden/v1
```

Required API client scope

Hosts: read

Parameters

Name	In	Type	Description
`filter` *optional*	query	string	The FQL filter expression used to limit the result set. See Appendix A: Device filters for the list of available filters.
`offset` *optional*	query	integer	The zero-based position of the first record to return. Default value: 0
`limit` *optional*	query	integer	The maximum number of records to return. [1-5000] Default value: 100
`sort` *optional*	query	string	The attribute and direction to order the results.

Example: Get all hidden host IDs in your environment.

Example request

```
curl -X GET  'https://api.crowdstrike.com/devices/queries/devices-hidden/v1' \
-H 'Accept: application/json' \
-H 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response


```
{
   "meta": {
       "query_time": 0.005022823,
           "pagination": {
           "offset": 19,
           "limit": 100,
           "total": 19
       },
       "powered_by": "api",
       "trace_id": "ca21da7c-ad7b-4424-a081-3fd72b1d7d2a"
   },
   "resources": [
       "902a450d47aede504f0eb6fd4cb68424",
       "826ef26529a5479b8d27ed0693981b49",
```

```
      "a3fc35a55dcdaa6ea4c6990ded315680",
      "2051ac12aceba7705a4a8f962084a04d",
      "89194f8afaba8e82aa84267b34afaf1c"
   ],
   "errors": []
}
```

Retrieving host NIC history

Get a history of the last 10 IP addresses and MAC addresses used by a host. The NIC history is obtained from Threat Graph and adheres to your organization's retention policy.

Note: The timestamp value is displayed in UTC time zone and represents when the IP and MAC address were captured and cached by ThreatGraph. If the host was not connected to the cloud when the IP and MAC address were used, the timestamp value indicates when the host connected to the cloud.

Example: Retrieving host NIC history

To get NIC history info for one or more hosts, specify the customer ID (CID) in your request header and the agent ID (AID) in your request body.

Note: You can specify a maximum of 500 agent IDs in your request.

Example request

Get the NIC history of a host with the AID `abcd1234wxyz56`:

```
curl -X POST "https://api.crowdstrike.com/devices/combined/devices/network-address-history/v1" \
 -H "accept: application/json" \
 -H "X-CS-CUSTID: 0123456789ABCDEFGHIJKLMNOPQRSTUV-WX" \
 -H "Content-Type: application/json" \
 -d "{ \"ids\": [ \"abcd1234wxyz56\" ]}"
```

Example response

```
{
 "meta": {
  "query_time": 0.05071079,
  "powered_by": "device-api",
  "trace_id": "111bd7c5-...974e-6f341f0195e7"
 },
 "resources": [
  {
   "device_id": "abcd1234wxyz56",
   "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV-WX",
   "history": [
    {
     "ip_address": "192.0.2.100",
     "mac_address": "00-00-5E-00-53-00",
     "timestamp": "2021-08-17T19:07:49.872Z"
    },
    {
     "ip_address": "192.0.2.225",
     "mac_address": "00-00-5E-00-53-FF",
     "timestamp": "2021-08-17T15:26:53.96Z"
    }
   ]
  }
 ],
 "errors": []
}
```

Retrieving info about last logged in users

Get the username and login time of the last 10 user accounts to log into the device. This history is obtained from Threat Graph and adheres to your organization's retention policy.

Note: Login time is displayed in UTC time zone and is accurate if the host is connected to the cloud when the user account logs in. If the host was not connected to the cloud when the user account logged in, the login time indicates when the host connected to the cloud.

Example: Retrieving last logged in users info

To get last logged in users info for one or more hosts, specify the customer ID (CID) in your request header and the agent ID (AID) in your request body.

Note: With the v1 endpoint, you can specify a maximum of 500 host IDs in your request. The v1 endpoint returns all accounts that have logged into a host. The v2 endpoint is the API used by the Host information panel in Host setup and management > Host management. The v2 endpoint returns only the top 10 interactive user accounts. An interactive account is more likely to be a human login, rather than a system account login.

Example v1 request

Get the last logged in users details of a host with the agent ID `85ae98xxxxxxd9a8f2`:

```
curl -X POST "https://api.crowdstrike.com/devices/combined/devices/login-history/v1" \
 -H "accept: application/json" \
 -H "X-CS-CUSTID: 0123456789ABCDEFGHIJKLMNOPQRSTUV-WX" \
 -H "Content-Type: application/json" \
 -d "{ \"ids\": [ \"abcd1234wxyz56\" ]}"
```

Example v1 response


```
{
 "meta": {
  "query_time": 0.037558862,
  "powered_by": "device-api",
  "trace_id": "2f73859c-...b224-792c003f4584"
 },
 "resources": [
  {
   "device_id": "a1b2c3d4xxxxxxh8i9j0k1l2m3n4o5p6",
   "recent_logins": [
    {
     "user_name": "root@sample-vm-2.local\\root",
     "login_time": "2021-08-17T20:14:15Z"
    },
    {
     "user_name": "_spotlight@testmachine.local\\_spotlight",
     "login_time": "2021-08-17T19:16:18Z"
    },
    {
     "user_name": "johndoe@sample-vm-2.local\\johndoe",
     "login_time": "2021-08-17T19:07:50Z"
    },
    {
     "user_name": "johndoe@sample-vm-2.local\\johndoe",
     "login_time": "2021-08-17T19:07:50Z"
    },
    {
     "user_name": "_netbios@sample-vm-2.local\\_netbios",
     "login_time": "2021-08-17T15:26:53Z"
    },
   ]
  }
 ],
 "errors": []
}
```


Example v2 request

Get the last logged in user details of a host with the agent ID `85ae98xxxxxxd9a8f2`:

```
curl -X POST "https://api.crowdstrike.com/devices/combined/devices/login-history/v2" \
 -H "accept: application/json" \
 -H "X-CS-CUSTID: 0123456789ABCDEFGHIJKLMNOPQRSTUV-WX" \
 -H "Content-Type: application/json" \
 -d "{ \"ids\": [ \"abcd1234wxyz56\" ]}"
```

Example v2 response


```
{
  "meta": {
    "query_time": 0.27126414,
    "powered_by": "device-api",
    "trace_id": "254a0878-...-9bbf-0a1712bdb4aa"
  },
  "resources": [
    {
      "device_id": "a1b2c3d4xxxxxxh8i9j0k1l2m3n4o5p6",
      "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV-WX",
      "recent_logins": [
        {
          "user_name": "techw1",
          "login_time": "2024-12-31T07:32:07Z"
        },
        {
          "user_name": "datanj",
          "login_time": "2024-12-31T12:36:32Z"
        },
        {
          "user_name": "cloudm",
          "login_time": "2025-01-02T15:33:09Z"
        },
        {
          "user_name": "projg5",
          "login_time": "2025-01-02T17:49:18Z"
        },
        {
          "user_name": "innosb",
          "login_time": "2025-01-02T19:21:06Z"
        },
        {
          "user_name": "analyt",
          "login_time": "2025-01-02T21:51:11Z"
        },
        {
          "user_name": "cybrs8",
          "login_time": "2025-01-02T22:31:42Z"
        },
```

```
        {
          "user_name": "prodpr",
          "login_time": "2025-01-02T23:18:22Z"
        },
        {
          "user_name": "strats",
          "login_time": "2025-01-03T01:48:54Z"
        },
        {
          "user_name": "solsag",
          "login_time": "2025-01-03T05:10:53Z"
        }
      ]
    }
  ],
  "errors": []
}
```


Get host online status

Get the online status for one or more hosts by specifying each host's unique ID. Successful requests return an HTTP 200 code and the status for each host identified by a `state` of `online`, `offline`, or `unknown` in the response.

Tip: Make a `GET` request to `/devices/queries/devices/v1` to get a list of host IDs.

Endpoint

```
GET /devices/entities/online-state/v1
```

Required API client scope

Hosts:read

Parameters

Name	In	Type	Description
`ids` *required*	query	string	The unique ID of the host to get the online status of. You can send multiple IDs (up to 100 max) using the syntax `ids={a}&ids={b}`.

Example request

```
curl --location --request GET 'https://api.crowdstrike.com/devices/entities/online-state/v1?ids=5b62f6d1a451c8c1a8828ce28265d65b' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response


```
{
   "meta": {
      "query_time": 0.14602766,
      "trace_id": "69c8732e-c895-4969-bf6a-2080ad0a994d"
   },
   "resources": [
      {
         "id": "5b62f1a451c8c1a8826d8ce28265d65b",
         "cid": "6ad3bdc7a6aa4b9aa499e1283cf518fc",
         "last_seen": "2022-04-11T15:56:07Z",
         "state": "online"
      }
   ],
   "errors": null
}
```


Response fields

Name	Type	Description
`id`	string	The unique ID of the host.

Name	Type	Description
`state`	string	The host's current online status. Possible values: **online**: The host was seen recently and we are confident it's currently online. **offline**: The host has not been seen for some time and we are confident it's currently offline. **unknown**: The host has not been seen recently and we are not confident about its current state.
`last_seen`	string	The UTC date and time that the host was last seen. This field is only returned if the `state` is **online** or **unknown**.
`cid`	string	The customer ID that the host belongs to. This field is only returned if the `last_seen` field is also in the response.

Add or remove Falcon grouping tags

Use Falcon grouping tags to dynamically assign hosts to host groups based on custom keywords you define. Send the host ID and the add or remove action in the request body. Successful requests return an HTTP 200 code.

- There is a 256 character limit for a tag. This limit includes the FalconGroupingTag prefix.
- You can add up to 50 tags per host and 1000 tags per CID.
- You can add or remove tags for up to 5000 hosts at a time.
- For more information about grouping tags, see Using grouping tags.

Falcon Flight Control support

Falcon Flight Control customers can add and remove tags on child CID hosts from the parent CID. When making requests from the parent CID, specify the IDs of the child CID hosts you want to add or remove tags from.

Endpoint

`PATCH /devices/entities/devices/tags/v1`

Required API client scope

Hosts: write

Parameters

Name	In	Type	Description
`device_ids` *required*	body	string	The ID of the host to add or remove tags from. Send multiple `device_ids` (5000 max) as a comma-separated array.
`action` *required*	body	string	The action to perform. Available values: • `add` • `remove`
`tags` *required*	body	string	The tags to assign to or remove from the specified device IDs. Each tag must use the format `FalconGroupingTags/{tagName}`.

Example: Adding Falcon grouping tags named "tag1" and "tag2" to a host. You must include the FalconGroupingTags prefix to each tag.

Example request

```
curl -X PATCH "https://api.crowdstrike.com/devices/entities/devices/tags/v1" \
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json' \
```

```
 -H 'Accept: application/json' \
 -d '{
  "device_ids": [
  "bf4fbxxxxxx4b8026"
  ],
  "action": "add",
  "tags": [
   "FalconGroupingTags/tag1",
   "FalconGroupingTags/tag2"
  ]
 }'
```

Example response

```
{
 "meta": {
  "query_time": 0.023300596,
  "powered_by": "device-api",
  "trace_id": "0825d561-b558-4ee0-8461-a3cca7140713"
 },
 "resources": [
  {
   "device_id": "bf4fbxxxxxx4b8026",
   "updated": true,
   "code": 200
  }
 ],
 "errors": null
}
```

Example: Removing Falcon grouping tags named “tag1” and “tag2” from a host. You must include the FalconGroupingTags prefix to each tag.

Example request

```
curl -X PATCH "https://api.crowdstrike.com/devices/entities/devices/tags/v1" \
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json' \
 -H 'Accept: application/json' \
 -d '{
  "device_ids": [
   "bf4fbxxxxxx4b8026"
  ],
  "action": "remove",
  "tags": [
   "FalconGroupingTags/tag1",
   "FalconGroupingTags/tag2"
  ]
 }'
```

Example response

```
{
 "meta": {
  "query_time": 0.017340768,
  "powered_by": "device-api",
  "trace_id": "cdf85993-28ee-44b3-9438-682d6b40f344"
 },
 "resources": [
  {
   "device_id": "bf4fbxxxxxx4b8026",
   "updated": true,
   "code": 200
  }
 ],
 "errors": null
}
```

Contain, lift containment, hide, or restore hosts

Perform various actions on one or more host IDs such as containing or lifting containment, and hiding or restoring a hidden host. Successful requests return an HTTP 202 code.

Tip: Get host IDs from the GET /devices/queries/devices/v1 endpoint, the Falcon console, or the Streaming API.

About host containment

To prevent a potentially compromised host from communicating, network contain the host. After you've investigated and remediated, you can lift containment on that host to return its network communications to normal.

About hiding hosts

To prevent unnecessary detections from an inactive or a duplicate host you can hide the host.

Hiding a Windows, Mac, or Linux host doesn't uninstall or deactivate its sensor. If you hide an active host, it's moved to the Host setup and management > Manage endpoints > Host management page, and continues to send events and enforce policies.

Use caution if you hide Android or iOS hosts. When you hide a mobile host:

- It is completely removed from the Falcon console, and will not remain active or appear on Host setup and management > Manage endpoints > Host management page.
- All data associated with the CrowdStrike Falcon app is removed.

See Managing inactive and duplicate hosts for more information about hiding and restoring hosts.

Falcon Flight Control support

Falcon Flight Control customers can perform actions on child CID hosts from the parent CID. Specify the IDs of the child CID hosts and the action you want to perform when making requests from the parent CID.

Endpoint

```
POST /devices/entities/devices-actions/v2
```

Required API client scope

Hosts: write

Parameters

Name	In	Type	Description
`ids` *required*	body	string	The host agent ID (AID) of the host you want to perform an action on. Get an agent ID from a detection, the Falcon console, or the Streaming API. Provide the ID in JSON format with the key `ids` and the value in square brackets, such as: `"ids": ["123456789"]`
`action_name` *required*	query	string	The action to perform. Available values: • `contain`: Contains the host and stops any network communications to locations other than the CrowdStrike cloud and IPs specified in your containment policy. • `lift_containment`: Lifts containment on the host and returns its network communications to normal. • `lift_filesystem_containment_all`: Lifts file system containment on all hosts. • `hide_host`: Hides a host. In the Falcon console, it's moved to the Hidden Host view under Host Management. After the host is hidden, no new detections for the host will be reported through the UI or API. Each API request can hide a maximum of 5000 hosts. • `unhide_host`: Restores a host. Detection reporting resumes after the host is restored.

Example: Contain a host with the ID abcd1234wxyz56.

Example request

```
curl  -X POST 'https://api.crowdstrike.com/devices/entities/devices-actions/v2?action_name=contain' \
-H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
-H 'Accept: application/json' \
-H 'Content-Type: application/json' \
-d '{ "ids": ["abcd1234wxyz56"]}'
```

Example response

```
{
  "meta": {
    "query_time": 0.070339531,
    "powered_by": "device-api",
    "trace_id": "d24a6be3-504c-498d-861b-2ce8c754ea60"
  },
  "resources": [
    {
      "id": "abcd1234wxyz56",
      "path": "/devices/entities/devices/v2"
    }
  ],
  "errors": []
}
```

Example: Hide a host with the ID of abcd1234wxyz56.

Example request

```
curl  -X POST 'https://api.crowdstrike.com/devices/entities/devices-actions/v2?action_name=hide_host' \
-H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
-H 'Content-Type: application/json' \
-H 'Accept: application/json' \
-d '{ "ids": ["abcd1234wxyz56"]}'
```

Example response

```
{
 "meta": {
    "query_time": 0.070339531,
    "powered_by": "device-api",
    "trace_id": "d24a6be3-504c-498d-861b-2ce8c754ea60"
  },
  "resources": [
    {
      "id": "abcd1234wxyz56",
      "path": "/devices/entities/devices/v2"
    }
  ],
  "errors": []
}
```

Example: Restore a host with the ID of abcd1234wxyz56.

Example request

```
curl  -X POST 'https://api.crowdstrike.com/devices/entities/devices-actions/v2?action_name=unhide_host' \
-H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
-H 'Accept: application/json' \
-H 'Content-Type: application/json' \
-d '{ "ids": ["abcd1234wxyz56"]}'
```

Example response

```
{
 "meta": {
  "query_time": 0.070339531,
  "powered_by": "device-api",
  "trace_id": "d24a6be3-504c-498d-861b-2ce8c754ea60"
 },
 "resources": [
  {
   "id": "abcd1234wxyz56",
   "path": "/devices/entities/devices/v2"
  }
 ],
 "errors": []
}
```

Managing host groups

Host groups are collections of hosts. Policies, such as prevention policies or sensor update policies, are assigned to host groups, and the policy settings are applied to the individual hosts in those groups.

For more info, see Host and Host Group Management.

Creating host groups

Host groups determine which policies are applied to which hosts. The host group type can be dynamic or static. After a group is created, its type can't be changed.

For dynamic host groups, you specify an assignment rule that determines whether a host belongs to a group. Hosts that match the rule's criteria are automatically added to the group. If a host no longer matches the criteria, it's automatically removed from the group.

Important: Some assignment rules created using the CrowdStrike API display Assignment rule unsupported by Falcon Console UI in the Falcon console. This message displays when the rule that you want to view or modify uses complex FQL filtering syntax that is available only through the API. An example of a complex filtering rule is using the and (+) operator between attributes of the same filter type, such as `tag:'Tag1'+tag:'Tag2'`

For static host groups, you manually add and remove hosts after creating the group.

- Create a host group with POST /devices/entities/host-groups/v1

Example: Creating a dynamic host group with no assignment rule

Example request

```
curl -X POST "https://api.crowdstrike.com/devices/entities/host-groups/v1" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json' \
 -d '{
  "resources": [
```

```
   {
    "name": "Example dynamic group",
    "description": "example group",
    "group_type": "dynamic"
   }
  ]
}'
```

Example response

```
{
 "meta": {
  "query_time": 9.8e-8,
  "trace_id": "55e7e40c-b92b-4c2a-83ed-77b1993c0153"
 },
 "errors": null,
 "resources": [
  {
   "id": "e296exxxxxxxxb029",
   "group_type": "dynamic",
   "name": "Example dynamic group",
   "description": "example group",
   "created_by": "api-client-id:2e6dxxxxxxxx4914",
   "created_timestamp": "2021-11-18T17:11:43.190497077Z",
   "modified_by": "api-client-id:2e6dxxxxxxxx4914",
   "modified_timestamp": "2021-11-18T17:11:43.190497077Z"
  }
 ]
}
```

Example: Creating a dynamic host group with a single assignment rule

Example request

Create a dynamic group containing hosts with the Falcon grouping tag `example_tag`.

```
curl -X POST "https://api.crowdstrike.com/devices/entities/host-groups/v1" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json' \
 -d '{ "resources": [
        {
         "name": "Dynamic group",
         "description": "example group",
         "group_type": "dynamic",
           "assignment_rule": "tags:'FalconGroupingTags/example_tag'"
        }
    ]
 }'
```

Example response

```
{
    "meta": {
        "query_time": 1.27e-7,
        "trace_id": "91ff253a-ff8c-43fe-ab58-403e006ee556"
    },
    "errors": null,
    "resources": [
        {
            "id": "d5fcxxxxxxxx0ab8",
            "group_type": "dynamic",
            "name": "Dynamic group",
            "description": "example group",
            "assignment_rule": "tags:'FalconGroupingTags/example_tag'",
            "created_by": "api-client-id:2e6dxxxxxxxx4914",
            "created_timestamp": "2021-05-18T20:37:36.787205291Z",
            "modified_by": "api-client-id:2e6dxxxxxxxx4914",
            "modified_timestamp": "2021-05-18T20:37:36.787205291Z"
        }
    ]
}
```

Example: Creating a dynamic host group with multiple assignment rules

Example request

Create a dynamic host group with assignments based on the hostname and grouping tags.

```
curl -X POST "https://api.crowdstrike.com/devices/entities/host-groups/v1" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json' \
 -d '{
  "resources": [
   {
```

```
    "name": "Dynamic group",
    "description": "example group",
    "group_type": "dynamic",
    "assignment_rule": "tags:\''FalconGroupingTags/exampletag'\'' + hostname:'\''CS-WIN10'\''"
   }
  ]
 }'
```

Example response

```
{
    "meta": {
        "query_time": 1.21e-7,
        "trace_id": "65cd74c3-272d-46e5-8993-c98cba3302a1"
    },
    "errors": null,
    "resources": [
        {
            "id": "5bf0xxxxxxx6fc3",
            "group_type": "dynamic",
            "name": "Dynamic group",
            "description": "example group",
            "assignment_rule": "tags:'FalconGroupingTags/exampletag' + hostname:'CS-WIN10'",
            "created_by": "api-client-id:2e6dxxxxxxxx4914",
            "created_timestamp": "2021-11-18T17:53:41.645844771Z",
            "modified_by": "api-client-id:2e6dxxxxxxxx4914",
            "modified_timestamp": "2021-11-18T17:53:41.645844771Z"
        }
    ]
}
```

Example: Creating a static host group

Example request

```
curl -X POST "https://api.crowdstrike.com/devices/entities/host-groups/v1" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json' \
 -d '{
  "resources": [
   {
    "name": "Test Group 45",
    "description": "A demo group",
    "group_type": "static"
   }
  ]
 }'
```

Example response

```
{
    "meta": {
        "query_time": 2.13e-7,
        "trace_id": "9605b9de-74e8-458e-9f92-6d30df76ff82"
    },
    "errors": [],
    "resources": [
        {
            "id": "8015xxxxxxxx105d",
            "group_type": "static",
            "name": "Test Group 45",
            "description": "A demo group",
            "created_by": "api-client-id:2e6dxxxxxxxx4914",
            "created_timestamp": "2019-02-01T05:39:53.560719802Z",
            "modified_by": "api-client-id:2e6dxxxxxxxx4914",
            "modified_timestamp": "2019-02-01T05:39:53.560719802Z"
        }
    ]
}
```

Managing hosts in a static host group

After creating a static host group, you must manually assign hosts to the group. You can also remove hosts that no longer belong in the group.

- To add hosts, provide each host ID to POST /devices/entities/host-group-actions/v1?action_name=add-hosts
- To remove hosts, provide each host ID to POST /devices/entities/host-group-actions/v1?action_name=remove-hosts

Example: Managing hosts in a static host group

Example request

Add or remove hosts belonging to a group.

- Use the `value` parameter to specify the host IDs to add or remove.
- Use the `ids` parameter to specify the host group ID.
- Specify either the `add-hosts` or `remove-hosts` action to add or remove hosts, respectively. This action is used with the `action_name` parameter.

The following example adds 3 hosts to a group with the ID `8015xxxxxxxx105d`.

```
curl -X POST "https://api.crowdstrike.com/devices/entities/host-group-actions/v1?action_name=add-hosts" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json' \
 -d '{
  "action_parameters": [
       {
    "name": "filter",
    "value": "(device_id:['e139xxxxxxxx5885', '8393xxxxxxxx9650','389axxxxxxxx5e80'])"
   }
  ],
  "ids": [
   "8015xxxxxxxx105d"
  ]
 }'
```

Example response


```
{
    "meta": {
        "query_time": 1.92e-7,
        "trace_id": "5b5f13b7-4bbf-4bbc-9273-827abe3ee465"
    },
    "errors": [],
    "resources": [
        {
            "id": "8015xxxxxxxx105d",
            "group_type": "static",
            "name": "Test Group 45",
            "description": "A demo group",
            "assignment_rule": "device_id:[],hostname:[]",
            "created_by": "api-client-id:2e6dxxxxxxxx4914",
            "created_timestamp": "2019-02-01T05:39:53.560719802Z",
            "modified_by": "api-client-id:2e6dxxxxxxxx4914",
            "modified_timestamp": "2019-02-01T05:39:53.560719802Z"
        }
    ]
}
```


Finding host groups

You can find host groups and get host group details in these ways:

- Search for host group IDs, then get details by ID:
    1. Get host group IDs by specifying an optional FQL filter or limit with GET /devices/queries/host-groups/v1

       Note: When searching for a host group by name, provide the name in all lowercase letters, even if the host group's name includes uppercase letters.

    2. Get host group details with GET /devices/entities/host-groups/v1?ids={id}
- View details for multiple host groups by specifying an optional FQL filter or limit with GET /devices/combined/host-groups/v1

Note: The /devices/queries/host-groups and /devices/combined/host-groups endpoints return data only if the response set includes 500 or fewer items. This limit applies to the total API response size, regardless of your pagination sizes with the `limit` and `offset` parameters. If your response set would include more than 500 items, the CrowdStrike API returns an HTML 500 response instead. To avoid this issue, use the `filter` parameter to reduce the total number of items in the API response.

Example: Retrieving host group IDs with a filter

Example request

List static host groups.

```
curl -G -X GET "https://api.crowdstrike.com/devices/queries/host-groups/v1?filter=group_type:'static'" \
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json' \
```

Example response


```
{
 "meta": {
  "query_time": 1.14e-7,
  "pagination": {
   "offset": 100,
   "limit": 100,
   "total": 127
  },
  "trace_id": "68f366ea-bd9f-4dfd-b862-dc6d9e553218"
 },
 "resources": [
```

```
  "93e8xxxxxxxx4515"
  "44a2xxxxxxxx9b15"
  …
  "9640xxxxxxxx00a2"
  "aa93xxxxxxxx95bc"
 ],
 "errors": []
}
```


Example: Retrieving host group IDs with a limit

Example request

List the first 10 host groups in your environment. Host groups are sorted alphabetically by host group name.

```
curl -X GET "https://api.crowdstrike.com/devices/queries/host-groups/v1?limit=10" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json'
```

Example response


```
{
    "meta": {
        "query_time": 1.82e-7,
        "pagination": {
            "offset": 10,
            "limit": 10,
            "total": 184
        },
        "trace_id": "bd39f709-4a96-43f7-bdd8-d5dfd44b608c"
    },
    "resources": [
        "c8b7xxxxxxxxe2db",
        "93e8xxxxxxxx9b15",
        "3fa1xxxxxxxx0c38",
        "3ce1xxxxxxxxb98b",
        "532cxxxxxxxxcb3f",
        "c909xxxxxxxxd2b6",
        "9bbdxxxxxxxx6ed0",
        "006exxxxxxxxa3e7",
        "9588xxxxxxxxa455",
        "eafbxxxxxxxx5125"
    ],
    "errors": []
}
```


Example: Getting details of a host group by ID

Example request

```
curl -X GET "https://api.crowdstrike.com/devices/entities/host-groups/v1?ids=eafbxxxxxxxx5125" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json'
```

Example response


```
{
  "meta": {
   "query_time": 1.14e-7,
    "trace_id": "15a87de7-3aa7-419c-a3af-83fb50094313"
  },
  "errors": [],
 "resources": [
    {
      "id": "eafbxxxxxxxx5125",
      "group_type": "dynamic",
      "name": "Example dynamic group",
      "description": "",
      "assignment_rule": "tags:'FalconGroupingTags/example_tag'",
      "created_by": "example@crowdstrike.com",
      "created_timestamp": "2020-08-20T08:43:48.22333875Z",
      "modified_by": "example@crowdstrike.com",
      "modified_timestamp": "2020-11-12T08:42:04.016448639Z"
    }
  ]
}
```


Example: Getting details of multiple host groups

Example request

Get details of the first 3 host groups in your environment. Host groups are sorted alphabetically by host group name.

```
curl -X GET "https://api.crowdstrike.com/devices/combined/host-groups/v1?limit=3" \
 -H 'Authorization: Bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json'
```

Example response


```
{
  "meta": {
    "query_time": 9.7e-8,
    "pagination": {
      "offset": 10,
      "limit": 10,
      "total": 463
    },
    "trace_id": "8107d3b6-b4a0-41c3-8cdb-f59996f46e39"
  },
  "errors": [],
  "resources": [
    {
      "id": "c8b7xxxxxxxxe2db",
      "group_type": "dynamic",
      "name": "Dynamic1",
      "description": "",
      "assignment_rule": "hostname:'ABCD'",
      "created_by": "example.crowdstrike.com",
      "created_timestamp": "2021-03-16T12:03:33.426643573Z",
      "modified_by": "example@crowdstrike.com",
      "modified_timestamp": "2021-03-16T12:03:33.426643573Z"
    },
    {
      "id": "93e8xxxxxxxx9b15",
      "group_type": "static",
     "name": "Static1",
      "description": "",
     "assignment_rule": "device_id:[''],hostname:['DESKTOP-1234']",
      "created_by": "example@crowdstrike.com",
      "created_timestamp": "2020-09-21T00:19:33.305115518Z",
      "modified_by": "example@crowdstrike.com",
      "modified_timestamp": "2021-02-26T15:33:15.323839953Z"
    },
    {
      "id": "3fa1xxxxxxxx0c38",
      "group_type": "dynamic",
      "name": "Z Dynamic2",
      "description": "",
      "assignment_rule": "tags:'SensorGroupingTags/tag1'",
      "created_by": "example@crowdstrike.com",
      "created_timestamp": "2020-12-20T08:43:48.55333874Z",
      "modified_by": "example@crowdstrike.com",
      "modified_timestamp": "2021-01-12T08:33:04.017448636Z"
    }
  ]
}
```


Modifying host group details

Modify the name or description of a host group. For dynamic groups, you can also modify the assignment rule.

For info about adding or removing hosts belonging to a static group, see Managing hosts in a static host group.

- Modify host group details with PATCH /devices/entities/host-groups/v1

Example: Modifying a host group

Example request

Specify the group's ID in the body of the request with the `id` parameter.

This example modifies the name of the host group.

```
curl -X PATCH  "https://api.crowdstrike.com/devices/entities/host-groups/v1" \
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json' \
 -d '{
  "resources": [
   {
    "name": "Example group 1",
    "id": "006exxxxxxxxa3e7"
   }
  ]
 }'
```

Example response


```
{
  "meta": {
    "query_time": 1.02e-7,
    "trace_id": "7603b19c-5143-4f91-9f81-dc727081e2cd"
},
  "errors": null,
  "resources": [
    {
      "id": "006exxxxxxxxa3e7",
      "group_type": "static",
      "name": "Example group 1",
      "description": "",
      "created_by": "api-client-id:2e6dxxxxxxxx4914",
      "created_timestamp": "2021-05-19T15:39:57.219794519Z",
      "modified_by": "api-client-id:2e6dxxxxxxxx4914",
      "modified_timestamp": "2021-05-19T15:43:03.095976343Z"
    }
  ]
}
```


Deleting host groups

Delete host groups that are no longer needed.

- Delete a host group with DELETE /devices/entities/host-groups/v1?ids={id}

Example: Deleting a host group

Example request

```
curl -X DELETE "https://api.crowdstrike.com/devices/entities/host-groups/v1?ids=006exxxxxxxxa3e7" \
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Content-Type: application/json'
```

Example response


```
{
 "meta": {
  "query_time": 1.14e-7,
  "trace_id": "c55e1c5f-3496-4dd2-88a4-09dc0ccc39b6"
 },
 "resources": [
  "006exxxxxxxxa3e7"
 ],
 "errors": []
}
```


Finding host group members

Search for hosts belonging to a host group.

- Get the IDs of hosts in a host group with GET /devices/queries/host-group-members/v1?id={id}
- Get the details of hosts in a host group with GET /devices/combined/host-group-members/v1?id={id}

Example: Retrieving the IDs of hosts in a host group

Example request

List the IDs of the first 5 hosts in the host group with the ID `006exxxxxxxxa3e7`. Hosts are sorted alphabetically by host name.

