# Halo REST API Developer Guide

## How to use the Halo REST API

- API Overview
- API Best Practices

## Topic | REST API Endpoints
--- | ---
**Halo agent upgrades** | Agent Upgrades

**Cloud Secure**
- CSP Accounts
- CSP Resources
- CSP Findings
- CSP Scanner Settings

**Container Secure**
- Halo Connectors
- Containers
- Container Batch (for container inspection)
- Container Events
- Container Images
- Container Image Summaries
- Container Processes
- Container Registries
- Container Repositories
- Container Software Packages

**Halo groups**
- Server Groups

**Halo-protected servers**
- Servers
  - Server Accounts
  - Server Commands
  - Server Connections
  - Server Processes
  - Server Scans
<table>
<thead>
<tr>
<th>Section</th>
<th>Subsections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Firewall logs</td>
<td></td>
</tr>
<tr>
<td>Server Local Firewall</td>
<td></td>
</tr>
<tr>
<td>Local server users</td>
<td>Local user accounts</td>
</tr>
<tr>
<td></td>
<td>Local user groups</td>
</tr>
<tr>
<td>Historical Halo scans</td>
<td>Scan History</td>
</tr>
<tr>
<td>Issues</td>
<td>Issues</td>
</tr>
<tr>
<td>Configuration Security Monitoring</td>
<td>Configuration Policies</td>
</tr>
<tr>
<td>File Integrity Monitoring</td>
<td>File Integrity Policies</td>
</tr>
<tr>
<td></td>
<td>File Integrity Baselines</td>
</tr>
<tr>
<td>Software Vulnerability Assessment</td>
<td>CVE Details</td>
</tr>
<tr>
<td></td>
<td>CVE Exceptions</td>
</tr>
<tr>
<td>Workload Firewall Management</td>
<td>Firewall Policies</td>
</tr>
<tr>
<td></td>
<td>Firewall Rules</td>
</tr>
<tr>
<td></td>
<td>Firewall Interfaces</td>
</tr>
<tr>
<td></td>
<td>Firewall Services</td>
</tr>
<tr>
<td></td>
<td>Firewall Zones</td>
</tr>
<tr>
<td>Log-Based Intrusion Detection</td>
<td>Log-Based Intrusion Detection Policies</td>
</tr>
<tr>
<td>Halo event logging and alerting</td>
<td>Special Events Policies</td>
</tr>
<tr>
<td></td>
<td>Events</td>
</tr>
<tr>
<td></td>
<td>Alert Profiles</td>
</tr>
<tr>
<td>Server search</td>
<td>Saved Searches</td>
</tr>
<tr>
<td>Scanner Settings</td>
<td>Global Scanner Settings</td>
</tr>
<tr>
<td></td>
<td>Group Scanner Settings</td>
</tr>
<tr>
<td>Site Administration</td>
<td>Users</td>
</tr>
<tr>
<td>System information</td>
<td>System Announcements</td>
</tr>
</tbody>
</table>
 Deprecated Endpoints

v1/issues
v1/image_issues
API Overview

This document is a guide for programmers that describes the server-security operations available to you from the CloudPassage API. In addition, it is a detailed reference that includes sample requests, responses, and errors for all supported calls.

REST API

The CloudPassage API is a representational state transfer (REST) API. It is a collection of calls that accept and return stored Halo resources. The REST API provides access to those resources via URL paths. To use a REST API call, your application makes an HTTP request and parses the response. The request and response are in JSON format.

Because the REST API is based on open standards, you can access the API using any web development language.

Supported Methods

The methods you call are the standard HTTP methods GET, PUT, POST, and DELETE.

Encrypted HTTP Only

The CloudPassage REST API is served over HTTPS only. To ensure data privacy, unencrypted HTTP is not supported.

API Versions

The CloudPassage API is version controlled. The current version is v1, though in some cases, v2 or v3 is also available. The API version number is independent of the CloudPassage Halo agent release number. The API version number must appear in the URL of every call. For example, you use the following URL structure to request a list of firewall policies through version v1 of the CloudPassage API:

https://api.cloudpassage.com/v1/firewall_policies/

API Endpoints

The Halo API currently includes many documented API endpoints—the Halo resources that you can access through the API. An endpoint is defined by its URL, its associated objects (such as user accounts or configuration policies), and the HTTP methods used to manipulate those objects. The organization of this guide is based on those endpoints.

Call Authentication
The Halo API follows best security practices, starting with a token-based authentication system. API clients must authenticate with an ID and secret key, and receive a bearer token which can be used to fetch resources for 15 minutes until a new token is required. The secret key and ID can only be obtained through the user interface and all views of the secret portion of the key are logged. Users can restrict the IP addresses from which an API key can be used, and keys can be created with read-only or read/write permissions.

Because all access to the CloudPassage API requires authentication, the client must first authenticate with the authorization server by sending a POST request to the authorization endpoint to request an access token. This is the authorization endpoint:

https://api.cloudpassage.com/oauth/access_token?grant_type=client_credentials

The client has to provide client credentials (API key ID and API key secret) in the request. To retrieve your client credentials, access the Halo Portal web interface, select a group in the group tree, and navigate to Edit Group Settings > API Keys. The existing keys for that group are listed.

Note: API keys are created in the Halo portal by site administrators. Besides containing a client ID and client secret value, an API key can be defined as full access or read-only. A full-access key allows the client to both read from the Halo database and write modifications or new information to it. An API key can also optionally contain a list of IP addresses that restrict a client using that key to authenticate to the API from one of those addresses. For more information, see Managing Group API Keys in the Halo Operations Guide.

Send the API key ID and API key secret in an Authorization header of the POST request. Construct the Authorization header as follows:

1. Combine the API key ID and API key secret into a string "key_id:key_secret" (with a colon separating the two elements).
2. Encode the resulting string using Base64.
3. Construct the Authorization header value by specifying the authorization method followed by a space, followed by the encoded string. For example:

   Authorization: Basic aGFsbzpjbG91ZHBhc3NhZ2U=

If the request is valid, the authorization server issues an access token. The response also includes an expiration timeout (expires_in) for the access token, expressed in seconds. This is an example response:

POST https://api.cloudpassage.com/oauth/access_token?grant_type=client_credentials

HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

```
{
    "access_token": "ffad76cc550110fc4c84a18397b6e104",
    "token_type": "bearer",
    "expires_in": 900
}
```

Once your client obtains an access token, the client can use it to access protected resources until the token expires. Once the access token expires, you'll need to obtain a new token from the authorization endpoint.

When making a call to the API, pass the access token in an Authorization header field. Include the Bearer authentication scheme specification in the field, followed by a space and then the token. For example:

Authorization: Bearer ffad76cc550110fc4c84a18397b6e104

**Call Formats**
Note: In the API calls in this document, metaparameters that you must replace with values are shown with curly brackets (for example, \...{id}\}). In your call, you replace the metaparameter with the actual value (for example, \...{id}\).

Retrieving Resources with the HTTP GET Method

You can retrieve a representation of a resource by GETting its URL. For example:

```
GET https://api.cloudpassage.com/v1/servers
```

Note the use of HTTPS, and note the API version number in the URL. This call returns a list of your Halo servers and their profile information, in JSON format.

Creating or Updating Resources with the HTTP POST and PUT Methods

Creating or updating a resource involves performing an HTTP PUT or HTTP POST to a resource URL. In the PUT or POST, you represent the properties of the object you wish to update as JSON objects. Be sure that the HTTP Content-Type header is set to `application/json` for your requests. Here is an example call:

```
POST https://api.cloudpassage.com/v1/groups
```

This call creates a new group structure for your account in the Halo database. The body of your request lists, in JSON format, the required fields and optionally supplies default values for them. The response, also JSON, lists all of the new group's fields and their values, including the group's assigned URL and group ID.

Deleting Resources with the HTTP DELETE Method

To delete a resource, make an HTTP DELETE request to the resource's URL. Not all CloudPassage API resources support the DELETE operation. Here is an example that does:

```
DELETE https://api.cloudpassage.com/v1/groups/{id}
```

This call deletes the group whose group ID is `{id}`. Note that the group must be empty (must contain no servers) before you can delete it. For this action, both the call and the response have no body; the response contains only a status code in the header.

Response Codes and Error Messages

The response for every call includes a status code in a response header field with the format "HTTP/1.1 200 OK". The possible status values differ, depending on which HTTP method is used.

### Possible GET Response Status Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Status</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
<td>The request was successful and the response body contains the representation requested.</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized</td>
<td>The supplied credentials, if any, are not sufficient to access the resource.</td>
</tr>
<tr>
<td>403</td>
<td>Forbidden</td>
<td>The authorization level is not sufficient to access the resource.</td>
</tr>
<tr>
<td>404</td>
<td>Not Found</td>
<td>Resource not found.</td>
</tr>
<tr>
<td>500</td>
<td>Server Error</td>
<td>We could not return the representation due to an internal server error.</td>
</tr>
</tbody>
</table>
### Possible POST or PUT Response Status Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Status</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Created</td>
<td>The request was successful, we created a new resource and the response body contains the representation.</td>
</tr>
<tr>
<td>202</td>
<td>Accepted</td>
<td>The request was successful, new resource was accepted for processing.</td>
</tr>
<tr>
<td>204</td>
<td>No Content</td>
<td>The request was successful.</td>
</tr>
<tr>
<td>400</td>
<td>Bad Request</td>
<td>The data given in the POST or PUT failed validation. Inspect the response body for details.</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized</td>
<td>The supplied credentials, if any, are not sufficient to create or update the resource.</td>
</tr>
<tr>
<td>404</td>
<td>Not Found</td>
<td>Resource not found.</td>
</tr>
<tr>
<td>500</td>
<td>Server Error</td>
<td>We could not create or update the resource. Please try again.</td>
</tr>
</tbody>
</table>

### Possible DELETE Response Status Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Status</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>204</td>
<td>No Content</td>
<td>The request was successful; the resource was deleted.</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized</td>
<td>The supplied credentials, if any, are not sufficient to delete the resource.</td>
</tr>
<tr>
<td>404</td>
<td>Not Found</td>
<td>Resource not found.</td>
</tr>
<tr>
<td>500</td>
<td>Server Error</td>
<td>We could not delete the resource. Please try again.</td>
</tr>
</tbody>
</table>

### Custom Error Messages

#### Validation Errors

If a validation error occurs, a 422 (Unprocessable Entity) HTTP response is returned. The response body contains error details:

```
Status: 422

{
    "message": "Validation Failed",
    "errors": [
        {"code": "taken",
         "field": "name"
    ]
}
```

#### Resource Not Found Errors

If a resource not found error occurs, a 404 (Not Found) HTTP response is returned. The response body contains error details:

```
Status: 404

{
    "resource": "FirewallRule",
    "field": "id",
    "value": "3e74aaf07288012e23f3442c031a719c"
}
```

#### Server errors

If a server error occurs, a 500 (Internal Server Error) HTTP response is returned. The response body contains error details:
Pagination of Results

Results from calls that return lists of items can be paginated, and the results of some calls that typically return very large numbers of items—such as List events and List historical scans—are paginated by default. The default page size is 10 items. You can use the per_page parameter to specify a custom page size (up to 100 items), and you can use the page parameter to specify which individual page you want returned. For example:

https://api.cloudpassage.com/v1/events?per_page=50&page=4

The pagination info is included in the Link response header:

Link: <https://api.cloudpassage.com/v1/events?page=3&per_page=50>; rel="next",
<https://api.cloudpassage.com/v1/events?page=1&per_page=50>; rel="prev"

where the value for rel indicates which URL to use to retrieve the previous or next page of results.