```
curl -X GET "https://api.crowdstrike.com/devices/queries/host-group-members/v1?id=006exxxxxxxxa3e7&limit=5" \
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response


```
{
  "meta": {
    "query_time": 9.6e-8,
    "pagination": {
      "offset": 5,
      "limit": 5,
      "total": 61
    },
    "trace_id": "74466c0d-2dd0-4a10-8cd1-a1754c6b9381"
  },
  "resources": [
    "62d5xxxxxxxx43f0",
    "0f53xxxxxxxxc77b",
    "c790xxxxxxxx8d52",
    "b215xxxxxxxx8d4d",
```

```
    "ab62xxxxxxxxa478"
  ],
  "errors": []
}
```


Example: Retrieving the details of hosts in a host group

Example request

List host details for the first 2 hosts in the host group with the ID `006exxxxxxxxa3e7`. Hosts are sorted alphabetically by host name.

```
curl -X GET "https://api.crowdstrike.com/devices/combined/host-group-members/v1?id=006exxxxxxxxa3e7&limit=2" \
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response


```
{
  "meta": {
    "query_time": 1.36e-7,
    "pagination": {
      "offset": 2,
      "limit": 2,
      "total": 61
    },
    "trace_id": "e6bc7724-3339-4544-9fb0-677d2943c3d8"
  },
  "errors": [],
  "resources": [
    {
   "device_id": "62d5xxxxxxxx43f0",
   "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV",
   "agent_load_flags": "0",
   "agent_local_time": "2021-03-29T22:07:01.728Z",
   "agent_version": "6.xx.xxxxx.0",
   …
   "status": "normal",
   "system_manufacturer": "VMware, Inc.",
   "system_product_name": "VMware Virtual Platform",
   "tags": [],
   "modified_timestamp": "2021-04-19T22:28:45Z",
   "meta": {
    "version": "3xxxxx"
   }
    },
    {
   "device_id": "0f53xxxxxxxxc77b",
   "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV",
   "agent_load_flags": "0",
   "agent_local_time": "2021-04-16T08:42:52.169Z",
   "agent_version": "6.xx.xxxxx.0",
   …
   "status": "normal",
   "system_manufacturer": "VMware, Inc.",
   "system_product_name": "VMware Virtual Platform",
   "tags": [],
   "modified_timestamp": "2021-04-21T14:51:15Z",
   "meta": {
    "version": "3xxxxx"
   }
    }
  ]
}
```


Appendix A: Device filters

Use these fields for filtering or querying. Read our Falcon Query Language (FQL) Reference for details on how filtering works.

Name	Type	Supports filter operators?	Description	Example
device_id	String	No	The ID of the device.	`"061a51ec742c44624a176f079d742052"`
agent_load_flags	String	No	CrowdStrike agent configuration notes	
agent_version	String	No	CrowdStrike agent configuration notes	
bios_manufacturer	String	No	Bios manufacture name.	`"Phoenix Technologies LTD"`

Name	Type	Supports filter operators?	Description	Example
bios_version	String	No	Bios version.	`"6.00"`
cid	String	No	The unique customer ID.	
config_id_base	String	No	CrowdStrike agent configuration notes	
config_id_build	String	No	CrowdStrike agent configuration notes	
config_id_platform	String	No	CrowdStrike agent configuration notes	
cpu_signature	String	Yes	The CPU signature of the device.	`"GenuineIntel"`
external_ip	IP Address	Yes	External IP of the device, as seen by CrowdStrike.	`192.0.2.100`
first_seen	Timestamp	Yes	Timestamp of device's first connection to Falcon, in "YYYY-MM-DDTHH:MM:SSZ" format.	`"2016-07-19T11:14:15Z"`
groups	String	No	A list of hosts that are in a given group	`"0bd018b7bd8b47cc8834228a294eabf2"`
hostname	String	Yes	The name of the machine. Supports prefix and suffix searching with *wildcard, so you can search for terms like abc* and *abc. Use`:[]` (the in list filter) to do an exact case-sensitive search for a hostname that exactly matches one of the items in the list.	`WinPC9251`
service_provider_account_id	String	No	The cloud account id	`"04929999429"`
service_provider	String	No	The cloud service provider	`"AWS_EC2_V2"`
instance_id	String	No	Cloud resource information.	`"i-0dc41d0939384cd15"`
kernel_version	String	No	Kernel version of the host OS.	`"6.1.7601.18741"`
last_login_timestamp	Timestamp	Yes	User logon event timestamp, once a week.	
last_seen	Timestamp	Yes	Timestamp of device's most recent connection to Falcon, in "YYYY-MM-DDTHH:MM:SSZ" format.	`"2016-07-19T11:14:15Z"`
local_ip	IP Address	No	The device's local IP address. As a device management parameter, this is the IP address of this device at the last time it connected to the CrowdStrike Cloud.	`192.0.2.1`

local_ip.raw	IP Address with wildcards (*)	No	A portion of the device's local IP address, used only for searches that include wildcard characters. Using a wildcard requires specific syntax: when you specify an IP address with this parameter, prefix the IP address with an asterisk (*) and enclose the IP address in single quotes.	Search for a device with the IP address 192.0.2.100:
				`local_ip.raw:*'192.0.2.*'`
				`local_ip.raw:*'*.0.2.100'`

mac_address	String	No	The MAC address of the device	`0a-de-48-69-11-45`
machine_domain	String	No	Active Directory domain name.	
major_version	String	No	Major version of the Operating System	

Name	Type	Supports filter operators?	Description	Example
minor_version	String	No	Minor version of the Operating System	
modified_timestamp	Timestamp	Yes	The last time that the machine record was updated. Can include status like containment status changes or configuration group changes	
os_version	String	No	Operating system version.	`"Windows 7"`
ou	String	No	Active Directory organizational unit name.	
platform_id	String	No	CrowdStrike agent configuration notes	

platform_name	String	No	Operating system platform.	`"Windows"`
				`"Mac"`
				`"Linux"`

product_type_desc	String	No	Name of product type.	`"Workstation"`
				`"Server"`
				`"Domain Controller"`

reduced_functionality_mode	String	Yes	Reduced functionality mode (RFM) status: • Yes • No • Unknown (displayed as a blank string) Unknown is used for hosts with an unavailable RFM status: • The sensor was deployed less than 24 hours ago and has not yet provided an RFM status. • The sensor version does not support RFM.	
release_group	String	No	Name of the Falcon deployment group, if the this machine is part of a Falcon sensor deployment group.	
serial_number	String	Yes	Serial number of the device.	`"C42AFKEBM563"`
site_name	String	No	Active Directory site name.	

status	String	No	Containment Status of the machine. "Normal" denotes good operations; other values might mean reduced functionality or support.	`"Normal"`
				`"containment_pending"`
				`"contained"`
				`"lift_containment_pending"`

system_manufacturer	String	No	Name of system manufacturer	`"VMware, Inc."`
system_product_name	String	No	Name of system product	`"VMware Virtual Platform"`
tags	String	No	Sensor and cloud tags of the host	`tags:'FalconTag'`

Flight Control APIs

Manage CID groups, user groups, and role assignments in your MSSP or multi-CID environment.

About CrowdStrike APIs

CrowdStrike provides use cases and example requests and responses for interacting with a specific set of our OAuth2-based APIs. For general info about CrowdStrike APIs, see CrowdStrike OAuth2-Based APIs, which covers these topics:

- Details on getting started, such as authentication and API scopes
- Domains used in base URLs by cloud
- Links to our Swagger API specification by cloud

Using Flight Control APIs

Use Flight Control APIs to manage CID groups, user groups, and role assignments in your MSSP or multi-CID environments.

CID groups are collections of child CIDs that determine which CIDs users can access. You can categorize your child CIDs into logical groupings that fit your organization's needs, such as CID groups for different departments or business units, geographic regions, and more.

User groups are collections of users that determine what roles and access they have to different CID groups. You can categorize users into different user groups in whatever way best suits your organization's needs, similar to CID groups.

Between user groups and CID groups, you can assign user groups to CID groups to determine which CIDs they have access to, and you can give role assignments to user groups to determine which roles users have in the CID groups to which they've been assigned.

Managing CID groups

Get a list of CID groups by ID

1. Retrieve a CID group ID with GET /mssp/queries/cid-groups/v1
2. Provide the CID group ID with GET /mssp/entities/cid-groups/v1

Example request

```
curl -X GET \
'https://api.crowdstrike.com/mssp/entities/cid-groups/v1?cid_group_ids=5f9fd7d58dca4ab99a5fcb8c9fb48eea' \
 -H 'Accept: application/json' \
 -H 'Authorization: Bearer '<oauth_token>' \
 -H 'Content-Type: application/json' \
```

Example response

```
{
 "meta": {
  "query_time": 0.005567811,
  "powered_by": "csam",
  "trace_id": "7ddeceb1-c57c-4d3a-92a5-39cba0be0415"
 },
  "resources": [
   {
    "cid_group_id": "5f9fd7d58dca4ab99a5fcb8c9fb48eea",
    "name": "Default",
    "description": "Auto generated CID group"
   }
  ],
  "errors": []
 }
```

Create a CID group

- Create a new CID group using POST /mssp/entities/cid-groups/v1

Note: You can have up to 500 CID groups.

Example request

```
curl -X POST \
https://api.crowdstrike.com/mssp/entities/cid-groups/v1 \
 -H 'Accept: application/json' \
 -H 'Authorization: Bearer '<oauth_token>' \
 -H 'Content-Type: application/json' \
 -d '{"resources":[{"name":"Manual Testing","description":"manual testing."}]}'
```

Example response

```
{
 "meta": {
  "query_time": 0.016649372,
  "writes": {
   "resources_affected": 1
  },
```

```
   "powered_by": "csam",
   "trace_id": "a5f0ae73-a021-4a72-939c-67828db442ff"
 },
 "resources": [
  {
   "cid_group_id": "e20d7f90765c45888e635e76a8fe1615",
   "name": "Manual Testing",
   "description": "manual testing."
  }
 ],
 "errors": []
}
```


Updating CID groups

Update a CID group's name or description:

1. Retrieve a CID group ID using GET /mssp/queries/cid-groups/v1
2. Update the CID group with PATCH /mssp/entities/cid-groups/v1

Example request

```
curl -X PATCH \
  https://api.crowdstrike.com/mssp/entities/cid-groups/v1 \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer '<oauth_token>' \
  -H 'Content-Type: application/json' \
  -d '{"resources":[{"cid_group_id":"e20d7f90765c45888e635e76a8fe1615","name":"Updated Name","description":"updated name for manual testing"}]}'
```

Example response

Delete a CID group

1. Retrieve a CID group ID using GET /mssp/queries/cid-groups/v1
2. Provide the CID group ID using DELETE /mssp/entities/cid-groups/v1

Example request

```
curl -X DELETE \
'https://api.crowdstrike.com/mssp/entities/cid-groups/v1?cid_group_ids=e20d7f90765c45888e635e76a8fe1615' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer '<oauth_token>' \
  -H 'Content-Type: application/json' \
```

Example response


```
{
    "meta": {
        "query_time": 0.024062408,
        "writes": {
            "resources_affected": 1
        },
        "powered_by": "csam",
        "trace_id": "67f09889-e175-48f8-ba23-bd1a74c904a6"
    },
    "resources": [
        "e20d7f90765c45888e635e76a8fe1615"
    ],
    "errors": []
}
```


Managing user groups

User groups are collections of users that can be assigned to CID groups, determining what they have access to, which roles they have, and more. Users can only be assigned to a user group if they have access to the same CID the user group belongs to.

Get user groups by ID

1. Retrieve a user group ID using GET /mssp/queries/user-groups/v1
2. Provide the user group ID using GET /mssp/entities/user-groups/v1

Example request

```
curl -X GET \
'https://api.crowdstrike.com/mssp/entities/user-groups/v1?user_group_ids=51a08d4b045f4e2dbe582336d82a21ef' \
  -H 'Accept: application/json' \
```

```
  -H 'Authorization: Bearer '<oauth_token>' \
  -H 'Content-Type: application/json' \
```

Example response


```
{
    "meta": {
        "query_time": 0.005714689,
        "powered_by": "csam",
        "trace_id": "36bd0582-e5ff-4b52-ad50-28630950e801"
    },
    "resources": [
        {
            "user_group_id": "51a08d4b045f4e2dbe582336d82a21ef",
            "name": "Manual Testing",
            "description": "manual testing."
        }
    ],
    "errors": []
}
```


Create a user group

- Create a new user groups using POST /mssp/entities/user-groups/v1

Example request

```
curl -X POST \
  https://api.crowdstrike.com/mssp/entities/user-groups/v1 \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer '<oauth_token>' \
  -H 'Content-Type: application/json' \
  -d '{"resources":[{"name":"Manual Testing","description":"manual testing."}]}'
```

Example response


```
{
    "meta": {
        "query_time": 0.016760886,
        "writes": {
            "resources_affected": 1
        },
        "powered_by": "csam",
        "trace_id": "ca74405c-b714-4d18-9fc4-f5dff5234661"
    },
    "resources": [
        {
            "user_group_id": "51a08d4b045f4e2dbe582336d82a21ef",
            "cid": "6d48d3a0567147d493b4f45c0668dafc",
            "name": "Manual Testing",
            "description": "manual testing."
        }
    ],
    "errors": []
}
```


Delete a user group

1. Retrieve a user group ID using GET /mssp/queries/user-groups/v1
2. Provide the user group ID using DELETE /mssp/entities/user-groups/v1

Example request

```
curl -X DELETE \
'https://api.crowdstrike.com/mssp/entities/user-groups/v1?user_group_ids=51a08d4b045f4e2dbe582336d82a21ef' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json'
```

Example response


```
{
    "meta": {
        "query_time": 0.01522713,
        "writes": {
            "resources_affected": 1
        },
        "powered_by": "csam",
        "trace_id": "f91c573b-8661-4895-8126-b800876a1dce"
    },
```

```
    "resources": [
        "51a08d4b045f4e2dbe582336d82a21ef"
    ],
    "errors": []
}
```


Managing CID group members

Get a list of CID group members by CID group ID

1. Retrieve a CID group ID using GET /mssp/queries/cid-group-members/v1
2. Provide the CID group ID using GET /mssp/entities/cid-group-members/v1

Example request

```
curl -X GET \
'https://api.crowdstrike.com/mssp/entities/cid-group-members/v1?cid_group_ids=c3e2e2d0b55d4baeb515658df7f6c2ac' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json'
```

Example response


```
{
    "meta": {
        "query_time": 0.010488969,
        "powered_by": "csam",
        "trace_id": "1f6b78f5-6621-447b-b8c3-c4bf7343d69f"
    },
    "resources": null,
    "errors": [
        {
            "code": 404,
            "message": "No members found for cid_group_id=c3e2e2d0b55d4baeb515658df7f6c2ac"
        }
    ]
}
```


Add a CID to a CID group

1. Retrieve a CID group ID using GET /mssp/queries/cid-group-members/v1
2. Provide the CID group ID and the CID using POST /mssp/entities/cid-group-members/v1

Example request

```
curl -X POST \
  https://api.crowdstrike.com/mssp/entities/cid-group-members/v1 \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"resources":[{"cid_group_id":"c3xxxxxxxxxxxxxxxxxxxxxxxxxxxxxac","cid":"","cids":["0123456789ABCDEFGHIJKLMNOPQRSTUV"]}]}'
```

Example response


```
{
    "meta": {
        "query_time": 0.030225497,
        "writes": {
            "resources_affected": 1
        },
        "powered_by": "csam",
        "trace_id": "2f2f9fe4-271e-4b7b-9a76-6e68b07e96ef"
    },
    "resources": [
        {
            "cid_group_id": "c3e2e2d0b55d4baeb515658df7f6c2ac",
            "parent_cid": "6d48d3a0567147d493b4f45c0668dafc",
            "cids": [
                "9316f3dd24ba413990822659d531ffa9"
            ]
        }
    ],
    "errors": []
}
```


Remove a CID from a CID group

1. Retrieve a CID group ID using GET /mssp/queries/cid-group-members/v1

2. Provide the CID group ID and the CID using DELETE /mssp/entities/cid-group-members/v1

Example request

```
curl -X DELETE \
  https://api.crowdstrike.com/mssp/entities/cid-group-members/v1 \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"resources":[{"cid_group_id":"c3e2e2d0b55d4baeb515658df7f6c2ac","cids":["9316f3dd24ba413990822659d531ffa9"]}]}'
```

Example response

```
{
    "meta": {
        "query_time": 0.022675653,
        "writes": {
            "resources_affected": 1
        },
        "powered_by": "csam",
        "trace_id": "94072e2c-9363-4c70-b949-894c428b4175"
    },
    "resources": [
        {
            "cid_group_id": "c3e2e2d0b55d4baeb515658df7f6c2ac",
            "cids": [
                "9316f3dd24ba413990822659d531ffa9"
            ]
        }
    ],
    "errors": []
}
```

Managing user group members

Get a list of user group members by user group ID

1. Retrieve a user group ID using GET /mssp/queries/user-groups/v1

2. Provide the user group ID using GET /mssp/entities/user-group-members/v1

Example request

```
curl -X GET \ 'https://api.crowdstrike.com/mssp/entities/user-group-members/v1?user_group_ids=d5bfc0af-f102-448a-8558-28d0073caf77' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
```

Example response

```
{
    "meta": {
        "query_time": 0.009317748,
        "pagination": {
            "offset": 0,
            "limit": 10,
            "total": 0
        },
        "powered_by": "csam",
        "trace_id": "41ec0e0e-8458-40da-9408-031db3b41e4e"
    },
    "resources": null,
    "errors": []
}
```

Add a user to a user group

- Provide the user ID and user group ID using POST /mssp/entities/user-group-members/v1

Example request

```
curl -X POST \
  https://api.crowdstrike.com/mssp/entities/user-group-members/v1 \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"resources":[{"user_group_id":"85bbf22aa2174f528af224122c42da8c","user_uuids":["d5bfc0af-f102-448a-8558-28d0073caf77"]}]}'
```

Example response


```
{
    "meta": {
        "query_time": 0.064118679,
        "writes": {
            "resources_affected": 1
        },
        "powered_by": "csam",
        "trace_id": "25f1526f-8259-4c19-87e0-0457f293d244"
    },
    "resources": [
        {
            "user_group_id": "85bbf22aa2174f528af224122c42da8c",
            "user_uuids": [
                "d5bfc0af-f102-448a-8558-28d0073caf77"
            ]
        }
    ],
    "errors": []
}
```


Remove a user from a user group

- Provide the user ID and user group ID using DELETE /mssp/entities/user-group-members/v1

Example request

```
curl -X DELETE \
  https://api.crowdstrike.com/mssp/entities/user-group-members/v1 \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"resources":[{"user_group_id":"85bbf22aa2174f528af224122c42da8c","user_uuids":["d5bfc0af-f102-448a-8558-28d0073caf77"]}]}'
```

Example response


```
{
    "meta": {
        "query_time": 0.016941826,
        "writes": {
            "resources_affected": 1
        },
        "powered_by": "csam",
        "trace_id": "eaad940a-8e56-4c01-8162-8e6c9bbaeb0f"
    },
    "resources": [
        {
            "user_group_id": "85bbf22aa2174f528af224122c42da8c",
            "user_uuids": [
                "d5bfc0af-f102-448a-8558-28d0073caf77"
            ]
        }
    ],
    "errors": []
}
```


Managing role assignments

Use Flight Control APIs to find role assignments between user groups and CID groups, assign new roles between user groups and CID groups, and remove roles that have been assigned to user groups.

Get role assignments

- Get role assignments with GET /mssp/entities/mssp-roles/v1

Example request

```
curl -X GET \
'https://api.crowdstrike.com/mssp/entities/mssp-roles/v1?ids=85bbf22aa2174f528af224122c42da8c:c3e2e2d0b55d4baeb515658df7f6c2ac' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
```

Example response


```
{
    "meta": {
        "query_time": 0.014227704,
        "powered_by": "csam",
```

```
        "trace_id": "291539d4-1c46-4f01-97a1-a6e5eee0c402"
    },
    "resources": [
        {
            "cid_group_id": "c3e2e2d0b55d4baeb515658df7f6c2ac",
            "user_group_id": "85bbf22aa2174f528af224122c42da8c",
            "role_ids": [
                "falconhost_analyst"
            ]
        }
    ],
    "errors": []
}
```


Create a role assignment

- Assign a new MSSP role between a user group and a CID group with POST /mssp/entities/mssp-roles/v1

Example request

```
curl -X POST \
  https://api.crowdstrike.com/mssp/entities/mssp-roles/v1 \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"resources":[{"cid_group_id":"c3e2e2d0b55d4baeb515658df7f6c2ac","user_group_id":"85bbf22aa2174f528af224122c42da8c","role_ids":["falconhost_admin"]}]}'
```

Example response


```
{
    "meta": {
        "query_time": 0.020251931,
        "writes": {
            "resources_affected": 1
        },
        "powered_by": "csam",
        "trace_id": "f4d5de85-bc76-43f4-8e8e-2ce895d4a9c1"
    },
    "resources": [
        {
            "cid_group_id": "c3e2e2d0b55d4baeb515658df7f6c2ac",
            "user_group_id": "85bbf22aa2174f528af224122c42da8c",
            "role_ids": [
                "falconhost_admin"
            ]
        }
    ],
    "errors": []
}
```


Delete a role assignment

- Delete a role assignment between a user group and a CID group using DELETE /mssp/entities/mssp-roles/v1

Example request

```
curl -X DELETE \
  https://api.crowdstrike.com/mssp/entities/mssp-roles/v1 \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"resources":[{"cid_group_id":"c3e2e2d0b55d4baeb515658df7f6c2ac","user_group_id":"85bbf22aa2174f528af224122c42da8c"}]}'
```

Example response


```
{
    "meta": {
        "query_time": 0.011895713,
        "writes": {
            "resources_affected": 1
        },
        "powered_by": "csam",
        "trace_id": "883ee1b3-743e-4d3f-af54-01fdd350255f"
    },
    "resources": [
        {
            "cid_group_id": "c3e2e2d0b55d4baeb515658df7f6c2ac",
            "user_group_id": "85bbf22aa2174f528af224122c42da8c",
            "role_ids": null
        }
    ],
    "errors": []
}
```

Migrating hosts between CIDs

Migrate hosts from one CID to another by creating migration jobs in a Falcon Flight Control parent CID.
Important: You can only migrate hosts between CIDs that are managed by the same parent CID and that are in the same CrowdStrike cloud. Additionally, there must be one domain in common between all original CIDs and the destination CID of a migration job. See Host migration CID domain requirements. For info about host minimum sensor version requirements, see Host migration requirements.

Existing detections and telemetry are not migrated, they stay associated with the existing host record in the original CID. After migration, only new detections and telemetry appear in the destination CID for a migrated host.

Hosts are migrated using migration jobs. You can create multiple migration jobs. Each migration job includes one or more hosts migrating to the same destination CID. Migration jobs are managed in the migration queue.

For more info, see Migrating hosts between CIDs. Specifically, for details about actions and configurations included in a migration, see Migration process overview.

You can use the CrowdStrike API to perform these host migration tasks:

1. Creating and starting a migration job: Create a migration job that includes the hosts to be migrated, manage static host group assignments, remove hosts from a migration job, delete an unstarted migration job, and start a migration job.
2. Managing a migration job: Get info about hosts in migration jobs, such as migration IDs and migration event details. Rename a migration job. Cancel a running migration job.
3. Managing the migration queue: Get a list of migration jobs and get details about each migration job.

Host migration required scopes

API clients used for host migration must include these scopes:

- Host Migration: Read and Write
- Flight Control: Read
- Hosts: Read

Important: Requests must be made from the parent CID.

Host migration IDs

Host migration APIs use these IDs related to the migration:

- Migration job ID: Each migration job is assigned a unique identifier
- Host migration ID: Each host in a migration job is assigned an ephemeral unique identifier for the purposes of the migration

Important: Each host migration API endpoint uses one or both of these IDs in a parameter named `id` or `ids`. Ensure you understand which ID value to use in your request.

Creating and starting a migration job

Create a migration job with up to 1,000 hosts, manage static host groups assignments for the destination CID, remove hosts, if necessary, and then start the migration job. You can also delete a migration job that hasn't been started.

1. Get valid destination CIDs: Ensure you have a valid destination CID value for all hosts you want to migrate
2. Create a migration job: Create a migration job that includes the hosts you want to migrate and the destination CID
3. Manage static host group assignments: If desired, add or remove static hosts group assignments from the hosts in the migration job
4. Remove hosts from an unstarted migration job: If needed, remove one or more hosts from a migration job
5. Delete an unstarted migration job: If needed, delete a migration job
6. Start a migration job: After you are finished configuring migration settings, start the migration job

Get valid destination CIDs

A migration job can have only one destination CID, and all hosts in the migration job must be able to migrate to the specified destination CID. This means that you must verify a valid destination CID before creating a migration job.

Get the CID for specific hosts by device ID or based on attributes such as platform, hostname, or status. Successful requests return an HTTP 200 code and array of CID names and IDs that match the request criteria.

Important: You can only migrate between CIDs that are children of the parent CID where you create the migration job. Additionally, the original CID and destination CID must be in the same CrowdStrike cloud.

To get a list of valid destination CID values:

- `POST /host-migration/entities/migration-destinations/GET/v1`

Parameters

The `/host-migration/entities/migration-destinations/GET/v1` endpoint accepts these parameters to specify the hosts to query.

Parameter	In	Type	Description
`device_ids` required	body	array [string]	Specify an array of device IDs for the hosts to get the destination CID for. For more info about obtaining device IDs, see List host IDs.

Example request

```
curl -X POST 'https://api.crowdstrike.com/host-migration/entities/migration-destinations/GET/v1' \
  -H 'Accept: application/json' \
```

```
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"device_ids":['ca857xxxxxx72878', '26fa5xxxxxxe4c079fd9ff', '9dfbbb8xxxxxxc59a6fdca2']}'
```

Example response

```
{
 "meta": {
  "query_time": 0.195013802,
  "trace_id": "8b5a1c61xxxxxx386e03"
 },
 "resources": [
  {
   "cid": "d671caaf47xxxxxxe4a677",
   "name": "Child CID 3"
  },
  {
   "cid": "e89a8dxxxxxx64ef1b74",
   "name": "Parent CID"
  }
 ]
}
```

Create a migration job

Hosts are migrated using host migration jobs. You can create multiple migration jobs. Each migration job includes one or more hosts migrating to the same destination CID. Migration jobs are managed in the migration queue.

Successful requests return an HTTP 201 code and array of the migration ID, the number of hosts in the migration, and the number of hosts with a migration error.

To create a migration job:

- `POST /host-migration/entities/migrations/v1`

Parameters

The `/host-migration/entities/migrations/v1` endpoint accepts these parameters to create a migration job:

Parameter	In	Type	Description
`name` required	body	string	Specify a name for the migration job. Lowercase and uppercase letters, numbers, spaces, and the special characters - _ : ; . ! are allowed.
`target_cid` required	body	array[string]	Specify the ID of the destination CID. There can only be one destination CID for all hosts in the migration job. See Get valid destination CIDs.
`device_ids` required	body	string	Specify an array of IDs for the hosts to include in the migration job. For more info about obtaining device IDs, see List host IDs. A maximum of 1,000 hosts are allowed per migration job. Hosts must be Windows, Mac, or Linux and must have Falcon sensor version 7.16 or later.

The migration job is created but not yet started. To manage an unstarted migration job, see these topics:

- Manage static host group assignments
- Remove hosts from an unstarted migration job
- Delete an unstarted migration job
- Start a migration job

Example request

```
curl -X POST 'https://api.crowdstrike.com/host-migration/entities/migrations/v1' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"device_ids":['ca85717533xxxxxx5872878', '26fa52xxxxxxb9ab79fd9ff', '9dfbbb8xxxxxx586fdca2'],"name":"New Migration
Job","target_cid":"d671caaf47xxxxxxbe4a677"}'
```

Example response

```
{
 "meta": {
  "query_time": 0.398092564,
  "powered_by": "hostmigration",
  "trace_id": "65708be8xxxxxxcdbec3e5"
 },
```

```
 "resources": [
  {
   "migration_id": "697fee3xxxxxx592dae",
   "hosts_queued": 3,
   "hosts_errored": 0
  }
 ],
 "errors": null
}
```


Manage static host group assignments

Static host groups for the destination CID can be assigned to specific hosts in a migration job before it's started. After the migration is completed successfully, the hosts are protected by policies enabled for the assigned static host groups.
Important: Migrated hosts are automatically included in qualifying dynamic host groups in the destination CID, regardless of whether they are manually assigned to static host groups.

You can only manage static host group assignments for migration jobs that have been created but not started.

- To add host groups to the specified hosts: `/host-migration/entities/host-migrations-actions/v1?action_name=add_host_groups&id=<migration_job_id>`
- To remove host groups from the specified hosts: `/host-migration/entities/host-migrations-actions/v1?action_name=remove_host_groups&id=<migration_job_id>`
  Note: Use `POST /host-migration/entities/host-migrations/GET/v1` to view current static host group assignments for one or more hosts. See Get host migration event details.

Parameters

The `/host-migration/entities/host-migrations-actions/v1` endpoint accepts these parameters to specify host groups to add or remove, as well as the hosts to apply the assignment changes to.

Note: This endpoint requires both the `id` parameter for migration job ID and the `ids` parameter for host migration IDs.

Parameter	In	Type	Description
`id` required	query	string	Specify the Migration job ID.
`action_name` required	query	string	Specify the host migration action to perform. These are the possible values for managing static host group assignments: `add_host_groups`: Assign host groups to the specified hosts. `remove_host_groups`: Remove host groups currently assigned to the specified hosts. You can only use this action if all of the hosts you include using either the ids or filter parameter are currently assigned the static host groups you want to remove.
`action_parameters` required	Body	string	You must include an `action_parameters` array in the body of the request to specify one or more host group IDs: `{"name":"host_group","value":"<host_group_ID>"}` For example: `{"name":"host_group","value":"8e13a190xxxxxxaaff1b11dbf"}` For more info about finding host group IDs, see Finding host groups.
`ids` required	body	array[string]	Specify the host migration IDs of the hosts that you want to update static host group assignments for. To view host migration IDs for a migration job, use `GET /host-migration/queries/host-migrations/v1`. For more info, see Get host migration IDs.

Example request

```
curl -X POST \
  'https://api.crowdstrike.com/host-migration/entities/host-migrations-actions/v1?id=a70e9814xxxxxx6c11109fb9&action_name=add_host_groups' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"ids":['026c61bxxxxxxbeba92', '8ea0887xxxxxxa3ee6b', '9cbb63xxxxxxb697c'],"action_parameters":[{"name":"host_group","value":"8e13a190xxxxxxaaff1b11dbf"}]}'
```

Example response


```
{
 "meta": {
  "query_time": 0.268429346,
  "powered_by": "hostmigration",
  "trace_id": "15a84763xxxxxx40dc5"
 },
 "resources": [
  "8ea0887xxxxxxa3ee6b",
  "026c61bxxxxxxbeba92",
  "9cbb63xxxxxxb697c"
```

```
 ]
}
```

Remove hosts from an unstarted migration job

You can remove hosts from a migration job that has been created but not started.

- `POST /host-migration/entities/host-migrations-actions/v1?action_name=remove_hosts&id=<migration_job_id>`

Parameters

The `/host-migration/entities/host-migrations-actions/v1` endpoint accepts these parameters to specify hosts to remove from the migration job.

Parameter	In	Type	Description
`id` required	query	string	Specify the Migration job ID.
`action_name` required	query	string	Specify the `action_name` value of `remove_hosts`.
`ids` required	body	array[string]	Specify an array of host migration IDs to apply the static group assignment change. To view host migration IDs for a migration job, use `GET /host-migration/queries/host-migrations/v1`. For more info, see Get host migration IDs.

Example request

```
curl -X POST \
  'https://api.crowdstrike.com/host-migration/entities/host-migrations-actions/v1?id=697fee3xxxxxx8599592dae&action_name=remove_hosts' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"ids":['6848600xxxxxxc33d3e']}'
```

Example response

```
{
 "meta": {
  "query_time": 0.100255176,
  "powered_by": "hostmigration",
  "trace_id": "1696ba7dcxxxxxx47ca92edc9f"
 },
 "resources": [
  "6848600xxxxxc33d3e"
 ]
}
```

Delete an unstarted migration job

You can delete one or more migration jobs that have been created but not started.

- `POST /host-migration/entities/migrations-actions/v1?action_name=delete_migration`

Note: For more info about canceling a migration job that has started, see Cancel a running migration.

Parameters

The `/host-migration/entities/migrations-actions/v1` endpoint accepts these parameters to specify migration jobs to delete.

Parameter	In	Type	Description
`action_name` required	query	string	Specify the `action_name` value of `delete_migration`
`ids` required	body	array[string]	Specify an array of migration job IDs to delete. To view migration job IDs, use `GET /host-migration/queries/migrations/v1`. For more info, see Get a list of migration jobs.

Example request

```
curl -X POST \
  'https://api.crowdstrike.com/host-migration/entities/migrations-actions/v1?action_name=delete_migration' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"ids":["697fee3xxxxxx599592dae"]}'
```

Example response

```
{
 "meta": {
  "query_time": 0.049257064,
  "powered_by": "hostmigration",
  "trace_id": "ad0231cc46xxxxxx0d2e200b2"
 },
 "resources": [
  "697fee3xxxxxx599592dae"
 ]
}
```

Start a migration job

Start a migration job:

- `POST /host-migration/entities/migrations-actions/v1?action_name=start_migration`

Parameters

The `/host-migration/entities/migrations-actions/v1` endpoint accepts these parameters to specify migration jobs to start.

Parameter	In	Type	Description
`action_name` required	query	string	Specify the `action_name` value of `start_migration`
`ids` required	body	array[string]	Specify an array of migration job IDs to start. To view migration job IDs, use `GET /host-migration/queries/migrations/v1`. For more info, see Get a list of migration jobs.

Example request

```
curl -X POST \
  'https://api.crowdstrike.com/host-migration/entities/migrations-actions/v1?action_name=start_migration' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"ids":["a70e981xxxxxx9-426c11109fb9"]}'
```

Example response

```
{
 "meta": {
  "query_time": 0.201865451,
  "powered_by": "hostmigration",
  "trace_id": "8748e11d20axxxxxx7504df48b"
 },
 "resources": [
  "a70e981xxxxxx9-426c11109fb9"
 ]
}
```

Managing a migration job

Manage a migration job that has started. You can view information for hosts in the migration job, such as ID and migration event details. You can also rename or cancel a running migration.

- Get host migration event details
- Get host migration IDs
- Rename a migration job
- Cancel a running migration

Get host migration event details

Get migration event details for hosts in one or more migration jobs. Events include actions taken on the host, such as assigned or removed static host groups or when the migration status value was updated. Each event includes a timestamp.

- `POST /host-migration/entities/host-migrations/GET/v1`

  For more info about host migration status values, see Host migration status.

  For more info about troubleshooting hosts with a migration status of `failed`, see Troubleshooting host migrations.

Parameters

The `/host-migration/entities/host-migrations/GET/v1` endpoint accepts this parameter to specify which migration jobs to get event details for:

Parameter	In	Type	Description
`ids` required	body	array, string	Specify an array of host migration IDs to query. To view host migration IDs for a migration job, use `GET /host-migration/queries/host-migrations/v1`. For more info, see Get host migration IDs.

Example request

```
curl -X POST \
  'https://api.crowdstrike.com/host-migration/entities/host-migrations/GET/v1' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"ids":["9cbb6xxxxxx84b-26ca5eeb697c"]}'
```

Example response


```
{
 "meta": {
  "query_time": 0.145795198,
  "powered_by": "hostmigration",
  "trace_id": "70bc1305c8xxxxxxd0ea34ac9b6"
 },
 "resources": [
  {
   "host_migration_id": "9cbb6xxxxxx84b-26ca5eeb697c",
   "migration_id": "a70e981xxxxxx11109fb9",
   "source_cid": "051fbe94xxxxxx136e20f",
   "source_device_id": "1820db43xxxxxxc4b7dcce65",
   "target_cid": "6ad3bdcxxxxxx83cf518fc",
   "target_device_id": null,
   "hostname": "Migration test host",
   "platform": "Mac",
   "hostgroups": [
    "45fb416c4xxxxxa76a5f720"
   ],
   "status": "queued",
   "status_details": "",
   "events": [
    {
     "action": "added",
     "user": "user@example.com",
     "time": "2024-06-24T20:12:39.821780336Z"
    },
    {
     "action": "assigned_static_host_groups",
     "user": "user@example.com",
     "ids": [
      "8e13a190axxxxxxaaff1b11dbf",
      "45fb416c4xxxxxa76a5f720"
     ],
     "time": "2024-06-24T20:13:04.822062977Z"
    },
    {
     "action": "removed_static_host_groups",
     "user": "user@example.com",
     "ids": [
      "8e13a190axxxxxxaaff1b11dbf"
     ],
     "time": "2024-06-24T20:13:53.692160434Z"
    }
   ],
   "created_time": "2024-06-24T20:12:39.811765Z",
   "updated_time": "2024-06-24T20:13:53.688891Z"
  },
 ],
 "errors": null
}
```

Get host migration IDs

Get a list of host migration IDs for one or more migration jobs. These host migration IDs are ephemeral IDs assigned to hosts only for the purposes of the migration job and are not the same as the host ID.

- `GET /host-migration/queries/host-migrations/v1?id=<migration_job_ID>`

Parameters

The `/host-migration/queries/host-migrations/v1` endpoint accepts these parameters to specify the hosts to query:

Parameter	In	Type	Description
`id` required	query	string	Specify the migration job ID to query. To view migration job IDs, use `GET /host-migration/queries/migrations/v1`. For more info, see Get a list of migration jobs.
`offset` optional	query	integer	Offset the records in the response. For example, an offset value of **`50`** specifies that the first 50 records aren't included in the response.
`limit` optional	query	integer	Limit the maximum number of records returned. The acceptable range for this value is between **`1`** and **`10,000`**.

`sort`
optional
	query	string	Specify a sort order for the response. These sort values are available:
			`hostname|asc`
			`hostname|desc`
			`target_cid|asc`
			`target_cid|desc`
			`migration_id|asc`
			`migration_id|desc`
			`id|asc`
			`id|desc`
			`static_host_groups|asc`
			`static_host_groups|desc`
			`hostgroups|asc`
			`hostgroups|desc`
			`status|asc`
			`status|desc`
			`source_cid|asc`
			`source_cid|desc`
			`created_time|asc`
			`created_time|desc`
			`host_migration_id|asc`
			`host_migration_id|desc`
			`groups|asc`
			`groups|desc`

`filter`
optional
	query	expression	Specify an FQL filter. Hosts that meet this filter are included. These fields are available:
			`groups`
			`hostgroups`
			`static_host_groups`
			`hostname`
			`status`
			`target_cid`
			`source_cid`
			`migration_id`
			`id`

			host_migration_id created_time

Example request

```
curl -X POST \
  'https://api.crowdstrike.com/host-migration/queries/host-migrations/v1?id=a70e9814-
d31xxxxxx09fb9&offset=0&limit=20&filter=host_migration_id%3A%5B%27026c61b1xxxxxx2854dbeba92%27%2C%20%278ea0887xxxxxxad46a3ee6b%27%2C%20%279cbb63d7-
add0xxxxxxeeb697c%27%5D' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json'
```

Example response

```
{
 "meta": {
  "query_time": 0.17307596,
  "pagination": {
   "offset": 0,
   "limit": 20,
   "total": 3
  },
  "powered_by": "hostmigration",
  "trace_id": "d1f4f7b81adxxxxxxbfd77d7a"
 },
 "resources": [
  "026c61b1xxxxxx2854dbeba92",
  "8ea0887xxxxxxad46a3ee6b",
  "9cbb63d7-add0xxxxxxeeb697c"
 ]
}
```

Rename a migration job

Rename a migration job:

- `POST /host-migration/entities/migrations-actions/v1?action_name=rename_migration`

Parameters

The `/host-migration/entities/migrations-actions/v1` endpoint accepts these parameters to specify migration jobs to rename and the value to update the job name to.

Parameter	In	Type	Description
`action_name` required	query	string	Specify the `action_name` value of `rename_migration`
`action_parameters` required	Body	array[string]	You must include an `action_parameters` array in the body of the request to specify a new migration name value. Lowercase and uppercase letters, numbers, spaces, and the special characters - _ : ; . ! are allowed. `{"name":"migration_name","value":"<new_migration_name>"}` For example: `{"name":"migration_name","value":"TestRename"}` For more info about finding host group names and IDs, see Finding host groups.
`ids` required	body	array[string]	Specify an array with the migration job ID of the migration job to rename. You can only specify one migration job ID. To view migration job IDs, use `GET /host-migration/queries/migrations/v1`. For more info, see Get a list of migration jobs.

Example request

```
curl -X POST \
  'https://api.crowdstrike.com/host-migration/entities/migrations-actions/v1?action_name=rename_migration' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"action_parameters":[{"name":"migration_name","value":"TestRename"}],"ids":['a70e981xxxxxx-426c11109fb9']}'
```

Example response

```
{
 "meta": {
  "query_time": 0.175950814,
  "powered_by": "hostmigration",
  "trace_id": "33187a26ffdxxxxxxbaf808"
 },
 "resources": [
  "a70e981xxxxxx-426c11109fb9"
 ]
}
```

Cancel a running migration

You can cancel a migration job that has started and has a status of **Active**. This action cancels the migration only for hosts that haven't finished migrating. If hosts in the job have finished migrating, their status is **Completed** and their migration can't be canceled.

- `POST /host-migration/entities/migrations-actions/v1?action_name=cancel_migration`

Parameters

The `/host-migration/entities/migrations-actions/v1` endpoint accepts these parameters to specify migration jobs to cancel.

Parameter	In	Type	Description
`action_name` required	query	string	Specify the `action_name` value of `cancel_migration`
`ids` required	body	array[string]	Specify an array of migration job IDs to cancel. To view migration job IDs, use `GET /host-migration/queries/migrations/v1`. For more info, see Get a list of migration jobs.

Example request

```
curl -X POST \
  'https://api.crowdstrike.com/host-migration/entities/migrations-actions/v1?action_name=cancel_migration' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json' \
  -d '{"ids":["a70e9814-d31axxxxxx109fb9"]}'
```

Example response

```
{
 "meta": {
  "query_time": 0.230548997,
  "powered_by": "hostmigration",
  "trace_id": "83fc1e6f018xxxxxx94cdc04"
 },
 "resources": [
  "a70e9814-d31axxxxxx109fb9"
 ]
}
```

Managing the migration queue

You can view the progress and status of current host migration jobs and you can view a history of completed, failed, or partially failed migration jobs for up to 45 days.

- Get a list of migration jobs
- Get migration job details

Get a list of migration jobs

Get a list of all migration jobs in the migration queue:

- `GET /host-migration/queries/migrations/v1`

Parameters

The `/host-migration/queries/migrations/v1` endpoint accepts these parameters to query migration jobs:

Parameter	In	Type	Description
`offset`	query	integer	Offset the records in the response by this value.

optional			For example, an offset value of `50` specifies that the first 50 records aren't included in the response.
`limit` optional	query	integer	Limit the maximum number of records returned. The acceptable range for this value is between `1` and `10,000`.

`sort`
optional
	query	string	Specify a sort order for the response. These sort values are available:
			`created_time|asc`
			`created_time|desc`
			`name|asc`
			`name|desc`
			`id|asc`
			`id|desc`
			`migration_id|asc`
			`migration_id|desc`
			`target_cid|asc`
			`target_cid|desc`
			`status|asc`
			`status|desc`
			`migration_status|asc`
			`migration_status|desc`
			`created_by|asc`
			`created_by|desc`

`filter`
Optional
	query	expression	Specify an FQL filter. Migration jobs that meet this filter are returned. These fields are available:
			`created_by`
			`created_time`
			`name`
			`id`
			`migration_id`
			`target_cid`
			`status`
			`migration_status`

Example request

```
curl -X POST \
  'https://api.crowdstrike.com/host-migration/queries/migrations/v1' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json'
```

Example response


```
{
 "meta": {
  "query_time": 0.054295122,
  "pagination": {
   "offset": 0,
   "limit": 50,
   "total": 5
  },
  "powered_by": "hostmigration",
  "trace_id": "4fb7197e1ab5xxxxxx89ded523a"
 },
 "resources": [
  "8c6c09e9-4xxxxxxc465",
  "137f09ec-18xxxxxx04807c980",
  "41a5fxxxxxxd-b1b58fac44ad",
  "2fbda5xxxxxx0f3-d8b0a22b3c72",
  "bd0c90xxxxxxe587b321"
```

```
 ]
}
```

Get migration job details

Get migration job details for one or more migration jobs in the migration queue, including migration status, target CID, number of hosts in the job:

- `GET /host-migration/entities/migrations/v1?ids=<migration_job_id>`

  For more info about host migration job status values, see Migration job status.

  For more info about troubleshooting migration jobs with a status of `failed` or `partially failed`, see Troubleshooting host migrations.

Parameters

The `/host-migration/entities/migrations/v1` endpoint accepts this parameter to specify which migration jobs get details for:

Parameter	In	Type	Description
`ids` required	query	array[string]	Specify one or more migration job IDs to get details for. To view migration job IDs, use `GET /host-migration/queries/migrations/v1`. For more info, see Get a list of migration jobs.

Example request

```
curl -X POST \
  'https://api.crowdstrike.com/host-migration/entities/migrations/v1?ids=8c6c09e9-44xxxxx-a9fe30adc465' \
  -H 'Accept: application/json' \
  -H 'Authorization: Bearer <bearer_token>' \
  -H 'Content-Type: application/json'
```

Example response

```
{
 "meta": {
  "query_time": 0.050059464,
  "trace_id": "63a4fb2a5fxxxxxx0680fbab1b"
 },
 "resources": [
  {
   "migration_id": "8c6c09e9-44xxxxx-a9fe30adc465",
   "name": "Migration job test 1",
   "target_cid": "8fb102c70xxxxxx0c7d44a1f",
   "migration_status": "active",
   "total_hosts": 3,
   "created_by": "user@example.com",
   "updated_by": "user@example.com",
   "canceled_by": "",
   "started_time": "2024-06-17T21:37:20.998996Z",
   "completed_time": null,
   "created_time": "2024-06-17T21:37:20.626274Z",
   "updated_time": "2024-06-17T21:37:20.998996Z"
  }
 ]
}
```

Endpoint Security APIs

Automate incident monitoring, enforce device and firewall control, perform Real Time Response actions, assess zero trust posture, and manage security policies.

Detection and Prevention Policy APIs

Configure and manage policies that define triggers for detections and preventions on your hosts.

About CrowdStrike APIs

CrowdStrike provides use cases and example requests and responses for interacting with a specific set of our OAuth2-based APIs. For general info about CrowdStrike APIs, see CrowdStrike OAuth2-Based APIs, which covers these topics:

- Details on getting started, such as authentication and API scopes
- Domains used in base URLs by cloud
- Links to our Swagger API specification by cloud

Incident and Alert Monitoring APIs

Manage security incidents and alerts across your environment.

About CrowdStrike APIs

CrowdStrike provides use cases and example requests and responses for interacting with a specific set of our OAuth2-based APIs. For general info about CrowdStrike APIs, see CrowdStrike OAuth2-Based APIs, which covers these topics:

- Details on getting started, such as authentication and API scopes
- Domains used in base URLs by cloud
- Links to our Swagger API specification by cloud

Manage incidents and behaviors

Incidents are made of detections and associated processes on the hosts in your environment, as well as the connections between them, including parent-child relationships and thread injections. In the API, each incident has one or more associated *behaviors*. Because attacks often consist of coordinated activity happening together on a single host, incidents help you see important and relevant information more quickly.

Use the CrowdStrike API to perform these common tasks related to incidents and their behaviors:

- Find incidents
- Modify incidents
- Find behaviors

Find incidents

Find and get info about incidents to learn more about activity in your environment.

Relevant API endpoints

- GET /incidents/queries/incidents/v1
- POST /incidents/entities/incidents/GET/v1

This API endpoint data returns are trimmed to 500 records. If you specify a limit in your request, the maximum value should be set to 500. This limit applies to the total API response size, regardless of your pagination sizes with the `limit` and `offset` parameters. If your response set would include more than 500 items, the CrowdStrike API returns an error code 400. To avoid this issue, use the `filter` parameter to reduce the total number of items in the API response.

Steps

1. Get an incident's ID using /incidents/queries/incidents/v1. Optionally, you can use an FQL query or sort parameter to filter and sort incidents.
2. Provide one or more incident IDs to /incidents/entities/incidents/GET/v1 to get info about those incidents. This API endpoint uses a POST request with a JSON payload to retrieve information.

Filtering options

Name	Description	Sample
host_ids	The device IDs of all the hosts on which the incident occurred.	9a07d39f8c9f430eb3e474d1a0c16ce9
lm_host_ids	If lateral movement has occurred, this field shows the remote device IDs of the hosts on which the lateral movement occurred.	c4e9e4643999495da6958ea9f21ee597
lm_hosts_capped	Indicates that the list of lateral movement hosts has been truncated. The limit is 15 hosts.	True
name	The name of the incident. Initially the name is assigned by CrowdScore, but it can be updated through the API.	Incident on DESKTOP-27LTE3R at 2019-12-20T19:56:16Z
description	The description of the incident. Initially the description is assigned by CrowdScore, but it can be updated through the API.	Objectives in this incident: Keep Access.\nTechniques: Masquerading.\nInvolved hosts and end users: DESKTOP-27LTE3R, DESKTOP-27LTE3R$.
users	The usernames of the accounts associated with the incident.	someuser
tags	Tags associated with the incident. CrowdScore will assign an initial set of tags, but tags can be added or removed through the API.	Objective/Keep Access
fine_score	The incident score. Divide the integer by 10 to match the displayed score for the incident.	56

Name	Description	Sample
start	The recorded time of the earliest behavior.	2017-01-31T22:36:11Z
end	The recorded time of the latest behavior.	2017-01-31T22:36:11Z
assigned_to_name	The name of the user the incident is assigned to.	
state	The incident state: “open” or “closed”	open
status	The incident status as a number: 20: New 25: Reopened 30: In Progress 40: Closed	20
modified_timestamp	The most recent time a user has updated the incident.	2021-02-04T05:57:04Z

Show CrowdScores

Return the calculated CrowdScores for your environment.

Relevant API endpoints

- GET /incidents/combined/crowdscores/v1

Filtering options

Name	Description	Sample
timestamp	The time at which the CrowdScore was calculated.	2017-01-31T22:36:11Z
score	The value of the CrowdScore	55

Modify incidents

Update the status or other aspects of one or more incidents. You can modify a maximum of 5,000 incidents in a request.

Relevant API endpoints

- POST /incidents/entities/incident-actions/v1

Steps

Make a request to `/incidents/entities/incident-actions/v1` with a payload similar to:

```
{
 "action_parameters": [
  {
   "name": "string",
   "value": "string"
  }
 ],
 "ids": [
  "string"
 ]
}
```

One or more action_parameters and ids can be supplied. Each action_parameter value will be applied to each incident whose id is listed in ids.

Action Parameters Name:

action_parameters	Description
`add_tag`	Adds the associated value as a new tag on all the incidents of the `ids` list.
`delete_tag`	Deletes tags matching the value from all the incidents in the `ids` list
`unassign`	Unassigns all users from all of the incidents in the `ids` list. This action does not require a `value` parameter. For example: `"action_parameters": [ { "name": "unassign" }]`
`update_name`	Updates the name to the parameter value of all the incidents in the `ids` list.
`update_assigned_to_v2`	Assigns the user matching the UUID in the parameter value to all of the incidents in the `ids` list. Tip: For information on getting the UUID of a user, see Find existing users.
`update_description`	Updates the description to the parameter value of all the incidents listed in the `ids` list.
`update_status`	Updates the status to the parameter value of all the incidents in the `ids` list. Valid status values are `20`, `25`, `30`, or `40`: • `20`: New • `25`: Reopened • `30`: In Progress • `40`: Closed

Example request

Assign a user to an incident by their UUID, and update the status to `30` ("In Progress"):

```
curl --request POST 'https://api.crowdstrike.com/incidents/entities/incident-actions/v1' \
--header 'Authorization: bearer eyJhbGci...xYg1NNI' \
--header 'Content-Type: application/json' \
--data-raw '{
    "action_parameters": [
        {
            "name": "update_assigned_to_v2",
            "value": "82402aed-xxxx-xxxx-xxxx-83510507b7d8"
        },
        {
            "name": "update_status",
            "value": "30"
        }
    ],
    "ids": [
        "inc:6926xxxxx42af:4638xxxxx9503"
    ]
}'
```

Example response

Successful requests return an HTTP 200 OK message, and an empty errors array in the JSON response.

```
{
    "meta": {
        "query_time": 0.480404495,
        "powered_by": "incident-api",
        "trace_id": "12fe5621-0c10-4b07-9277-5fc045a84cb0"
    },
    "resources": [],
    "errors": []
}
```

Updating detection statuses to match incidents

Update the status of the detections involved in incidents using the endpoint used to modify incidents. You can modify a maximum of 5,000 incidents in a request.

Note: These status updates can be applied to detections available in Endpoint security > Monitor > Endpoint detections. Contextual detections, which are significant specifically within the context of the incident, are not shown in Endpoint security > Monitor > Endpoint detections and don't have statuses to update.

Relevant API endpoints

- POST /incidents/entities/incident-actions/v1?update_detects=value&overwrite_detects=value

Steps

Make a request to: `/incidents/entities/incident-actions/v1?update_detects=value&overwrite_detects=value` with a payload similar to:

```
{
 "action_parameters": [
  {
   "name": "string",
   "value": "string"
  }
 ],
 "ids": [
  "string"
 ]
}
```

The update_status action parameter and ids can be supplied. The update_status value will be applied to each incident whose id is listed in ids. The response specifies which detections were and were not updated.

update_detects	overwrite_detects	What happens to involved detections
false	true or false	No changes to any involved detections
true	true	If the request includes an action value in the `update_status` parameter: those action values will be applied to all of the involved detections' `status` parameters.
true	false	If the request includes an action value in the `update_status` parameter: those action values will be applied to the involved detections' `status` parameters that have a value of **new**.

Find behaviors

Find and get info about behaviors to learn more about activity in your environment.

Relevant API endpoints

- GET /incidents/queries/behaviors/v1
- POST /incidents/entities/behaviors/GET/v1

This API endpoint returns data only if the response set includes 500 or fewer items. This limit applies to the total API response size, regardless of your pagination sizes with the `limit` and `offset` parameters. If your response set would include more than 500 items, the CrowdStrike API returns an error code 400. To avoid this issue, use the `filter` parameter to reduce the total number of items in the API response.

Steps

1. Get a behavior's ID using /behaviors/queries/behaviors/v1. Optionally, you can use an FQL query to filter and sort detections.
2. Provide one or more incident IDs to /behaviors/queries/behaviors/v1 to get info about those incidents. This API endpoint uses a POST request with a JSON payload to retrieve information.

Filtering options

Name	Description	Sample
aid	The agent id that reported the behavior.	62e9c3d557a5479258d9ac63a2efb118
incident_id	The id of the incident this behavior is associated with.	inc:62e9c3d557a5479258d9ac63a2efb118:131b500232ee4d9ca10c70d81eceb5dc
pattern_id	The pattern ID of the behavior.	5
template_instance_id	The template instance ID of the behavior.	0
timestamp	The recorded time the behavior was detected.	2019-09-16T13:53:34Z

Manage alerts

An alert indicates a potential security issue exists that requires you to investigate, triage, or take action.

These are some of the sources that can generate alerts:

- Falcon Data Protection
- Falcon Endpoint Protection
- Falcon for Mobile
- Falcon Identity Protection
- Falcon Insight XDR
- Falcon Next-Gen SIEM
- Third-party data

You can perform these actions on alerts:

- View full details
- Change the status
- Assign or unassign a user
- Add tags and comments

Note: Use the `/alerts` endpoints described here.

Required API client scope

To access the alerts API, your API client must be provisioned with the following scope and permissions:

- Alerts: Read and Write

For more info, see API clients.

Finding alert IDs

The `/alerts/queries/alerts` endpoint returns a default of 100 IDs, with a maximum of 10,000. You can use the offset parameter to page through results. You can also use the limit parameter or Falcon Query Language (FQL) queries to reduce the number of IDs returned. If your response set includes more than 10,000 items, you can use the `/combined/` endpoint to search for and retrieve alert details in 1 step and get unlimited results. For more info, see Bulk alert retrieval.

1. Get the list of IDs with GET /alerts/queries/alerts/v2.
2. Optional. Specify a filter query parameter to limit IDs to a particular product:
    - Return only Automated Lead Context alert IDs: `filter=product:'automated-lead-context'`
    - Return only Automated Lead alert IDs: `filter=product:'automated-lead'`
    - Return only Cloud Workload Protection alert IDs: `filter=product:'cwpp'`
    - Return only Data Protection alert IDs: `filter=product:'data-protection'`
    - Return only Endpoint Protection alert IDs: `filter=product:'epp'`
    - Return only Falcon for Mobile alert IDs: `filter=product:'mobile'`
    - Return only Identity Protection alert IDs: `filter=product:'idp'`
    - Return only Insight XDR alert IDs: `filter=product:'xdr'`
    - Return only Next-Gen SIEM alert IDs: `filter=product:'ngsiem'`
    - Return only third-party data alert IDs: `filter=product:'thirdparty'`
3. Optional. Specify the `include_hidden` query parameter to include or exclude hidden alerts. The default value for `include_hidden` is `true`.
4. If needed, retrieve the next set of items using the unique offset provided by the response: `GET /alerts/queries/alerts/v2?offset={offset}`

Note: This endpoint replaces GET /alerts/queries/alerts/v1, which is being deprecated. Although this endpoint can be used in the following examples during the deprecation period, we encourage you to migrate to the updated endpoint as soon as possible so there is time for testing and to avoid any service disruption.

Example: Finding Falcon Identity Protection alert IDs

Example request: Falcon Identity Protection

List the IDs of the first 5 Falcon Identity Protection alerts in your environment.

```
curl -X GET "https://api.crowdstrike.com/alerts/queries/alerts/v2?filter=product:'idp'&limit=5" \
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response: Falcon Identity Protection


```
{
 "meta": {
  "query_time": 0.044395707,
  "pagination": {
   "offset": 0,
   "limit": 5,
   "total": 10000
 },
 "writes": {
  "resources_affected": 0
 },
 "powered_by": "detectsapi",
 "trace_id": "f755297a-e287-4012-b5e3-ff88691e95e9"
 },
 "resources": [
  "28a1xxxxxxxx3914:ind:a618xxxxxxxx4d85:1328xxxxxxxx1933-117-3675xxxxxxxx5616",
  "28a1xxxxxxxx3914:ind:8647xxxxxxxxbe64:1328xxxxxxxx9683-5702-7386xxxxxxxx6359",
  "28a1xxxxxxxx3914:ind:8647xxxxxxxxbe64:1328xxxxxxxx2431-5702-6181xxxxxxxx8615",
  "28a1xxxxxxxx3914:ind:8647xxxxxxxxbe64:1328xxxxxxxx0612-5702-3468xxxxxxxx7877",
  "28a1xxxxxxxx3914:ind:a618xxxxxxxx4d85:1328xxxxxxxx1933-117-1930xxxxxxxx9544"
 ],
 "errors": []
}
```

Example: Finding third-party data alert IDs

Example request: Third-party data

List the IDs of the first third-party data alert in your environment. For more information, see Data Connectors.

```
curl -X GET "https://api.crowdstrike.com/alerts/queries/alerts/v2?filter=product:'thirdparty'&limit=1"
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json'
```

Example response: Third party data


```
{
  "meta": {
    "query_time": 0.032735683,
    "pagination": {
      "offset": 0,
      "limit": 1,
      "total": 7567
    },
    "writes": {
      "resources_affected": 0
    },
    "powered_by": "detectsapi",
    "trace_id": "7c8xxxxxxxxx438"
  },
  "resources": [
    "cb28a1bf5xxxxxxxxx698253914:thirdparty:cb28a1bf5axxxxxxxxxx698253914:5efcd0feb3xxxxxxxxxxab190ab39a"
  ]
}
```


Example: Finding OverWatch alert IDs

Example request: Overwatch detections

List the IDs of the first 5 OverWatch alerts in your environment.

```
curl -X GET "https://api.crowdstrike.com/alerts/queries/alerts/v2?filter=tactic_id:'%27CSTA0006%27&limit=5" \
-H 'Authorization: bearer eyJhbGci...xYg1NNI' \
-H 'Accept: application/json'
```

If you want to request OverWatch hunting leads, you must do the following instead.

- Set `product=overwatch`, `type=lead`
- Specify the `include_hidden` query parameter to include hidden alerts. The default value for `include_hidden` is `true`. For more info about hunting leads, see Hunting leads.

Example response: Overwatch


```
{
    "meta": {
        "query_time": 0.044395707,
        "pagination": {
            "offset": 0,
            "limit": 5,
            "total": 10000
        },
        "writes": {
            "resources_affected": 0
        },
        "powered_by": "detectsapi",
        "trace_id": "f755297a-e287-4012-b5e3-ff88691e95e9"
    },
    "resources": [
        "28a1xxxxxxxx3914:lead:a618xxxxxxxx4d85:1328xxxxxxxx1933-117-3675xxxxxxxx5616",
        "28a1xxxxxxxx3914:lead:8647xxxxxxxxbe64:1328xxxxxxxx9683-5702-7386xxxxxxxx6359",
        "28a1xxxxxxxx3914:lead:8647xxxxxxxxbe64:1328xxxxxxxx2431-5702-6181xxxxxxxx8615",
        "28a1xxxxxxxx3914:lead:8647xxxxxxxxbe64:1328xxxxxxxx0612-5702-3468xxxxxxxx7877",
        "28a1xxxxxxxx3914:lead:a618xxxxxxxx4d85:1328xxxxxxxx1933-117-1930xxxxxxxx9544"
    ],
    "errors": []
}
```


Retrieving alert details

Get detailed information about an alert.

- Provide the alert `composite_id` in the body of POST /alerts/entities/alerts/v2.

  Optionally, specify the `include_hidden` query parameter to include or exclude hidden alerts. The default value for `include_hidden` is `'true'`

Note: This endpoint replaces POST /alerts/entities/alerts/v1, which is deprecated.
Note: This endpoint does not support legacy detection IDs, which start with the prefix `ldt`.

Example: Retrieving alert details

Example request

```
curl -X POST "https://api.crowdstrike.com/alerts/entities/alerts/v2" \
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json' \
 -H 'Content-Type: application/json' \
 -d '{
  "composite_ids": [
   "28a1xxxxxxxx3914:ind:a618xxxxxxxx4d85:1328xxxxxxxx1933-117-1930xxxxxxxx9544"
  ]
 }'
```

Example response

Note: This response is truncated. Depending on the type of detection or event, there could be a large amount of information provided in the response.


```
{
 "meta": {
  "query_time": 0.004553092,
  "writes": {
   "resources_affected": 0
  },
  "powered_by": "detectsapi",
  "trace_id": "e3a17704-d33e-4f70-a769-6a3ddc01844f"
 },
 "errors": [],
 "resources": [
  {
   "activity_id": "3D14C6B6-XXXX-460EC4FCD27D",
   "aggregate_id": "aggind:dca1XXXX1660:097877B9-C71F-42C7-A836-2944D119B6CB",
   "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV-WX",
   "comment": "previously Login with jsmith from to Suspicious unusual IP location from verified user's The associated user geolocates not confirmed a account for
they are traveling",
   "comments": [
    {
     "falcon_user_id": "email@example.com",
     "timestamp": "2025-07-24T11:47:29.239509031Z",
     "value": "Suspicious login for jsmith. IP geolocates to a location not previously associated with this user's account."
    },
    {
     "falcon_user_id": "email@example.com",
     "timestamp": "2025-07-24T12:08:42.021585471Z",
     "value": "Login from unusual location verified. The user confirmed they're currently traveling."
    }
   ],
   "composite_id": "28a1xxxxxxxx3914:ind:a618xxxxxxxx4d85:1328xxxxxxxx1933-117-1930xxxxxxxx9544",
   "confidence": 30,
   "context_timestamp": "2025-07-24T10:32:00.000Z",
   "created_timestamp": "2025-07-24T11:34:56.887790892Z",
   "description": "User access from an unusual location",
   "display_name": "Unusual user geolocation",
   "end_time": "2025-07-24T10:32:00.000Z",
   "falcon_host_link": "https://falcon.crowdstrike.com/identity-protection/detections/dca1xxxx1660",
   "id": "ind:a618xxxxxxxx4d85:1328xxxxxxxx1933-117-1930xxxxxxxx9544",
   "location_country_code": "US",
   "mitre_attack": [
    {
     "pattern_id": 51125,
     "tactic_id": "TA0001",
     "technique_id": "T1036",
     "tactic": "Initial Access",
     "technique": "Valid Accounts"
    }
   ],
   "name": "AnomalousGeoLocationAccess",
   "objective": "Gain Access",
   "okta_application_id": "0oa1xxxxL5d7",
   "pattern_id": 51125,
   "product": "idp",
   "scenario": "machine_learning",
   "severity": 31,
   "show_in_ui": true,
   "source_account_name": "demo.user@example.com",
   "source_account_okta_id": "00u4xxxxf5d7",
   "source_endpoint_address_ip4": "192.0.2.100",
   "source_endpoint_ip_address": "192.0.2.100",
   "sso_application_identifier": "Okta Admin Console",
   "sso_application_uri": "0oa1xxxxL5d7",
   "start_time": "2025-07-24T10:32:00.000Z",
   "status": "new",
   "tactic": "Initial Access",
   "tactic_id": "TA0001",
   "technique": "Valid Accounts",
   "technique_id": "T1078",
   "timestamp": "2025-07-24T10:34:56.509Z",
   "type": "idp-session-source-user-endpoint-target-info",
   "updated_timestamp": "2025-07-24T12:08:42.021585471Z"
  }
 ]
}
```

Filtering options

Field	Description	Sample Value
agent_id	Agent ID associated with the given alert	77d11725xxxxxxxxxxxxxxxxxxxxc48ca19
aggregate_id	A unique identifier which links multiple alerts	aggind:77d1172532c8xxxxxxxxxxxxxxxxxxxx49030016385
assigned_to_name	User name of the Falcon user account this alert is assigned to	Example User
assigned_to_uid	UserID of the Falcon user account this alert is assigned to	example.user@example.com
assigned_to_uuid	Unique ID of the Falcon user account this alert is assigned to	dc54xxxxxxxxxxxxxxx1658
cid	ID of customer	d61501xxxxxxxxxxxxxxxxxxxxa2da2158
comments.value	A single term in an alert comment. Matching is case sensitive. Partial match and wildcard search are not supported.	suspicious
composite_id	A global unique identifier that identifies an alert	d61501501a6a49e4b47459f9a2da2158:ind:77d1172532c8480fa0e61d676c48ca19:13353086628595915867-18079738568385718072
confidence	A 1-100 integer value denoting the confidence that the alert equates to malicious activity	80
crawled_timestamp	A timestamp reserved for internal use	2024-02-22T15:15:05.637684718Z
created_timestamp	A timestamp reserved for internal use	2024-02-22T14:16:04.973070837Z
data_domains	Domain to which this alert belongs to. Possible values: • Endpoint • Identity • Cloud • Email • Web • Network	["Endpoint"]
description	A system generated short description of the 'display_name' alert value.	Process accessed credential-containing NTDS.dit in a Volume Shadow Snapshot
display_name	A system generated description of the alert	NtdsFileAccessedViaVss
email_sent	Indicates whether an email was sent for this alert	TRUE
external	A field reserved for internal use	FALSE
mitre_attack.tactic	Description of the tactic as defined by the MITRE ATT&CK matrix	Credential Access
mitre_attack.tactic_id	Identifier of the tactic as defined by the MITRE ATT&CK matrix	TA0006
mitre_attack.technique	Description of the technique as defined by the MITRE ATT&CK matrix	OS Credential Dumping
mitre_attack.technique_id	Identifier of the technique as defined by the MITRE ATT&CK matrix.	T1003
name	Pattern name for the alert	NtdsFileAccessedViaVss
objective	The name of the objective associated with the behavior as defined by the MITRE ATT&CK matrix	Gain Access
pattern_id	A unique identifier reserved for internal use	67
platform	A value representing the Operating System	Windows
product	Specifies the domain of the alert. Possible domains:	epp

Field	Description	Sample Value
	• cwpp • data-protection • epp • idp • mobile • ngsiem • overwatch • thirdparty • xdr	
`scenario`	A unique identifier reserved for CrowdStrike's internal use	credential_theft
`seconds_to_resolved`	Time that it took to move an alert from new to closed.	0
`seconds_to_triaged`	Time that it took to move an alert from new to in_progress.	0
`severity`	A qualitative ranking of security risk in a scale from 1-100 with 100 being the most severe.	100
`show_in_ui`	Indicates if this alert should be shown in the UI	TRUE
`source_products`	Products associated with the source of this alert	["Falcon Insight"]
`source_vendors`	Vendors associated with the source of this alert	["CrowdStrike"]
`status`	Reflects the current status. Possible values: • new • in_progress • closed • reopened	in_progress
`tactic`	Description of the tactic as defined by the MITRE ATT&CK matrix Note: This field is deprecated. Use `mitre_attack.tactic` instead.	Credential Access
`tactic_id`	Identifier of the tactic as defined by the MITRE ATT&CK matrix Note: This field is deprecated. Use `mitre_attack.tactic_id` instead.	TA0006
`tags`	Contains a separated list of FalconGroupingTags and SensorGroupingTags	["fc/offering/falcon_complete" "fc/exclusion/pre-epp-migration" "fc/exclusion/nonlive"]
`technique`	Description of the technique as defined by the MITRE ATT&CK matrix Note: This field is deprecated. Use `mitre_attack.technique` instead.	OS Credential Dumping
`technique_id`	Identifier of the technique as defined by the MITRE ATT&CK matrix. Note: This field is deprecated. Use `mitre_attack.technique_id` instead.	T1003
`timestamp`	Timestamp of the alert	2024-02-22T14:15:03.112Z
`type`	Type of alert. Possible values: • ldt • ods • xdr • ofp • ssd • windows_legacy	ldt

Field	Description	Sample Value
`updated_timestamp`	A timestamp which indicates when the alert was last modified	2024-02-22T15:15:05.637481021Z

Bulk alert retrieval

The combined endpoint provides large-scale alert data retrieval, consolidating 2 operations into a single step and supporting responses with more than 10,000 results. Instead of offset pagination, it leverages cursor-based pagination to eliminate result restrictions, ensure sequential data flow, and optimize retrieval at any scale.