The pagination info is also included in the response JSON:

```json
{
  "count": 300,
  "pagination": {
    "next": "https://api.cloudpassage.com/v1/events?page=3&per_page=50",
    "prev": "https://api.cloudpassage.com/v1/events?page=1&per_page=50"
  }
}
```

API Examples, Sample Code, and the Halo Toolbox

CloudPassage customers use the API to construct their own server-security management tools and to integrate Halo with other systems. In addition, CloudPassage provides code samples, scripts and libraries that demonstrate use of the API to accomplish various useful tasks.

The Halo Toolbox is a set of GitHub repositories where CloudPassage customers and employees can share and compare code that automates tasks by calling the Halo REST API. The Toolbox facilitates collaboration:

- You are encouraged to fork any of the repo's in the toolbox that interest you, then extend or improve them.
- If you would like to share your extension or improvement, just send a pull request.
- Click Watch for any repo to be alerted of changes to it.

The following list describes a few examples of the kinds of automation and integration solutions that have been developed by CloudPassage customers and employees and are posted to the Toolbox.

**Authenticating to Halo**

Any client that uses the API must first authenticate to the Halo API's "Authorization" endpoint by providing the Halo account's API
key, and then submit the returned session token when making each API call. This ensures constant API security.

The authentication method is an HTTPS POST call, as documented earlier in this section. But your software can use other languages to accomplish this task, as in this Python example:

```python
connection = httpbin.HTTPSConnection(host)
authstring = "Basic " + base64.b64encode(clientid + ":" + clientsecret)
header = {"Authorization": authstring}
params = urllib.urlencode({'grant_type': 'client_credentials'})
connection.request("POST", '/oauth/access_token', params, header)
response = connection.getresponse()
jdata = response.read().decode() data = json.loads(jdata)
key = data['access_token']
```

...or as in this Ruby example:

```ruby
client = OAuth2::Client.new(clientid, clientsecret,
    :connection_opts => { :proxy => my_proxy },
    :site => "https://#{host}",
    :token_url => '/oauth/access_token'
)
token = client.client_credentials.get_token.token
```

### Retrieving user or server information

After authenticating, your client could, for example, call the API's "Servers" endpoint to retrieve information for all active Halo-protected servers, and then print out a list of server names before closing the connection. The call is documented in the API Guide as an HTTPS GET request. In Python, it might look like this:

```python
tokenheader = {"Authorization": 'Bearer ' + key}
connection.request("GET", "/v1/servers", '', tokenheader)
response = connection.getresponse()
jdata = response.read().decode()
data = json.loads(jdata)
# iterate through json result and print out hostnames
servers = data['servers']
for server in servers:
    print server['hostname']

close()
```

...or in Ruby, like this:

```ruby
result = RestClient.get "https://#{host}/v1/servers", {
    'Authorization' => "Bearer #{token}"
}

data = JSON result.body
servers = data['servers']
servers.each do |server|
    puts server['connecting_ip_address'] + " " + server['hostname']
end
```

To examine the complete source code of these specific examples in the Toolbox, go to https://github.com/cloudpassage/api_examples.
Exporting Halo events to third-party SIEM or log-management tools

The Halo REST API includes an Events endpoint that clients can query to obtain complete information on all Halo security events (for example, detected server configuration errors or file-tampering) within a range of dates. You can use this capability to create an integration tool that feeds event data to a third-party tool for analysis.

CloudPassage has developed such a tool (the Halo Event Connector) and has made it available to customers. The tool provides direct integration with Splunk Enterprise and SumoLogic, and integration through syslog to ArcSight and other tools. For more information, see https://github.com/cloudpassage/halo-event-connector-python.

Other example API client code

Here are a few other code examples that you can examine by browsing through the Toolbox. They demonstrate a variety of ways that you can exploit the power of the Halo REST API to automate and streamline your server-security monitoring tasks.

- **Manipulating Halo workload firewall policies**
  Two Ruby examples use the API to add a rule to a firewall policy and to modify a firewall policy's source or destination IP zone.

- **Copying security policies and saving to archives**
  An example Ruby script downloads all firewall policies and file integrity policies for a Halo account, and formats them as a report for use in auditing policy changes.

- **Discovering servers that have no installed Halo agent**
  An example script uses the Ruby fog library to retrieve all of your server IP addresses from cloud providers and then cross-checks them against servers that have installed Halo agents, to let you determine whether you have any unprotected cloud servers.

- **Scanning servers within a group to detect differences among them**
  A script calls the "Server Issues" method of the Servers API endpoint for all servers in each group in turn, analyzes the results, and prepares a report for each group that summarizes how well the servers in the group have the same consistent configuration status.

- **Detecting server-local accounts whose passwords should be changed**
  A script searches all of your Linux servers for local user accounts whose passwords are stale or expired and should be changed. The script accesses the Servers API endpoint to examine all local accounts on all servers in all groups, then reports on any accounts whose last change date is older than the system-specified maximum password age.

- **Identifying the IP addresses from which Halo users have logged into the portal**
  This sample accesses the Events API endpoint and extracts the values of the user name, IP address, and country of every Halo login event within the time range that you choose.
API Best Practices

There are often multiple ways to accomplish any one objective with API interaction. We have assembled here a set of best practices for interacting with the CloudPassage Halo REST API; following these practices will make your CloudPassage Halo API integrations faster, more efficient, and more resilient.

Some of the practices already have been engineered into the CloudPassage Halo Python SDK, so we recommend using the SDK whenever your integration projects can accommodate its inclusion.

Token management

When a token has expired, the API will respond with HTTP code 402. Given that virtual machines can experience time drift, it is more predictable and programmatically concise to trigger a token update in your integration code based on the HTTP 402 response than to calculate the end of a token's lifetime and preemptively update the session token.


Pagination

Pagination takes time. You can reduce the number of pages returned from the Halo API by using specific queries. For example: instead of getting a list of all servers and iterating through the list to find the server with a specific connecting IP address, use the connecting_ip_address field in a query filter.

Example of using filters to narrow search results:

- GET https://api.cloudpassage.com/v1/servers?connecting_ip_address=8.8.8.8 gets servers with the connecting IP address of 8.8.8.8

If you use filters:

- Your responses will be more specific (less client-side processing)
- You'll have smaller response sets, which can be beneficial for avoiding API rate limits

General pagination guidance:

- Don't go more than 50 pages deep into a query.
- Query responses get slower with deeper query pagination.
- Concurrent threads against a single endpoint should not exceed 10


Time-series queries

- Time-series queries apply to endpoints that can be queried using time-oriented fields like 'since'. For instance:
If you request a 'since' value which, according to the grid, has not happened yet, you will get an HTTP response of 422: unprocessable entity. This can happen if you create a `v1/events` or `v1/scans` endpoint poller that starts at the current time and is intended to run indefinitely, and your system's current time is ahead of the Halo grid's current time.

If you are in an environment where time drift causes you to get HTTP 422 responses for requesting a 'since' value based on your system's clock (This is very common in virtualized environments), consider basing the 'since' value on the most recent item from the endpoint:

- Request the most recent item from the endpoint:
  
  https://api.cloudpassage.com/v1/events?sort_by=created_at.desc&per_page=1

- Use the timestamp from this event for the 'since' field in your query.

- Pagination and query depth best practices apply here, so use the last item's timestamp from page 50 to begin a new query. This will perform much better because deep pagination can get slower the deeper the query goes

**Authentication credential storage**

Don't save credentials in your code. Use an environment variable or a configuration file outside of your source code repository.


**Rate limiting**

Halo applies rate-limiting on a per-endpoint basis.

- You will get a HTTP 429 response code in response to overly-frequent queries against a specific API endpoint.
- In accordance with RFC 6585, you can expect a 'Retry-After' header in the HTTP response. You should wait at least the indicated number of seconds before retrying the request.
- Additionally, the response will include json, as shown below:

  ```json
  {"code": "429","message":"Too many requests","count":93,"limit":60,"retry_after":60}
  ```

  - **code**: This is the HTML response code
  - **message**: Explains the reason for the error code
  - **count**: Number of requests in the last minute
  - **limit**: Rate-limit threshold (per minute)
  - **retry-after**: Wait until this many seconds have passed before retrying your query.

**API key scope**

Follow the principle of least privilege:

- Unless it is absolutely necessary, do not create an API key with global R/W access to your account.
- Create API keys which are scoped only to the areas of concern within your group structure.
- Don't create R/W keys if RO is all that's necessary.
- Use Halo's IP address restrictions for API keys, whenever possible. This increases the level of difficulty for the user of leaked API keys.
Agent Upgrades

Site administrators can use the Agent Upgrades endpoint to schedule an agent upgrade on one or more out-of-date agents on active servers. The endpoint can also be used to find agents that need to be upgraded, cancel an agent upgrade request that was submitted, view the status of an upgrade, and view a list of all agent upgrade request jobs that were submitted.

- Prerequisites
- Find agents that need to be upgraded
- Object Representation
- Post an upgrade request
- Delete an upgrade request
- Get the status of a specific upgrade
- List all scheduled upgrades

Prerequisites

The Agent Upgrades endpoint has prerequisites that must be met to ensure successful upgrades. See these prerequisites in the Upgrading Halo Agents Remotely section of the Halo Operations Guide.

Find agents that need to be upgraded

Before you create upgrade tasks, you can see if you have agents that need to be upgraded. The following are examples of the most common queries. For a list of the most common attributes that you can use for this query, see Attributes. You can also refer to the Servers endpoint for additional attributes.

Find all agents that need to be upgraded:


Find all agents in a group that need to be upgraded:

GET https://api.cloudpassage.com/v1/servers?agent_version_lt=latest&group_id={group ID}

Note: If no servers are returned after using queries like the above, it means there are no servers that match the query that need to be upgraded.

Object Representation

Agent upgrades object location

api.cloudpassage.com/v1

├── agent_upgrades

│   └── id
Agent upgrades object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The ID of the agent upgrade request job.</td>
</tr>
<tr>
<td>total_agents</td>
<td>Once the job begins to run, this field represents the total number of agents that will be upgraded.</td>
</tr>
<tr>
<td>completed_agents</td>
<td>The number of agents in this object that have completed the upgrade.</td>
</tr>
<tr>
<td>failed</td>
<td>The number of agents that did not upgrade because the upgrade failed.</td>
</tr>
<tr>
<td>deactivated</td>
<td>The number of agents that did not upgrade because the agent had a status of deactivated.</td>
</tr>
<tr>
<td>missing</td>
<td>The number of agents that did not upgrade because the agent had a status of missing.</td>
</tr>
<tr>
<td>succeeded</td>
<td>The number of agents that successfully upgraded.</td>
</tr>
<tr>
<td>skipped</td>
<td>The number of agents that were skipped, usually because they were already up-to-date.</td>
</tr>
<tr>
<td>scheduled_at</td>
<td>The date-time at which this agent is scheduled for an upgrade (ISO-8601 format). The date and time must occur in the future.</td>
</tr>
<tr>
<td>started_at</td>
<td>The date-time at which this agent's upgrade began (ISO-8601 format).</td>
</tr>
<tr>
<td>status</td>
<td>The status of the upgrade job: scheduled, started, canceled, complete.</td>
</tr>
<tr>
<td>notify_on_complete</td>
<td>true if the person who requested the upgrade will receive an e-mail notification upon completion; otherwise it defaults to false. Note: This field is not supported for agent upgrade tasks created through the API.</td>
</tr>
</tbody>
</table>

Attributes used to specify agents to be upgraded

The following table provides attributes that you can use to specify agents to upgrade, along with examples of the JSON syntax for their variables. These are used in the POST request to create the agent upgrade task. For some attributes, you can combine multiple variables with a comma.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The Halo ID of the agent. Note that this not the same ID as the one returned in a POST response. You can separate multiple IDs with a comma. Example: &quot;id&quot;: &quot;62061ba0c11911e6a10113d2fb59ad2b&quot;, &quot;1f8fb232c13111e6a10113d2fb59ad2b&quot;, &quot;bcd55105bbe49fff6d3b2e5717d997a3&quot;</td>
</tr>
<tr>
<td>group_id</td>
<td>The Halo ID of the group to which the server belongs. Example: &quot;group_id&quot;: &quot;1f429fb6165311e7b4660fadc3c5dfce&quot; When you use group_id, all active, out-of-date agents within a group are upgraded.</td>
</tr>
<tr>
<td>os_type</td>
<td>Family of the currently installed operating system: windows or linux. Example: &quot;os_type&quot;: &quot;windows&quot;</td>
</tr>
<tr>
<td>agent_version</td>
<td>The version number of the currently installed Halo agent. Example: &quot;agent_version&quot;: &quot;latest&quot;</td>
</tr>
<tr>
<td>agent_version_gte</td>
<td>An agent version that is greater than, or equal to, the agent version specified. Example: &quot;agent_version_gte&quot;: &quot;4.1.1&quot;</td>
</tr>
<tr>
<td>agent_version_gt</td>
<td>An agent version that is greater than the agent version specified. Example: &quot;agent_version_gt&quot;: &quot;4.0.0&quot;</td>
</tr>
<tr>
<td>agent_version_lte</td>
<td>An agent version that is less than, or equal to, the agent version specified. Example: &quot;agent_version_lte&quot;: &quot;4.1.3&quot;</td>
</tr>
<tr>
<td>agent_version_lt</td>
<td>An agent version that is less than the agent version specified. Example: &quot;agent_version_lt&quot;: &quot;latest&quot;</td>
</tr>
</tbody>
</table>
Post an upgrade request

Upgrading out-of-date agents through the Halo API involves posting an upgrade request that:

- Specifies the agent(s) you want to upgrade by using attributes from the **Attributes** table.
- Indicates the time at which you want the upgrade task to run.

When you make an upgrade request call, you are creating an upgrade request job that contains the servers that meet the attributes you specify. You are simultaneously creating a task to run the job.

*Note:* If there are more than 2,500 agents included in the upgrade task, only 2,500 will be upgraded. You can make another request to upgrade additional agents.

To post an upgrade request, follow these steps:

1. Determine which agents you want to upgrade:
   - If you already know which agents you want to upgrade, use the **Attributes** table to find the combination of attributes and variables that you will use to formulate the upgrade request.
   - If you are not yet sure which agents you want to upgrade, find the agents that need to be upgraded. Then, use attributes from the response to formulate the upgrade request.

2. Formulate a standard request JSON for a POST call using the attributes and variables from the previous step.

   For example, if you want to upgrade active, out-of-date Linux agents that are in a specific group, you would use the following attributes: **os_type, group_id, agent_version_lt**.

   To schedule the upgrade task, use **scheduled_at**, which is a future date-time when you want the upgrade to occur (in ISO-8601 format). No value indicates "now."

   Examples:

   **Upgrade (now) all active, out-of-date Linux agents in a specific group:**

   ```json
   { "upgrade": { "os_type": "linux", "group_id": "1f429fb6165311e7b4660fadc3c5dfce", "agent_version_lt": "latest", "scheduled_at": "" }, } ```

   **Upgrade only specific active agents, and schedule the upgrade to occur at a specific time:**

   ```json
   { "upgrade": { "id": "62061ba0c11911e6a10113d2fb59ad2b", "1f8fb232c13111e6a10113d2fb59ad2b", "bcd55105bbe49fff6d3b2e5717d997a3", "scheduled_at": "2017-10-27T17:57:21.912Z" }, } ```

3. Post your request to the agent_upgrades endpoint:

   ```
   ```

Response
Delete a scheduled upgrade

Deletes a scheduled upgrade job that you specify by ID. If the call is successful, the scheduled upgrade request is canceled and no action is taken on any of the agents within that job.

*Note:* Scheduled upgrade requests can only be canceled by the user who created them.

**DELETE** https://api.cloudpassage.com/v1/agent_upgrades/{id of the agent upgrade request}

**Response**

**Status:** 204

Get status of a specific agent upgrade

You can use this request to view the progress of each agent upgrade request. You can make this call within 24 hours after an upgrade completes to view the completed status. Returns JSON-formatted results listing the status of a specific scheduled and started upgrade request.

*Note:* Scheduled upgrade requests can only be viewed by the user who created them.

**GET** https://api.cloudpassage.com/v1/agent_upgrades/{id of the agent upgrade request}

**Response**

**Status:** 200

```json
{
  id: "480bc016bb4011e781a44dbd0ad693e2",
  total_agents: 1,
  completed_agents: 1,
  failed: 0,
  deactivated: 0,
  succeeded: 0,
  missing: 0,
  skipped: 0,
  notify_on_complete: false
}
```
List all scheduled agent upgrades

Returns JSON-formatted results listing all of your scheduled and started upgrade requests.

**Note:** Scheduled upgrade requests can only be viewed by the user who created them.

**GET** https://api.cloudpassage.com/v1/agent_upgrades

**Response**

**Status:** 200

```
{
  upgrades : [
    {
      id: "480bc016bb4011e781a44dbd0ad693e2",
      total_agents: 3,
      completed_agents: 0,
      failed: 0,
      deactivated: 0,
      missing: 0,
      succeeded: 0,
      skipped: 0,
      started_at: "2017-10-27T18:00:11.437Z",
      status: "started",
      notify_on_complete: false
    },
    {
      id: "048969b4c95b11e7ac8c15557c542f6a",
      total_agents: null,
      completed_agents: 0,
      failed: 0,
      deactivated: 0,
      missing: 0,
      succeeded: 0,
      skipped: 0,
      scheduled_at: "2017-11-14T16:44:01.341Z",
      started_at: null,
      status: "scheduled",
      notify_on_complete: false
    }
  ]
}
```
Halo Connectors

A Halo connector is a specialized Halo agent that can access container registries (private Docker registries or Amazon EC2 registries), which hold container images. Use the Halo Connectors endpoint to list and view the details of the Halo connectors (spelled collectors in the API) in your environment.

- Object Representation
- List collectors
- Get a single collector

Object Representation

Collector object location

api.cloudpassage.com/v1

```
collectors
  id
```

Collector fields

These fields are returned by the List collectors method and the Get single collector method.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The Halo ID of this connector.</td>
</tr>
<tr>
<td>registry_id</td>
<td>The Halo ID of the private Docker registry that this connector accesses.</td>
</tr>
<tr>
<td>group_id</td>
<td>The Halo ID of the group to which this connector belongs.</td>
</tr>
<tr>
<td>status</td>
<td>The status of the connector: active, missing, or deactivated.</td>
</tr>
<tr>
<td>hostname</td>
<td>The hostname of the server on which this connector is installed.</td>
</tr>
<tr>
<td>server_label</td>
<td>The Halo label, if any, attached to this connector's host server.</td>
</tr>
<tr>
<td>fqdn</td>
<td>The fully qualified domain name of this connector's host server.</td>
</tr>
<tr>
<td>platform</td>
<td>The platform (linux or windows) of this connector's host server.</td>
</tr>
<tr>
<td>os_version</td>
<td>The version number of the connector's operating system.</td>
</tr>
<tr>
<td>os_name</td>
<td>The name of the operating system.</td>
</tr>
<tr>
<td>version</td>
<td>The Halo agent version number of the connector.</td>
</tr>
<tr>
<td>connecting_ip_address</td>
<td>The IP address that this connector uses to access an image registry.</td>
</tr>
<tr>
<td>created_at</td>
<td>The date-time at which this connector was created. (ISO-8601 format)</td>
</tr>
<tr>
<td>updated_at</td>
<td>The date-time at which this connector was last modified. (ISO-8601 format)</td>
</tr>
<tr>
<td>self_verification_failed</td>
<td>true if the connector's last self-verification test failed; otherwise false.</td>
</tr>
<tr>
<td>last_self_verification_at</td>
<td>The date-time at which the connector's last self-verification test was performed. (ISO-8601 format)</td>
</tr>
</tbody>
</table>
List collectors

Returns JSON-formatted results listing the fields for all deployed Halo connectors.

GET https://api.cloudpassage.com/v1/collectors/

Response

Status: 200

```
{
  "collectors": [
    {
      "id": "f2d43e8d-a093-4a89-9d1e-33b26ee9ef0c",
      "registry_ids": [
        "2d76fa60-1540-4f0e-8008-43bf33844bec"
      ],
      "group_id": "b3da420ce5c711e784874b84dddbc1aa",
      "status": "active",
      "hostname": "ip-10-10-15-217",
      "server_label": "Connector-Demo",
      "fqdn": "ip-10-10-15-217.us-west-1.compute.internal",
      "platform": "Linux",
      "os_version": "16.04",
      "os_name": "ubuntu",
      "version": "4.1.6",
      "connecting_ip_address": "52.53.149.31",
      "created_at": "2017-12-20T20:58:17.130277Z",
      "updated_at": "2017-12-20T20:58:19.610275Z",
      "self_verification_failed": false,
      "last_self_verification_at": "2017-12-21T17:58:19.353737Z"
    }
  ],
  "count": 1,
  "pagination": {}
}
```

Get a single collector

Returns the fields of the Halo connector specified by ID in the method URL. To obtain the ID required for this method, you can first call the List collectors method.

GET https://api.cloudpassage.com/v1/collectors/{id}

Response

Status: 200

```
{
  "collector": {
    "id": "f2d43e8d-a093-4a89-9d1e-33b26ee9ef0c",
    "registry_ids": [
      "2d76fa60-1540-4f0e-8008-43bf33844bec"
    ],
    "group_id": "b3da420ce5c711e784874b84dddbc1aa",
    "status": "active",
    "hostname": "ip-10-10-15-217",
    "server_label": "Connector-Demo",
    "fqdn": "ip-10-10-15-217.us-west-1.compute.internal",
    "platform": "Linux",
    "os_version": "16.04",
    "os_name": "ubuntu",
    "version": "4.1.6",
    "connecting_ip_address": "52.53.149.31",
    "created_at": "2017-12-20T20:58:17.130277Z",
    "updated_at": "2017-12-20T20:58:19.610275Z",
    "self_verification_failed": false,
    "last_self_verification_at": "2017-12-21T17:58:19.353737Z"
  }
}
```
}

}

"updated_at
": "2017-12-20T20:58:19.610275Z"
,
"self_verification_failed
": false ,
"last_self_verification_at
": "2017-12-21T17:58:19.353737Z"

20


Containers

Containers are lightweight executable software packages that provide complete environments within which applications can execute as standardized units. Use the Containers endpoint to retrieve the attributes of one or all instantiated containers in your Halo-protected server environment.