With this endpoint, you don't need to make separate requests to look up alert IDs and retrieve alert details. Everything is performed in a single operation, reducing API overhead and improving response times. You can send requests without parameters to get data for all alerts in your CID. By default, results are arranged in descending order by `created_timestamp`. For more targeted results, you can apply FQL filters and get alerts based on specific properties. You can also use a `sort` parameter to arrange the returned data by a different field or change the direction that the results are presented in. For more info, see Filtering options and Sorting results.

Note: Sorting by certain fields may impact the results. For more info, see Sorting results.

Cursor pagination

To support large dataset retrieval, the combined endpoint relies on cursor-based pagination. With this method, you get unlimited results that are divided across multiple pages and returned in a sequence instead of all at once.

Specifying page size

You can use the `limit` parameter to define the number of results to return on a page. The default page size is 100. You can set a custom page size from 1 to 1000 results.

Understanding pagination tokens

Cursor pagination makes use of a token to navigate through pages. The token serves as a reference point in the dataset for the last record retrieved, and it allows you to get the next set of results. When there are more matching results than the response `limit`, the `after` field in the `pagination` part of the response is populated with a token. You can call the API again with the `after` token value to get the next set of results.

Retrieving next pages

If your response contains an `after` token, make the same request and provide the token value as a body parameter to get the next set of results. This tells the API where your last response left off and the next set of results should begin.

Continue making follow-up requests to retrieve new pages of results until all alerts are returned and the `after` token is no longer present in the response.

Sorting results

Pagination is performed on live data and relies on a sort order to determine the next set of records. To ensure consistent results, keep these considerations in mind when setting a sort property:

- Data changes that occur during page requests (such as adding or updating alerts) can cause ordering inconsistencies that result in duplicate or missing records.
    - Whenever possible, sort on properties that do not change over time, such as `created_timestamp` or `composite_id`.
    - When data is sorted by `timestamp|asc`, each new page of results will have timestamp values greater than the current page.
- If an alert is modified during data retrieval and its `updated_timestamp` value changes, the alert's position in the dataset also changes. Depending on the direction of the sort order, this could cause the alert to be duplicated or skipped in the result set. For example:
    - When sorting by `updated_timestamp|desc`, ifthe new `updated_timestamp` value repositions the alert on a page of results that was already retrieved, the alert is missing from the result set.
- You can't modify sorting while data retrieval is in progress. If you need to change the sort order, a new query is required.

Pagination response example

The pagination part of the response contains attributes that are helpful in determining whether additional pages of records are available for retrieval or if you've reached the end of the dataset.

```
"pagination": {
    "total": 60970,
    "limit": 100,
    "after": "eyJ2ZXxxxxMDB9Cg=="
  }
```

Pagination response attributes

Attribute	Description
`total`	The total number of alerts that matched the query. This number might change during pagination if new alerts are created or old ones expire.
`limit`	The maximum number of results to return per page.

	Default: 100 Minimum: 1 Maximum: 1000
`after`	A token used to retrieve the next page of results. The `after` token is only present when additional results are available.

Endpoint

```
POST /alerts/combined/alerts/v1
```

Required API client scope

Alerts: Read

Parameters

Name	Required	In	Type	Description
`after`	`no`	body	string	A pagination token used to access the next page of results. The `after` token first appears in the response from your initial request when more results are available. Provide the `after` token value in your next request to retrieve the next page of results and a new token. Repeat the process until `after` is empty, indicating all results have been returned.
`filter`	`no`	body	string	The FQL filter expression used to limit the results. For available filters, see Filtering options.
`include_hidden`	`no`	query	boolean	When set to `true`, hidden alerts are included in the result set. To exclude hidden results, set to `false`. Default: `true`
`limit`	`no`	body	integer	The maximum number of items to return per page. Use this with the `after` parameter to manage pagination of results. Default: `100` Max: `1000`

`sort`	`no`	body	string	The property and direction to order the results. Data can be sorted in ascending (smallest to largest) or descending order (largest to smallest). The sort parameter is provided in the request body in the format `sort={property}|{asc/desc}`.
				These are some of the commonly used sort properties:
				`aggregate_id`
				`assigned_to_name`
				`assigned_to_uid`
				`assigned_to_uuid`
				`composite_id`
				`created_timestamp`
				`mitre_attack.tactic_id`
				`mitre_attack.tactic`
				`mitre_attack.technique_id`
				`mitre_attack.technique`
				`pattern_id`
				`product`
				`status`
				`tactic_id`
				`tactic`
				`technique`
				`technique_id`
				`timestamp`
				`updated_timestamp`
				Note: The `tactic_id`, `tactic`, `technique_id`, and `technique` properties are deprecated. Use these properties prefixed with `mitre_attack.` instead.

Example: Paginating over matched results

Retrieve alerts before July 25, 2025, using the `created_timestamp` filter. Order the results in ascending order by `created_timestamp` and limit each response to 50 alerts.

Example request: Get the first page of results

To retrieve the first page of alerts, pass the `filter` , `sort`, and `limit` parameters in the request body.

```
curl -X POST 'https://api.crowdstrike.com/alerts/combined/alerts/v1' \
  -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
  "filter": "created_timestamp:<'\''2025-07-25'\''",
  "sort": "created_timestamp.asc",
  "limit": 50
}'
```

Example response: Get the first page of results

The response contains the first page of results. Because the `total` number of matches exceeds the set `limit` of 50, the `after` token is populated and can be used to continue collecting the next set of results.

Note: This response is truncated. Depending on the type of alert, there could be a large amount of information provided in the response.


```
{
  "meta": {
    "query_time": 0.301021758,
    "pagination": {
      "total": 60970,
      "limit": 50,
      "after": "eyJ2ZXxxxxMDB9Cg=="
    },
    "powered_by": "detectsapi",
    "trace_id": "e4b26031-d116-45e9-a2c6-218468c76b87"
  },
  "errors": [],
  "resources": [
    {
      "agent_id": "a1baxxxxxxxxaa68e",
      "aggregate_id": "aggind:a1baxxxxxxxxaa68e:1882xxxxxxxxa5847",
      "alleged_filetype": "exe",
      "cid": "cb28xxxxxxxxa3914",
      "cmdline": "C:\\windows\\winipbin\\wlcnthr.exe",
      "comment": "File jsmith quarantined by Suspicious is until uploaded investigation file complete",
      "comments": [
       {
        "falcon_user_id": "email@example.com",
        "timestamp": "2025-07-24T18:55:42.021585471Z",
        "value": "File quarantined until investigation is complete."
       },
       {
        "falcon_user_id": "email@example.com",
        "timestamp": "2025-07-24T18:47:29.239509031Z",
        "value": "Suspicious file uploaded by jsmith."
    }
   ],
      "composite_id": "cb28xxxxxxxxa3914:ind:a1baxxxxxxxxa68e:5539xxxxxxxx4682-2021-1882xxxxxxxxx5848",
      "confidence": 70,
      "control_graph_id": "ctg:a1baxxxxxxxxaa68e:1882xxxxxxxxa5847",
      "created_timestamp": "2025-07-24T16:17:21.531611083Z",
      "description": "A process launched that meets the cloud-based behavioral machine learning model threshold low confidence threshold for malware. It might be
malware and/or part of an adversary's toolkit. Investigate the process tree and review the file.",
      "device": {
        "agent_version": "5.25.10701.0",
        "last_seen": "2025-07-24T15:15:58Z",
        "platform_name": "Windows",
      },
      "display_name": "Windows Post Exploitation Executable Payload",
      "falcon_host_link": "https://falcon.crowdstrike.com/activity-v2/detections/cb28xxxxxxxxa3914:ind:a1baxxxxxxxxa68e:5539xxxxxxxx4682-2021-1882xxxxxxxxx5848",
      "filename": "wlcnthr.exe",
      "filepath": "\\Device\\HarddiskVolume3\\Windows\\foobar\\wlcntdy.exe",
      "id": "ind:a1baxxxxxxxxa68e:5539xxxxxxxx4682-2021-1882xxxxxxxx5848",
      "ioc_source": "Post-exploitation Executable Payload",
      "ioc_type": "Compounded micro-behavior activity",
      "ioc_value": "01f4edxxxxxfaea0a",
      "md5": "cda4xxxxxbf70a",
      "mitre_attack": [
       {
        "pattern_id": 2021,
        "tactic_id": "CSTA0010",
        "technique_id": "T1204.002",
        "tactic": "AI Powered IOA",
        "technique": "Malicious File"
       }
      ],
      "name": "CloudDetectLow",
      "objective": "Falcon Detection Method",
      "parent_process_id": "23xxxx39",
      "pattern_id": 2021,
      "platform": "Windows",
      "process_end_time": "1737735358",
```

```
      "process_id": "553xxxx682",
      "process_start_time": "1737735358",
      "product": "epp",
      "scenario": "attacker_methodology",
      "severity": 30,
      "severity_name": "Low",
      "sha256": "01f4edxxxxxfaea0a",
      "show_in_ui": true,
      "status": "new",
      "tactic": "AI Powered IOA",
      "tactic_id": "CSTA0010",
      "technique": "Malicious File",
      "technique_id": "T1204.002",
      "timestamp": "2025-07-24T16:16:00.931Z",
      "tree_id": "1882xxxxxxxxa5847",
      "tree_root": "55xxxx82",
      "triggering_process_graph_id": "pid:a1baxxxxxxxxaa68e:553xxxx4682",
      "type": "ldt",
      "updated_timestamp": "2025-07-24T17:16:21.519191908Z"
    },
........

  ]
}
```

Example request: Retrieve the second page of results

To retrieve the second page of alerts, send the same request and include the `after` token from the previous response.

```
curl -X POST 'https://api.crowdstrike.com/alerts/combined/alerts/v1' \
  -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
  "filter": "created_timestamp:<'\''2025-07-25'\''",
  "sort": "created_timestamp.asc",
  "limit": 50,
  "after": "eyJ2ZXxxxxMDB9Cg=="
}'
```

Example response: Retrieve the second page of results

The response contains the second page of results and a new `after` token to get the next set of alerts.

Note: This response is truncated. Depending on the type of alert, there could be a large amount of information provided in the response.

```
{
  "meta": {
    "query_time": 0.293590541,
    "pagination": {
      "total": 60970,
      "limit": 50,
      "after": "eyJ2ZXxxxxMjAwfQo="
    },
    "powered_by": "detectsapi",
    "trace_id": "4751bded-65bc-4a86-bc1b-5e0720f97910"
  },
  "errors": [],
  "resources": [
    {
      "agent_id": "5f5cxxxxxxxxa65d1",
      "aggregate_id": "aggind:5f5cxxxxxxxxa65d1:1338xxxxxxxxa9273",
      "alleged_filetype": "exe",
      "child_process_ids": [
        "pid:5f5cxxxxxxxxa65d1:133822076450489978"
      ],
      "cid": "cb28xxxxxxxxa3914",
      "cmdline": "C:\\WINDOWS\\System32\\sdhost.exe -Embedding",
      "composite_id": "cb28xxxxxxxxa3914:ind:5f5cxxxxxxxxa65d1:1338xxxxxxxxa3425-10150-1506xxxxxxxxa4342",
      "confidence": 80,
      "control_graph_id": "ctg:5f5cxxxxxxxxa65d1:1338xxxxxxxxa9273",
      "created_timestamp": "2025-07-24T03:04:47.913424496Z",
      "description": "An unusual process accessed lsas. This might indicate an attempt to dump credentials. Investigate the process tree.",
      "device": {
        "agent_version": "6.46.16008.0",
        "hostname": "SD-WIN10",
        "platform_name": "Windows",
      },
      "display_name": "ProcAccessLsas",
      "falcon_host_link": "https://falcon.crowdstrike.com/activity-v2/detections/cb28xxxxxxxxa3914:ind:5f5cxxxxxxxxa65d1:1338xxxxxxxxa3425-10150-
1506xxxxxxxxa4342",
      "filename": "sdhost.exe",
      "filepath": "\\Device\\HarddiskVolume2\\Windows\\System32\\sdhost.exe",
      "id": "ind:5f5cxxxxxxxxa65d1:1338xxxxxxxxa3425-10150-1506xxxxxxxxa4342",
      "indicator_id": "ind:5f5cxxxxxxxxa65d1:1338xxxxxxxxa3425-10150-1506xxxxxxxxa4342",
      "logon_domain": "ABCLABS",
      "md5": "6a21bxxxxxxx888a",
      "mitre_attack": [
       {
        "pattern_id": 10150,
```

```
        "tactic_id": "TA0006",
        "technique_id": "T1003",
        "tactic": "Credential Access",
        "technique": "OS Credential Dumping"
       }
      ],
      "name": "ProcAccessLsas",
      "objective": "Gain Access",
      "parent_process_id": "1338xxxxx5911",
      "pattern_disposition": 0,
      "pattern_disposition_description": "Detection, standard detection.",
      "pattern_id": 10150,
      "platform": "Windows",
      "process_id": "133xxxxx425",
      "process_start_time": "1737687633",
      "product": "epp",
      "scenario": "credential_theft",
      "severity": 70,
      "severity_name": "High",
      "sha256": "7618xxxxx323a",
      "status": "new",
      "tactic": "Credential Access",
      "tactic_id": "TA0006",
      "technique": "OS Credential Dumping",
      "technique_id": "T1003",
      "template_instance_id": "834",
      "timestamp": "2025-07-24T03:03:47.113Z",
      "tree_id": "1338xxxxxxxxa9273",
      "tree_root": "1338xxxxx3425",
      "triggering_process_graph_id": "pid:5f5cxxxxxxxxa65d1:133822076445943425",
      "type": "ldt",
      "updated_timestamp": "2025-07-24T04:03:47.924444597Z",
      "user_id": "S-1-5-21-18xxx43-38xxx75-41xxx35-1xx9",
      "user_name": "llxxxxxxod",
      "user_principal": "XDR-XXXXXXXX.com"
    },
......
  ]
}
```


Updating alerts

Note: This endpoint replaces PATCH /alerts/entities/alerts/v2, which is deprecated.
As you work on an alert, you'll often need to perform actions such as update the status, assign it to a user, or add comments with additional info.

When updating an alert, you set the actions you want to perform as an array of `action_parameters` objects in the request body. In most cases, each element in the array will have both the action `name`, such as `update_status`, and a value, such as `in_progress`. Some actions accept empty values.

Here's an example of the syntax:

```
"action_parameters": [
   {
    "name": "update_status",
    "value": "in_progress"
   }
  ]
```

Supported action parameters

You can perform these actions on alerts:

Action name	Description
`add_tag`	Add a tag (keyword) to the specified alerts. Set the tag text as the `value`.
`append_comment`	Appends a new comment to any existing comments for the specified alerts. Set the comment text as the `value`.
`assign_to_name`	Assign the specified alerts to a user based on their username.
`assign_to_user_id`	Assign the specified alerts to a user based on their email address. Set the email as the `value`.
`assign_to_uuid`	Assign the specified alerts to a user based on their UUID. Set the UUID as the `value`.
`remove_tag`	Remove a tag from the specified alerts. Set the tag text as the `value`
`remove_tags_by_prefix`	Remove all tags containing a given prefix from the specified alerts. Set the tag prefix as the `value`.

Action name	Description
`show_in_ui`	If the value specified is `true`, display the specified alerts in the Falcon console. Any other value, including an empty value, prevents the specified alerts from appearing in the Falcon console.
`unassign`	If there are any users currently assigned to the specified alerts, unassign them. This action doesn't require a value; if one is specified, the value is ignored.
`update_status`	Update the status for the specified alerts. Valid status values are: • `closed` • `in_progress` • `new` • `reopened`

Adding comments

You can add comments to existing alerts with the `append_comment` action parameter. Each comment represents a single object in the request's `action_parameters` with the `name` set to `append_comment` and the `value` holding the comment text.

Notes:

- A comment can contain up to 1024 characters.
- To add multiple comments in the same request, set each comment as a separate object.
- Currently, the API only allows alert comments to be added.

Comment limit

Each alert can store up to 100 comments. When the limit is reached and a new comment is added, a first in, first out (FIFO) mechanism is applied. The oldest comment (first in) is deleted from the alert (first out) to make room for the newest one.

On alerts that reach 100 comments, the API continues to post new comments and return an HTTP 200 (success) status. The response for these requests includes an `error` field with a 400 `code` and a `message` indicating that the alert's comment limit was reached and the oldest comments were overwritten to accommodate new ones.

Reviewing alert comments

Alert comments appear in the response when Retrieving alert details and performing Bulk alert retrieval. The response contains both a `comment` and a `comments` field.

- `comment`: Returns a random ordering of keywords from all of an alert's comments. This field's values are used for searching.
- `comments`: Returns an array with a chronological history of an alert's comments in their original form, ordered with the oldest comment at the top. Each comment in the array includes the complete comment text, a timestamp, and the comment author.

The `falcon_user_id` response field shows the author of the comment. When comments are added using the API, this field returns the user's API client ID.

Endpoint

```
PATCH /alerts/entities/alerts/v3
```

Parameters

Name	In	Type	Required or optional	Description
`composite_ids`	body	array of strings	required	The unique identifier of the alerts to perform the specified actions on. Legacy detection IDs (which start with the prefix `ldt`) are not supported.
`include_hidden`	query	boolean	optional	When set to `true`, hidden alerts are included in the result set. To exclude hidden results, set to `false`. Default: `true`
`action_parameters`	body	array of objects	required	The actions to perform. Each action is a separate object in the array. Add multiple comments individually as separate objects.
`action_parameters.name`	body	string	required	The name of the action to perform. For valid action names, see Supported action parameters.
`action_parameters.value`	body	string	required*	The action value. For info about valid values, see Supported action parameters.

				*Most actions require a value. For more info, see Supported action parameters.

Example: Update alerts by ID

Example request

Assign a user and add a tag to the specified alert IDs.

```
curl -X PATCH "https://api.crowdstrike.com/alerts/entities/alerts/v3" \
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json' \
 -H 'Content-Type: application/json' \
 -d '{
  "action_parameters": [
   {
    "name": "assign_to_user_id",
    "value": "example@crowdstrike.com"
   },
   {
    "name": "add_tag",
    "value": "red_team"
   }
  ],
  "composite_ids": [
   "28a1xxxxxxxx3914:ind:a618xxxxxxxx4d85:1328xxxxxxxx1933-117-1930xxxxxxxx9544","28a1xxxxxxxx3914:ind:a618xxxxxxxx4d67:1328xxxxxxxx1933-118-1865xxxxxxxx9884"
  ]
 }'
```

Example response

```
{
 "meta": {
  "query_time": 0.209774393,
  "writes": {
   "resources_affected": 2
  },
  "powered_by": "detectsapi",
  "trace_id": "8326daf7-d03a-4268-a6f9-8e7195a50ec6"
 }
}
```

Getting aggregates of alerts

Get aggregate counts of alerts grouped by various parameters provided in the body of the request. For more info, see Appendix A: Aggregation parameters.

- Get aggregate counts with POST /alerts/aggregates/alerts/v2

  Optionally, specify the `include_hidden` query parameter to include or exclude hidden alerts. The default value for `include_hidden` is `'true'`

Note: This endpoint replaces POST /alerts/aggregates/alerts/v1, which is being deprecated. Although this endpoint can be used in the following examples during the deprecation period, we encourage you to migrate to the updated endpoint as soon as possible to allow time for testing and to avoid any service disruption.

Example: Getting aggregated alerts by severity

Example request

Retrieve the number of alerts, grouped by the severity.

```
curl -X POST "https://api.crowdstrike.com/alerts/aggregates/alerts/v2" \
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json' \
 -H 'Content-Type: application/json' \
 -d '[
  {
   "name": "Severity aggregates",
   "field": "severity",
   "type": "terms"
  }
 ]'
```

Example response

```
{
    "meta": {
        "query_time": 0.014132521,
        "writes": {
            "resources_affected": 0
        },
        "powered_by": "detectsapi",
        "trace_id": "b42fa8d5-e5c7-47a9-bd4f-997c12cc2697"
    },
    "resources": [
```

```
        {
            "name": "severity aggregates",
            "buckets": [
                {
                    "label": 60,
                    "count": 25
                },
                {
                    "label": 40,
                    "count": 15
                },
                {
                    "label": 80,
                    "count": 10
                },
                {
                    "label": 10,
                    "count": 18
                },
                {
                    "label": 0,
                    "count": 2
                }
            ]
        }
    ],
    "errors": []
}
```


Example: Getting aggregated alerts by week and by severity

Example request

Retrieve the number of alerts for each severity, grouped by week.

```
curl -X POST "https://api.crowdstrike.com/alerts/aggregates/alerts/v2" \
 -H 'Authorization: bearer eyJhbGci...xYg1NNI' \
 -H 'Accept: application/json' \
 -H 'Content-Type: application/json' \
 -d '[
  {
   "name": "Severity aggregates by week",
   "field": "created_timestamp",
   "type": "date_histogram",
   "interval": "week",
   "sub_aggregates":[
    {
     "name":"severity",
      "field":"severity",
     "type":"terms"
    }
   ]
  }
 ]'
```

Example response


```
{
    "meta": {
        "query_time": 0.034447314,
        "writes": {
            "resources_affected": 0
        },
        "powered_by": "detectsapi",
        "trace_id": "4b9b09fe-e9eb-4f44-8f21-f158c97fc1b8"
    },
    "resources": [
        {
            "name": "Severity aggregates by week",
            "buckets": [
                {
                    "label": 1639353600000,
                    "key_as_string": "2021-12-13T00:00:00.000Z",
                    "count": 32,
                    "sub_aggregates": [
                        {
                            "name": "severity",
                            "buckets": [
                                {
                                    "label": 10,
                                    "count": 17
                                },
                                {
                                    "label": 0,
                                    "count": 14
                                },
                                {
                                    "label": 40,
                                    "count": 1
```

```
                            }
                        ]
                    }
                ]
            },
            {
                "label": 1639958400000,
                "key_as_string": "2021-12-20T00:00:00.000Z",
                "count": 60,
                "sub_aggregates": [
                    {
                        "name": "severity",
                        "buckets": [
                            {
                                "label": 100,
                                "count": 9
                            },
                            {
                                "label": 80,
                                "count": 31
                            },
                            {
                                "label": 40,
                                "count": 20
                            }
                        ]
                    }
                ]
            },
            {
                "label": 1640563200000,
                "key_as_string": "2021-12-27T00:00:00.000Z",
                "count": 106,
                "sub_aggregates": [
                    {
                        "name": "severity",
                        "buckets": [
                            {
                                "label": 70,
                                "count": 21
                            },
                            {
                                "label": 90,
                                "count": 42
                            },
                            {
                                "label": 60,
                                "count": 18
                            }
                        ]
                    }
                ]
            }
        ]
    }
],
"errors": []
}
```


Managing automated leads and context alerts

Automated leads, and relevant context included within them, are made available via the Alerts API. For more info on these leads, see Automated Leads.

The API returns the following relevant components:

- Automated lead: This is the primary automated lead entity intended for investigation alongside its relevant context and detections. For a list of fields, see Appendix E: Automated lead alert attributes.
- Automated lead context: These are the alerts generated by CrowdStrike Signal. These alerts should be investigated together as part of the complete lead found on Automated leads, not individually. These alerts can include data from IOAs that typically do not create detections. For a list of relevant fields, see Appendix F: Automated lead context alert attributes.
- All endpoint detections found on Next-Gen SIEM Detections or Endpoint detections that are associated with an automated lead For a list of relevant fields, see Appendix B: EPP alert attributes.

Filtering automated leads and context alerts

Since automated leads and their associated context alerts are not designed for individual investigation, you should filter out these alerts to avoid mixing them with actionable detections.

The following options are available for filtering alerts:

- Filter by specific products: Include a filter that limits results to only the products you are interested in. For example, `"product:['epp']"` or `"product:['epp', 'fcs', 'ngsiem', 'thirdparty']"`.
- Exclude automated lead products: Include a filter that excludes all alerts related to automated leads. For example, `"product:! ['automated-lead','automated-lead-context']"`.
- Programmatic filtering: If you use custom code or automation for processing, you can programmatically filter by product fields to exclude these alerts.
- View all data associated with an automated lead: Include a filter that searches for any records associated with a particular lead, including the automated lead, context, and associated Endpoint detections. For example, `"lead_id:"<lead_id of an automated lead>"`

Appendix A: Aggregation parameters for alerts

Parameter Name	Type	Required?	Description
`name`	String	Yes	Name of the aggregate query, as chosen by the user. Used to identify the results returned to you.
`type`	String	Yes	Type of aggregation. Valid values include: • `date_histogram`: Aggregates counts on a specified time interval. Requires use of the `interval` field. • `date_range`: Aggregates counts on custom defined date range buckets. Can include multiple ranges. (Similar to time series, but the bucket sizes are variable). Date formats to follow ISO 8601. • `terms`: Buckets alerts by the value of a specified field. For example, if the field used is `scenario`, then detections will be bucketed by the various detection scenario names. • `range`: Buckets alerts by specified (numeric) ranges of a specified field. For example, if doing a range aggregation on the max_severity field, the detects will be counted by the specified ranges of severity. • `cardinality`: Returns the count of distinct values in a specified field. • `max`: Returns the maximum value of a specified field. • `min`: Returns the minimum value of a specified field. • `avg`: Returns the average value of the specified field. • `sum`: Returns the total sum of all values for the specified field. • `percentiles`: Returns these percentiles for the specified field: `[ 1, 5, 25, 50, 75, 95, 99 ]`
`field`	String	Yes	The field on which to compute the aggregation. This can be any field returned in a query response, such as `severity` or `mitre_attack.tactic_id`.
`interval`	String	Required only if `type = date_histogram`	Time interval for date histogram aggregations. Valid values include: • `year` • `month` • `week` • `day` • `hour` • `minute`
`filter`	String	No	Contains FQL filter conditions.
`q`	String	No	Full text search across all metadata fields.
`include`	String	No	Performs post-filtering on queried fields.
`ranges`	Array	No	Applies to range aggregations. Range values depend on the field. For example, if `max_severity` is used, ranges might look like: `[{"From": 0,"To": 70},{"From": 70,"To": 100}]`
`date_ranges`	Array	No	Applies to date_range aggregations. For example: `[{"from": "2016-05-28T09:00:31Z","to": "2016-05-30T09:00:31Z"},{"from": "2016-06-01T09:00:31Z","to": "2016-06-10T09:00:31Z"}]`
`missing`	String	No	Specifies a value to be used when the aggregation field is missing from the object. Defines how results that are missing a value should be treated. By default they will be ignored, but it is also possible to treat them as if they had a value.
`min_doc_count`	Int	No	Only return buckets if values are greater than or equal to the specified value.
`size`	Int	No	The maximum number of term buckets to be returned.
`sort`	String	No	Sort bucket results. • `_count`: sort by document count • `_term`: sort by the string value alphabetically

Parameter Name	Type	Required?	Description
			You can sort by `asc` or `desc`, such as: `_count | desc`
`timezone`	String	No	Timezone to specify when bucketing results.
`sub_aggregates`	Array	No	A nested aggregation. For example: `sub_aggregates": [{"name": "max_first_behavior","type": "max","field": "first_behavior"}]"` You can specify a maximum of 3 nested aggregations per request.

Appendix B: EPP alert attributes

Field	Nested field 1	Nested field 2	Type	Description	Example valu
`agent_scan_id`			String	The sensor generated ID for a specific on-demand scan occurrence.	`44c1xxxxx`
`aggregate_id`			String	A unique identifier that links multiple alerts associated with the same process tree.	`aggind:77c`
`alleged_filetype`			String	The extension of the main executable for the target process.	`exe`
`child_process_ids`			String array	The list of unique identifiers for the child process of the target process (unique in sensor scope).	`["pid:9a8c`
`cloud_indicator`			Boolean	Indicates whether or not the alert was identified by the cloud module.	`FALSE`
`cmdline`			String	The command line used to create the target process.	`cmd.exe \C`
`detection_context`			Object	Adds template-specific context collection format to detection events.	
	`authentication_id`		UInt64	The identifier for the authentication activity.	`82xxx62`
	`logon_domain`		String	The name of the domain used to authenticate the owner of the logon session.	`DESKTOP-AE`
	`logon_server`		String	The name of the server used to authenticate the owner of the logon session.	`W10BVT-VLA`
	`logon_time`		String	A UTC timestamp of the time the session owner logged on.	`2023-11-29`
	`logon_type`		String enum	A Ulong defining the type of logon. Possible values:	`3`

				• 2 (INTERACTIVE) - The security principal is logging on interactively. • 3 (NETWORK) - The security principal is logging on using a network. • 4 (BATCH) - The logon is for a batch process. • 5 (SERVICE) - The logon is for a service account. • 6 (PROXY) - Not supported. • 7 (UNLOCK) - The logon is an attempt to unlock a workstation. • 8 (NETWORK_CLEARTEXT) - The logon is a network logon with plaintext credentials. • 9 (NEW_CREDENTIALS) - Allows the caller to clone its current token and specify new credentials for outbound connections. The new logon session has the same local identity but uses different credentials for other network connections. • 10 (REMOTE_INTERACTIVE) - A terminal server session that is both remote and interactive. • 11 (CACHED_INTERACTIVE) - Attempt to use the cached credentials without going out across the network. • 12 (CACHED_REMOTE_INTERACTIVE) - Same as REMOTE_INTERACTIVE, except used internally for auditing purposes. • 13 (CACHED_UNLOCK) - The logon is an attempt to unlock a workstation.	
	`remote_address_ip4`		String	The remote IPv4 address in the order that turns the IP 0.0.0.1 into the number 1. Commonly known as "host byte order".	`19x.xxx.x.`
	`remote_address_ip6`		String	The remote IPv6 address in network-byte order.	`0:0:0:0:0:`
	`user_is_admin`		Boolean	Indicates whether the user is an admin (`true`) or not an admin (`false`).	`true`
	`user_name`		String	The name of the user.	`example-us`
	`user_sid`		String	A SID (security identifier) that uniquely indicates a user (or service account) in the system. This is contrary to LUIDs that are generated on the fly as needed and are never persisted across system reboots. SIDs are statically assigned to a user account and persisted.	`AQxxxxxxx`
`device`			Object	Info about the associated device.	
	`agent_load_flags`		String	Whether the sensor loaded during or after the Windows host's boot process. This is a bitfield, and may contain more than one value. Possible Values: • 0: The sensor loaded after startup, indicating a newly installed or updated sensor. (For Mac and Linux hosts, this value is always 0.) • 1: The sensor loaded during the boot process, indicating the host booted normally with the sensor installed. • 2: Used for Falcon system diagnostic purposes. • 3: A combination of values 0 and 1.	`3`

	agent_local_time		String	A UTC timestamp of when the event was generated in the device's local time.	2015-07-31
	agent_version		String	Version of the Falcon sensor installed on the device.	5.25.10701
	bios_manufacturer		String	The manufacturer of the host's BIOS.	Phoenix Te
	bios_version		String	The version of the host's BIOS.	6
	cid		String	The customer ID for the associated host.	d615xxxxx
	device_id		String	The agent ID of the sensor running on the host.	9a8d0d2fe0
	external_ip		String	The external IPv4 address of the asset the application is on.	3x.xxx.xx
	external_ipv6		String	The external IPv6 address of the asset the application is on.	20xx:xxx:x
	first_seen		String	A UTC timestamp of the first time the sensor was seen by the CrowdStrike cloud.	2024-02-22
	groups		String array	The IDs of host groups the device is a part of.	3877xxxxx
	hostinfo		Object	Information about the associated host.	
		active_directory_dn_display	String array	The distinguished active directory name.	"Domain Co
		domain		The Windows domain name the machine is currently connected to.	"DOMAIN.lo
	hostname		String	The hostname for the associated host.	example-ho
	host_hidden_status		String	Indicates whether the host is visible or hidden.	visible
	last_seen		String	A UTC timestamp of the last time the sensor was seen by the CrowdStrike cloud.	2024-02-22
	instance_id		String	The unique identifier for the instance of the device.	i-0c2xxxx
	local_ip		String	The IPv4 address of the device.	10.xx.xx.x
	local_ipv6		String	The IPv6 address of the device.	20xx:xxxx:
	mac_address		String	The unique network address for the device.	00:xx:xx:x
	machine_domain		String	The Windows domain name the machine is currently connected to.	DOMAIN.loc
	major_version		String	The major version part of the OS version number.	3
	minor_version		String	The minor version part of the OS version number.	10
	modified_timestamp		String	A UTC timestamp of when the host was last updated (on device).	2024-02-22
	os_version		String	The OS major version.	Windows
	ou		String array	The Active Directory organizational unit.	["Laptops"
	platform_id		String	The numeric ID corresponding to the high-level platform type. Possible values returned: • 0 (Windows) • 1 (Mac) • 3 (Linux)	0
	platform_name		String	The text-based platform name based on the `device.platform_id`.	Windows
	pod_id		UUID	The unique identifier for the pod running the device.	22c1xxxxx
	pod_labels		String	Kubernetes labels of the pod running the sensor container. Null if the device is not in	["app:dete