- Object Representation
- List containers
- Get a single container

Object Representation

Container object location

```
api.cloudpassage.com/v1
containers

id
```

Container object fields

These fields and the fields of the `details` object (described below) are returned by the List containers call and the Get a single container call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer_id</td>
<td>(not used)</td>
</tr>
<tr>
<td>id</td>
<td>The Halo ID of the container. (This is also its Docker ID.)</td>
</tr>
<tr>
<td>native_id</td>
<td>The Halo ID of the container. (This is also its Docker ID.)</td>
</tr>
<tr>
<td>os_name</td>
<td>The operating system provided by the container to its applications. Supported systems are ubuntu, centos, redhat, debian, and amazon.</td>
</tr>
<tr>
<td>os_version</td>
<td>The version number of the operating system.</td>
</tr>
<tr>
<td>created_at</td>
<td>The date and time of the creation (instantiation) of the container.</td>
</tr>
<tr>
<td>started_at</td>
<td>The date and time at which the container was most recently started.</td>
</tr>
<tr>
<td>discovered</td>
<td>The date and time at which the container was first detected.</td>
</tr>
<tr>
<td>last_scan_at</td>
<td>The date and time at which the container was most recently scanned.</td>
</tr>
<tr>
<td>exited_at</td>
<td>The date and time at which the container was last shut down.</td>
</tr>
<tr>
<td>paused_at</td>
<td>the date and time at which all processes in the container were last paused.</td>
</tr>
<tr>
<td>unpause_at</td>
<td>The date and time at which all processes in the container resumed execution after a pause.</td>
</tr>
<tr>
<td>stopped_at</td>
<td>The date and time at which the container was last stopped.</td>
</tr>
<tr>
<td>removed_at</td>
<td>The date and time at which the container was removed from its server.</td>
</tr>
<tr>
<td>image_id</td>
<td>The ID of the image from which the container was instantiated.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sha</td>
<td>The Docker SHA-256 representation of the container's image.</td>
</tr>
<tr>
<td>image</td>
<td>An array of attributes of the container's image. Includes the following subfields:</td>
</tr>
<tr>
<td>registry_id</td>
<td>The ID of the registry in which this image is stored.</td>
</tr>
<tr>
<td>registry</td>
<td>Attributes the registry in which this image is stored.</td>
</tr>
<tr>
<td>id</td>
<td>The Halo ID of the registry.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the registry.</td>
</tr>
<tr>
<td>repository_id</td>
<td>The Halo ID of the repository in which this image is stored.</td>
</tr>
<tr>
<td>repository</td>
<td>Attributes the repository in which this image is stored. Includes the following subfields:</td>
</tr>
<tr>
<td>tag</td>
<td>The version tag assigned to the container's image.</td>
</tr>
<tr>
<td>id</td>
<td>The Halo ID of the container's image.</td>
</tr>
<tr>
<td>sha</td>
<td>The Docker SHA-256 representation of the container's image.</td>
</tr>
<tr>
<td>digest</td>
<td>A cryptographic digest (hash) of the container's image.</td>
</tr>
<tr>
<td>current</td>
<td><strong>true</strong> if the image is the most recently built one in its repository; <strong>false</strong> if not.</td>
</tr>
<tr>
<td>status</td>
<td>The Halo monitoring status of the image: monitored, unmonitored, or missing.</td>
</tr>
<tr>
<td>image_os</td>
<td>The operating system internal to the container's image.</td>
</tr>
<tr>
<td>image_os_version</td>
<td>The version number of the operating system internal to the container's image.</td>
</tr>
<tr>
<td>repo_name</td>
<td>The name of the repository that stores this container's image.</td>
</tr>
<tr>
<td>server_id</td>
<td>The Halo ID of the server on which this container runs.</td>
</tr>
<tr>
<td>server</td>
<td>An array of attributes of the server on which the container is running. Includes the following subfields:</td>
</tr>
<tr>
<td>os_name</td>
<td>The container's host OS: the operating system of the server that the container runs on. Supported values are amazon, centos, debian, fedora, oracle, redhat, ubuntu, windows.</td>
</tr>
<tr>
<td>os_version</td>
<td>The version number of the server's operating system.</td>
</tr>
<tr>
<td>name</td>
<td>The hostname of the server.</td>
</tr>
<tr>
<td>group_id</td>
<td>The Halo ID of the group to which the server belongs.</td>
</tr>
<tr>
<td>status</td>
<td>Current runtime status of the container. Possible values are running, exited, paused, stopped, killed, removed, monitored, created.</td>
</tr>
<tr>
<td>foreground</td>
<td><strong>true</strong> if the container process runs in the foreground; <strong>false</strong> if it runs in the background.</td>
</tr>
<tr>
<td>interactive</td>
<td><strong>true</strong> if the container has a shell interface; <strong>false</strong> if not.</td>
</tr>
<tr>
<td>auto_remove</td>
<td><strong>true</strong> if the container is configured to remove itself when it exits; <strong>false</strong> if not.</td>
</tr>
<tr>
<td>logging_driver</td>
<td>The name of the Docker logging driver.</td>
</tr>
<tr>
<td>workdir</td>
<td>Path to the working directory of the container process.</td>
</tr>
<tr>
<td>pid</td>
<td>The process ID of the container process.</td>
</tr>
<tr>
<td>uts</td>
<td>The UTS namespace of the container.</td>
</tr>
<tr>
<td>ipc</td>
<td>The container's IPC setting, for controlling shared memory.</td>
</tr>
<tr>
<td>restart_policy</td>
<td>The restart policy, if any, used by the container. Supported values are no, on-failure, always, unless-stopped.</td>
</tr>
<tr>
<td>app_armor_profile</td>
<td>Name of the container's AppArmor profile.</td>
</tr>
<tr>
<td>cgroup</td>
<td>The container's control group, if any.</td>
</tr>
<tr>
<td>driver</td>
<td>The container's storage driver, if any.</td>
</tr>
<tr>
<td>error</td>
<td>The container's error output. If not specified, it is <strong>STDERR</strong>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>network_mode</td>
<td>The type of Docker network that the container uses. Supported values are <code>default (= bridge)</code> and <code>host</code>.</td>
</tr>
<tr>
<td>path</td>
<td>Value of the container's PATH environment variable.</td>
</tr>
<tr>
<td>ports</td>
<td>Array of the container's open ports.</td>
</tr>
<tr>
<td>entrypoint</td>
<td>Array of Docker ENTRYPOINT commands for the container.</td>
</tr>
<tr>
<td>command</td>
<td>Array of command-line options for the entrypoint command.</td>
</tr>
<tr>
<td>args</td>
<td>Array of additional arguments, if any, for the entrypoint command.</td>
</tr>
<tr>
<td>security_options</td>
<td>Array of security options, if any, for the entrypoint command.</td>
</tr>
<tr>
<td>capabilities</td>
<td>An array of the commands accepted by the container. Supported values are AUDIT_WRITE, CHOWN, DAC_OVERRIDE, FSETID, FOWNER, KILL, MKNOD, NET_RAW, NET_BIND_SERVICE, SETUID, SETGID, SETFCAP, SETCAP, SYS_CHROOT</td>
</tr>
<tr>
<td>volumes</td>
<td>Array of external volumes represented in the container's file system.</td>
</tr>
<tr>
<td>labels</td>
<td>Array of labels that have been assigned to the container.</td>
</tr>
<tr>
<td>env</td>
<td>An array of the defined environment variables used by the container.</td>
</tr>
<tr>
<td>mounts</td>
<td>An array of the mount points of external storage devices in the container's file system.</td>
</tr>
<tr>
<td>writable</td>
<td><code>true</code> if the container accepts data input; <code>false</code> if it is read-only.</td>
</tr>
<tr>
<td>rogue</td>
<td><code>true</code> if the container's image is unknown to Halo; <code>false</code> if the image is accessible.</td>
</tr>
<tr>
<td>vulnerable</td>
<td><code>true</code> if the container contains one or more known software vulnerabilities (CVEs); <code>false</code> if not.</td>
</tr>
<tr>
<td>privileged</td>
<td><code>true</code> if the container belongs to the root Halo group; <code>false</code> if it does not.</td>
</tr>
<tr>
<td>details</td>
<td>Docker-generated information about the container. This information is returned by the <code>docker inspect</code> command, and it is also displayed under the Container Details &gt; Inspect tab in the Halo portal. The fields of this object are described in the following table, &quot;Container details object fields&quot;.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the container.</td>
</tr>
</tbody>
</table>

**Container details object fields**

This object and its fields are contained within the `details` subobject of the `containers` object (above), which is returned by the `List containers` call and the `Get a single container` call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppArmorProfile</td>
<td>The AppArmor security profile associated with the container. Default profile name = <code>docker-default</code>. Contains the following subfields:</td>
</tr>
<tr>
<td>Args</td>
<td>An array of name-value arguments for the profile command line.</td>
</tr>
<tr>
<td>Config</td>
<td>An array of configuration settings for the profile.</td>
</tr>
<tr>
<td>Created</td>
<td>The timestamp (in ISO-8601 format) of the creation of the container.</td>
</tr>
<tr>
<td>Driver</td>
<td>Information describing drivers used by the container. Includes the following subobjects:</td>
</tr>
<tr>
<td>GraphDriver</td>
<td>Path to an external graph driver, if used.</td>
</tr>
<tr>
<td>HostConfig</td>
<td>A set of host configuration settings needed by the driver.</td>
</tr>
<tr>
<td>HostnamePath</td>
<td>Path to the container's hostname file.</td>
</tr>
<tr>
<td>HostsPath</td>
<td>Path to the container's hosts file.</td>
</tr>
<tr>
<td>id</td>
<td>The Docker ID of the container.</td>
</tr>
<tr>
<td>image</td>
<td>The SHA-256 hash of the container's image.</td>
</tr>
<tr>
<td>LogPath</td>
<td>The path to the containers log file.</td>
</tr>
<tr>
<td>MountLabel</td>
<td>A label associated with the container's mount point.</td>
</tr>
<tr>
<td>Mounts</td>
<td>An array of external mounted on the container's file system.</td>
</tr>
<tr>
<td>Name</td>
<td>The pathname of the container.</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>NetworkSettings</td>
<td>The container's network settings plus the settings of the container's implemented network type (such as &quot;bridge&quot;).</td>
</tr>
<tr>
<td>Path</td>
<td>The path to the shell for accessing the container.</td>
</tr>
<tr>
<td>Platform</td>
<td>The container's platform: <strong>linux</strong> or <strong>windows</strong>.</td>
</tr>
<tr>
<td>ProcessLabel</td>
<td></td>
</tr>
<tr>
<td>ResolveConfPathl</td>
<td></td>
</tr>
<tr>
<td>RestartCount</td>
<td>The number of times the container has been restarted.</td>
</tr>
<tr>
<td>State</td>
<td>A set of attributes that describe the current execution state of the container.</td>
</tr>
</tbody>
</table>

**Sorting**

You can sort the results of the **List containers** call by the values of the following attributes. Use the operator suffixes `.asc` and `.desc` to specify ascending or descending order—for example, specify `name.asc` to sort by the container name in ascending order.

- `name`
- `server_os`
- `image_name`
- `image_sha`
- `image_current`
- `registry_name`

**Grouping**

You can group the results of the **List containers** call by values of the following attribute:

- `group_id`

**List containers**

Returns JSON-formatted results listing all instantiated containers, whether currently running or not, on all the Halo-protected servers in your environment.