				Kubernetes.	
	pod_name		String	The name of the pod.	arn:aws:ec
	pod_namespace		String	The namespace of the pod.	default
	pod_service_account_name		String	The service account name of the pod.	default
	product_type		String	The type of the device.	1
	product_type_desc		String	The string description of the type.	Workstatio
	service_provider		String	The service provider of the product.	AWS_EC2_V2
	service_provider_account_id		String	The account id of the service provider.	983xxxxxx2
	site_name		String	The site name of the domain the machine is joined with.	Default-Fi
	status		String	The network containment status of the host.	normal
	system_manufacturer		String	BIOS manufacturer name according to SMBIOS standard.	VMware Inc
	system_product_name		String	Product name according to SMBIOS standard.	VMware Vir
	tags		String	The sensor and cloud tags of the host.	["SensorGr
falcon_host_link			String	A link to view the alert in the Falcon console.	https://fa
filename			String	The file name of the triggering process.	cmd.exe
filepath			String	The full path of the triggering process.	\\Device\\
global_prevalence			String enum	A value representing how common this indicator is in the global environment. Possible returned values: • unique • low • common	common
grandparent_details			Object	A value representing the grandparent process.	
	cmdline		String	The command line used to create the grandparent process.	winlogon.e
	filename		String	The file name of the main executable for the grandparent process.	winlogon.e
	filepath		String	The full path to the main executable for the grandparent process.	\\Device\\
	local_process_id		String	The unique identifier for the OS internal grandparent process (unique on the device).	3xxx
	md5		String	The MD5 hash of the related file for the grandparent process.	fc0bxxxxx
	process_graph_id		String	The unique identifier for the grandparent process (unique in falcon).	pid:77d1x
	process_id		String	The unique object identifier for the grandparent process (unique in falcon)	1335xxxxx
	sha256		String	The SHA-256 hash of the related file for the grandparent process.	7148xxxxx
	timestamp		String	A UTC timestamp of the time the grandparent process was executed.	2024-02-22
	user_graph_id		String	Threat Graph ID of the user who executed the grandparent process.	uid:77d1x
	user_id		String	The user security identifier of the user who executed the grandparent process.	S-1-5-18
	user_name		String	User name of the user who executed the grandparent process.	example-us
id			String	The unique identifier of the alert.	ind:9a8d0c

incident			Object	Information about the associated CrowdScore incident.	
	created		String	A UTC timestamp with the date and time the incident was created.	2024-02-22
	end		String	A UTC timestamp of the latest alert that's part of the incident.	2024-02-22
	id		String	The ID of the associated CrowdScore incident.	inc:9a8d0c
	score		String	The score for the CrowdScore Incident.	61.2354104
	start		String	A UTC timestamp of the earliest alert that's part of the incident.	2024-02-22
indicator_id			String	The unique identifier of the indicator.	ind:77d117
ioc_context			Object array	List of indicators that triggered the alert	[{"ioc_des file.exe",
	ioc_description		String	The description of the IOC.	/home/sfdc
	ioc_source		String	The source of the IOC.	library_lo
	ioc_type		String	The type of the IOC.	hash_sha25
	ioc_value		String	The value of the IOC.	7a3fxxxxx
	md5			The MD5 hash of the IOC.	eaedxxxxx
	sha256		String	The SHA-256 hash of the IOC.	7a3fxxxxx
	ioc_created_by			The user who created the IOC in IOCManager, if applicable.	john.smith
	type		String	The type of IOC. Possible returned values: • module • script • customioc	module
local_prevalence			String	A value of how common this indicator is in your local environment. Possible returned values: • unique • low • common	common
local_process_id			String	The unique identifier for the OS internal target process (unique in sensor scope).	4xxx
logon_domain			String	The name of the domain used to authenticate the logon session.	VICTIMNET
md5			String	The MD5 hash of the related file for the target process.	fc0bxxxxx
network_accesses			Object array		
	access_timestamp		String	The timestamp of the network access activity in 10-digit Unix epoch format.	1727123320
	access_type		Integer	The connection flag of the network access.	0
	connection_direction		String enum	The connection direction of the network access. Possible returned values: • outbound • inbound • neither	outbound
	isIPV6		Boolean	Whether the network access is IPv6.	false

	local_address		String	The local IP address of the network access.	2x.xx.xx.x
	local_port		String	The local port of the network access.	5xxxx
	protocol		String	The network protocol.	TCP
	remote_address		String	The remote IP address of the network access.	2x.xxx.xx.
	remote_port		String	The remote port of the network access.	1xxx
os_name			String	The operating system name.	Windows
parent_details			Object	Associated parent process info.	
	cmdline		String	The command line used to create the parent process.	utilman.ex
	filename		String	The file name of the main executable for the parent process.	Utilman.ex
	filepath		String	The full path to the main executable for the parent process.	\\Device\\
	local_process_id		String	The unique identifier for the OS internal parent process.	4012
	md5		String	The MD5 hash of the related file for the parent process.	fc0bxxxxx
	process_graph_id		String	Threat Graph ID of the parent process.	pid:9a8d0c
	process_id		String	The unique ID of the parent process.	1336xxxxx
	sha256		String	The SHA-256 hash of the related file for the parent process.	cd84xxxxx
	timestamp		String	A UTC timestamp of the time the parent process was executed.	2024-02-22
	user_graph_id		String	Threat Graph ID of the user who executed the parent process.	uid:978e47
	user_id		String	The user security identifier of the user who executed the parent process.	S-1-5-18
	user_name		String	Name of the user who executed the parent process.	example-us
parent_process_id			String	The unique identifier for the parent process.	133530866
pattern_disposition			Integer	A bitfield value that represents actions taken by the Falcon sensor in response to malicious activity. Bit values come from response bits and modifier bits, where response bits are actions taken or attempted, and modifier bits are reasons the attempt was unsuccessful. If PatternDisposition's value is 0, no response was attempted. For more info, see the `PatternDisposition` field description in the AssociateIndicator table under Sensor events.	0
pattern_disposition_description			String	A short system-generated description of what dispositions were taken.	Detection
pattern_disposition_details			Object	A true/false map indicating which actions were taken. For more info, see .	
process_end_time			String	The time the process ended (derived from the device) in 10-digit Unix epoch format.	170861130
process_id			String	The unique ID of the process running on the host.	1335xxxxx
process_start_time			String	The time the process started (derived from the device) in 10-digit UNIX EPOCH format.	170861130
quarantined			Boolean	Indicates the quarantine status of an on-demand scan malicious file.	true
quarantined_files			Object array		

	filename		String	The name of the quarantined file.	\\Device\\
	id		String	The unique identifier for the quarantined file.	b5dfxxxxx
	sha256		String	The hash of the quarantined file.	e6e3xxxxx
	state		String	The state of the quarantined file.	quarantine
scan_id			String	The ID of the related on-demand scan occurrence.	21c1xxxxx
sha1			String	A SHA1 hash of the process.	0c2exxxxx
sha256			String	A SHA-256 hash of the process.	0b9bxxxxx
template_instance_id			Integer enum	The instance ID from a template match, used for debugging.	206
template_interface_id			Integer	An integer value mapping to the Template Interface ID of the context collection definition used for detection context. Possible returned values: • 26 (FileSystemOperationContext) • 27 (WindowsUserDetectionContext) • 28 (RegistryValueModifiedUIContext)	28
template_interface_name			String enum	The name to determine Template Interface for the Detection Context. Maps to the template_interface_id. Possible returned values: • FileSystemOperationContext • WindowsUserDetectionContext • RegistryValueModifiedUIContext	FileSystem
tree_id			String	The unique identifier of the tree.	1335308490
tree_root			String	The unique identifier of the tree root.	1335308662
triggering_process_graph_id			String	The Threat Graph ID of the triggering process.	pid:77d117
user_id			String	The User Security Identifier of the user that performed the operation.	S-1-5-18
user_name			String	The short account name for the security principal.	DA1$
user_principal			String	The user principal name for the user. This will be present in domain-based accounts.	DA1$@ABCNE

Appendix C: OverWatch alert attributes

Field	Description
agent_id	Agent ID associated with the given detection
cid	ID of customer associated with the given detection
composite_id	Opaque ID that uniquely identifies the alert
crawled_timestamp	Timestamp of updated detection
created_timestamp	Timestamp of when the detection was initially created
detect_type	Is always 'lead', for all overwatch hunting activity detections

Field	Description
host_name	Name of host which the agent is reporting the given detection
host_type	The type of host which the agent is reporting the given detection: (Workstation, Server, Domain Controller)
id	Detection type with a unique identifier of the given detection
operating_system	The operating system of the host
ow_severity	Severity of the hunting activity detection
pattern_id	Identifies the pattern used for the detection
process_id	Process ID of the process running on the host
product	Always `overwatch` for this type of alert
show_in_ui	Determine whether to show the detetion in the UI
tags	Tags show additional information, such as the status, severity
timestamp	Timestamp of the detection
tree_id	Internal ID specifying the graph id of the detection
type	Always `lead` for this type of alert
target_file_name	File name, if applicable, which caused the detection
endpoint_detection_id	Parent ID used for grouping together several `process_ids` to create a process tree or execution timeline
image_file_name	Image file name, if applicable, which caused the detection
command_line	Command line, if applicable, which was executed to cause the detection
updated_timestamp	Timestamp of when the detection was last modified

Appendix E: Automated lead alert attributes

Field Name	Type	Description	Example value
cid	String	The ID of the customer associated with the given automated lead.	d615xxxxxxxx2158
composite_id	String	The Opaque ID that uniquely identifies the automated lead.	d615xxxxxxxx2158:automated-lead:d615xxxxxxxx2158:db910223310d15509afcda5fac38901f7cc1c30724eb5fb1571350f6f2452a9c
created_timestamp	String	The timestamp that displays when the alert was created.	2025-07-09T19:30:23.86626953Z
display_name	String	The display name associated with the alert.	TBOB-WIN11-T at 2025-07-09T19:30:10Z

falcon_host_link	String	A link to the Falcon console.	https://falcon.crowdstrike.com/automated-leads/d615xxxxxxxx2158:automated-lead:d615xxxxxxxx2158:db910223310d15509afcda5fac38901f7cc1c30724eb5fb1571350f6f2452a9c?_cid=g020xxxxxxxxqwzi
id	String	The unique identifier of the automated lead alert.	automated-lead:d615xxxxxxxx2158:db910223310d15509afcda5fac38901f7cc1c30724eb5fb1571350f6f2452a9c
is_closed	Bool	Displays if lead is closed, which means no new information is expected.	true
lead_id	String	The ID given to the lead. This ID can be used to look up all associated detections and other context for the lead.	db910223310d15509afcda5fac38901f7cc1c30724eb5fb1571350f6f2452a9c
lead_type	String	The type of lead.	simple
mitre_attack[0].pattern_id	Integer	The unique identifier for the Mitre attack pattern.	405
mitre_attack[0].tactic_id	String	The unique identifier for the Mitre ATT&CK tactic.	TA0005
mitre_attack[0].technique	String	The Mitre ATT&CK technique associated with the lead.	Process Injection
mitre_attack[0].technique_id	String	The unique identifier for the Mitre ATT&CK technique.	T1055
mitre_attack[0].tactic	String	The Mitre ATT&CK tactic associated with the lead.	Defense Evasion
name	String	Name	TBOB-WIN11-T at 2025-07-09T19:30:10Z
pattern_id	Integer	The Product ID of the lead.	185000
product	String	Product	automated-lead
score	Integer	The lead confidence score.	100
signal_start_timestamp	String	The timestamp of when the first indicator was added to the lead.	2025-07-09T19:30:10Z
signal_end_timestamp	String	Timestamp of when the last indicator was added to the lead.	2025-07-09T19:30:10Z
signal_updated_timestamp	String	The last time the lead was updated with new information or when it was closed.	2025-07-09T19:30:10Z
source_products	Array String	Source product	Falcon Signal
source_vendors	Array String	Source vendors	CrowdStrike
status	String	The status of the lead.	new
timestamp	String	Time when the data was received by the cloud platform.	2025-07-09T19:35:25Z
updated_timestamp		The last time the record was updated through any means, including API.	2025-07-09T19:35:25.918302523Z
type	String	The type of lead.	automead-lead

threatgraph_indicators[0].severity	Integer	Level of threat criticality.	70
threatgraph_indicators[0].process_id	String	Unique identifier of the running process.	1765091414
threatgraph_indicators[0].hostname	String	Name of the host machine where activity was detected.	TBOB-WIN11-T
threatgraph_indicators[0].pattern_id	Integer	Unique identifier for the attack pattern.	405
threatgraph_indicators[0].signal_association_timestamp	String	Timestamp of when the indicator was added to the lead.	2025-07-09T19:30:10Z
threatgraph_indicators[0].indicator_id	String	Unique identifier used to locate associated detections using filter product: ["epp","automated-lead-context"]+indicator_id:"{indicator_id}"	ind:a5eaxxxxxxxxe49e:1765091414-24-676482185940600855
threatgraph_indicators[0].template_instance_id	String	Unique identifier for the specific instance of the detection template.	0
threatgraph_indicators[0].host_id	String	Unique identifier assigned to the endpoint or host.	a5eaxxxxxxxxe49e
threatgraph_indicators[0].pattern_disposition	String	Current status or outcome of the detected pattern.	0

Appendix F: Automated lead context alert attributes

Field	Type	Description	Example value
lead_id	String	Lead ID is used to identify all the resources linked to the same lead ID. To get the lead object, you can use the filter `"product:'automated-lead'+lead_id:'{lead_id}'"`	db910223310xxxxxxxxxxxxxxxxxxxx2452a9c
aggregate_id	String	A unique identifier that links multiple automated lead context alerts associated with the same lead ID. This value is equivalent to `lead_id`. Some products, such as `epp`, might have `aggregate_id` set to a different value, so using `lead_id` will give you a more accurate way to find anything related to a specific lead ID.	db910223310xxxxxxxxxxxxxxxxxxxx2452a9c
alleged_filetype	String	The extension of the main executable for the target process.	exe
child_process_ids	String array	The list of unique identifiers for the child process of the target process. Each identifier is unique within the sensor scope.	["pid:9a8d0d2fe0xxxxxxxxxxxxxxxxxxc74c:1336xxxxxxxxxx2640","pid:9a8d0d2fe0xxxxxxxxxx
cmdline	String	The command line used to create the target process.	cmd.exe \C:\\Windows\\System32\\osk.exe\" "
detection_context[0].authentication_id	UInt64	The identifier for the authentication activity.	82xxx62
detection_context[0].logon_domain	String	The name of the domain used to authenticate the owner of the logon session.	DESKTOP-ABCDEFG
detection_context[0].logon_server	String	The name of the server used to authenticate the owner of the logon session.	W10BVT-VLAB

detection_context[0].logon_time	String	A UTC timestamp of the time the session owner logged on.	2023-11-29T05:29:32.7729046Z
detection_context[0].logon_type	String enum	A Ulong defining the type of logon. Possible values returned include the following: • 2 (INTERACTIVE) - The security principle is logging on interactively. • 3 (NETWORK) - The security principle is logging on using a network. • 4 (BATCH) - The logon is for a batch process. • 5 (SERVICE) - The logon is for a service account. • 6 (PROXY) - Not supported. • 7 (UNLOCK) - The logon is an attempt to unlock a workstation. • 8 (NETWORK_CLEARTEXT) - The logon is a network logon with plaintext credentials. • 9 (NEW_CREDENTIALS) - Allows the caller to clone its current token and specify new credentials for outbound connections. The new logon session has the same local identity but uses different credentials for other network connections. • 10 (REMOTE_INTERACTIVE) - A terminal server session that is both remote and interactive. • 11 (CACHED_INTERACTIVE) - Attempt to use the cached credentials without going out across the network. • 12 (CACHED_REMOTE_INTERACTIVE) - Same as REMOTE_INTERACTIVE, except used internally for auditing purposes. • 13 (CACHED_UNLOCK) - The logon is an attempt to unlock a workstation.	3
detection_context[0].remote_address_ip4	String	The remote IPv4 address in the order that turns the IP 0.0.0.1 into the number 1. Commonly known as **host byte order**.	19x.xxx.x.x3
detection_context[0].remote_address_ip6	String	The remote IPv6 address in network-byte order.	0:0:0:0:0:xxxx:xxxx:0221
detection_context[0].user_is_admin	Boolean	The value **true** indicates whether the user is an admin. The value **false** indicates the user is not an admin.	true
detection_context[0].user_name	String	The name of the user.	example-user-name
detection_context[0].user_sid	String	A security identifier (SID) that uniquely indicates a user, or service account, in the system. This is contrary to LUIDs that are generated as needed and are never persisted across system reboots. SIDs are statically assigned to a user account and persisted.	AQxxxxxxxxANENBV/6u/Qxxxxxp7QxxxA==
device[0].agent_load_flags	String	Whether the sensor loaded during or after the Windows host's boot process. This is a bitfield, and may contain more than one value. Possible Values:	3

		• 0: The sensor loaded after startup, indicating a newly installed or updated sensor. For Mac and Linux hosts, this value is always 0. • 1: The sensor loaded during the boot process, indicating the host booted normally with the sensor installed. • 2: Used for Falcon system diagnostic purposes. • 3: A combination of values 0 and 1.	
device[0].agent_local_time	String	A UTC timestamp of when the event was generated in the device's local time.	2015-07-31T14:07:40.193Z
device[0].agent_version	String	Version of the Falcon sensor installed on the device.	5.25.10701.0
device[0].bios_manufacturer	String	The manufacturer of the host's BIOS.	Phoenix Technologies LTD
device[0].bios_version	String	The version of the host's BIOS.	6
device[0].cid	String	The customer ID for the associated host.	d615xxxxxxxx2158
device[0].device_id	String	The agent ID of the sensor running on the host.	9a8d0d2fe0xxxxxxxxxxxxxxxxxxc74c
device[0].external_ip	String	The external IPv4 address of the asset the application is on.	3x.xxx.xxx.xxx
device[0].external_ipv6	String	The external IPv6 address of the asset the application is on.	20xx:xxx:xxxx:xxxx:5555:6666:7777:8888
device[0].first_seen	String	A UTC timestamp of the first time the sensor was seen by the CrowdStrike cloud.	2024-02-22T14:15:03Z
device[0].groups	String array	The IDs of host groups the device is a part of.	3877xxxxxxxxxxxxxxxxxxxxxxxx8549,e773xxxxxxxxxxxxxxxxxxxxxxxx6508
device[0].hostinfo.active_directory_dn_display	String array	The distinguished active directory name.	"Domain Controllers"
device[0]. hostinfo.domain		The Windows domain name the machine is currently connected to.	"DOMAIN.local"
device[0].hostname	String	The hostname for the associated host.	example-host
device[0].host_hidden_status	String	Indicates whether the host is visible or hidden.	visible
device[0].last_seen	String	A UTC timestamp of the last time the sensor was seen by the CrowdStrike cloud.	2024-02-22T14:15:03Z
device[0].instance_id	String	The unique identifier for the instance of the device.	i-0c2xxxxxxxxxxe12
device[0].local_ip	String	The IPv4 address of the device.	10.xx.xx.xx
device[0].local_ipv6	String	The IPv6 address of the device.	20xx:xxxx:xxxx:xxxx:0000:0000:0000:0001
device[0].mac_address	String	The unique network address for the device.	00:xx:xx:xx:4D:5E
device[0].machine_domain	String	The Windows domain name the machine is currently connected to.	DOMAIN.local
device[0].major_version	String	The major version part of the OS version number.	3
device[0].minor_version	String	The minor version part of the OS version number.	10
device[0].modified_timestamp	String	A UTC timestamp of when the host was last updated (on device).	2024-02-22T14:15:08Z
device[0].os_version	String	The OS major version.	Windows
device[0].ou	String array	The Active Directory organizational unit.	["Laptops","Downtown Memorial","IRF","Windows10","Clients"]
device[0].platform_id	String	The numeric ID corresponding to the high-level platform type. Possible values returned:	0

		• 0 (Windows) • 1 (Mac) • 3 (Linux)	
device[0].platform_name	String	The text-based platform name is based on the device.platform_id.	Windows
device[0].pod_id	UUID	The unique identifier for the pod running the device.	22c1xxxxxxxxxxxxxxxxxxxxxxxx727f
device[0].pod_labels	String	Kubernetes labels of the pod running the sensor container. Null if the device is not in Kubernetes.	["app:detection-container","app.kubernetes/component:agent","pod-template-hash:76xxxxxx54
device[0].pod_name	String	The name of the pod.	arn:aws:ecs:us-east-1:53xxxxxxxx73:task/default/22c1xxxxxxxxxxxxxxxxxxxxxxxx727f
device[0].pod_namespace	String	The namespace of the pod.	default
device[0].pod_service_account_name	String	The service account name of the pod.	default
device[0].product_type	String	The type of the device.	1
device[0].product_type_desc	String	The string description of the type.	Workstation
device[0].service_provider	String	The service provider of the product.	AWS_EC2_V2
device[0].service_provider_account_id	String	The account id of the service provider.	983xxxxxx254
device[0].site_name	String	The site name of the domain the machine is joined with.	Default-First-Site-Name
device[0].status	String	The network containment status of the host.	normal
device[0].system_manufacturer	String	BIOS manufacturer name according to SMBIOS standard.	VMware Inc.
device[0].system_product_name	String	Product name according to SMBIOS standard.	VMware Virtual Platform
device[0].tags	String	The sensor and cloud tags of the host.	["SensorGroupingTags/ecs","SensorGroupingTags/fargate","SensorGroupingTags/detections"]
falcon_host_link	String	A link to view the alert in the Falcon console.	https://falcon.crowdstrike.com/automated-leads/ed0dxxxxxxxxxxxxxxxxxxxxxxb8db:ind:873axxxxxxxxxxxxxxxxxxxxxxx75e6:2997xxxxxxx
filename	String	The file name of the triggering process.	cmd.exe
filepath	String	The full path of the triggering process.	\\Device\\HarddiskVolume1\\Windows\\System32\\cmd.exe
global_prevalence	String enum	A value representing how common this indicator is in the global environment. Possible returned values: • unique • low • common	common
grandparent_details[0].cmdline	String	The command line used to create the grandparent process.	winlogon.exe
grandparent_details[0].filename	String	The file name of the main executable for the grandparent process.	winlogon.exe
grandparent_details[0].filepath	String	The full path to the main executable for the grandparent process.	\\Device\\HarddiskVolume1\\Windows\\System32\\winlogon.exe
grandparent_details[0].local_process_id	String	The unique identifier for the OS internal grandparent process (unique on the device).	3xxx
grandparent_details[0].md5	String	The MD5 hash of the related file for the grandparent process.	fc0bxxxxxxxxxxxxxxxxxxxxxxxx2d25
grandparent_details[0].process_graph_id	String	The unique identifier for the grandparent process (unique in falcon).	pid:77d1xxxxxxxxxxxxxxxxxxxxxxxxca19:1335xxxxxxxxxx2300
grandparent_details[0].process_id	String	The unique object identifier for the grandparent process (unique in falcon)	1335xxxxxxxxxx2300
grandparent_details[0].sha256	String	The SHA-256 hash of the related file for the grandparent process.	7148xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx8f68

grandparent_details[0].timestamp	String	A UTC timestamp of the time the grandparent process was executed.	2024-02-22T14:15:03Z
grandparent_details[0].user_graph_id	String	ThreatGraph ID of the user who executed the grandparent process.	uid:77d1xxxxxxxxxxxxxxxxxxxxxx48ca19:S-1-5-18
grandparent_details[0].user_id	String	The user security identifier of the user who executed the grandparent process.	S-1-5-18
grandparent_details[0].user_name	String	User name of the user who executed the grandparent process.	example-user-name
id	String	The unique identifier of the alert.	ind:9a8d0d2fe0xxxxxxxxxxxxxxxxxxc74c:1336xxxxxxxxxx1294-32-7878xxxxxxxxxxx1122
indicator_id	String	The unique identifier of the indicator.	ind:77d1172532c8480fa0e61d676c48ca19:133530866285959158-67-1807973856838571807 2ind:9a8d0d2fe0xxxxxxxxxxxxxxxxxxc74c:1336xxxxxxxxxx1294-32-78
ioc_context[0].ioc_description	String	The description of the IOC.	/home/sfdc/current/abcservices/abcservicesprevious/AbcServer/bin/abc-dataset-to-csv
ioc_context[0].ioc_source	String	The source of the IOC.	library_load
ioc_context[0].ioc_type	String	The type of the IOC.	hash_sha256
ioc_context[0].ioc_value	String	The value of the IOC.	7a3fxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx4c18
ioc_context[0].md5		The MD5 hash of the IOC.	eaedxxxxxxxxxxxxxxxxxxxxxxxxd2f7
ioc_context[0].sha256	String	The SHA-256 hash of the IOC.	7a3fxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx4c18
ioc_context[0].ioc_created_by		The user who created the IOC in IOCManager, if applicable.	john.smith@email.net
ioc_context[0].type	String	The type of IOC. Possible returned values: • module • script • customioc	module
local_prevalence	String	A value of how common this indicator is in your local environment. Possible returned values: • unique • low • common	common
local_process_id	String	The unique identifier for the OS internal target process (unique in sensor scope).	4xxx
logon_domain	String	The name of the domain used to authenticate the logon session.	VICTIMNET
md5	String	The MD5 hash of the related file for the target process.	fc0bxxxxxxxxxxxxxxxxxxxxxxxx2d25
network_accesses[0].access_timestamp	String	The timestamp of the network access activity in 10-digit Unix epoch format.	1727123320
network_accesses[0].access_type	Integer	The connection flag of the network access.	0
network_accesses[0].connection_direction	String enum	The connection direction of the network access. Possible returned values: • outbound • inbound • neither	outbound
network_accesses[0].isIPV6	Boolean	Whether the network access is IPv6.	false
network_accesses[0].local_address	String	The local IP address of the network access.	2x.xx.xx.xxx
network_accesses[0].local_port	String	The local port of the network access.	5xxxx
network_accesses[0].protocol	String	The network protocol.	TCP

network_accesses[0].remote_address	String	The remote IP address of the network access.	2x.xxx.xx.xx
network_accesses[0].remote_port	String	The remote port of the network access.	1xxx
parent_details[0].cmdline	String	The command line used to create the parent process.	utilman.exe /debug
parent_details[0].filename	String	The file name of the main executable for the parent process.	Utilman.exe
parent_details[0].filepath	String	The full path to the main executable for the parent process.	\\Device\\HarddiskVolume1\\Windows\\System32\\Utilman.exe
parent_details[0].local_process_id	String	The unique identifier for the OS internal parent process.	4012
parent_details[0].md5	String	The MD5 hash of the related file for the parent process.	fc0bxxxxxxxxxxxxxxxxxxxxxxxx2d25
parent_details[0].process_graph_id	String	The ThreatGraph ID of the parent process.	pid:9a8d0d2fe0xxxxxxxxxxxxxxxxxxc74c:1336xxxxxxxxxx4664
parent_details[0].process_id	String	The unique ID of the parent process.	1336xxxxxxxxxx4664
parent_details[0].sha256	String	The SHA-256 hash of the related file for the parent process.	cd84xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx38a0
parent_details[0].timestamp	String	A UTC timestamp of the time the parent process was executed.	2024-02-22T14:15:03Z
parent_details[0].user_graph_id	String	ThreatGraph ID of the user who executed the parent process.	uid:978e47d94ded40c58af5416e6e26fe07:0
parent_details[0].user_id	String	The user security identifier of the user who executed the parent process.	S-1-5-18
parent_details[0].user_name	String	Name of the user who executed the parent process.	example-user-name
parent_process_id	String	The unique identifier for the parent process.	133530866285020085
pattern_disposition	Integer	A bitfield value that represents actions taken by the Falcon sensor in response to malicious activity. Bit values come from response bits and modifier bits, where response bits are actions taken or attempted, and modifier bits are reasons the attempt was unsuccessful. If the PatternDisposition value is 0, no response was attempted. For more info, see the PatternDisposition field description in the AssociateIndicatortable under Sensor events.	0
pattern_disposition_description	String	A short system-generated description of what dispositions were taken.	Detection standard detection.
pattern_disposition_details	Object	A true/false map indicating which actions were taken. For more info, see .	
process_end_time	String	The time the process ended, derived from the device, in 10-digit Unix epoch format.	1708611303
process_id	String	The unique ID of the process running on the host.	1335xxxxxxxxx9158
process_start_time	String	The time the process started (derived from the device) in 10-digit UNIX EPOCH format.	1708611303
quarantined_files[0].filename	String	The name of the quarantined file.	\\Device\\HarddiskVolume3\\Users\\Public\\Documents\\Agent_ABC.exe
quarantined_files[0].id	String	The unique identifier for the quarantined file.	b5dfxxxxxxxxxxxxxxxxxxxxxxxxdeee_e6e3xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx1277
quarantined_files[0].sha256	String	The hash of the quarantined file.	e6e3xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx1277
quarantined_files[0].state	String	The state of the quarantined file.	quarantined
sha1	String	A SHA1 hash of the process.	0c2exxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx6764
sha256	String	A SHA-256 hash of the process.	0b9bxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx19f5
template_instance_id	Integer enum	The instance ID from a template match, used for debugging.	206

template_interface_id	Integer	An integer value mapping to the Template Interface ID of the context collection definition used for detection context. Possible returned values: • 26 (FileSystemOperationContext) • 27 (WindowsUserDetectionContext) • 28 (RegistryValueModifiedUIContext)	28
template_interface_name	String enum	The name to determine Template Interface for the Detection Context. Maps to the template_interface_id. Possible returned values: • FileSystemOperationContext • WindowsUserDetectionContext • RegistryValueModifiedUIContext	FileSystemOperationContext
threatgraph_indicators[0].description	String	The description associated with the attack pattern.	A command intended to perform reconnaissance has been executed under a web service.
threatgraph_indicators[0].display_name	String	The display name associated with the attack pattern.	ReconUnderWebService
threatgraph_indicators[0].indicator_type	String	The type of indicator.	AssociateIndicator
tree_id	String	The unique identifier of the tree.	133530849030016385
tree_root	String	The unique identifier of the tree root.	133530866285020085
triggering_process_graph_id	String	The ThreatGraph ID of the triggering process.	pid:77d1172532c8480fa0e61d676c48ca19:133530866285959158
user_id	String	The User Security Identifier of the user that performed the operation.	S-1-5-18
user_name	String	The short account name for the security principal.	DA1$
user_principal	String	The user principal name for the user. This will be present in domain-based accounts.	DA1$@ABCNET.local

Real Time Response APIs

Execute real-time commands and actions on endpoints for investigation and remediation.

About CrowdStrike APIs

CrowdStrike provides use cases and example requests and responses for interacting with a specific set of our OAuth2-based APIs. For general info about CrowdStrike APIs, see CrowdStrike OAuth2-Based APIs, which covers these topics:

- Details on getting started, such as authentication and API scopes
- Domains used in base URLs by cloud
- Links to our Swagger API specification by cloud

Interact with hosts through Real Time Response

Use these APIs to run commands remotely on hosts using Real Time Response functionality. When you issue a command using these APIs, the command is first sent to the CrowdStrike cloud. The CrowdStrike cloud processes and orchestrates your command, then sends it to one or more hosts. For a list of available commands and usage information, see About Real Time Response.

Important: The RTR scope with read access gives you visibility into the full contents of any file or registry key, even the keys and files that contain credentials. Even read-only access to RTR API is equivalent to Domain Admin level access to any computer in your environment. The RTR API read access is scoped to the **RTR Read Only Analyst**, the least permissive RTR role.

Each command sent to hosts is processed as a "batch," even if you're targeting only a single host. Batches are an abstraction layer that handles components of the cloud-to-sensor communication for you: connection sessions, get requests, cloud requests, and sequence chunks.

To interact with hosts, specify one or more hosts by their host IDs. You can get host IDs from host management APIs or from the Falcon console.

Note: Actions taken in Real Time Response sessions are recorded. You can audit Real Time Response commands using our event streams APIs.

You can use the CrowdStrike API to perform these tasks related to Real Time Response:

- Send Real Time Response commands to a batch of hosts
- Send Real Time Response commands to a single host
- Manage Real Time Response scripts
- Manage Real Time Response files

Send Real Time Response commands to a batch of hosts

Use these APIs to run commands remotely on multiple hosts using Real Time Response functionality. For a list of available commands and usage information, see our full Real Time Response documentation.

To send commands to hosts, you first initialize a Real Time Response session. When you issue a command using these APIs, the command is first sent to the CrowdStrike cloud. The CrowdStrike cloud processes and orchestrates your command, then sends it to one or more hosts. Your session expires unless you send a keep-alive command around every 5 minutes.

As with Real Time Response sessions in the Falcon console, each API client can have only one active connection per host.

Relevant API endpoints

- POST /real-time-response/combined/batch-init-session/v1
- POST /real-time-response/combined/batch-command/v1
- POST /real-time-response/combined/batch-active-responder-command/v1
- POST /real-time-response/combined/batch-admin-command/v1
- POST /real-time-response/combined/batch-refresh-session/v1

Steps

1. Start a session with one or more hosts using `POST /real-time-response/combined/batch-init-session/v1`
2. Send commands to hosts using one of these API endpoints. The endpoint you use depends on your client's API scopes:

   Note: For the full list of available Real Time Response commands used in the `base_command` and `command_string` params, see Real Time Response commands.

   - Real Time Response scope with **read** access (equivalent to the role **RTR Read Only Analyst**):

     `POST /real-time-response/combined/batch-command/v1`

   - Real Time Response scope with **write** access (equivalent to the role **RTR Active Responder**):
     - `POST /real-time-response/combined/batch-active-responder-command/v1` for most commands
     - `POST /real-time-response/combined/batch-get-command/v1` for the Real Time Response GET command
   - Real Time Response (admin) scope with **write** access (equivalent to the role **RTR Administrator**):

     `POST /real-time-response/combined/batch-admin-command/v1`
3. Roughly every 5 minutes, refresh your Real Time Response session using `POST /real-time-response/combined/batch-refresh-session/v1`
4. For Real Time Response GET commands, check the status using `GET /real-time-response/combined/batch-get-command/v1`

Send Real Time Response commands to a single host

If you want more specific control over a Real Time Response session, connect directly to a single host rather than using "batch" connections. When you connect directly to a single host, you must handle some session management tasks that are automatically performed by the "batch" connection API endpoints. However, connecting to a single host can be useful for hosts with slow connections, because you can wait longer for responses, even after a "batch" command would automatically stop listening.

As with Real Time Response sessions in the Falcon console, each API client can have only one active connection per host.