**GET** https://api.cloudpassage.com/v1/containers/

**Response**

**Status: 200**

```json
{
  "containers": [
    {
      "customer_id": "eb37841a-e051-11e7-8749-63337ee05204",
      "id": "d144f22d3067edace690afcb287f50c9f6f6178e5e30839f79e0d468a484aa4d74e",
      "native_id": "d144f22d3067edace690afcb287f50c9f6f6178e5e30839f79e0d468a484aa4d74e",
      "os_name": "",
      "os_version": "",
      "created_at": "2017-12-13T22:29:48Z",
      "started_at": "2017-12-13T22:29:48.884Z",
      "discovered": "2017-12-13T22:29:55.299Z",
      "last_scan_at": "2017-12-13T22:29:55.299Z",
      "exited_at": null,
      "paused_at": null,
      "unpaused_at": null,
      "stopped_at": null,
```
null,
"image_id": "unknown",
"sha": "d144f22d3067edac690afcb287f50e9f6178e5e30839f79e0d468a484aa4d74e",
"image": 
  
  "registry": 
    
    "id": "",
    "name": "",
  
  "repository": 
    
    "id": "",
    "name": "sha256:de800dceea774ec5379e86c5f59f9bab99984d03aae5d7cdef1e859cb52388"
  
  "tag": "",
  
  "id": "d144f22d3067edac690afcb287f50e9f6178e5e30839f79e0d468a484aa4d74e",
  
  "sha": "sha256:de800dceea774ec5379e86c5f59f9bab99984d03aae5d7cdef1e859cb52388",
  
  "digest": "",
  
  "current": false,
  
  "status": "",
  
  "image_os": "",
  
  "image_os_version": ""

"repo_name": "sha256:de800dceea774ec5379e86c5f59f9bab99984d03aae5d7cdef1e859cb52388",
"server_id": "121ef60ce05311e7a37b258db8fca227",
"server": 
  
  "os_name": "ubuntu",
  
  "os_version": "16.04",
  
  "name": "ip-10-10-12-95",
  
  "group_id": "eb4e21ce05111e7874963337ee05204"

"status": "created",
"foreground": false,
"interactive": false,
"auto_remove": false,
"logging_driver": "json-file",
"workdir": "",
"pid": "private",
"uts": "default",
"ipc": "shareable",
"restart_policy": "",
"app_armor_profile": "docker-default",
"cgroup": "",
"driver": "overlay2",
"error": "",
"network_mode": "default",
"path": "/bin/sh",
"ports": [],
"entrypoint": [],
"command": [],
"args": [],
"security_options": [],
"capabilities": [],
"AUDIT_WRITE",
"CHOWN",
"DAC_OVERRIDE",
"FOWNER",
"KILL",
"MKMKNOD",
"NET_RAW",
"NET_BIND_SERVICE",
"SETUID",
"SETGID",
"SETPCAP",
"SETPFCAP",
"SYS_CHROOT"

"volumes": [],
"labels": [],
"env": [],
"PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

"mounts": [],
"writable": true,
"rogue": false,
"vulnerable": false,
"privileged": false,
"details": ""
"AppArmorProfile": "docker-default",
"Args": [
  "-c",
  "echo -n KERNEL= && uname -r && echo -n KERNEL_NAME= && uname -s && echo -n ...
]
},
"Config": {
  "AttachStderr": false,
  "AttachStdin": false,
  "AttachStdout": false,
  "Domainname": "",
  "Entrypoint": [
    "bin/sh",
    "-c",
    "echo -n KERNEL= && uname -r && echo -n KERNEL_NAME= && uname -s && echo ...
  ],
  "Env": [
    "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
  ],
  "Hostname": "d144f22d3067",
  "Image": "sha256:de800dceea774ec5379ef86c6f5f9f9bab99984d03aec5d7cdeffe9859c52388",
  "Labels": [],
  "OpenStdin": false,
  "StdinOnce": false,
  "Tty": false,
  "User": "",
  "WorkingDir": ""
},
"Created": "2017-12-13T22:29:48.614863393Z",
"Driver": "overlay2",
"GraphDriver": {
  "Name": "overlay2"
},
"HostConfig": {
  "AutoRemove": false,
  "BlkioWeight": 0,
  "Cgroup": "",
  "CgroupParent": "",
  "ConsoleSize": [0, 0],
  "ContainerIDFile": "",
  "CpuCount": 0,
  "CpuPercent": 0,
  "CpuPeriod": 0,
  "CpuQuota": 0,
  "CpuRealtimePeriod": 0,
  "CpuRealtimeRuntime": 0,
  "CpuShares": 0,
  "CpusetCpus": "",
  "CpusetMems": "",
  "DiskQuota": 0,
  "IOMaximumBandwidth": 0,
  "IOMaximumIOps": 0,
  "IpcMode": "shareable",
  "Isolation": "",
  "KernelMemory": 0,
  "LogConfig": {
    "Config": [],
    "Type": "json-file"
  },
  "Memory": 0,
  "MemoryReservation": 0,
  "MemorySwap": 0,
  "NanoCpus": 0,
  "NetworkMode": "default",
  "OomKillDisable": false,
  "OomScoreAdj": 0,
  "PidsLimit": 0,
  "Privileged": false,
  "PublishAllPorts": false,
  "ReadonlyRootfs": false,
  "RestartPolicy": {
    "MaximumRetryCount": 0,
    "Name": ""
  },
  "Runtime": "runc",
  "ShmSize": 67108864,
  "UTSMode": ""
Get a single container

Returns JSON-formatted results displaying the attributes of the individual container specified by ID in the call URL.
GET https://api.cloudpassage.com/v1/containers/{id}

Response

Status: 200

```
{
  "container": {
    "customer_id": "eb37841a-e051-11e7-8749-63337ee05204"
  },
  "id": "edd3d81384dbda2e3f08276a2b314ddfd3cd48975807ba87ba8d62f38c7e61029"
},
  "created_at": "2017-12-13T22:24:33Z",
  "started_at": "2017-12-13T22:24:33.845Z",
  "discovered": "2017-12-13T22:24:34.637Z",
  "last_scan_at": "2017-12-13T22:24:34.637Z",
  "exited_at": null,
  "paused_at": null,
  "unpaused_at": null,
  "stopped_at": null,
  "removed_at": null,
  "image_id": null,
  "sha": "edd3d81384dbda2e3f08276a2b314ddfd3cd48975807ba87ba8d62f38c7e61029"
},
  "image": {
    "registry_id": "",
    "registry": {
      "id": "",
      "name": ""
    },
    "repository_id": "",
    "repository": {
      "id": "",
      "name": "sha256:79dbcfa8f169d0a0b5ec24cd257a1d503ad4045c237972d52be5b2f65fed049"
    },
    "tag": "",
    "id": "edd3d81384dbda2e3f08276a2b314ddfd3cd48975807ba87ba8d62f38c7e61029"
  },
  "repo_name": "sha256:79dbcfa8f169d0a0b5ec24cd257a1d503ad4045c237972d52be5b2f65fed049",
  "server_id": "121ef60ce5531e7a37b258db8fca227",
  "server": {
    "os_name": "ubuntu",
    "os_version": "16.04",
    "name": "ip-10-10-12-95",
    "group_id": "eb4c2a1ce0511e7874963337ee05204"
  },
  "status": "running",
  "foreground": false,
  "interactive": false,
  "auto_remove": false,
  "logging_driver": "json-file",
  "workdir": "",
  "pid": "private",
  "uts": "default",
  "ipc": "shareable",
  "restart_policy": ""
}
```

28
"FSETID",  
"OWNER",  
"KILL",  
"MKNOD",  
"NET_RAW",  
"NET_BIND_SERVICE",  
"SETUID",  
"SETGID",  
"KILL",  
"MKNOD",  
"SETGID",  
"SETFCAP",  
"NET_RAW",  
"NET_BIND_SERVICE",  
"SETUID",  
"SETGID",  
"SETPCAP",  
"SETFCAP",  
"SYS_CHROOT"
],
"volumes": [],
"labels": [],
"env": {
  "PATH": "/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
},
"mounts": [],
"writable": true,
"rogue": false,
"volatile": false,
"volumes": [],
"labels": [],
"env": {
  "PATH": "/usr/local/bin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
},
"labels": [],
"env": {
  "PATH": "/usr/local/bin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
},
"hostname": "ed3d81384db",
"image": "sha256:79dbcfa8f169d0a00b5ec224cd257a1d303ad4045c237972d52be5b2f65fed049",
"labels": [],
"labels": [],
"env": {
  "PATH": "/usr/local/bin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
},
"created": "2017-12-13T22:24:33.572769282Z",
"driver": "overlay2",
"graphDriver": {
  "data": {
    "lowerDir": "/var/lib/docker/overlay2/ca0a402b2a2fafe877cc72e43169e41049077c6f49c7f48...",
    "mergedDir": "/var/lib/docker/overlay2/ca0a402b2a2fafe877cc72e43169e41049077c6f49c7f48...",
    "upperDir": "/var/lib/docker/overlay2/ca0a402b2a2fafe877cc72e43169e41049077c6f49c7f48...",
    "workDir": "/var/lib/docker/overlay2/ca0a402b2a2fafe877cc72e43169e41049077c6f49c7f48..."
  },
  "name": "overlay2"
},
"hostConfig": {
  "autoRemove": false,
  "blkioWeight": 0,
  "cgroup": "",
  "cgroupParent": "",
  "consoleSize": [0, 0],
  "containerIdFile": "",
  "cpuCount": 0,
  "cpuPercent": 0,
  "cpuPeriod": 0,
  "cpuQuota": 0,
  "cpuRealtimePeriod": 0,
  "cpuRealtimeRuntime": 0,
  "cgroup": "",
  "cgroupParent": "",
  "cgroup": "",
  "cgroupParent": "",
  "cgroup": "",
  "cgroup": "",
  "diskQuota": 0,
  "gpm": "",
  "iOMaximumBandwidth": 0,
  "iOMaximumIOps": 0,
  "ipMode": "shareable",
  "isolation": "",
  "kernelMemory": 0,
  "logConfig": {
    "config": []
  }
}
Container Batch (for container inspection)

Use the Batch API endpoint to turn container inspection on or off for one or more Halo-protected servers. For a discussion of what container inspection means, see Activating and Enabling Container Secure in the Container Secure User Guide.

- Object Representation
- Set container inspection state

Object Representation

Summary object location

api.cloudpassage.com/v1

├── servers
│   └── batch

Batch object fields

These fields are specified in the Set container inspection state method call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ids</td>
<td>A comma-separated array of the Halo IDs of servers whose container inspection state is to be set.</td>
</tr>
<tr>
<td>docker_inspection</td>
<td>Specify true to enable inspection, false to disable inspection.</td>
</tr>
</tbody>
</table>

Set container inspection state

Sets the container-inspection state of the server or servers specified in the request JSON to the value specified in the request JSON.

A successful call returns a multistatus code of 207, with a status of 204 for each individual server whose inspection status successfully changed.

POST https://api.cloudpassage.com/v1/servers/batch

Request

```
{
   "ids": ["252874a45fc311e8df121b3c3c9b29f"],
   "data": {
      "docker_inspection": true
   }
}
```
Response

Status: 207

```json
{
  "multistatus": [
    {
      "href": "https://api-cpg.ng.cloudpassage.com/v1/servers/342d0ef45f5c11e889447f37612c6c00",
      "status": 204
    },
    {
      "href": "https://api-cpg.ng.cloudpassage.com/v1/servers/126c7eac5f5d11e8acbc1bd26eef1a4c",
      "status": 204
    }
  ]
}
```
Container Events

Use the Container Events endpoint to retrieve the event history of a specified container.

- Object Representation
- List container events

Object Representation

Container events object location

api.cloudpassage.com/v1

container_events

id

Container events object fields

These fields are returned by the List container events method.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The Halo ID of the container event.</td>
</tr>
<tr>
<td>created_at</td>
<td>The date and time when the event was created (in ISO-8601 format).</td>
</tr>
<tr>
<td>type</td>
<td>The type of the event. See Supported event types, below.</td>
</tr>
<tr>
<td>user</td>
<td>The Halo user that was logged in at the time of the event's creation.</td>
</tr>
<tr>
<td>command</td>
<td>The Docker command that led to the creation of the event.</td>
</tr>
</tbody>
</table>

Supported event types

<table>
<thead>
<tr>
<th>Event type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attach</td>
<td>Local standard input, output, and error streams connected to the container.</td>
</tr>
<tr>
<td>commit</td>
<td>Changed container saved as a new image.</td>
</tr>
<tr>
<td>copy</td>
<td>Files or folders copied to or from the container.</td>
</tr>
<tr>
<td>create</td>
<td>Container created.</td>
</tr>
<tr>
<td>destroy</td>
<td>Container permanently deleted.</td>
</tr>
<tr>
<td>detach</td>
<td>Local standard input, output, and error streams disconnected from the container.</td>
</tr>
<tr>
<td>die</td>
<td>Container instructed to cease running.</td>
</tr>
<tr>
<td>exec_create</td>
<td>A create command executed within the container.</td>
</tr>
<tr>
<td>exec_detach</td>
<td>A detach command executed within the container.</td>
</tr>
<tr>
<td>exec_start</td>
<td>A start command executed within the container.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>export</td>
<td>The container's file system exported as a tar archive.</td>
</tr>
<tr>
<td>health_status</td>
<td>Container health-check occurred.</td>
</tr>
<tr>
<td>kill</td>
<td>Non-running container stopped permanently.</td>
</tr>
<tr>
<td>oom</td>
<td>Container killed due to an out-of-memory condition.</td>
</tr>
<tr>
<td>pause</td>
<td>Running container paused execution.</td>
</tr>
<tr>
<td>rename</td>
<td>Container renamed.</td>
</tr>
<tr>
<td>resize</td>
<td>Container size changed.</td>
</tr>
<tr>
<td>restarted</td>
<td>Container restarted.</td>
</tr>
<tr>
<td>start</td>
<td>Non-running container instructed to start.</td>
</tr>
<tr>
<td>stop</td>
<td>Container stopped.</td>
</tr>
<tr>
<td>top</td>
<td>Container's running processes displayed.</td>
</tr>
<tr>
<td>unpause</td>
<td>Container resumed running from a pause.</td>
</tr>
<tr>
<td>update</td>
<td>Container configuration updated.</td>
</tr>
</tbody>
</table>

**List Container Events**

Returns JSON-formatted results listing all container-related events that have occurred for the container specified in the call URL, since it was first instantiated.