Relevant API endpoints

- POST /real-time-response/entities/sessions/v1
- POST /real-time-response/entities/command/v1
- GET /real-time-response/entities/command/v1
- POST /real-time-response/entities/refresh-session/v1

Steps

1. Open a single-host session with `POST /real-time-response/entities/sessions/v1`. A successful response includes:
   - No error messages
   - A printed root-level directory, such as `C:\\`, in the `pwd` field for your host
   - A session ID you'll use to manage this session in further requests
   - All valid commands you can run with the `POST /real-time-response/entities/command/v1` request
2. Now that your session is active, run commands on your Real Time Response session:

   a. Run a command by using `POST /real-time-response/entities/command/v1`. The response includes a `cloud_request_id`.

b. Check the status of your command using `GET /real-time-response/entities/commands/v1`. In your GET request, provide the `cloud_request_id` from running the command and `sequence_id` starting with 0.

c. In the response, if the `complete` field is `false`, it means that you have not fully retrieved your response. Store the `sequence_id` from the response for your next GET request.

If the `sequence_id` in the response differs from the `sequence_id` that you requested, there is partial output that you should store. Make another `GET /real-time-response/entities/commands/v1` request. In your next GET request, provide the same `sequence_id` from the previous response.

Repeat these GET requests and combine their partial outputs until the `complete` indicator's value is `true`.

3. Every 5 minutes, make a `POST /real-time-response/entities/refresh-session/v1` request to keep your session active.

Note: As in the Falcon console, a Real Time Response session automatically ends after 10 minutes. We recommend sending a refresh request every 5 minutes to maintain your connection.

Manage Real Time Response scripts

With Real Time Response, you can create and save scripts for frequent use. First, upload the script to the CrowdStrike cloud, then run the script on hosts using the Real Time Response `runscript` command.

Your API client must have the **Real Time Response** scope with **write** access to manage or run scripts.

You can use the CrowdStrike API to perform these tasks related to Real Time Response scripts:

- Create a script
- Find and get details on an existing script
- Update an existing script
- Delete an existing script

Create a new Real Time Response script

Before you can run a script with Real Time Response commands, write your script locally and upload it to Falcon.

Relevant API endpoints

- POST /real-time-response/entities/scripts/v1
- POST /real-time-response/combined/batch-active-responder-command/v1

Steps

1. Create and test your script locally
2. Upload your script to Falcon using `POST /real-time-response/entities/scripts/v1`. You must specify:
    - `name`: Label for your script
    - `permission_type`: Sets permissions for users and API clients who can run this script
        - `private`: To run this script, users must have the **RTR Administrator** role. API clients must have the **Real Time Response (admin)** scope.
        - `group`: To run this script, users must have the **RTR Administrator** role. API clients must have the **Real Time Response (admin)** write scope.
        - `public`: To run this script, users must have the **RTR Administrator** or **RTR Active Responder** role. API clients must have the **Real Time Response (admin)** or **Real Time Response** write scope.
    - `content`: Contents of your PowerShell script
3. Run your script using `POST /real-time-response/combined/batch-active-responder-command/v1`, where the `base_command` parameter uses the `runscript` Real Time Response command

Find and get info on an existing Real Time Response script

Search your uploaded scripts using FQL filters. You can filter on any script attribute shown in the response of `POST /real-time-response/entities/scripts/v1`.

For more info about FQL filters, see our Falcon Query Language reference.

Relevant API endpoints

- GET /real-time-response/queries/scripts/v1
- GET /real-time-response/entities/scripts/v1

Steps

1. Find scripts using `GET /real-time-response/queries/scripts/v1`, which returns one or more script IDs
2. Provide script IDs to `GET /real-time-response/entities/scripts/v1` to get more detail on the scripts

Update an existing Real Time Response script

Replace an existing script with a modified version of that script. The script's contents and metadata can be updated, but its ID remains the same.

Relevant API endpoints

- PATCH /real-time-response/entities/scripts/v1

Steps

1. Find the ID of the script you want to update using `GET /real-time-response/queries/scripts/v1`
2. Upload a revised version of that script with `PATCH /real-time-response/entities/scripts/v1`. You must specify:
    - `name`: Label for your script
    - `permission_type`: Sets permissions for users and API clients who can run this script
        - `private`: To run this script, users must have the **RTR Administrator** role. API clients must have the **Real Time Response (admin)** scope.
        - `group`: To run this script, users must have the **RTR Administrator** role. API clients must have the **Real Time Response (admin)** write scope.
        - `public`: To run this script, users must have the **RTR Administrator** or **RTR Active Responder** role. API clients must have the **Real Time Response (admin)** or **Real Time Response** write scope.
    - `content`: Contents of your PowerShell script

Delete an existing Real Time Response script

Permanently delete an existing Real Time Response script.

Relevant API endpoints

- DELETE /real-time-response/entities/scripts/v1

Steps

1. Find the ID of the script you want to update using `GET /real-time-response/queries/scripts/v1`
2. Delete the script using `DELETE /real-time-response/entities/scripts/v1`

List Falcon script IDs

Get a list of Falcon script IDs. You can send your request with FQL filters to get IDs based on specific attributes. Successful requests return an HTTP 200 code and an array of Falcon script IDs that match the query criteria.

FQL Filters

Filter	Description	Example
`name`	The Falcon script name. Names are case sensitive. The full name must be provided exactly as it appears in the Falcon console	`filter=name:'FileInfo'`
`categories`	The Falcon script category. Available values: • `Troubleshooting` • `Asset reporting` • `Incident response`	`filter=categories:'Troubleshooting'`
`modified_timestamp`	The full ISO 8601 timestamp of when the script was last modified.	`filter=modified_timestamp:<'2023-09-12T03:00'`
`workflow_enabled`	A boolean that indicates that a script is available to use in Fusion SOAR workflows when set to `true`.	`filter=workflow_enabled:true`

Endpoint

`GET /real-time-response/queries/falcon-scripts/v1`

Required API client scope

Real Time Response Admin: write

Parameters

Name	In	Type	Description

`filter` *optional*	query	string	The FQL filter used to limit the results. For more info, see FQL Filters.
			Available filters:
			`name`
			`categories`
			`modified_timestamp`
			`workflow_enabled`

`sort` *optional*	query	string	The attribute and direction to order the result set.
			Available options:
			`name.asc` (default)
			`name.desc`
			`modified_timestamp.asc`
			`modified_timestamp.desc`

`offset` *optional*	query	integer	The zero-based position of the first record to return. Default value: 0
`limit` *optional*	query	integer	The maximum number of records to return. [1-500] Default value: 100

Example request

```
curl -X GET  'https://api.crowdstrike.com/real-time-response/queries/falcon-scripts/v1?filter=workflow_enabled:true&offset=1&limit=3&sort=name.desc' \
' \
-H 'Accept: application/json' \
-H 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response

```
{
    "meta": {
        "query_time": 0.009020794,
        "pagination": {
            "offset": 1,
            "limit": 3,
            "total": 3
        },
        "powered_by": "empower-api",
        "trace_id": "..."
    },
    "resources": [
        "0c6f9d2f84c343a19efbacfc9925f5ba",
        "e4621684265647efb0080e41ee97ffff",
        "1107d594cbc044f59e5d23180639e077"
    ]
}
```

Get Falcon script details by ID

Get detailed information for a specific Falcon script ID. Successful requests return an HTTP 200 code and a Falcon script object for each specified ID, listed in the order they were provided in the request.

Endpoint

```
GET /real-time-response/entities/falcon-scripts/v1
```

Required API client scope

Real Time Response Admin: write

Parameters

Name	In	Type	Description
`ids` *required*	query	string	The ID of the Falcon script to retrieve. Send multiple `ids` formatted as `ids=<a>&ids=<b>`.

Example request

```
curl -X GET  'https://api.crowdstrike.com/real-time-response/entities/falcon-scripts/v1?ids=0c6f9d2f84c343a19efbacfc9925f5ba&ids=1107d594cbc044f59e5d23180639e077'
\
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response


```
{
    "meta": {
        "query_time": 0.001455846,
        "powered_by": "empower-api",
        "trace_id": "..."
    },
    "resources": [
        {
            "id": "0c6f9d2f84c343a19efbacfc9925f5ba",
            "name": "RestorePoint",
            "description": "List available System Restore points",
            "use_case": "Useful during troubleshooting as system restore points can help roll back system files, program files, and registry information to a
previous state.",
            "categories": [
                "Asset reporting",
                "Troubleshooting"
            ],
            "access_roles": [
                "administrator"
            ],
            "sha256": "a3f045ebe70f803f12c031866fc342fc8d486e88fd5f45e23a92adbfb7ca5aa5",
            "size": 1791,
            "platform": "Windows",
            "content": "...",
            "created_by": "CrowdStrike",
            "created_timestamp": "2023-08-29T03:57:41Z",
            "modified_by": "CrowdStrike",
            "modified_timestamp": "2023-08-29T03:57:41Z",
            "revision": 0,
            "workflow_enabled": true,
            "workflow_input_schema": "...",
            "workflow_output_schema": "...",
            "is_disruptive": false,
            "modifies_system": false
        },
        {
            "id": "1107d594cbc044f59e5d23180639e077",
            "name": "Printer",
            "description": "List installed printers and any active print jobs",
            "use_case": "Useful for IT admins to understand what printers are connected to a host. Additionally,  printers serve as a data storehouses for
organizations and thus are an attractive first point of attack for attackers looking for a network foothold.",
            "categories": [
                "Asset reporting",
                "Troubleshooting"
            ],
            "access_roles": [
                "administrator"
            ],
            "sha256": "0104acf42dff7d1e0a7f304bd76bb15c99a190ea8d9185da2666927f2d8f5efc",
            "size": 1868,
            "platform": "Windows",
            "content": "...",
            "created_by": "CrowdStrike",
            "created_timestamp": "2023-08-29T03:57:41Z",
            "modified_by": "CrowdStrike",
            "modified_timestamp": "2023-08-29T03:57:41Z",
            "revision": 0,
            "workflow_enabled": true,
            "workflow_input_schema": "...",
            "workflow_output_schema": "...",
            "is_disruptive": false,
            "modifies_system": false
        }
```

```
    ]
}
```

Manage files sent through Real Time Response

With the Real Time Response "put" command, you can send files to hosts. First, you upload or update a file, then send files to hosts using the "put" command.

Your API client must have the **Real Time Response (admin)** scope with **write** access to manage "put" files.

You can use the CrowdStrike API to perform these tasks related to Real Time Response files:

- Create a file
- Find and get info on an existing file
- Update an existing file
- Delete an existing file

Create a new Real Time Response file

Before you can send files to hosts using Real Time Response's "put" command, upload the files to the CrowdStrike cloud.

Relevant API endpoints

- POST /real-time-response/entities/put-files/v1
- POST /real-time-response/combined/batch-active-responder-command/v1

1. Create or locate your file
2. Upload your file to the CrowdStrike cloud using `POST /real-time-response/entities/put-files/v1`. You must specify:
    - `name`: a label for your file (usually the filename)
    - `file`: the file you want to upload
3. Send your file from the CrowdStrike Cloud to your hosts, where the `base_command` parameter uses the `put` Real Time Response command

Find and get info on an existing Real Time Response file

Search your uploaded Real Time Response using FQL filters. You can filter on any script attribute shown in the response of `POST /real-time-response/entities/put-files/v1`.

For more info about FQL filters, see our Falcon Query Language reference.

Relevant API endpoints

- GET /real-time-response/queries/put-files/v1
- GET /real-time-response/entities/put-files/v1

Steps

1. Find files using `GET /real-time-response/queries/put-files/v1`, which returns one or more file IDs
2. Provide file IDs to `GET /real-time-response/entities/put-files/v1` to get more detail on the files

Delete an existing Real Time Response file

Permanently delete an existing Real Time Response "put" file.

Relevant API endpoints

- GET /real-time-response/queries/put-files/v1
- DELETE /real-time-response/entities/put-files/v1

Steps

1. Find the ID of the file you want to update using `GET /real-time-response/queries/put-files/v1`
2. Delete the file using `DELETE /real-time-response/entities/put-files/v1`

Get a list of files for a specific RTR session

Get a list of files along with upload progress for a specific RTR session ID. Use this request to retrieve files and monitor upload status when using the RTR `get` command in an active RTR session. Successful requests return a 200 OK and an array of file objects for the RTR session. Each file object in the response includes the following properties to help you track the progress, completion, and any errors of the file upload:

- Stage: Requested files are tracked through a series of upload and compression stages, such as `upload_requested` or `compression_in_progress`.
- Progress: The progression of each stage displays as a value between 0 and 1.
- Status: Additional details about the current stage to indicate what's happening with the upload (such as `ok`) or any problems that occur (such as `file_too_large`).

In sessions that contain multiple files, the files are uploaded one at a time. You can continue querying this endpoint to follow the progression of each file to completion.

Tip: Make a `GET` request to `real-time-response/queries/sessions/v1` to retrieve RTR session IDs.

Endpoint

```
GET /real-time-response/entities/file/v2
```

Required API client scope

real-time-response:write

Parameters

Name	Type	In	Description
`session_id` *required*	string	query	The unique RTR session ID to retrieve files for.

Example request

Get a list of file objects with upload status for RTR session ID `c95f7bd6-1f20-4e81-88fd-e9316e60ba5a6e6`.

```
curl --location --request GET 'https://api.crowdstrike.com/real-time-response/entities/file/v2?session_id=c95f7bd6-1f20-4e81-88fd-e9316e60ba5a6e6' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response on success (200)


```
{
   "meta": {
      "query_time": 0.049485415,
      "trace_id": "7d1519bb-8d4b-4f37-8734-ee8b59b9bb42"
   },
   "resources": [
      {
         "id": "04cd4670-89cd-4841-a99a-4259b7c1cbd1",
         "cloud_request_id": "04c7460d-89cd-4841-a99a-4259b7c1cbd1",
         "created_at": "2022-03-28T15:34:04Z",
         "updated_at": "2022-03-28T15:34:04Z",
         "deleted_at": null,
         "error_message": null,
         "name": "\\Device\\uxsvr\\Users\\csmith\\Desktop\\some.file",
         "progress": 1,
         "session_id": "c95f7bd6-1f20-4e81-88fd-e9316e60ba5a6e6",
         "sha256": "93b055a42522d9f0111baee587962ee08de50258627f5f3a7fb851877f5c4b55",
         "size": 51200,
         "stage": "compression_completed",
         "status": "ok",
         "complete": true
      },
      {
         "id": "4d4ab33e-852a-4ec4-9f79-c3fbdb4b52ef",
         "cloud_request_id": "4db334ae-852a-4ec4-9f79-c3dbfb4b52ef",
         "created_at": "2022-04-21T16:50:44Z",
         "updated_at": "2022-04-21T16:51:40Z",
         "deleted_at": null,
         "error_message": null,
         "name": "\\Device\\uxsvr\\Users\\csmith\\Desktop\\image.jpg",
         "progress": 0.14515188,
         "session_id": "c95f7bd6-1f20-4e81-88fd-e9316e60ba5a6e6",
         "sha256": "0494ccf4d3f285aa63f61170721d9e2001cc606ae29204f9ab5bbec746385b8c",
         "size": 256000000,
         "stage": "upload_in_progress",
         "status": "ok",
         "complete": false
      }
   ],
   "errors": []
}
```

Response fields (file object)

Name	Type	Description
`id`	string	The unique system-assigned ID of the file.
`cloud_request_id`	string	The ID of the specific RTR `get` command execution that was run to retrieve the session files.
`created_at`	string	The UTC date and time when the file was created.
`updated_at`	string	The UTC date and time when the file was last updated.
`deleted_at`	string	The UTC date and time when the file was manually deleted. If the file was not deleted, the value is **null**.
`error_message`	string	The message that displays if the upload fails. Otherwise, shows **null**.
`name`	string	The name of the file.
`progress`	float	The progress of the current `stage`, expressed as a float between 0 (started) and 1 (complete). Each stage resets the progress to 0.
`session_id`	string	The unique ID of the RTR session.
`sha256`	string	The SHA-256 hash of the file.
`size`	integer	The total size of the uploaded file in bytes.
`stage`	string	The stage that the file is in. Stages typically follow a sequence through upload and compression but can be skipped. Possible values: • upload_requested • upload_in_progress • upload_completed • compression_started • compression_in_progress • compression_completed
`status`	string	The status of the current `stage`. Possible values: • **ok:** No issues occurred. • **file_not_needed:** The upload has been rejected. Additional information is provided in the `error_message` field. • **file_too_large:** The file exceeds the maximum file size of 4GB. • **too_many_retries:** The maximum number of retry attempts (10) to upload the file was reached. • **feature_disabled:** The RTR feature is disabled on the account. • **permission_denied:** The user performing the RTR session does not have the permissions required to execute the RTR `get` command. • **retrying:** The system is making another attempt to upload the file. A maximum of 10 retries is allowed. • **error:** The upload failed due to an error. Additional information is provided in the `error_message` field. • **file_already_exists:**The file has already been uploaded. Previously uploaded files are not reprocessed and immediately show a `complete` value of **true**.
`complete`	boolean	Shows true when the `status` is **ok**, **file_not_needed**, or **file_already_exists** to indicate the upload is complete and the file is ready to download.

Delete an uploaded RTR file

Manually delete an uploaded RTR session file. Uploaded RTR files are stored in the CrowdStrike cloud for 7 days, but you can call this method to delete them sooner. This request takes the file ID and session ID returned in `GET /real-time-response/entities/file/v2` and returns an HTTP 204 status with no content in the response body.

Note: After deleting a file, you can make a `GET` request to `/real-time-response/entities/file/v2` with the session ID to confirm deletion. Deleted files show a timestamp value in the `deleted_at` field of the response.

Endpoint

```
DELETE /real-time-response/entities/file/v2
```

Required API client scope

real-time-response:write

Parameters

Name	Type	In	Description
`ids` *required*	string	query	The unique ID of the file to delete. Only one ID is supported per request.
`session_id` *required*	string	query	The unique RTR session ID that the file belongs to.

Example request

Delete a file with the file ID `04cd4670-89cd-4841-a99a-4259b7c1cbd1` and session ID `c95f7bd6-1f20-4e81-88fd-e9316e60ba5a6e6`.

```
curl --location --request DELETE 'https://api.crowdstrike.com/real-time-response/entities/file/v2?ids=04cd4670-89cd-4841-a99a-4259b7c1cbd1&session_id=c95f7bd6-1f20-4e81-88fd-e9316e60ba5a6e6' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response on success (204)

Successful requests return no content.

Real Time Response Policy APIs

Configure and manage policies governing real-time response capabilities and permissions.

About CrowdStrike APIs

CrowdStrike provides use cases and example requests and responses for interacting with a specific set of our OAuth2-based APIs. For general info about CrowdStrike APIs, see CrowdStrike OAuth2-Based APIs, which covers these topics:

- Details on getting started, such as authentication and API scopes
- Domains used in base URLs by cloud
- Links to our Swagger API specification by cloud

About Real Time Response

Real Time Response (RTR) allows you to directly access systems and run a variety of commands to perform many common response and remediation tasks on your remote hosts. If you're new to RTR you can familiarize yourself with the concepts, requirements, and more in our Real Time Response and Network Containment guide.

Understanding Real Time Response policies

Real Time Response uses policies that define which RTR commands can be executed on your Windows, macOS, or Linux hosts. A policy contains settings that you enable to allow certain response capabilities to be performed. For example, you might want to allow custom scripts to be run on some hosts while prohibiting file extraction. After a policy is created, you assign it to your host groups and enable it to apply the settings on the target hosts. Using the CrowdStrike API, you can configure and manage custom Real Time Response policies for different host groups to enable the right level of response action for your environment's security and compliance needs.

Real Time Response policy settings

Each real time response policy contains settings that describe the actions that can be performed on associated target hosts. These settings are disabled by default and can be enabled using the API to allow availability of the capability.

Enable/disable

Setting id	Capabilities when enabled
`RealTimeFunctionality`	This is the basic policy setting required to perform any Real Time Response actions on hosts. When enabled, it allows those with the Real Time Responder role to remotely connect to hosts. This setting must be enabled for all Real Time Responder commands and scripts to work as well as for partner software update policies.

Custom scripts

Setting id	Capabilities when enabled
`CustomScripts`	Allows those with RTR Active Responder and RTR Administrator roles to run custom scripts.

High risk commands

The settings in this category control the availability of commands that have a higher potential to cause problems if improperly executed.

Setting id	Capabilities when enabled
`GetCommand`	Extract files from a remote host using the CrowdStrike cloud.
`PutCommand`	Send files to a remote host using the CrowdStrike cloud. Required for partner software update policies.
`MemDumpCommand`	Dump process memory of a remote host.
`XMemDumpCommand`	Dump the complete memory of a remote host. (Windows only)
`ExecCommand`	Run any executable on the remote host. (Windows only)

Using Real Time Response APIs

API client requirements

To interact with the APIs covered in this guide, your API client credentials must have the following scopes enabled:

- Response Policies: read and write access
- Host Groups: read access

API clients are managed through Support and resources > Resources and tools > API clients and keys in the Falcon UI.

Example requests and responses

The examples provided in this document are designed as a reference to help you properly structure your requests and see what a successful response looks like. They do not use client information or valid account values. For request fields that require account-specific data (such as a policy ID or host group ID), replace the value given in the example with your own.

Examples in this guide use the base URL for US-1:

US-1: `https://api.crowdstrike.com`

If you use another CrowdStrike cloud environment, substitute the base URL in the examples with the one for your cloud:

- US-2: `https://api.us-2.crowdstrike.com`
- EU-1: `https://api.eu-1.crowdstrike.com`
- US-GOV-1: `https://api.laggar.gcw.crowdstrike.com`
- US-GOV-2: `https://api.us-gov-2.crowdstrike.mil`

Encoding URL string parameters

All string parameters containing non-ASCII characters set in the query part of a URL must be URL encoded.

Real Time Response policy object properties

Name	Description / Example
`name` string	The user-defined name of the policy. The name can contain lowercase and uppercase letters, numbers, spaces, and the special characters - _ : ; . !.
`description` string	A brief description of the policy.
`platform_name` string	The name of the operating system. Can be Windows, Mac, or Linux.
`enabled` boolean	Defines whether or not the RTR policy is in an enabled state. Either true (enabled) or false (disabled). By default, an RTR policy is turned off when it's created. This field is required to be set to true to perform any real time response action on hosts. Individual prevention-level settings in the policy can also be enabled, however they will not take effect if this field is not set to true.
`groups` array	An array with details about the host groups currently assigned to the policy. Each element in the array represents a separate host group.
`created_by` string	The user identification of the person who created the policy. This can be an email, username, or API client ID.
`created_timestamp` string	The date and time the policy was created in ISO 8601 format YYYY-MM-DDThh:mm:ss.sTZD.
`modified_by` string	The user identification of the person who modified the policy. This can be an email, username, or API client ID.
`modified_timestamp` string	The date and time the policy was last modified in ISO 8601 format YYYY-MM-DDThh:mm:ss.sTZD.
`settings` array	Policy settings that determine what response actions you want to allow users to perform on your hosts. Each element in the array represents a specific setting by id that can be enabled or disabled.
`settings.name` string	The name of the setting category. Category names are returned in the policy object but do not display in the UI. Available category names are Enable/Disable, Custom scripts, and High risk commands.
`settings.name.settings` array	The individual settings of each settings category. Each element in the array represents a different setting and contains a `name`, `id`, `type`, `description`, and `value`.
`settings.name.settings.name` string	The name of the setting. Setting names are returned in the policy object and also display to users in the UI.
`settings.name.settings.id` string	The ID of the setting. You enter the setting ID when you enable or disable the setting. The setting ID is returned in the policy object but is not visible in the UI to users. Available setting ID values include RealTimeFunctionality, CustomScripts, GetCommand, PutCommand, MemDumpCommand, XMemDumpCommand, and ExecCommand.
`settings.name.settings.description` string	The human readable description of the setting. This field is not configurable. It's returned in the policy object and also displays to users in the UI.

Name	Description / Example
`settings.name.settings.type` string	The type of UI component used to enable or disable the setting. All settings use a `"type": "toggle"` in the UI to turn the setting on or off.
`settings.name.settings.value` boolean	A boolean that indicates whether the setting is enabled or disabled (toggled on or off in the UI). Either `"enabled": true` or `"enabled": false`.

Other Real Time Response policy properties

Name	Description / Example
`action_name` string	The action to be performed on the response policy object. This parameter is provided in the query string to add/remove host groups or enable/disable the overall policy. Only one action is supported per request. Either add-host-group, remove-host-group, enable, or disable.
`action_parameters` array	An array of host group IDs to assign to or remove from the policy.
`action_parameters.name` string	The action parameter name used in the request body when adding or removing a host group from a policy. Must be group_id, entered in all lowercase letters.
`action_parameters.value` string	The unique ID of the host group to add to or remove from the policy. You can provide multiple host group IDs separated by commas to assign or remove more than one host group at a time.
`offset` integer	The zero-based position of the first record to return. The default is 0.
`limit` integer	The maximum number of records to return. The limit can range from 1–5000. The default is 100.

Policy search filters

In GET requests, you can pass a filter expression on the query string to limit the results. The `filter` field uses a standard set of enums appended with a free text value. Any value you add to an enum must be enclosed in single quotes and placed immediately after the colon with no space.

For greater granularity, you can use an operator to combine two filters or a filter and a sort option in a single request.

+ AND

The + (plus sign) can be used as an "and" operator between parameters to return policies where both values are present. For example, `filter=name:'test'+name:'policy'` returns policies with “test” and “policy” in the policy name.

, OR

A , (comma) can be used as an "or" operator between parameters to return policies where either value is found. For example,

`filter=name:'test',created_by:'diana.hudson'` returns any policy that contains “test” in the policy name or was created by the user “diana.hudson”.

& AND

An & (ampersand) can be used as an "and" operator between a filter and a sort parameter to return policies with the filter value in the specified sort order. For example, `filter=name:'test',created_by:'diana.hudson'&sort=created_timestamp.asc` returns policies with “test” in the policy name or that were created by “diana.hudson” in ascending order by date created.

Filter name	Description / Example
`created_by`	The username, email, or API client ID of the person who created the policy, as identified in the policy object. When specifying an email, the @ sign is not accepted. Enter the email username or the domain as the value. For example, to filter on policies created by the email address diana.hudson@email.com: `filter=created_by:'diana.hudson'` (correct) `filter=created_by:'email.com'` (correct)

Filter name	Description / Example
	`filter=created_by:'diana.hudson@email.com'` (incorrect) `filter=created_by:'diana'` (incorrect) Enter only the alphanumeric ID when providing an API client ID. For example, to filter on api-client-id:7a1284d634af196bff5988fb1775721b: `filter=created_by:'7a1284d634af196bff5988fb1775721b'` (correct) `filter=created_by:'api-client-id:7a1284d634af196bff5988fb1775721b'` (incorrect) `filter=created_by:'api-client-id'` (incorrect)
`created_timestamp`	The full timestamp of when the policy was created in ISO 8601 format. (YYYY-MM-DDTHH:mm:ss.sssZ) The timezone is always UTC as denoted by the suffix "Z". `filter=created_timestamp:'2020-11-23T19:36:24.129652084Z'`
`description`	Search for a term found in the policy description. The value must be entered in lowercase letters. `filter=description:'policy'`
`enabled`	Find policies by their enabled status. Use true to find enabled policies or false to find disabled policies. `filter=enabled:'true'`
`groups`	Enter a host group ID to find the policy it's been assigned to. `filter=groups:'1ef31aa47604b90a9aa1d38a7c35b0fe'`
`modified_by`	The username, email, or API client ID of the person who modified the policy, as identified in the policy object. Values for this field follow the same rules as the `created_by` filter.
`modified_timestamp`	The full timestamp of when the policy was modified in ISO 8601 format. (YYYY-MM-DDTHH:mm:ss. sssZ) The timezone is always UTC as denoted by the suffix "Z". Values for this field follow the same rules as the `created_timestamp` filter.
`name`	Performs a free text search on single words found in a policy name. Values must be entered as lowercase and enclosed in single quotes. You can provide multiple name values separated by an &. `filter=name:'test'`
`name.raw`	Filters on exact matches to the full policy name. Searches on this field are case sensitive and require the correct input of capital and lowercase letters. `filter=name.raw:'Test RTR Policy 1'`
`platform_name`	The name of the operating system listed in the policy. `filter=platform_name:'Windows'`

Policy sort options

The `sort` parameter is a string that defines the criteria for ordering the result set in `GET` requests. This field uses a standard list of enum values in ascending and descending order. Ascending order arranges policies with the smallest/oldest/earliest at the top of the list, while descending places the largest/newest/last policy at the top. Only one `sort` value can be used in a request at a time, however requests that accept this parameter support combining it with a `filter` using the & operator.

Sort name	Description / Example
`created_by.asc`	Lists policies in ascending order by the `created_by` field. `sort=created_by.asc`
`created_by.desc`	Lists policies in descending order by the `created_by` field. `sort=created_by.desc`
`created_timestamp.asc`	Lists policies in ascending order by the `created_timestamp` field. `sort=created_timestamp.asc`

Sort name	Description / Example
`created_timestamp.desc`	Lists policies in descending order by the `created_timestamp` field. `sort=created_timestamp.desc`
`enabled.asc`	Lists policies in ascending order by the `enabled` field with disabled (`false`) policies appearing first. `sort=enabled.asc`
`enabled.desc`	Lists policies in descending order by the `enabled` field with enabled (`true`) policies appearing first. `sort=enabled.desc`
`modified_by.asc`	Lists policies in ascending order by the `modified_by` field. `sort=modified_by.asc`
`modified_by.desc`	Lists policies in descending order by the `modified_by` field. `sort=modified_by.desc`
`modified_timestamp.asc`	Lists policies in ascending order by the `modified_timestamp` field. `sort=modified_timestamp.asc`
`modified_timestamp.desc`	Lists policies in descending order by the `modified_timestamp` field. `sort=modified_timestamp.desc`
`name.asc`	Lists policies in ascending order by the `name` field. `sort=name.asc`
`name.desc`	Lists policies in descending order by the `name` field. `sort=name.desc`
`platform_name.asc`	Lists policies in ascending order by the `platform_name` field. `sort=platform_name.asc`
`platform_name.desc`	Lists policies in descending order by the `platform_name` field. `sort=platform_name.desc`
`precedence.asc`	Lists policies in ascending order according to the policy `precedence`. `sort=precedence.asc`
`precedence.desc`	Lists policies in descending order according to the policy `precedence`. `sort=precedence.desc`

HTTP response codes

The Real Time Response API uses the HTTP status codes below to indicate the success or failure of API requests.

HTTP code	Description
`200 OK`	The request was completed without any issues or errors.
`201 Created`	The request was completed without any issues or errors.
`400 Bad Request`	The request contains one or more errors and could not be processed.

HTTP code	Description
`401 Unauthorized`	Access token is missing or invalid.
`403 Forbidden`	The access token does not have permissions to perform the request.
`404 Not Found`	The resource could not be found.
`429 Too Many Requests`	The allowed rate limit has been reached.
`500 Internal Server Error`	The server encountered an unexpected error that prevented your request from being completed.

Workflow for creating a Real Time Response policy

We recommend the following workflow for creating and applying Real Time Response policies using the CrowdStrike API:

- Step 1. Create a new policy: Create a new policy with default settings.
- Step 2. Enable the policy settings: Enable settings in the policy to allow Real Time Response actions.
- Step 3. Assign host groups to the policy: Assign the host groups where you want the response policy settings to be applied.
- Step 4. Enable the policy: Turn the policy on to enable response actions on the target hosts.

Step 1. Create a new policy

Create a new Real Time Response policy with default settings. Successful requests return an HTTP 201 code and a Real Time Response policy object. The object that is created contains details about the policy including a unique policy `id` that you use in subsequent calls and various `settings` that you enable in the next step.

Endpoint

`POST /policy/entities/response/v1`

Parameters

Name	Description
`name` required	The user-defined name of the policy. Lowercase and uppercase letters, numbers, spaces, and the special characters - _ : ; . ! are allowed.
`description` optional	A brief description of the policy.
`platform_name` required	The operating system name. One of **Windows**, **Mac**, or **Linux**. Enter the value as shown with the first letter capitalized.

Example request

```
curl --location --request POST 'https://api.crowdstrike.com/policy/entities/response/v1' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI' \
--data-raw '{
 "resources": [
  {
   "name": "Test RTR Policy 2",
   "description": "Short description of test RTR policy 2.",
   "platform_name": "Windows"
  }
 ]
}'
```

Example response


```
{
 "meta": {
  "query_time": 0.288187594,
  "trace_id": "67fdc91a-9818-4e34-94bb-08bd1157031e"
 },
 "errors": null,
 "resources": [
  {
   "id": "6f32f2941b1a4fdc9931053e4cc9e76feb",
   "name": "Test RTR Policy 2",
   "description": "Short description of test RTR Policy 2.",
   "platform_name": "Windows",
   "groups": [],
   "enabled": false,
   "created_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
   "created_timestamp": "2021-04-09T23:44:53.211690986Z",
   "modified_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
   "modified_timestamp": "2021-04-09T23:44:53.211690986Z",
   "prevention_settings": [
    {
     "name": "Enable/Disable",
     "settings": [
      {
       "id": "RealTimeFunctionality",
       "name": "Real Time Response",
       "type": "toggle",
       "description": "Allow those with Real Time Responder roles to remotely connect to hosts. Required for all RTR commands and scripts and for partner software
update policies.",
       "value": {
        "enabled": false
       }
      }
     ]
    },
    {
     "name": "Custom scripts",
     "settings": [
      {
       "id": "CustomScripts",
       "name": "Custom Scripts",
       "type": "toggle",
       "description": "Allows those with RTR Active Responder and RTR Administrator roles to run custom scripts",
       "value": {
        "enabled": false
       }
      }
     ]
    },
    {
     "name": "High risk commands",
     "settings": [
      {
       "id": "GetCommand",
       "name": "get",
       "type": "toggle",
       "description": "Extract files from a remote host via the CrowdStrike cloud",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "PutCommand",
       "name": "put",
       "type": "toggle",
       "description": "Send files to a remote host via the CrowdStrike cloud. Required for partner software update policies",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "MemDumpCommand",
       "name": "memdump",
       "type": "toggle",
       "description": "Dump process memory of a remote host",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "XMemDumpCommand",
       "name": "xmemdump",
       "type": "toggle",
       "description": "Dump the complete memory of a remote host",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "ExecCommand",
       "name": "run",
       "type": "toggle",
       "description": "Run any executable on the remote host",
```

```
      "value": {
       "enabled": false
      }
     }
    ]
   }
  ]
 }
}
```

Step 2. Enable the policy settings

Adjust the settings in the policy based on how you want it to function. By default, your policy was created with all response settings turned off. You use this request to enable the settings for the Real Time Response actions you want to be allowed to execute on your hosts. Only the settings you wish to enable need to be provided in the request. Settings not specified will remain unchanged. Successful requests return an HTTP 200 code along with the full updated policy details in the response.