**GET** https://api.cloudpassage.com/v1/container_events?container_id={id}

**Response**

**Status:** 200

```json
{
    "container_events": [
        {
            "id": "77c6c7f3-2381-449f-bd58-27b0d9f8e285",
            "command": "docker create f646fe13d0459e11c79472e33908e730cc5d1680711d2d16e33754cf29ce7923",
            "user": "",
            "type": "create",
            "created_at": "2017-11-03T16:15:53Z"
        },
        {
            "id": "68e6a935-9ba3-4d7d-b966-3df6f734476d",
            "command": "docker top f646fe13d0459e11c79472e33908e730cc5d1680711d2d16e33754cf29ce7923",
            "user": "",
            "type": "top",
            "created_at": "2017-11-03T16:16:00Z"
        },
        {
            "id": "e9c25b60-162a-4f19-9147-9d60d8f232cb",
            "command": "docker top f646fe13d0459e11c79472e33908e730cc5d1680711d2d16e33754cf29ce7923",
            "user": "",
            "type": "top",
            "created_at": "2017-11-03T16:16:16Z"
        },
        {
            "id": "2678ffee-7045-4564-9de1-2e5867b3b2cc",
            "command": "docker top f646fe13d0459e11c79472e33908e730cc5d1680711d2d16e33754cf29ce7923",
            "user": "",
            "type": "top",
            "created_at": "2017-11-03T16:19:56Z"
        }
    ],
    "count": 4,
    "pagination": {}
}
```
Container Images

A container image is the stored snapshot of a container. Use the Container Images endpoint to list and view the images known to Halo.

- Object Representation
- List images
- Get a single image

Object Representation

Image object location

api.cloudpassage.com/v1/images

Image object summary fields

These fields are returned from the List images call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The Halo ID of this container image.</td>
</tr>
<tr>
<td>registry_id</td>
<td>The Halo ID of the registry containing the image.</td>
</tr>
<tr>
<td>repository_id</td>
<td>The Halo ID of the repository containing the image.</td>
</tr>
<tr>
<td>tag</td>
<td>The primary tag assigned to the image (the first entry in the tags array).</td>
</tr>
<tr>
<td>created_at</td>
<td>Date-time when the image was created. (ISO-8601 format)</td>
</tr>
<tr>
<td>imported_at</td>
<td>Date-time when the image was imported into its repository. (ISO-8601 format)</td>
</tr>
<tr>
<td>in_use</td>
<td>The number of running or paused containers that were instantiated from this image.</td>
</tr>
<tr>
<td>sha</td>
<td>Docker SHA-256 image representation.</td>
</tr>
<tr>
<td>short_sha</td>
<td>The first 12 bytes of image_sha.</td>
</tr>
<tr>
<td>current</td>
<td>true if this image is the most recently built image in its repository; false if not.</td>
</tr>
<tr>
<td>status</td>
<td>The Halo monitoring status of the image: monitored, unmonitored, or missing.</td>
</tr>
<tr>
<td>inspection_status</td>
<td>The Halo inspection status of the image: inspected, not_inspected, or unknown.</td>
</tr>
<tr>
<td>last_scan_at</td>
<td>Date-time of the most recent Halo connector scan of this image. (ISO-8601 format)</td>
</tr>
<tr>
<td>repository</td>
<td>An array of information about the image’s repository. Contains the following fields:</td>
</tr>
<tr>
<td></td>
<td>id</td>
</tr>
<tr>
<td></td>
<td>name</td>
</tr>
<tr>
<td>registry</td>
<td>An array of information about the image’s registry. Contains the following fields:</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>id</td>
<td>The Halo ID of this container image.</td>
</tr>
<tr>
<td>registry_id</td>
<td>The Halo ID of the registry containing the image.</td>
</tr>
<tr>
<td>repository_id</td>
<td>The Halo ID of the repository containing the image.</td>
</tr>
<tr>
<td>sha</td>
<td>Docker SHA-256 image representation</td>
</tr>
<tr>
<td>short_sha</td>
<td>The first 12 bytes of <code>image_sha</code>.</td>
</tr>
<tr>
<td>os_name</td>
<td>The name (<code>windows</code> or <code>linux</code> or a Linux distribution name) of the image's operating system.</td>
</tr>
<tr>
<td>os_version</td>
<td>The version number of the image's operating system.</td>
</tr>
<tr>
<td>os_type</td>
<td>The platform (<code>linux</code> or <code>windows</code>) of the image's operating system.</td>
</tr>
<tr>
<td>current</td>
<td><code>true</code> if this image is the most recently built image in its repository; <code>false</code> if not.</td>
</tr>
<tr>
<td>labels</td>
<td>An array of labels that have been attached to the image.</td>
</tr>
<tr>
<td>size</td>
<td>The size of the stored image, in bytes.</td>
</tr>
<tr>
<td>created_at</td>
<td>Date-time when the image was created. (ISO-8601 format)</td>
</tr>
<tr>
<td>imported_at</td>
<td>Date-time when the image was imported into its repository. (ISO-8601 format)</td>
</tr>
<tr>
<td>status</td>
<td>The Halo monitoring status of the image: <code>monitored</code>, <code>unmonitored</code>, or <code>missing</code>.</td>
</tr>
<tr>
<td>inspection_status</td>
<td>The Halo inspection status of the image: <code>inspected</code>, <code>not_inspected</code>, or <code>unknown</code>.</td>
</tr>
<tr>
<td>last_scan_at</td>
<td>Date-time of the most recent Halo connector scan of this image. (ISO-8601 format)</td>
</tr>
<tr>
<td>package_manager</td>
<td>The name of the package manager used by the image's operating system: <code>rpm</code> or <code>deb</code>.</td>
</tr>
<tr>
<td>tag</td>
<td>The primary tag assigned to the image.</td>
</tr>
<tr>
<td>digest</td>
<td>The full SHA-256 digest of the image. The first digest in <code>image_digests</code>.</td>
</tr>
<tr>
<td>short_digest</td>
<td>The first 12 bytes of the SHA-256 digest.</td>
</tr>
<tr>
<td>repository</td>
<td>An array of information about the image's repository. Contains the following fields:</td>
</tr>
<tr>
<td>registry</td>
<td>An array of information about the image's registry. Contains the following fields:</td>
</tr>
<tr>
<td>id</td>
<td>The repository ID.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the repository.</td>
</tr>
</tbody>
</table>

**Image object details fields**

These fields are returned from the **Get single image** call.

**Search filters**

You can use specific values of the following attributes as search filters to restrict the set of images returned from GET calls.

- `registry_id`
- `repository_id`
- `repository_name`
- `imported_at`
Sort by
You can sort the list of images by the values of the following attributes (append the _asc or _desc operator to the attribute):

- registry_id
- repository_id
- registry_name
- repository_name
- tag
- imported_at
- created_at
- in_use
- status
- inspection_status
- last_scan_at

List images

Returns JSON-formatted results listing all container images known to Halo.

GET https://api.cloudpassage.com/v1/images/

Response

Status: 200

[ "images": [ 
  { 
    "id": "002ecbdf-b728-4c70-a2f9-db34baf28233",
    "registry_id": "c11da753-c69e-4a73-b15b-52c317708df7",
    "repository_id": "ed843e1-1f75-47c3-85ef-49a330c686af",
    "tag": "latest",
    "created_at": "2017-04-19T21:33:02.766Z",
    "imported_at": "2017-08-22T12:35:05.288Z",
    "in_use": 0,
    "sha": "sha256:ed20e618ddd0a6f146852a2101f73c65bf313c2e91b45e5c0add6d45b5c40cd6",
    "short_sha": "ed20e618ddd0",
    "current": true,
    "status": "unmonitored",
    "inspection_status": "unknown",
    "last_scan_at": null,
    "repository": { 
        "id": "ed843e1-1f75-47c3-85ef-49a330c686af",
        "name": "vuln-oracle-7"
    },
    "registry": { 
        "id": "c11da753-c69e-4a73-b15b-52c317708df7",
        "name": "registry1.cs.cloudpassage.com"
    } 
  },
  ...
  { 
    "id": "59f2344c-c5fc-4519-9b5f-751b1cb2d57e",
    "registry_id": "c11da753-c69e-4a73-b15b-52c317708df7",
    "repository_id": "a21b25d3-879e-487d-8f59-62feade07761",
    "tag": "curl",
    "created_at": "2017-05-16T22:37:22.159Z",
    "imported_at": "2017-09-12T12:05:27.567Z",
  } ]
Get a single image

Returns the fields of the container image specified by ID in the call URL.

GET https://api.cloudpassage.com/v1/images/{id}

Response

Status: 200

```json
{
  "image": {
    "id": "002ecbdf-b728-4c70-a2f9-db34baf28233",
    "registry_id": "c11da753-c69e-4a73-b15b-52c317708df7",
    "repository_id": "ed843ea1-1f75-47c3-85ef-49a330c686af",
    "sha": "sha256:ed20e618dd0a6f146852a2101f73c65bf313c2e9145e5c0add645b5c40cd6",
    "short_sha": "ed20e618ddd0",
    "os_name": "",
    "os_version": "",
    "os_type": "linux",
    "current": true,
    "labels": [],
    "size": 869123708,
    "created_at": "2017-04-19T21:33:02.766Z",
    "imported_at": "2017-08-22T12:35:05.288Z",
    "status": "unmonitored",
    "inspection_status": "unknown",
    "last_scan_at": null,
    "package_manager": "",
    "tag": "latest",
    "digest": "registry1.cs.cloudpassage.com/vuln-oracle-7@sha256:4af449e58355477db572ba0dab1...",
    "short_digest": "4af449e58355",
    "repository": {
      "id": "ed843ea1-1f75-47c3-85ef-49a330c686af",
      "name": "vuln-oracle-7"
    },
    "registry": {
      "id": "c11da753-c69e-4a73-b15b-52c317708df7",
      "name": "registry1.cs.cloudpassage.com"
    }
  }
}
```
Container Image Registries

Use the Image Registries endpoint to manage a set of registries that store container images.