Endpoint

`PATCH /policies/entities/response/v1`

Parameters

Name	In	Description
`id` required	body	The unique ID of the Real Time Response policy.
`settings` required	body	An array of policy actions to be enabled. Each element in the array contains an `id` and a `value` that determines whether the setting is `enabled`.
`settings. id` required	body	The ID of the setting. Any of **GetCommand**, **PutCommand**, **MemDumpCommand**, **XMemDumpCommand** (Windows only), and **ExecCommand** (Windows only). Enter values exactly as shown. See the policy settings section for more information about individual settings. `"id": "PutCommand"`

`settings.value.enabled`
required
	body	Determines whether the command capabilities are turned on or off. Either **true** for enabled or **false** for disabled.
		`"value": {`
		`"enabled": true`
		`}`

Example request

```
curl --location --request PATCH 'https://api.crowdstrike.com/policy/entities/response/v1' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI' \
--data-raw '{
 "resources": [
  {
   "id": "6f32f2941b1a4fdc9931053e4cc9e76feb",
   "settings": [
    {
     "id": "RealTimeFunctionality",
     "value": {
      "enabled": true
     }
    },
    {
     "id": "CustomScripts",
     "value": {
      "enabled": true
     }
    },
    {
     "id": "GetCommand",
     "value": {
      "enabled": true
     }
    },
    {
     "id": "ExecCommand",
     "value": {
      "enabled": true
```

```
     }
    }
   ]
  }
 ]
}'
```

Example response


```
{
 "meta": {
  "query_time": 2.523455712,
  "trace_id": "04c5993b-9c31-452e-86d3-284f6d34c8e9"
 },
 "errors": null,
 "resources": [
  {
   "id": "6f32f2941b1a4fdc9931053e4cc9e76feb",
   "name": "Test RTR Policy 2",
   "description": "Short description of test RTR Policy 2.",
   "platform_name": "Windows",
   "groups": [],
   "enabled": false,
   "created_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
   "created_timestamp": "2021-04-09T23:44:53.211690986Z",
   "modified_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
   "modified_timestamp": "2021-04-09T23:53:01.441196891Z",
   "prevention_settings": [
    {
     "name": "Enable/Disable",
     "settings": [
      {
       "id": "RealTimeFunctionality",
       "name": "Real Time Response",
       "type": "toggle",
       "description": "Allow those with Real Time Responder roles to remotely connect to hosts. Required for all RTR commands and scripts and for partner software
update policies.",
       "value": {
        "enabled": true
       }
      }
     ]
    },
    {
     "name": "Custom scripts",
     "settings": [
      {
       "id": "CustomScripts",
       "name": "Custom Scripts",
       "type": "toggle",
       "description": "Allows those with RTR Active Responder and RTR Administrator roles to run custom scripts",
       "value": {
        "enabled": true
       }
      }
     ]
    },
    {
     "name": "High risk commands",
     "settings": [
      {
       "id": "GetCommand",
       "name": "get",
       "type": "toggle",
       "description": "Extract files from a remote host via the CrowdStrike cloud",
       "value": {
        "enabled": true
       }
      },
      {
       "id": "PutCommand",
       "name": "put",
       "type": "toggle",
       "description": "Send files to a remote host via the CrowdStrike cloud. Required for partner software update policies",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "MemDumpCommand",
       "name": "memdump",
       "type": "toggle",
       "description": "Dump process memory of a remote host",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "XMemDumpCommand",
       "name": "xmemdump",
       "type": "toggle",
```

```
       "description": "Dump the complete memory of a remote host",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "ExecCommand",
       "name": "run",
       "type": "toggle",
       "description": "Run any executable on the remote host",
       "value": {
        "enabled": true
       }
      }
     ]
    }
   ]
  }
 ]
}
```

Step 3. Assign host groups to the policy

Assign the host groups to the policy that you would like the response policy settings to apply to. To run this request, send the `action_name` parameter in the query string with the value `add-host-group`. In the body of the request, pass the unique Real Time Response policy `id` along with the ID of each host group you want to assign to the policy. You can retrieve a list of host group IDs for your environment using the `GET /devices/queries/host-groups/v1` endpoint. Successful requests return an HTTP 200 code with an array of host group details in the response.

Note:

- This request can also be used to remove host groups from a policy. Pass `remove-host-group` as the `action_name` value in the query string.
- Every host in your environment must be associated with a Real Time Response policy through a host group. Any host that is not assigned to a policy is placed in the default policy, which has all settings enabled except `CustomScripts` and `ExecCommand`. Only one policy should be associated with a host to eliminate conflicting response actions. If a host belongs to multiple host groups, which results in the host being assigned to more than one policy, the policy with the highest precedence that matches the host is applied.

Endpoint

`POST /policies/entities/response-actions/v1`

Parameters

Name	In	Description
`action_name` required	query	The action to be performed. Use add-host-group, entered in all lowercase letters. `/policy/entities/response-actions/v1?action_name=add-host-group`

`ids`
required
	body	The unique ID of the Real Time Response policy to assign the host group to.
		`"ids": [`
		`"6f32f2941b1a4fdc9931053e4cc9e7eb"`
		`]`

`action_parameters` required	body	The host group details to assign to the policy.
`action_parameters.name` required	body	The action parameter name. Must be group_id, entered in all lowercase letters. `"name": "group_id"`
`action_parameters.value` required	body	The unique ID of the host group to add to the policy. You can enter multiple host group IDs separated by commas to assign more than one host group to the policy. `"value": "1c0555a4e4617b0394989d93bf119dad"`

Example request

```
curl --location --request POST 'https://api.crowdstrike.com/policy/entities/response-actions/v1?action_name=add-host-group' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI' \
--data-raw '{
 "ids": [
  "6f32f2941b1a4fdc9931053e4cc9e7eb"
```

```
 ],
 "action_parameters": [
  {
   "name": "group_id",
   "value": "1c0555a4e4617b0394989d93bf119dad"
  }
 ]
}'
```

Example response


```
{
 "meta": {
  "query_time": 0.150144869,
  "trace_id": "f297961e-039b-49a9-88fc-207d5571cbf4"
 },
 "errors": null,
 "resources": [
  {
   "id": "6f32f2941b1a4fdc9931053e4cc9e76feb",
   "name": "Test RTR Policy 2",
   "description": "Short description of test RTR Policy 2.",
   "platform_name": "Windows",
   "groups": [
    {
     "id": "1c0555a4e4617b0394989d93bf119dad",
     "group_type": "static",
     "name": "Host group 2",
     "description": "Short description of host group 2.",
     "created_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
     "created_timestamp": "2021-03-09T16:06:07.021541506Z",
     "modified_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
     "modified_timestamp": "2021-03-09T16:06:07.021541506Z"
    }
   ],
   "enabled": false,
   "created_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
   "created_timestamp": "2021-04-09T23:44:53.211690986Z",
   "modified_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
   "modified_timestamp": "2021-04-09T23:55:32.634907231Z",
   "prevention_settings": [
    {
     "name": "Enable/Disable",
     "settings": [
      {
       "id": "RealTimeFunctionality",
       "name": "Real Time Response",
       "type": "toggle",
       "description": "Allow those with Real Time Responder roles to remotely connect to hosts. Required for all RTR commands and scripts and for partner software
update policies.",
       "value": {
        "enabled": true
       }
      }
     ]
    },
    {
     "name": "Custom scripts",
     "settings": [
      {
       "id": "CustomScripts",
       "name": "Custom Scripts",
       "type": "toggle",
       "description": "Allows those with RTR Active Responder and RTR Administrator roles to run custom scripts",
       "value": {
        "enabled": true
       }
      }
     ]
    },
    {
     "name": "High risk commands",
     "settings": [
      {
       "id": "GetCommand",
       "name": "get",
       "type": "toggle",
       "description": "Extract files from a remote host via the CrowdStrike cloud",
       "value": {
        "enabled": true
       }
      },
      {
       "id": "PutCommand",
       "name": "put",
       "type": "toggle",
       "description": "Send files to a remote host via the CrowdStrike cloud. Required for partner software update policies",
       "value": {
        "enabled": false
       }
      },
```

```
      {
       "id": "MemDumpCommand",
       "name": "memdump",
       "type": "toggle",
       "description": "Dump process memory of a remote host",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "XMemDumpCommand",
       "name": "xmemdump",
       "type": "toggle",
       "description": "Dump the complete memory of a remote host",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "ExecCommand",
       "name": "run",
       "type": "toggle",
       "description": "Run any executable on the remote host",
       "value": {
        "enabled": true
       }
      }
     ]
    }
   ]
  }
 ]
}
```

Step 4. Enable the policy

After host groups are assigned to your policy, the final step is to turn the policy on so that response actions can be performed on the target hosts. To run this request, send the `action_name` parameter in the query string with the value `enable`, and pass the Real Time Response policy `id` in the body of your request. Successful requests return an HTTP 200 code and the full policy details with the `enabled` attribute for the policy set to `true` in the response.

Note:

- This request can also be used to disable a policy. Pass `disable` as the `action_name` value in the query string.
- Although this request uses the same endpoint as the previous step for assigning host groups, the two steps cannot be combined. Only one `action_name` is allowed per request, so the steps must be completed separately.

Endpoint

```
POST /policies/entities/response-actions/v1
```

Parameters

Name	In	Description
`action_name` required	query	The action to be performed. Use enable, entered in all lowercase letters. `/policy/entities/response-actions/v1?action_name=enable`

`ids`
required
	body	The unique ID of the Real Time Response policy you want to enable. This request supports multiple policy IDs separated by commas if you wish to enable more than one policy.
		`"ids": [`
		`"6f32f2941b1a4fdc9931053e4cc9e76feb"`
		`]`

Example request

```
curl --location -g --request POST 'https://api.crowdstrike.com/policy/entities/response-actions/v1?action_name=enable' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI' \
--data-raw '{
 "ids": [
  "6f32f2941b1a4fdc9931053e4cc9e76feb"
 ]
}'
```

Example response


```
{
 "meta": {
  "query_time": 0.148683025,
  "trace_id": "d54915e0-5b71-443c-a10d-8527b33cf013"
 },
 "errors": null,
 "resources": [
  {
   "id": "6f32f2941b1a4fdc9931053e4cc9e76feb",
   "name": "Test RTR Policy 2",
   "description": "Short description of test RTR Policy 2.",
   "platform_name": "Windows",
   "groups": [
    {
     "id": "1c0555a4e4617b0394989d93bf119dad",
     "group_type": "static",
     "name": "Host group 2",
     "description": "Short description of host group 2.",
     "created_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
     "created_timestamp": "2021-03-09T16:06:07.021541506Z",
     "modified_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
     "modified_timestamp": "2021-03-09T16:06:07.021541506Z"
    }
   ],
   "enabled": true,
   "created_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
   "created_timestamp": "2021-04-09T23:44:53.211690986Z",
   "modified_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
   "modified_timestamp": "2021-04-09T23:57:44.693756296Z",
   "prevention_settings": [
    {
     "name": "Enable/Disable",
     "settings": [
      {
       "id": "RealTimeFunctionality",
       "name": "Real Time Response",
       "type": "toggle",
       "description": "Allow those with Real Time Responder roles to remotely connect to hosts. Required for all RTR commands and scripts and for partner software
update policies.",
       "value": {
        "enabled": true
       }
      }
     ]
    },
    {
     "name": "Custom scripts",
     "settings": [
      {
       "id": "CustomScripts",
       "name": "Custom Scripts",
       "type": "toggle",
       "description": "Allows those with RTR Active Responder and RTR Administrator roles to run custom scripts",
       "value": {
        "enabled": true
       }
      }
     ]
    },
    {
     "name": "High risk commands",
     "settings": [
      {
       "id": "GetCommand",
       "name": "get",
       "type": "toggle",
       "description": "Extract files from a remote host via the CrowdStrike cloud",
       "value": {
        "enabled": true
       }
      },
      {
       "id": "PutCommand",
       "name": "put",
       "type": "toggle",
       "description": "Send files to a remote host via the CrowdStrike cloud. Required for partner software update policies",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "MemDumpCommand",
       "name": "memdump",
       "type": "toggle",
       "description": "Dump process memory of a remote host",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "XMemDumpCommand",
       "name": "xmemdump",
```

```
       "type": "toggle",
       "description": "Dump the complete memory of a remote host",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "ExecCommand",
       "name": "run",
       "type": "toggle",
       "description": "Run any executable on the remote host",
       "value": {
        "enabled": true
       }
      }
     ]
    }
   ]
  }
 ]
}
```


Additional Real Time Response policy endpoints

The following additional endpoints are available to help you manage your Real Time Response policies.

List Real Time Response policies

Get a list of Real Time Response policy objects. You can send your request without parameters to retrieve all RTR policies in your environment, listed chronologically by date created in ascending order. Optionally, provide an FQL filter to narrow your results or a sort parameter to change the order in which the result set displays. Successful requests return an HTTP 200 code and an array of response policy objects that match the query criteria.

Endpoint

```
GET /policy/combined/response/v1
```

Parameters

Name	In	Description
`offset` optional	query	The zero-based position of the first record to return. The default is 0.
`limit` optional	query	The maximum number of records to return. The limit can range from 1–5000. The default is 100.
`filter` optional	query	The FQL filter expression used to limit the results. See the policy search filters section for more info. One of: created_by created_timestamp description enabled groups modified_by modified_timestamp name name.raw platform_name
`sort` optional	query	The policy property used to sort the results. See the policy sort options section for more info. One of: created_by.asc created_by.desc created_timestamp.asc created_timestamp.desc enabled.asc enabled.desc

Name	In	Description
		modified_by.asc modified_by.desc modified_timestamp.asc modified_timestamp.desc name.ascname.desc platform_name.asc platform_name.desc precedence.asc precedence.desc

Example request

The following request uses the `filter` and sort `parameters` to find policies with the word “test” in the `name` and order them by `modified_timestamp.asc`.

```
curl --location --request GET 'https://api.crowdstrike.com/policy/combined/response/v1?filter=name:%27test%27&sort=modified_timestamp.asc' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response


```
{
 "meta": {
  "query_time": 0.177423432,
  "pagination": {
   "offset": 0,
   "limit": 100,
   "total": 2
  },
  "trace_id": "ba31f8ed-3c43-4ce8-bd4a-7cfdbd389ddc"
 },
 "errors": [],
 "resources": [
  {
   "id": "ac94220a34e92b760d2ffb3a74991bb0",
   "name": "Test RTR Policy 1",
   "description": "Short description of test RTR Policy 1.",
   "platform_name": "Windows",
   "groups": [
    {
     "id": "167a006f481f9d6deb5e8ca38b27dadb",
     "group_type": "static",
     "name": "Host group 1",
     "description": "Short description of host group 1.",
     "created_by": "owen.dalton@email.com",
     "created_timestamp": "2020-12-02T16:53:18.436653214Z",
     "modified_by": "owen.dalton@email.com",
     "modified_timestamp": "2020-12-02T16:53:18.436653214Z"
    }
   ],
   "enabled": true,
   "created_by": "diana.hudson@email.com",
   "created_timestamp": "2021-04-08T20:11:45.920545088Z",
   "modified_by": "alison.brown@email.com",
   "modified_timestamp": "2021-04-09T00:36:27.87179559Z",
   "prevention_settings": [
    {
     "name": "Enable/Disable",
     "settings": [
      {
       "id": "RealTimeFunctionality",
       "name": "Real Time Response",
       "type": "toggle",
       "description": "Allow those with Real Time Responder roles to remotely connect to hosts. Required for all RTR commands and scripts and for partner software
update policies.",
       "value": {
        "enabled": true
       }
      }
     ]
    },
    {
     "name": "Custom scripts",
     "settings": [
      {
       "id": "CustomScripts",
       "name": "Custom Scripts",
       "type": "toggle",
       "description": "Allows those with RTR Active Responder and RTR Administrator roles to run custom scripts",
       "value": {
```

```
        "enabled": false
       }
      }
     ]
    },
    {
     "name": "High risk commands",
     "settings": [
      {
       "id": "GetCommand",
       "name": "get",
       "type": "toggle",
       "description": "Extract files from a remote host via the CrowdStrike cloud",
       "value": {
        "enabled": true
       }
      },
      {
       "id": "PutCommand",
       "name": "put",
       "type": "toggle",
       "description": "Send files to a remote host via the CrowdStrike cloud. Required for partner software update policies",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "MemDumpCommand",
       "name": "memdump",
       "type": "toggle",
       "description": "Dump process memory of a remote host",
       "value": {
        "enabled": true
       }
      },
      {
       "id": "XMemDumpCommand",
       "name": "xmemdump",
       "type": "toggle",
       "description": "Dump the complete memory of a remote host",
       "value": {
        "enabled": true
       }
      },
      {
       "id": "ExecCommand",
       "name": "run",
       "type": "toggle",
       "description": "Run any executable on the remote host",
       "value": {
        "enabled": true
       }
      }
     ]
    }
   ]
  },
  {
   "id": "6f32f2941b1a4fdc9931053e4cc9e76feb",
   "name": "Test RTR Policy 2",
   "description": "Short description of test RTR Policy 2.",
   "platform_name": "Windows",
   "groups": [
    {
     "id": "1c0555a4e4617b0394989d93bf119dad",
     "group_type": "static",
     "name": "Host group 2",
     "description": "Short description of host group 2.",
     "created_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
     "created_timestamp": "2021-03-09T16:06:07.021541506Z",
     "modified_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
     "modified_timestamp": "2021-03-09T16:06:07.021541506Z"
    }
   ],
   "enabled": true,
   "created_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
   "created_timestamp": "2021-04-09T23:44:53.211690986Z",
   "modified_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
   "modified_timestamp": "2021-04-09T23:57:44.693756296Z",
   "prevention_settings": [
    {
     "name": "Enable/Disable",
     "settings": [
      {
       "id": "RealTimeFunctionality",
       "name": "Real Time Response",
       "type": "toggle",
       "description": "Allow those with Real Time Responder roles to remotely connect to hosts. Required for all RTR commands and scripts and for partner software
update policies.",
       "value": {
        "enabled": true
       }
      }
     ]
```

```
    },
    {
     "name": "Custom scripts",
     "settings": [
      {
       "id": "CustomScripts",
       "name": "Custom Scripts",
       "type": "toggle",
       "description": "Allows those with RTR Active Responder and RTR Administrator roles to run custom scripts",
       "value": {
        "enabled": true
       }
      }
     ]
    },
    {
     "name": "High risk commands",
     "settings": [
      {
       "id": "GetCommand",
       "name": "get",
       "type": "toggle",
       "description": "Extract files from a remote host via the CrowdStrike cloud",
       "value": {
        "enabled": true
       }
      },
      {
       "id": "PutCommand",
       "name": "put",
       "type": "toggle",
       "description": "Send files to a remote host via the CrowdStrike cloud. Required for partner software update policies",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "MemDumpCommand",
       "name": "memdump",
       "type": "toggle",
       "description": "Dump process memory of a remote host",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "XMemDumpCommand",
       "name": "xmemdump",
       "type": "toggle",
       "description": "Dump the complete memory of a remote host",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "ExecCommand",
       "name": "run",
       "type": "toggle",
       "description": "Run any executable on the remote host",
       "value": {
        "enabled": true
       }
      }
     ]
    }
   ]
  }
 ]
}
```


List Real Time Response policy IDs

Get a list of Real Time Response policy IDs. You can send your request without any parameters to retrieve all response policy IDs in your environment, listed chronologically by date created in ascending order. Optionally, provide an FQL filter to narrow your results or a sort parameter to change the order in which the result set displays. Successful requests return an HTTP 200 code and an array of Real Time Response policy IDs that match the query criteria in the response.

Endpoint

```
GET /policy/queries/response/v1
```

Parameters

Name	In	Description
`offset` optional	query	The zero-based position of the first record to return. The default is 0.
`limit` optional	query	The maximum number of records to return. The limit can range from 1–5000. The default is 100.
`filter` optional	query	The FQL filter expression used to limit the results. See the policy search filters section for more info. One of: created_by created_timestamp description enabled groups modified_by modified_timestamp name name.raw platform_name
`sort` optional	query	The policy property used to sort the results. See the policy sort options section for more info. One of: created_by.asc created_by.desc created_timestamp.asc created_timestamp.desc enabled.asc enabled.desc modified_by.asc modified_by.desc modified_timestamp.asc modified_timestamp.desc name.asc name.desc platform_name.asc platform_name.desc precedence.asc precedence.desc

Example request

The following request uses the `filter` and `sort` parameters to find policy IDs `created_by` “diana.hudson” and order them by `name.desc`.

```
curl --location --request GET 'https://api.crowdstrike.com/policy/queries/response/v1?filter=created_by:%27diana.hudson%27&sort=name.desc' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response

```
{
 "meta": {
  "query_time": 0.022235996,
  "pagination": {
   "offset": 0,
   "limit": 100,
   "total": 2
```

```
  },
  "trace_id": "303d0fd9-9af6-4fa5-8468-9087eca5b11e"
 },
 "resources": [
  "ac94220a34e92b760d2ffb3a74991bb0",
  "1697fdac4ed4d0886a774b013e516e0d"
 ],
 "errors": []
}
```


Retrieve specific Real Time Response policies by ID

Retrieve the details of one or more Real Time Response policies by specifying the unique policy IDs. Successful requests return an HTTP 200 code and an array of response policy objects in the response that match the specified IDs in the order submitted in the request.

Endpoint

```
GET /policy/entities/response/v1
```

Parameters

Name	In	Description
`ids` required	query	The unique ID of the Real Time Response policy. Multiple IDs can be entered using the syntax `ids={a}&ids={b}`.

Example request

The following request searches for two Real Time Response policies by policy ID number.

```
curl --location --request GET 'https://api.crowdstrike.com/policy/entities/response/v1?
ids=ac94220a34e92b760d2ffb3a74991bb0&ids=6f32f2941b1a4fdc9931053e4cc9e7eb' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response


```
{
 "meta": {
  "query_time": 0.593934569,
  "trace_id": "759a9f15-ccf4-4752-8c2f-c4f486097138"
 },
 "errors": [],
 "resources": [
  {
   "id": "ac94220a34e92b760d2ffb3a74991bb0",
   "name": "Test RTR Policy 1",
   "description": "Short description of test RTR Policy 1.",
   "platform_name": "Windows",
   "groups": [
    {
     "id": "167a006f481f9d6deb5e8ca38b27dadb",
     "group_type": "static",
     "name": "Host group 1",
     "description": "Short description of host group 1.",
     "created_by": "owen.dalton@email.com",
     "created_timestamp": "2020-12-02T16:53:18.436653214Z",
     "modified_by": "owen.dalton@email.com",
     "modified_timestamp": "2020-12-02T16:53:18.436653214Z"
    }
   ],
   "enabled": true,
   "created_by": "diana.hudson@email.com",
   "created_timestamp": "2021-04-08T20:11:45.920545088Z",
   "modified_by": "alison.brown@email.com",
   "modified_timestamp": "2021-04-09T00:36:27.87179559Z",
   "prevention_settings": [
    {
     "name": "Enable/Disable",
     "settings": [
      {
       "id": "RealTimeFunctionality",
       "name": "Real Time Response",
       "type": "toggle",
       "description": "Allow those with Real Time Responder roles to remotely connect to hosts. Required for all RTR commands and scripts and for partner software
update policies.",
       "value": {
        "enabled": true
       }
      }
```

```
    ]
   },
   {
    "name": "Custom scripts",
    "settings": [
     {
      "id": "CustomScripts",
      "name": "Custom Scripts",
      "type": "toggle",
      "description": "Allows those with RTR Active Responder and RTR Administrator roles to run custom scripts",
      "value": {
       "enabled": false
      }
     }
    ]
   },
   {
    "name": "High risk commands",
    "settings": [
     {
      "id": "GetCommand",
      "name": "get",
      "type": "toggle",
      "description": "Extract files from a remote host via the CrowdStrike cloud",
      "value": {
       "enabled": true
      }
     },
     {
      "id": "PutCommand",
      "name": "put",
      "type": "toggle",
      "description": "Send files to a remote host via the CrowdStrike cloud. Required for partner software update policies",
      "value": {
       "enabled": false
      }
     },
     {
      "id": "MemDumpCommand",
      "name": "memdump",
      "type": "toggle",
      "description": "Dump process memory of a remote host",
      "value": {
       "enabled": true
      }
     },
     {
      "id": "XMemDumpCommand",
      "name": "xmemdump",
      "type": "toggle",
      "description": "Dump the complete memory of a remote host",
      "value": {
       "enabled": true
      }
     },
     {
      "id": "ExecCommand",
      "name": "run",
      "type": "toggle",
      "description": "Run any executable on the remote host",
      "value": {
       "enabled": true
      }
     }
    ]
   }
  ]
 },
 {
  "id": "6f32f2941b1a4fdc9931053e4cc9e76feb",
  "name": "Test RTR Policy 2",
  "description": "Short description of test RTR Policy 2.",
  "platform_name": "Windows",
  "groups": [
   {
    "id": "1c0555a4e4617b0394989d93bf119dad",
    "group_type": "static",
    "name": "Host group 2",
    "description": "Short description of host group 2.",
    "created_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
    "created_timestamp": "2021-03-09T16:06:07.021541506Z",
    "modified_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
    "modified_timestamp": "2021-03-09T16:06:07.021541506Z"
   }
  ],
  "enabled": true,
  "created_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
  "created_timestamp": "2021-04-09T23:44:53.211690986Z",
  "modified_by": "api-client-id:89511ce884ba885dce5568b328eb2c1d",
  "modified_timestamp": "2021-04-09T23:57:44.693756296Z",
  "prevention_settings": [
   {
    "name": "Enable/Disable",
    "settings": [
```

```
      {
       "id": "RealTimeFunctionality",
       "name": "Real Time Response",
       "type": "toggle",
       "description": "Allow those with Real Time Responder roles to remotely connect to hosts. Required for all RTR commands and scripts and for partner software
update policies.",
       "value": {
        "enabled": true
       }
      }
     ]
    },
    {
     "name": "Custom scripts",
     "settings": [
      {
       "id": "CustomScripts",
       "name": "Custom Scripts",
       "type": "toggle",
       "description": "Allows those with RTR Active Responder and RTR Administrator roles to run custom scripts",
       "value": {
        "enabled": true
       }
      }
     ]
    },
    {
     "name": "High risk commands",
     "settings": [
      {
       "id": "GetCommand",
       "name": "get",
       "type": "toggle",
       "description": "Extract files from a remote host via the CrowdStrike cloud",
       "value": {
        "enabled": true
       }
      },
      {
       "id": "PutCommand",
       "name": "put",
       "type": "toggle",
       "description": "Send files to a remote host via the CrowdStrike cloud. Required for partner software update policies",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "MemDumpCommand",
       "name": "memdump",
       "type": "toggle",
       "description": "Dump process memory of a remote host",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "XMemDumpCommand",
       "name": "xmemdump",
       "type": "toggle",
       "description": "Dump the complete memory of a remote host",
       "value": {
        "enabled": false
       }
      },
      {
       "id": "ExecCommand",
       "name": "run",
       "type": "toggle",
       "description": "Run any executable on the remote host",
       "value": {
        "enabled": true
       }
      }
     ]
    }
   ]
  }
 ]
}
```


Set Real Time Response policy precedence

Real Time Response policies are applied to host groups using a first-match method, based on policy precedence within a `platform_name` (for example, Windows). The default order sets precedence by date created, with the oldest policy ranked in the highest position as Precedence 1. If a host or host group is assigned to multiple policies, the policy with the highest precedence level is applied. All subsequent, lower precedence policy matches are ignored.

You can rearrange the order of precedence of your Real Time Response policies within a particular platform by sending the policy IDs listed from top to bottom in the way you would like to rank them. To run this request, you must specify a `platform_name` and include all Real Time Response policy IDs for that platform (except the default policy, which always takes lowest precedence and cannot be changed) in your environment. Successful requests return an HTTP 200 code.

Note: To retrieve a list of your Real Time Response policy IDs for a specific platform, make a `GET` request to `/policy/queries/response/v1` with the `platform_name` filter.

Endpoint

```
POST /policy/entities/response-precedence/v1
```

Parameters

Name	In	Description
`ids` required	body	An array of all Real Time Response policy IDs for a particular platform in your environment listed in the desired order of precedence with the highest priority policy ID at the top and the lowest priority at the bottom. Do not include the platform default policy ID.
`platform_name` required	body	The operating system name. One of **Windows**, **Mac**, or **Linux**. Enter the value as shown with the first letter capitalized.

Example request

The example below will set the policy precedence of the inputted Windows Real Time Response policy IDs in the order they are placed.

```
curl --location --request POST 'https://api.crowdstrike.com/policy/entities/response-precedence/v1' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI' \
--data-raw '{
 "ids": [
  "703d949584b74488a2da2c5c779078ec",
  "057f63a26f6d42c493a9a31532b068fe",
  "bb0ac94220a34e92b760d2ffb3a74991"
 ],
 "platform_name": "Windows"
}'
```

Example response

The response resources show empty, but the new precedence order can be verified in the Falcon UI under Host setup and management > Response and containment > Response policies .

```
{
 "meta": {
  "query_time": 0.094910092,
  "writes": {
   "resources_affected": 3
  },
  "trace_id": "d49a438d-0c6c-400e-8e0b-0ca85a1d9bd5"
 },
 "resources": [],
 "errors": null
}
```

List Real Time Response policy hosts

Get a list of hosts assigned to a Real Time Response policy. Supply the unique response policy `id` without any additional parameters to retrieve all hosts in the policy's assigned host groups. Alternatively, provide an optional FQL `filter` to narrow your results or a `sort` parameter to change the order in which the result set displays. Successful requests return an HTTP 200 code and an array of host details that matches the query criteria in the response.

Endpoint

```
GET /policy/combined/response-members/v1
```

Parameters

Name	In	Description
`id` required	query	The unique ID of the Real Time Response policy. This request does not support multiple policy IDs.
`offset` optional	query	The zero-based position of the first record to return. The default is 0.

Name	In	Description
`limit` optional	query	The maximum number of records to return. The limit can range from 1–5000. The default is 100.
`sort` optional	query	The property used to order the results. Sort values for this request relate to hosts, which are different from the policy sort values shown in other sections of this document. See our Falcon Query Language Reference guide for more information.
`filter` optional	query	The FQL filter expression used to limit the result set. The available values are specific to hosts, which are different from the policy filter values listed in other sections of this document. See our Falcon Query Language Reference guide for more information.

Example request

The example below returns a list of hosts for the specified Real Time Response policy ID.

```
curl --location --request GET 'https://api.crowdstrike.com/policy/combined/response-members/v1?id=6f32f2941b1a4fdc9931053e4cc9e76feb' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response

The following response has been shortened for documentation purposes. It limits the details returned to a single host from the assigned host group.


```
{
 "meta": {
  "query_time": 1.082876213,
  "pagination": {
   "offset": 0,
   "limit": 100,
   "total": 2
  },
  "trace_id": "cfe649f5-c45e-4052-8a93-6d86b33df9b6"
 },
 "errors": [],
 "resources": [
  {
   "device_id": "2b18395ba345128b7cd024a48a1f039b",
   "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV",
   "agent_load_flags": "1",
   "agent_local_time": "2021-03-02T08:33:25.423Z",
   "agent_version": "6.16.13008.0",
   "bios_manufacturer": "Example, Inc.",
   "bios_version": "Example71.00V.16722896.B64.2008100651",
   "build_number": "19042",
   "config_id_base": "65994753",
   "config_id_build": "13008",
   "config_id_platform": "3",
   "cpu_signature": "591594",
   "external_ip": "199.200.15.54",
   "mac_address": "00-0c-29-ed-f7-72",
   "hostname": "Example Hostname",
   "first_seen": "2021-03-02T16:09:32Z",
   "last_seen": "2021-03-02T16:34:55Z",
   "local_ip": "172.16.189.2",
   "major_version": "10",
   "minor_version": "0",
   "os_version": "Windows 10",
   "platform_id": "0",
   "platform_name": "Windows",
   "policies": [
    {
     "policy_type": "prevention",
     "policy_id": "1ffcb0ff58b16bf050fb9401e6dfafdd",
     "applied": true,
     "settings_hash": "8477040c",
     "assigned_date": "2021-03-02T16:10:39.456482321Z",
     "applied_date": "2021-03-02T16:10:45.775564748Z",
     "rule_groups": []
    }
   ],
   "reduced_functionality_mode": "no",
   "device_policies": {
    "prevention": {
     "policy_type": "prevention",
     "policy_id": "1ffff58b14016bf050fb9e6cb0dfafdd",
     "applied": true,
     "settings_hash": "8477040c",
     "assigned_date": "2021-03-02T16:10:39.456482321Z",
     "applied_date": "2021-03-02T16:10:45.775564748Z",
     "rule_groups": []
    },
```

```
    "sensor_update": {
     "policy_type": "sensor-update",
     "policy_id": "87ef20372e97c2d479fa5e8bf34d2bed",
     "applied": true,
     "settings_hash": "tagged|1;0",
     "assigned_date": "2021-03-02T16:17:07.608056515Z",
     "applied_date": "2021-03-02T16:19:44.213046715Z",
     "uninstall_protection": "DISABLED"
    },
    "device_control": {
     "policy_type": "device-control",
     "policy_id": "1697fdac4ed4d0886a774b013e516e0d",
     "applied": true,
     "assigned_date": "2021-03-02T16:22:26.335917439Z",
     "applied_date": "2021-03-02T16:24:37.870872866Z"
    },
    "global_config": {
     "policy_type": "globalconfig",
     "policy_id": "158fa20724bffabf05458f073c69429b",
     "applied": true,
     "settings_hash": "903890b2",
     "assigned_date": "2021-03-02T16:36:15.63829992Z",
     "applied_date": "2021-03-02T16:37:53.530896137Z"
    },
    "remote_response": {
     "policy_type": "remote-response",
     "policy_id": "6372d79a422f2324f4a9cf5667314a48",
     "applied": true,
     "settings_hash": "f472bd8e",
     "assigned_date": "2021-03-02T16:10:39.45647106Z",
     "applied_date": "2021-03-02T16:10:45.854924391Z"
    },
    "firewall": {
     "policy_type": "firewall",
     "policy_id": "c68f670c6477f9045ed36b2781e9a362",
     "applied": true,
     "assigned_date": "2021-03-02T16:10:39.456436769Z",
     "applied_date": "2021-03-02T16:11:39.710243073Z",
     "rule_set_id": "c68f81e670c6477f9045ed36b279a362"
    }
   },
   "groups": [
    "db1625080446479f1e7e276d1ad1baf2",
    "ed06109084c5f9a1b6593539deb69074"
   ],
   "group_hash": "24570bd61f017fa59c7b9bff357ac26e825c631188becb5d77fe57de836d9eb2",
   "product_type": "1",
   "product_type_desc": "Workstation",
   "provision_status": "Provisioned",
   "serial_number": "Example-56 4d 00 0d ca ce 41 07-07 55 82 ce 10 ed f7 72",
   "service_pack_major": "0",
   "service_pack_minor": "0",
   "pointer_size": "8",
   "status": "normal",
   "system_manufacturer": "Example, Inc.",
   "system_product_name": "Example",
   "tags": [],
   "modified_timestamp": "2021-03-02T16:37:53Z",
   "slow_changing_modified_timestamp": "2021-03-02T16:34:56Z",
   "meta": {
    "version": "25"
   }
  }
 ]
}
```


List Real Time Response policy agent IDs

Get a list of agent IDs for hosts assigned to a Real Time Response policy. Supply the unique response policy `id` without any additional parameters to retrieve all agent IDs in the policy's assigned host groups. Alternatively, provide an optional FQL `filter` to narrow your results or a `sort` parameter to change the order in which the result set displays. Successful requests return an HTTP 200 code and an array of agent IDs that match the query criteria in the response.

Endpoint

```
GET /policy/queries/response-members/v1
```

Parameters

Name	In	Description
`id` required	query	The unique ID of the Real Time Response policy. This request does not support multiple policy IDs.

Name	In	Description
`offset` optional	query	The zero-based position of the first record to return. The default is 0.
`limit` optional	query	The maximum number of records to return. The limit can range from 1–5000. The default is 100.
`sort` optional	query	The property used to order the results. Sort values for this request relate to hosts, which differ from the policy sort values shown in other sections of this document. See our Falcon Query Language Reference guide for more information.
`filter` optional	query	The FQL filter expression used to limit the result set. The available values are specific to hosts, which differ from the policy filter values listed in other sections of this document. See our Falcon Query Language Reference guide for more information.

Example request

```
curl --location --request GET 'https://api.crowdstrike.com/policy/queries/response-members/v1?id=6f32f2941b1a4fdc9931053e4cc9e76feb' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response

```
{
 "meta": {
  "query_time": 0.207242862,
  "pagination": {
   "offset": 0,
   "limit": 100,
   "total": 2
  },
  "trace_id": "d1949119-470c-408a-8784-95edcd76429e"
 },
 "resources": [
  "2b18395ba345128b7cd024a48a1f039b",
  "e8d959d04a259f6432a3e733489fd613"
 ],
 "errors": []
}
```

Delete a Real Time Response policy

Delete a Real Time Response policy from your environment. When a policy is deleted, hosts in the deleted policy's assigned host groups are placed in the default policy or reassigned to the policy with the next highest precedence (if associated with more than one policy). Successful requests return an HTTP 200 code.

Endpoint

```
DEL /policy/entities/response/v1
```

Parameters

Name	In	Description
`ids` required	query	The unique ID of the Real Time Response policy. Multiple IDs can be entered using the syntax `ids={a}&ids={b}`.

Example request

The example below deletes two Real Time Response policies with the specified ids.

```
curl --location --request DELETE 'https://api.crowdstrike.com/policy/entities/response/v1?
ids=c6c9a4264ff131068590dc3c3d0a9871&ids=5d3737bbd4e742baaa473def9d110645' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer eyJhbGci...xYg1NNI'
```

Example response

```
{
 "meta": {
  "query_time": 0.102603077,
  "trace_id": "5bf65118-70de-466e-a8f7-ec79740ec21b"
 },
 "resources": null,
 "errors": null
}
```

Windows On-Demand Scanning APIs

Start, schedule, manage, and retrieve details of on-demand scans for Windows hosts.

Windows On-Demand Scanning APIs

CrowdStrike provides use cases and example requests and responses for interacting with a specific set of our OAuth2-based APIs. For general info about CrowdStrike APIs, see CrowdStrike OAuth2-Based APIs, which covers these topics:

- Details on getting started, such as authentication and API scopes
- Domains used in base URLs by cloud
- Links to our Swagger API specification by cloud

API client requirements

To interact with the APIs covered in this section, your API client credentials must have the following scopes enabled:

- On-demand scans (ODS): **read** and **write** access

API clients are managed through API Clients and Keys (**Support and resources > Resources and tools > API clients and keys**) in the Falcon console.

Get scan details

Retrieve details about Windows on-demand scans and scheduled scans.

Find scan IDs

Find the IDs of your on-demand scans. The IDs can then be used to retrieve specific scans.

Narrow the result set by specifying FQL filters, or omit FQL filters to get a list of all scan IDs in your environment. For more info about FQL filters, see Falcon Query Language (FQL).

- Find scan IDs with `GET /ods/queries/scans/v1?filter=<string>&offset=<integer>&limit=<integer>&sort=<string>`

Parameters

Name	Type	Required?	Description
`offset`	Integer	No	Where in the scan index to start finding results
`limit`	Integer	No	The maximum number of results to return
`sort`	String	No	Values to sort results on

Example: Find the first 5 scan IDs

Example request

```
curl -X GET 'https://api.crowdstrike.com/ods/queries/scans/v1?filter=&offset=0&limit=5' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...7FZQTFo'
```

Example response

```
{
 "meta": {
  "query_time": 0.029337515,
  "pagination": {
   "offset": 0,
   "limit": 5,
   "total": 6193
  },
  "powered_by": "svc-odsapi",
  "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
```

```
 },
 "resources": [
  "f08aa4dc8468f2f47dc8b62a44e907e5",
  "d66a4c9e85a6d079ee3d4443bb33683",
  "9ee3d444dc846833686a4c9e8f47dc84",
  "6d079ee3d44dc8468f2f46a4c9e85x74",
  "f46a4c9e4dc8468f2f4079ee3d44e8f3"
 ],
 "errors": null
```


Retrieve scans by ID

Get details about specific scans.

- Retrieve scan details with `GET /ods/entities/scans/v1?ids=<ID>&ids=<ID>`

Example: Retrieve details about 2 scans by ID

Example request

```
curl -X GET 'https://api.crowdstrike.com/ods/entities/scans/v1?ids=2dee73cdaeeb4f65a5803d109eade919&ids=d64bd983adca46f4a4a210f72f9663c3' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...47FZQTFo'
```

Example response


```
{
 "meta": {
  "query_time": 0.387593886,
  "writes": {
   "resources_affected": 2
  },
  "powered_by": "svc-odsapi",
  "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
 },
 "resources": [
  {
   "id": "d64bd983adca46f4a4a210f72f9663c3",
   "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV",
   "profile_id": "24kdf8g294k43592m285cba6fb718g46",
   "description": "daily recurring 8:30 am for host group",
   "file_paths": [
    "c:\\program files\\internet explorer"
   ],
   "initiated_from": "cloud_scheduled",
   "quarantine": true,
   "cpu_priority": 1,
   "preemption_priority": 15,
   "metadata": [
    {
     "host_id": "6eu25920fd82395m302t8z73202f9486",
     "host_scan_id": "84bdeecc3b5d6ae9396325696183204e",
     "scan_host_metadata_id": "6c1f1bde8f77e6717bda6b434adda040",
     "filecount": {
      "scanned": 11,
      "malicious": 0,
      "quarantined": 0,
      "skipped": 2
     },
     "status": "completed",
     "started_on": "2022-11-01T16:27:57.909692601Z",
     "completed_on": "2022-11-01T16:43:13.898995584Z",
     "last_updated": "2022-11-01T16:43:13.900305203Z"
    },
    {
     "host_id": "174ca984c7be1973160f3c5ea2adf8b3",
     "scan_host_metadata_id": "fa0c6dc9a6a6155abdb9951dad53b4c9",
     "filecount": {},
     "status": "scheduled",
     "last_updated": "2022-11-01T16:27:57.947953877Z"
    },
    {
     "host_id": "39e7aa511929dcfa48e524604acc1115",
     "scan_host_metadata_id": "70409a2a1f9f6d8901b7bdb40484d3db",
     "filecount": {},
     "status": "scheduled",
     "last_updated": "2022-11-01T16:27:57.947953877Z"
    }
   ],
   "filecount": {},
   "status": "running",
   "host_groups": [
    "2a14c286ce8db729481080edf496c631"
   ],
   "endpoint_notification": true,
   "pause_duration": 2,
   "max_duration": 0,
   "max_file_size": 60,
   "sensor_ml_level_detection": 4,
```

```
   "sensor_ml_level_prevention": 3,
   "cloud_ml_level_detection": 3,
   "cloud_ml_level_prevention": 2,
   "scan_started_on": "2022-11-01T16:27:57.909692601Z",
   "created_on": "2022-11-01T16:27:57.909692601Z",
   "created_by": "aaronp@example.com",
   "last_updated": "2022-11-01T16:27:57.909692601Z"
  },
  {
   "id": "2dee73cdaeeb4f65a5803d109eade919",
   "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV",
   "profile_id": "401d8d37395151d09af7b1f4df588f56",
   "file_paths": [
    "C:\\"
   ],
   "initiated_from": "cloud_adhoc",
   "quarantine": true,
   "cpu_priority": 3,
   "preemption_priority": 1,
   "metadata": [
    {
     "host_id": "44f4224e1fd9d2a00ae5df97376b7b07",
     "scan_host_metadata_id": "59f9412e7d89c60ebc9835449e37ce7b",
     "filecount": {},
     "status": "failed",
     "last_updated": "2022-11-01T16:48:57.521328456Z"
    }
   ],
   "filecount": {},
   "status": "failed",
   "hosts": [
    "82395m302t8zea2u25978416be1973c5"
   ],
   "endpoint_notification": true,
   "pause_duration": 0,
   "max_duration": 0,
   "max_file_size": 60,
   "sensor_ml_level_detection": 4,
   "sensor_ml_level_prevention": 4,
   "cloud_ml_level_detection": 4,
   "cloud_ml_level_prevention": 4,
   "created_on": "2022-11-01T16:48:57.41971214Z",
   "created_by": "33b5417b7d0d40d0a2ec01cf782c112a",
   "last_updated": "2022-11-01T16:51:32.001623359Z"
  }
 ]
}
```


Find scheduled-scan IDs

Find the IDs of your scheduled scans. The IDs can then be used to retrieve specific scheduled scans.

Narrow the result set by specifying FQL filters, or omit FQL filters to get a list of all scan IDs in your environment. For more info about FQL filters, see Falcon Query Language (FQL).

- Find scheduled scan IDs with `GET /ods/queries/scheduled-scans/v1?filter=<string>&offset=<integer>&limit=<integer>&sort=<string>`

Example: Find the first 5 scheduled scan IDs

Example request

```
curl -X GET 'https://api.crowdstrike.com/ods/queries/scheduled-scans/v1?filter=&offset=0&limit=5' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...th69jX0'
```

Example response


```
{
    "meta": {
        "query_time": 0.035411159,
        "pagination": {
            "offset": 0,
            "limit": 5,
            "total": 19
        },
        "powered_by": "svc-odsapi",
        "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
    },
    "resources": [
        "f46a4c9e4dc8468f2f4079ee3d44e8f3",
        "6d079ee3d44dc8468f2f46a4c9e85x74",
        "9ee3d444dc846833686a4c9e8f47dc84",
        "66a4c9e85a6d079ee3d4443bb336835",
        "f08aa4dc8468f2f47dc8b62a44e907e5"
    ],
    "errors": null
}
```

Retrieve scheduled scans by ID

Get details about specific scheduled scans.

- Retrieve scheduled scan details with `GET /ods/entities/scheduled-scans/v1?ids=<ID>&ids=<ID>`

Example: Retrieve details about 2 scheduled scans by ID

Example request

```
curl -X GET 'https://api.crowdstrike.com/ods/entities/scheduled-scans/v1?ids=c846c347dff64ef59eee8c4febc96f6f&ids=e45ad39debf5424594a3a79e34e51355' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...th69jX0'
```

Example response


```
{
 "meta": {
  "query_time": 0.003633232,
  "powered_by": "svc-odsapi",
  "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
 },
 "resources": [
  {
   "id": "c846c347dff64ef59eee8c4febc96f6f",
   "cid": "3c74ca9ad4k43592ea2adf4ca94k4359",
   "description": "test scheduled scans at 2pm with exclusion - C:\\Program Files\\Internet Explorer scan path with exclusion set for **\\samples50\\**",
   "file_paths": [
    "C:\\Program Files"
   ],
   "scan_exclusions": [
    "**\\samples50\\**"
   ],
   "initiated_from": "cloud_scheduled",
   "cpu_priority": 2,
   "preemption_priority": 15,
   "status": "scheduled",
   "host_groups": [
    "6d170472df1154b119424d8e8b910f4b"
   ],
   "endpoint_notification": true,
   "pause_duration": 2,
   "max_duration": 0,
   "max_file_size": 60,
   "sensor_ml_level_detection": 4,
   "cloud_ml_level_detection": 4,
   "schedule": {
    "start_timestamp": "2022-11-01T14:00",
    "interval": 1
   },
   "created_on": "2022-10-28T18:19:02.370664426Z",
   "created_by": "klee@example.com",
   "last_updated": "2022-11-01T13:48:20.071070691Z",
   "deleted": false
  },
  {
   "id": "e45ad39debf5424594a3a79e34e51355",
   "cid": "91a0649f84749a38f6d939423bed5576",
   "description": "11:48 ",
   "file_paths": [
    "C:\\\\testpath"
   ],
   "initiated_from": "cloud_scheduled",
   "quarantine": true,
   "cpu_priority": 3,
   "preemption_priority": 15,
   "metadata": [
    {
     "host_id": "9db5954b355d9720583fee4a29b83dd1",
     "last_updated": "2022-11-01T17:46:20.070929551Z"
    },
    {
     "host_id": "3c0dbc99b5bfed342319c8dd6e15beeb",
     "last_updated": "2022-11-01T17:46:20.070929551Z"
    },
    {
     "host_id": "4200a3dfb4748f627ae6f83da29b14a1",
     "last_updated": "2022-11-01T17:46:20.070929551Z"
    },
    {
     "host_id": "34e8657dcbedaf9199d8b8a301b4e0b2",
     "last_updated": "2022-11-01T17:46:20.070929551Z"
    }
   ],
   "status": "scheduled",
   "host_groups": [
    "33e4782474dfabd8bd4925ecaa9f6c43",
    "603cf674607c63583e49d9ac0b2c6ce2"
   ],
   "endpoint_notification": true,
   "pause_duration": 0,
```

```
   "max_duration": 0,
   "max_file_size": 60,
   "sensor_ml_level_detection": 2,
   "sensor_ml_level_prevention": 2,
   "cloud_ml_level_detection": 2,
   "cloud_ml_level_prevention": 2,
   "schedule": {
    "start_timestamp": "2022-11-02T12:30",
    "interval": 1
   },
   "created_on": "2022-10-13T18:48:47.007527108Z",
   "created_by": "myoung@example.com",
   "last_updated": "2022-11-01T17:46:20.070929551Z",
   "deleted": false
  }
 ]
}
```


Find malicious-file IDs

Find the IDs of malicious portable executable (PE) files that were identified during a scan. The IDs can then be used to retrieve specific files.

Narrow the result set by specifying FQL filters, or omit FQL filters to get a list of all scan IDs in your environment. For more info about FQL filters, see Falcon Query Language (FQL).

- Find IDs of malicious files with `GET /ods/queries/malicious-files/v1?filter=<string>&offset=<integer>&limit=<integer>&sort=<string>`

Example: Find the first 5 malicious-file IDs

Example request

```
curl -X GET 'https://api.crowdstrike.com/ods/queries/malicious-files/v1?filter=&offset=0&limit=5&sort=' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...crqCiz64'
```

Example response


```
{
    "meta": {
        "query_time": 0.035411159,
        "pagination": {
            "offset": 0,
            "limit": 5,
            "total": 6071
        },
        "powered_by": "svc-odsapi",
        "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
    },
    "resources": [
        "66a4c9e85a6d079ee3d4443bb3368358",
        "f08aa4dc8468f2f47dc8b62a44e907e5",
        "9ee3d444dc846833686a4c9e8f47dc84",
        "6d079ee3d44dc8468f2f46a4c9e85x74",
        "f46a4c9e4dc8468f2f4079ee3d44e8f3"
    ],
    "errors": null
}
```


Retrieve malicious-file details by ID

Get details about specific malicious files.

- Retrieve details about malicious files with `GET /ods/entities/malicious-files/v1?ids=<ID>&ids=<ID>`

Example: Retrieve details about 2 malicious files by ID

Example request

```
curl -X GET 'https://api.crowdstrike.com/ods/entities/malicious-files/v1?ids=d684849d4cea435daec706e473743863&ids=e1cdd2143eae4e20b85d93664011e88b' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...rqCiz64'
```

Example response


```
{
 "meta": {
  "query_time": 0.150137045,
  "powered_by": "svc-odsapi",
  "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
 },
 "resources": [
  {
   "id": "d684849d4cea435daec706e473743863",
   "cid": "91a0649f84749a38f6d939423bed5576",
   "scan_id": "81c8009a59be4570b5c66f8946559205",
```

```
   "host_id": "3c7be1c5ea21849fa5c74ca9842f46a9",
   "host_scan_id": "4f9fea030a0626ed4dc53a7dec70a100",
   "filepath": "C:\\\\Windows\\Malicious\\Mimikatz_newzipp\\Mimikatz\\x86\\mimilib.dll",
   "filename": "mimilib.dll",
   "hash": "9ff1a527861a69b436b51a8d464aaee8d416e39ff1a52aee16e39b436b564a78",
   "pattern_id": 4004,
   "severity": 70,
   "quarantined": true,
   "last_updated": "2022-11-01T17:06:18.900620631Z"
  },
  {
   "id": "f46a4c9e4dc8468f2f4079ee3d44e8f3",
   "cid": "3c74ca9ad4k43592ea2adf4ca94k4359",
   "scan_id": "81c8009a59be4570b5c66f8946559205",
   "host_id": "5ea2ad4k43592m285cbd44dc8468f2f4",
   "host_scan_id": "92m285cbd44d8g294k4359d554f11826",
   "filepath": "C:\\\\Windows\\Malicious\\Mimikatz\\Mimikatz\\amd64\\kikikatz.exe",
   "filename": "kikikatz.exe",
   "hash": "464aaee16e39ff1a527869b4364aaee16e39ff1a69b436b51a8d6b51a8d45278",
   "pattern_id": 4004,
   "severity": 70,
   "quarantined": true,
   "last_updated": "2022-11-01T17:07:35.485183912Z"
  }
 ]
}
```


Find scan host IDs

Find the IDs of scan hosts. The IDs can then be used to retrieve specific hosts.

Narrow the result set by specifying FQL filters, or omit FQL filters to get a list of all scan IDs in your environment. For more info about FQL filters, see Falcon Query Language (FQL).

- Find IDs of scan hosts with `GET /ods/queries/scan-hosts/v1?filter=<string>&offset=<integer>&limit=<integer>&sort=<string>`

Example: Find the first 5 scan host IDs

Example request

```
curl -X GET 'https://api.crowdstrike.com/ods/queries/scan-hosts/v1?filter=&offset=0&limit=5' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...QL33t9ks'
```

Example response


```
{
    "meta": {
        "query_time": 0.032451659,
        "pagination": {
            "offset": 0,
            "limit": 5,
            "total": 4063
        },
        "powered_by": "svc-odsapi",
        "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
    },
    "resources": [
        "f46a4c9e4dc8468f2f4079ee3d44e8f3",
        "6d079ee3d44dc8468f2f46a4c9e85x74",
        "9ee3d444dc846833686a4c9e8f47dc84",
        "d66a4c9e85a6d079ee3d4443bb336835",
        "f08aa4dc8468f2f47dc8b62a44e907e5"
    ],
    "errors": null
}
```


Retrieve scan hosts by ID

Get details about scan hosts by `scan_host_metadata_id` value.

- Retrieve details about scan hosts with `GET /ods/entities/scan-hosts/v1`

Example: Retrieve details about a scan host by ID

Example request

```
curl -X GET 'https://api.crowdstrike.com/ods/entities/scan-hosts/v1?ids=185a0ad5e159418e8927d956c1a793d8' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...L33t9ks'
```

Example response


```
{
 "meta": {
```

```
  "query_time": 0.004331407,
  "powered_by": "svc-odsapi",
  "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
 },
 "resources": [
  {
   "id": "185a0ad5e159418e8927d956c1a793d8",
   "cid": "3c74ca9ad4k43592ea2adf4ca94k4359",
   "scan_id": "fadde07ee8a44a07988e009b3152e339",
   "profile_id": "ddf8914cca5f4ac595272fe8122e308f",
   "host_id": "82395m302t8zea2u25978416be1973c5",
   "host_scan_id": "7e80aa16a44d30cb819e27144d2603b0",
   "filecount": {
    "scanned": 1021,
    "malicious": 104,
    "quarantined": 0,
    "skipped": 9328
   },
   "status": "completed",
   "severity": 70,
   "started_on": "2022-11-01T18:54:59.39861174Z",
   "completed_on": "2022-11-01T19:08:17.903700092Z",
   "last_updated": "2022-11-01T19:08:17.903732519Z"
  }
 ]
}
```


Manage scans

Start, schedule, and manage Windows on-demand scans.

Start a scan

Start a scan immediately on specified hosts or host groups.

- Start a scan with `POST /ods/entities/scans/v1`

Requirements and properties:

- The `file_paths` value is required.
- File path exclusions can be formatted in glob syntax. For more info, see Glob Syntax.
- At least one `hosts` or `host_groups` value is required.
- The `max_file_size` value is in MB.
- The `max_duration` value is in hours. To allow an unlimited duration, specify a value of `0`.
- The `pause_duration` value is in hours.
- Machine learning (ML) detection and prevention values are required. The detection value must be greater than or equal to the associated prevention value. A detection value cannot be `0`. ML detection and prevention levels:
  - `0` = Disabled
  - `1` = Cautious
  - `2` = Moderate
  - `3` = Aggressive
  - `4` = Extra aggressive
- Values for `cpu_priority`:
  - `1` = up to 1% CPU utilization
  - `2` = up to 25% CPU utilization
  - `3` = up to 50% CPU utilization
  - `4` = up to 75% CPU utilization
  - `5` = up to 100% CPU utilization

Example: Start a scan on a specified host group

Example request

```
curl -X POST 'https://api.crowdstrike.com/ods/entities/scans/v1' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...WAPAMw' --data-raw '{"hosts":[],"host_groups":["f6eu25920fd82395m302t8z73202f9486"],"file_paths":
["C:\\Windows"],"scan_exclusions":[],"initiated_from":"falcon_adhoc","cpu_priority":1,"description":"test APIS
","quarantine":true,"endpoint_notification":true,"pause_duration":2,"sensor_ml_level_detection":2,"sensor_ml_level_prevention":2,"cloud_ml_level_detection":2,"clo
ud_ml_level_prevention":2,"max_duration":2}'
```

Example response


```
{
 "meta": {
```

```
  "query_time": 0.207790105,
  "writes": {
   "resources_affected": 1
  },
  "powered_by": "svc-odsapi",
  "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
 },
 "resources": [
  {
   "id": "d47f556620e74189acacfd7664a4a186",
   "cid": "3c74ca9ad4k43592ea2adf4ca94k4359",
   "profile_id": "ba18ad8667eb4885b974d889516ec6f4",
   "description": "test APIS ",
   "file_paths": [
    "C:\\Windows"
   ],
   "initiated_from": "falcon_adhoc",
   "quarantine": true,
   "cpu_priority": 1,
   "preemption_priority": 1,
   "metadata": [
    {
     "host_id": "2395m302t8z79345824kdf8g294a2u23",
     "scan_host_metadata_id": "94e44310878416be1973c590429c9408",
     "filecount": {},
     "last_updated": "0001-01-01T00:00:00Z"
    },
    {
     "host_id": "38d4a9964d270043a7f2554e409078d4",
     "scan_host_metadata_id": "34a09877d28db4bed947ad591afccd49",
     "filecount": {},
     "last_updated": "0001-01-01T00:00:00Z"
    }
   ],
   "filecount": {},
   "status": "pending",
   "host_groups": [
    "f6eu25920fd82395m302t8z73202f9486"
   ],
   "endpoint_notification": true,
   "pause_duration": 2,
   "max_duration": 2,
   "max_file_size": 60,
   "sensor_ml_level_detection": 2,
   "sensor_ml_level_prevention": 2,
   "cloud_ml_level_detection": 2,
   "cloud_ml_level_prevention": 2,
   "created_on": "2022-11-01T19:43:04.40585731Z",
   "created_by": "40d0a2ec01cf33b5417b787d0d2c112a",
   "last_updated": "2022-11-01T19:43:04.40585731Z"
  }
 ]
}
```


Cancel scans

Cancel a current instance of a scan by ID.

- Cancel running scans with `POST /ods/entities/scan-control-actions/cancel/v1`

Example: Cancel a scan instance by ID

Example request

```
curl -X POST 'https://api.crowdstrike.com/ods/entities/scan-control-actions/cancel/v1' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...WAPAMw' --data-raw '{"ids": ["d47f556620e74189acacfd7664a4a186"]}'
```

Example response


```
{
 "meta": {
  "query_time": 0.041849114,
  "writes": {
   "resources_affected": 1
  },
  "powered_by": "svc-odsapi",
  "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
 },
 "resources": [
  "d47f556620e74189acacfd7664a4a186"
 ],
 "errors": null
}
```

Schedule a scan

Schedule a scan for specified host groups. Scheduled scans are supported for host groups but not individual hosts.

- Schedule a scan with `POST /ods/entities/scheduled-scans/v1`

Requirements and properties:

- The `file_paths` value is required.
- File path exclusions can be formatted in glob syntax. For more info, see Glob Syntax.
- The `host_groups` value is required.
- The `max_file_size` value is in MB.
- The `max_duration` value is in hours. To allow an unlimited duration, specify a value of `0`.
- The `pause_duration` value is in hours.
- The `interval` value is required. It specifies, in days, how often to repeat a scheduled scan. To run the scan only once, specify a value of `0`.
- Machine learning (ML) detection and prevention values are required. The detection value must be greater than or equal to the associated prevention value. A detection value cannot be `0`. ML detection and prevention levels:
  - `0` = Disabled
  - `1` = Cautious
  - `2` = Moderate
  - `3` = Aggressive
  - `4` = Extra aggressive
- Values for `cpu_priority`:
  - `1` = up to 1% CPU utilization
  - `2` = up to 25% CPU utilization
  - `3` = up to 50% CPU utilization
  - `4` = up to 75% CPU utilization
  - `5` = up to 100% CPU utilization

Example: Schedule a scan for a specified host group

Example request

```
curl -X POST 'https://api.crowdstrike.com/ods/entities/scheduled-scans/v1' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...WAPAMw' --data-raw '{"description": "9:00PM daily schedule scan for My_Host_Group1",
            "host_groups": [
                "94e44310878416be1973c590429c9408"
            ],
            "file_paths": [
              "C:\\Program Files",
              "C:\\Users"
            ],
            "scan_exclusions": [
                "**\\Downloads\\**",
                "**\\Desktop\\**"
             ],
             "cloud_ml_level_detection": 2,
             "cloud_ml_level_prevention": 2,
             "sensor_ml_level_detection": 2,
             "sensor_ml_level_prevention": 2,
             "cpu_priority": 2,
             "endpoint_notification": true,
             "max_file_size": 60,
             "quarantine": true,
             "max_duration": 2,
             "pause_duration": 300,
             "initiated_from": "cloud_scheduled",
             "schedule": {
                "interval": 1,
                "start_timestamp": "2022-11-27T21:00"
             }
        }
'
```

Example response

```
{
 "meta": {
  "query_time": 0.40725059,
  "powered_by": "svc-odsapi",
  "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
 },
 "resources": [
  {
   "id": "603a1e157c1a4db5b3957f78ac726192",
```

```
   "cid": "0123456789ABCDEFGHIJKLMNOPQRSTUV",
   "description": "9:00PM daily schedule scan for My_Host_Group1",
   "file_paths": [
    "C:\\Program Files",
    "C:\\Users"
   ],
   "scan_exclusions": [
    "**\\Downloads\\**",
    "**\\Desktop\\**"
   ],
   "initiated_from": "cloud_scheduled",
   "quarantine": true,
   "cpu_priority": 2,
   "preemption_priority": 15,
   "metadata": [
    {
     "host_id": "94e44310878416be1973c590429c9408",
     "last_updated": "2022-11-01T19:56:49.208617165Z"
    },
    {
     "host_id": "2395m302t8z79345824kdf8g294a2u23",
     "last_updated": "2022-11-01T19:56:49.208617165Z"
    }
   ],
   "status": "scheduled",
   "host_groups": [
    "94e44310878416be1973c590429c9408"
   ],
   "endpoint_notification": true,
   "pause_duration": 300,
   "max_duration": 2,
   "max_file_size": 60,
   "sensor_ml_level_detection": 2,
   "sensor_ml_level_prevention": 2,
   "cloud_ml_level_detection": 2,
   "cloud_ml_level_prevention": 2,
   "schedule": {
    "start_timestamp": "2022-11-27T21:00",
    "interval": 1
   },
   "created_on": "2022-11-01T19:56:49.208617165Z",
   "created_by": "40d0a2ec01cf78337d0db5417b2c112a",
   "last_updated": "2022-11-01T19:56:49.208617165Z",
   "deleted": false
  }
 ]
}
```


Delete scheduled scans by ID

Deleting a scheduled scan prevents future instances of that scheduled scan from running.

- Delete a scheduled scan with `DELETE /ods/entities/scheduled-scans/v1?ids=<ID>&ids=<ID>`

Example: Delete a scheduled scan by ID

Example request

```
curl -X DELETE 'https://api.crowdstrike.com/ods/entities/scheduled-scans/v1?ids=603a1e157c1a4db5b3957f78ac726192' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...cyTh83M'
```

Example response


```
{
 "meta": {
  "query_time": 0.359221008,
  "powered_by": "svc-odsapi",
  "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
 },
 "resources": [
  "603a1e157c1a4db5b3957f78ac726192"
 ],
 "errors": null
}
```


Get scan aggregates and results

Retrieve aggregated data about Windows on-demand scans and scheduled scans.

Retrieve aggregated scan data

Get aggregated data about scans.

- Retrieve aggregated scan data with `POST /ods/aggregates/scans/v1`

Example: Retrieve aggregated scan data for specified criteria

Example request

```
curl -X POST 'https://api.crowdstrike.com/ods/aggregates/scans/v1' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...cyTh83M'  --data-raw '[
         {"type":"terms","field":"status","size":5,"filter":"","name":"status"},
         {"type":"terms","field":"initiated_from","size":5,"filter":"","name":"initiated_from"}
]'
```

Example response


```
{
 "meta": {
  "query_time": 0.007025571,
  "powered_by": "svc-odsapi",
  "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
 },
 "resources": [
  {
   "name": "status",
   "buckets": [
    {
     "label": "completed",
     "count": 4113
    },
    {
     "label": "running",
     "count": 1391
    },
    {
     "label": "canceled",
     "count": 409
    },
    {
     "label": "pending",
     "count": 241
    },
    {
     "label": "failed",
     "count": 29
    }
   ],
   "sum_other_doc_count": 24
  },
  {
   "name": "initiated_from",
   "buckets": [
    {
     "label": "endpoint_user",
     "count": 5206
    },
    {
     "label": "cloud_adhoc",
     "count": 433
    },
    {
     "label": "falcon_adhoc",
     "count": 311
    },
    {
     "label": "cloud_scheduled",
     "count": 232
    },
    {
     "label": "auto_usb",
     "count": 25
    }
   ],
   "sum_other_doc_count": 0
  }
 ],
 "errors": null
}
```


Retrieve aggregated scheduled-scan data

Get aggregated data about scheduled scans.

- Retrieve aggregated scheduled scan data with `POST /ods/aggregates/scheduled-scans/v1`

Example: Retrieve aggregated scheduled-scan data for specified criteria

Example request

```
curl -X POST 'https://api.crowdstrike.com/ods/aggregates/scheduled-scans/v1' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer eyJhbGci...yTh83M'  --data-raw '[{"type":"terms","field":"created_by","size":5,"filter":"","name":"created_by"}]'
```

Example response


```
{
 "meta": {
  "query_time": 0.02826553,
  "powered_by": "svc-odsapi",
  "trace_id": "e414e737-6d98-9d4f-c7ae-4e8acbf6ea70"
 },
 "resources": [
  {
   "name": "created_by",
   "buckets": [
    {
     "label": "mlee@example.com",
     "count": 25
    },
    {
     "label": "fjohnson@example.com",
     "count": 7
    },
    {
     "label": "mkim@example.com",
     "count": 1
    },
    {
     "label": "ogarcia@example.com",
     "count": 1
    }
   ],
   "sum_other_doc_count": 0
  }
 ],
 "errors": null
}
```