- Object Representation
- List registries
- Get a single registry
- Create a registry
- Update a registry
- Delete a registry

Object Representation

Registry object location

```
api.cloudpassage.com/v1
-registries
  -registry_id
```

Registry object fields

These fields are returned by the List registries method and the Get single registry method.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The Halo ID of this registry.</td>
</tr>
<tr>
<td>group_id</td>
<td>The ID of the Halo group to which the registry host belongs.</td>
</tr>
<tr>
<td>collector_ids</td>
<td>An array of IDs of the Halo connectors that have access to this registry.</td>
</tr>
<tr>
<td>server_url</td>
<td>The URL to the registry host.</td>
</tr>
<tr>
<td>username</td>
<td>The name of the Halo user account that created the registry.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the registry. An abbreviated version of server_url.</td>
</tr>
<tr>
<td>status</td>
<td>The current status of the registry: pending, active, or inactive.</td>
</tr>
<tr>
<td>sub_status</td>
<td>Additional registry status information, such as registry_unreachable.</td>
</tr>
<tr>
<td>type</td>
<td>The type of this registry. Supported values are dpr (Docker private registry) and ecr (Amazon EC2 container registry).</td>
</tr>
<tr>
<td>last_synced_at</td>
<td>The date-time of the most recent scan of this registry. (ISO-8601 format)</td>
</tr>
<tr>
<td>created_at</td>
<td>When this registry was initially created. (ISO-8601 format)</td>
</tr>
<tr>
<td>updated_at</td>
<td>The date-time of the most recent modification made to this registry. (ISO-8601 format)</td>
</tr>
<tr>
<td>sync_limit</td>
<td>How far back in the image version history to scan. By default, the connector scans the 10 most recent versions; the limit can be increased to as much as 100 versions.</td>
</tr>
<tr>
<td>auth_type</td>
<td>The type of authentication used to connect to the registry; for example, token, base, or</td>
</tr>
</tbody>
</table>
sts_assume_role.

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arn_role</td>
<td>The role Amazon resource name (ARN) associated with the AWS registry. Example: <code>arn:aws:iam::849489318606:role/registryrolename</code></td>
</tr>
<tr>
<td>stale_image_age</td>
<td>The age limit for scanning an image. Images older than this will not be scanned.</td>
</tr>
<tr>
<td>repositories_count</td>
<td>The number of repositories that the registry contains.</td>
</tr>
<tr>
<td>images_count</td>
<td>The total number of container images that the registry contains.</td>
</tr>
</tbody>
</table>

**Search filters**

This endpoint currently supports the following search filters for modifying the displayed list of registries:

- **name**
- **status**
- **last_synced_after**
- **last_synced_before**

**Sorting**

You can sort the registries list by the values in these fields, ascending or descending (append the `_asc` or `_desc` operator to the field name):

- **name**
- **status**
- **last_synced**
- **repositories_count**
- **images_count**

**List registries**

Returns JSON-formatted results listing all configured container-image registries in your environment that Halo can access.

**GET** `https://api.cloudpassage.com/v1/registries/`

This call supports optional parameters. You can use many of the core and details fields in the registry object as search filters for restricting the results returned from this call.

**Response**

**Status**: 200

```
{
  "registries": [{
    "id": "56c71a3a-6cb8-4fcf-a6e1-802a286d95a7",
    "group_id": "b3d8bec2-6d9a-11e8-a7c2-59b3c642f12b",
    "collector_ids": ["1196de44-5e6e-4d03-b8f1-01c1758a8a21"],
    "server_url": "https://357679622600.dkr.ecr.us-west-1.amazonaws.com",
    "username": null,
    "name": "ecr",
    "status": "active",
    "sub_status": "",
    "type": "ecr",
    "last_synced_at": "2019-04-29T16:59:07.612427068Z",
    "created_at": "2019-04-27T05:09:01.185002Z"
  }
}
```
Get single registry

Returns the fields of the container-image registry specified by scan ID in the call URL. You can obtain the registry ID required for this method by first calling the List registries method.

**GET https://api.cloudpassage.com/v1/registries/{id}**

Response

**Status: 200**

```json
{
  "registry": {
    "id": "56c71a3a-6cb8-4fcf-a6e1-802a286d95a7",
    "group_id": "b3d8bec2-6d9a-11e8-a7c2-59b3c642f12b",
    "collector_ids": [
      "1196de44-5e6e-4d03-b8f1-01c1758a8a21"
    ],
    "server_url": "https://357679622600.dkr.ecr.us-west-1.amazonaws.com",
    "username": null,
    "name": "ecr",
    "status": "active",
    "sub_status": "",
    "type": "ecr",
    "last_synced_at": "2019-04-29T16:59:07.612427Z",
    "created_at": "2019-04-27T05:09:01.185002Z",
    "updated_at": "2019-04-29T16:59:07.617571Z",
    "sync_limit": 0,
    "auth_type": "sts_assume_role",
    "stale_image_age": 30,
    "arn_role": "arn:aws:iam::357679622600:role/test2-registryrole",
    "repositories_count": 6,
    "images_count": 5,
    "imported_at": "2019-04-27T05:09:01.185002Z",
    "url": "https://portal-hotfix.ng.cloudpassage.com/v1/registries/56c71a3a-6cb8-4fcf-a6e1..."
  }
}
```

Create a registry

Creates a new image registry having the initial attributes that you specify in the request JSON, and returns the full set of initial attributes (including the registry ID) in the response JSON. The minimum attributes that you must specify values for are server_url, username, and password.

**POST https://api.cloudpassage.com/v1/registries/**

Request
Response

Status: 201

```
{
  "registry": {
    "id": "b2e8a0da-4c4b-420c-a2de-fdb295c164c4",
    "group_id": "b3d8bec2-6d9a-11e8-a7c2-59b3c642f12b",
    "collector_ids": [
      "18e6c653-deef-48ed-a53b-7db36bad4be",
    ],
    "server_url": "https://849489318606.dkr.ecr.us-east-2.amazonaws.com",
    "username": null,
    "name": "ecr",
    "status": "pending",
    "sub_status": "",
    "type": "ecr",
    "last_synced_at": null,
    "created_at": "2019-05-01T18:40:47.785793667Z",
    "updated_at": "2019-05-01T18:40:47.785793667Z",
    "sync_limit": 0,
    "auth_type": "sts_assume_role",
    "stale_image_age": 15,
    "arn_role": "arn:aws:iam::849489318606:role/test-registryrole"
  }
}
```

Update a registry

Updates the image registry specified by ID in the call URL with the attribute values you supply in the request JSON. Any of the attributes can be updated. The method returns only a result code.

When you make this call, you need specify only those values that you are changing. Other attributes will remain unchanged.

**PUT**  https://api.cloudpassage.com/v1/registries/{registry_id}

Request

```
{
  "registry": {
    "username": "qatest3",
  }
}
```

Response

Status: 204
Delete a registry

Deletes the image registry specified by ID in the call URL The method returns only a result code.

DELETE https://api.cloudpassage.com/v1/registries/{registry_id}

Response

Status: 204
Container Image Repositories

Within a registry, an image repository is a structure that contains one or more related container images. Use the Image Repositories endpoint to manage a set of image repositories.

- **Object Representation**
- **List repositories**
- **Get a single repository**

**Object Representation**

**Repository object location**

api.cloudpassage.com/v1

```
repositories
id
```

**Repository object fields**

These fields are returned by the **List repositories** call and the **Get a single repository** call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The Halo ID of this repository.</td>
</tr>
<tr>
<td>customer_id</td>
<td>(not used)</td>
</tr>
<tr>
<td>registry_id</td>
<td>The Halo ID of the repository's registry.</td>
</tr>
<tr>
<td>group_id</td>
<td>The Halo ID of the group to which the repository's host server belongs. (Currently, only the root group is supported.)</td>
</tr>
<tr>
<td>name</td>
<td>The name of the repository.</td>
</tr>
<tr>
<td>active</td>
<td><code>true</code> if the repository is active (scheduled for scanning); <code>false</code> if not.</td>
</tr>
<tr>
<td>images_sync_limit</td>
<td>How far back in the version history of images to scan. Default = 10 versions.</td>
</tr>
<tr>
<td>images_count</td>
<td>The total number of container images in the repository.</td>
</tr>
<tr>
<td>imported_at</td>
<td>The date-time of the most recent import of an image into the repository. (ISO-8601 format)</td>
</tr>
<tr>
<td>last_synced_at</td>
<td>The date-time of the most recent inventory of images in the repository. (ISO-8601 format)</td>
</tr>
<tr>
<td>last_scan_at</td>
<td>The date-time of the most recent Halo connector scan of the repository's images. (ISO-8601 format)</td>
</tr>
<tr>
<td>created_at</td>
<td>The date-time of the initial creation of the repository. (ISO-8601 format)</td>
</tr>
<tr>
<td>updated_at</td>
<td>The date-time of the most recent modification of the repository. (ISO-8601 format)</td>
</tr>
</tbody>
</table>

**Search filters**

You can use any of the following attributes as search filters to restrict results:
registry_id
id
name
images_count

Sorting of results

You can sort (ascending or descending) the results of this call by the values of the following attributes:

- name
- images_count
- imported_at

List repositories

Returns JSON-formatted results listing the image repositories that Halo can access.

GET https://api.cloudpassage.com/v1/repositories/

Response

Status: 200

```
{
    "repositories": [
    {
        "id": "9e15c6b5-6eaa-4f57-8e1e-0cf866053ae0",
        "customer_id": "e5b955f6-863b-11e7-acf6-4d1ec138f5fa",
        "registry_id": "c11da753-c69e-4a73-b15b-52c317708df7",
        "group_id": "e5d13bd0-863b-11e7-acf6-4d1ec138f5fa",
        "name": "alpine",
        "active": false,
        "images_sync_limit": 10,
        "images_count": 3,
        "imported_at": "2017-08-21T09:02:03.744Z",
        "last_synced_at": "2017-08-23T02:01:30.348Z",
        "last_scan_at": null,
        "created_at": "2017-09-15T19:19:00.769537884Z",
        "updated_at": "2017-09-15T19:19:00.769537884Z"
    },
    {
        "id": "61f73061-f10c-458c-ad9d-d3290201cf13",
        "customer_id": "e5b955f6-863b-11e7-acf6-4d1ec138f5fa",
        "registry_id": "85c4acbb-41e8-431e-9d85-c8ed32d56df",
        "group_id": "e5d13bd0-863b-11e7-acf6-4d1ec138f5fa",
        "name": "alpine",
        "active": true,
        "images_sync_limit": 10,
        "images_count": 3,
        "imported_at": "2017-08-21T09:02:03.744Z",
        "last_synced_at": "2017-08-23T02:01:30.348Z",
        "last_scan_at": null,
        "created_at": "2017-09-15T19:19:00.769537884Z",
        "updated_at": "2017-09-15T19:19:00.769537884Z"
    },
    ...
    {
        "id": "9aee4a0c-1d11-4e6b-896f-b8ad9e9e016d",
        "customer_id": "e5b955f6-863b-11e7-acf6-4d1ec138f5fa",
        "registry_id": "c11da753-c69e-4a73-b15b-52c317708df7",
        "group_id": "e5d13bd0-863b-11e7-acf6-4d1ec138f5fa",
        "name": "vuln-oracle-linux",
        "active": false,
        "images_sync_limit": 10,
        "images_count": 1,
        "imported_at": "2017-08-21T09:02:03.617Z",
        "last_synced_at": "2017-08-21T09:02:03.617Z",
        "last_scan_at": null,
        "created_at": "2017-08-21T09:02:03.617Z",
        "updated_at": "2017-08-21T09:02:03.617Z"
    }
    ]
```
Get a single repository

Returns the fields of the image repository specified by ID in the call URL.

GET https://api.cloudpassage.com/v1/repositories/{id}

Response

Status: 200

```json
{
  "repository": {
    "id": "8e4cfa56-5db5-480e-9c91-712a75b9e15c",
    "customer_id": "dd821b64-6784-11e7-a7d6-6901387c6a43",
    "registry_id": "60805e56-70e7-4694-a60c-9b72a340719d",
    "group_id": "dd99bc4c-6784-11e7-a7d6-6901387c6a43",
    "name": "alpine",
    "active": true,
    "images_sync_limit": 3,
    "images_count": 1,
    "last_synced_at": "2017-07-17T20:20:06.079Z",
    "last_scan_at": "2001-01-01T00:00:00Z",
    "created_at": "2017-07-13T05:03:18.799Z",
    "updated_at": "2017-07-17T20:20:06.12Z",
    "imported_at": "2017-07-13T05:03:18.799Z"
  }
}```
Container Image Summaries

Use the Image-Security Summaries endpoint to retrieve summary information describing the security issues detected in a specified registry or repository. The Halo portal uses this information to populate its Registry Summaries and Repository Summaries screens.

- Object Representation
- Get total vulnerable images in use
- Get total vulnerable images
- Get total unique CVEs
- Get top vulnerable packages
- Get top vulnerable images
- Get top CVEs
- Get summary for a registry
- Get summary for a repository

Object Representation

Summary object location

```
api.cloudpassage.com/v1
  └── summaries
      └── vulnerable_images_in_use
      └── vulnerable_images
      └── image_unique_cves
      └── top_vulnerable_packages
      └── top_images_by_cvss
      └── top_cve_by_cvss
```

Summaries object fields

These fields are returned by the Get vulnerable images in use method call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>The total number of images that have been instantiated as containers and have one or more vulnerabilities.</td>
</tr>
<tr>
<td>critical</td>
<td>The number of instantiated images that have at least one critical vulnerability.</td>
</tr>
<tr>
<td>non-critical</td>
<td>The number of instantiated images that have only non-critical vulnerabilities.</td>
</tr>
</tbody>
</table>

These fields are returned by the Get vulnerable images method call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>The total number of images that have one or more vulnerabilities.</td>
</tr>
<tr>
<td>critical</td>
<td>The number of images that have at least one critical vulnerability.</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>non-critical</td>
<td>The number of images that have only non-critical vulnerabilities.</td>
</tr>
</tbody>
</table>

These fields are returned by the **Get image unique CVEs** method call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>The total number of unique CVEs that exist across all vulnerable packages in all monitored images.</td>
</tr>
<tr>
<td>critical</td>
<td>The number of unique CVEs with a critical score.</td>
</tr>
<tr>
<td>non-critical</td>
<td>The number of unique CVEs with a non-critical score.</td>
</tr>
</tbody>
</table>

These fields are returned by the **Get top vulnerable packages** method call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the vulnerable package.</td>
</tr>
<tr>
<td>max_score</td>
<td>The maximum CVSS score of the CVEs in the vulnerable package.</td>
</tr>
<tr>
<td>image_count</td>
<td>The number of images in which the vulnerable package occurs.</td>
</tr>
</tbody>
</table>

These fields are returned by the **Get top images by CVSS** method call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A Halo-assigned ID of the image.</td>
</tr>
<tr>
<td>repository_id</td>
<td>The ID of the repository containing the image.</td>
</tr>
<tr>
<td>repository</td>
<td>An array of information identifying the repository. Contains these subfields:</td>
</tr>
<tr>
<td>id</td>
<td>The ID of the repository.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the repository.</td>
</tr>
<tr>
<td>tag</td>
<td>The image tag assigned to the image.</td>
</tr>
<tr>
<td>max_score</td>
<td>The maximum CVSS score of any of the packages in the vulnerable image.</td>
</tr>
<tr>
<td>image_sha</td>
<td>The Docker-assigned SHA-256 signature of the image.</td>
</tr>
</tbody>
</table>

These fields are returned by the **Get top CVEs by CVSS** method call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the CVE.</td>
</tr>
<tr>
<td>score</td>
<td>The CVSS score of the CVE.</td>
</tr>
<tr>
<td>image_count</td>
<td>The number of vulnerable images that contain this CVE.</td>
</tr>
</tbody>
</table>

**Get total vulnerable images in use**

Returns JSON-formatted results describing the total number of vulnerable images that have been instantiated as containers.

Unless you add a search filter to the URL, the returned values apply to all images in all registries that Halo monitors.

**GET https://api.cloudpassage.com/v1/summaries/vulnerable_images_in_use**

**Response**

**Status: 200**
Get total vulnerable images

Returns JSON-formatted results describing the total number of vulnerable images found.

Unless you add a search filter to the URL, the returned values apply to all images in all registries that Halo monitors.

GET https://api.cloudpassage.com/v1/summaries/vulnerable_images

Response

Status: 200

```json
{
  "summary": {
    "total": 20,
    "critical": 12,
    "non_critical": 8
  }
}
```

Get total unique CVEs

Returns JSON-formatted results describing the total number of unique CVEs found in the scanned images (duplicates removed).

Unless you add a search filter to the URL, the returned values apply to all images in all registries that Halo monitors.

GET https://api.cloudpassage.com/v1/summaries/image-unique-cves

Response

Status: 200

```json
{
  "summary": {
    "total": 218,
    "critical": 105,
    "non_critical": 113
  }
}
```

Get top vulnerable packages

Returns JSON-formatted results listing the highest-vulnerability packages found, based on maximum CVSS.

Unless you add a search filter to the URL, the returned values apply to all images in all registries that Halo monitors.

GET https://api.cloudpassage.com/v1/summaries/top_vulnerable_packages
Response

Status: 200

```json
{
  "summary": [
    {
      "name": "glibc",
      "max_score": 10,
      "images_count": 2
    },
    {
      "name": "glibc-common",
      "max_score": 10,
      "images_count": 2
    },
    {
      "name": "openssl-libs",
      "max_score": 10,
      "images_count": 2
    },
    {
      "name": "nss-tools",
      "max_score": 9.3,
      "images_count": 2
    },
    {
      "name": "nss-sysinit",
      "max_score": 9.3,
      "images_count": 2
    }
  ]
}
```

Get top vulnerable images

Returns JSON-formatted results listing the highest-vulnerability images, based on maximum CVSS.

Unless you add a search filter to the URL, the returned values apply to all images in all registries that Halo monitors.

**GET** https://api.cloudpassage.com/v1/summaries/top_images_by_cvss

Response

Status: 200

```json
{
  "summary": [
    {
      "id": "4b9c6334-5e7d-4d95-b4e9-0c8cb1158659",
      "repository_id": "ac81df48-f86b-48fb-82a1-292f126b8262",
      "repository": {
        "id": "ac81df48-f86b-48fb-82a1-292f126b8262",
        "name": "centos1"
      },
      "tag": "7.0.1406",
      "max_score": 10,
      "image_sha": "sha256:16e9fdecc1febc87fb1ca09271009cf5f28eb8d4aec5515922ef298c145a6726",
      "issues_count": 42
    },
    {
      "id": "16f6dd71-43ba-4631-88dd-fd6effc3f3ac",
      "repository_id": "ac81df48-f86b-48fb-82a1-292f126b8262",
      "repository": {
        "id": "ac81df48-f86b-48fb-82a1-292f126b8262",
        "name": "centos1"
      },
      "tag": "7.1.1503",
      "max_score": 10,
      "image_sha": "sha256:285396d0a019bceaf6d6a14f791cf6404decb17820a230ef8559619ce616df0"
  ]
}
```
Get top CVEs

Returns JSON-formatted results listing the highest-vulnerability CVEs found, based on CVSS score. Unless you add a search filter to the URL, the returned values apply to all images in all registries that Halo monitors.

GET https://api.cloudpassage.com/v1/summaries/top_cve_by_cvss

Response

Status: 200

```json
{
  "summary": [
  {
    "name": "cve-2015-0235",
    "score": 10,
    "images_count": 1
  },
  {
    "name": "cve-2016-2108",
    "score": 10,
    "images_count": 2
  },
  {
    "name": "cve-2016-2834",
    "score": 9.3,
    "images_count": 2
  }
  ]
}
```

Get summary for a registry

Use the search filter `registry_id` to restrict the results of a GET call to any of the summary endpoints. Only the information for all of the images within that registry are returned. For example:

GET https://api.cloudpassage.com/v1/summaries/vulnerable_images?registry_id={registry_id}

Response

Status: 200

```json
{
  "summary": {
    "total": 3,
    "critical": 1,
    "non_critical": 2
  }
}
```
Get summary for a repository

Use the search filter `repository_id` to restrict the results of a GET call to any of the summary endpoints. Only the platform_version for the images within that repository are returned. For example:

GET https://api.cloudpassage.com/v1/summaries/top_vulnerable_images?repository_id={repository_id}

Response

Status: 200

```json
{
  "summary": [
    {
      "id": "16f6dd71-43ba-4631-88dd-fd6effc3f3ac",
      "repository_id": "ac81df48-f86b-48fb-82a1-292f126b8262",
      "repository": {
        "id": "ac81df48-f86b-48fb-82a1-292f126b8262",
        "name": "centos1"
      },
      "tag": "7.1.1503",
      "max_score": 10,
      "image_sha": "sha256:285396d0a019bceaf6a14f791cf68404decb17820a230ef85599619ce616df0",
      "issues_count": 35
    }
  ]
}
```
Container Processes

Use the Container Processes endpoint to retrieve a list of the processes running in a specified container.

- Object Representation
- List container processes

Object Representation

Container processes object location

```
api.cloudpassage.com/v1
  └──container_processes
    └──id
```

Container processes object fields

These fields are returned by the List container processes method.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer_id</td>
<td>(not used)</td>
</tr>
<tr>
<td>container_id</td>
<td>The Halo ID of the container within which the process executes.</td>
</tr>
<tr>
<td>id</td>
<td>The Halo ID of the process (if it has a Halo ID).</td>
</tr>
<tr>
<td>pid</td>
<td>The process ID of the process.</td>
</tr>
<tr>
<td>user</td>
<td>The name of the user that the process is running as.</td>
</tr>
<tr>
<td>cpu_percent</td>
<td>The load that the process places on the Host server's CPU (in percent).</td>
</tr>
<tr>
<td>memory_percent</td>
<td>The memory usage of the process (in percent of total memory).</td>
</tr>
<tr>
<td>name</td>
<td>The name of the process.</td>
</tr>
<tr>
<td>command</td>
<td>The command that launched the process.</td>
</tr>
<tr>
<td>updated_at</td>
<td>The date-time (in ISO-8601 format) of the most recent Halo scan that detected the process.</td>
</tr>
</tbody>
</table>

List Container Processes

Returns JSON-formatted results listing all instantiated containers, whether currently running or not, on the container specified in the call URL.

```
GET https://api.cloudpassage.com/v1/container_processes?container_id={id}
```

Response
{
  "processes": [
    {
      "customer_id": "9acbb752-78dd-11e7-af4f-7bcb36df0a66",
      "container_id": "dd95b7c92758088a640618bb3072fc97db97b6168027247e15311e503d5888733",
      "id": "c7f61e33-d784-4e2b-8a74-9f5240c5ebb0",
      "pid": "3571",
      "user": "root",
      "cpu_percent": "0.0",
      "memory_percent": "0.5",
      "name": "cpconnector",
      "command": "/opt/cloudpassage/connector/bin/cpconnector --debug --pidfile=/var/run/cpconnectord.pid",
      "updated_at": "2017-11-03T15:47:07.601Z"
    },
    {
      "customer_id": "9acbb752-78dd-11e7-af4f-7bcb36df0a66",
      "container_id": "80c2222ecb2272870bc8870dbda6e99b2dbf77351849379522d89b62da597720",
      "id": "e8b9b822-eb9c-47fa-aee4-e52cd5d65ad",
      "pid": "4021",
      "user": "root",
      "cpu_percent": "0.0",
      "memory_percent": "0.5",
      "name": "cpconnector",
      "command": "/opt/cloudpassage/connector/bin/cpconnector --debug --pidfile=/var/run/cpconnector...",
      "updated_at": "2017-11-03T15:47:07.601Z"
    },
    ...
    {
      "customer_id": "9acbb752-78dd-11e7-af4f-7bcb36df0a66",
      "container_id": "f646fe13d0459e11c79472e33908e730cc5d1680711d3d5-e16e33754cf29ce7923",
      "id": "f9fdd666-a0af-470b-9b3d5-e3cb46164c08",
      "pid": "4350",
      "user": "999",
      "cpu_percent": "1.0",
      "memory_percent": "0.8",
      "name": "redis-server",
      "command": "redis-server *:6379",
      "updated_at": "2017-11-03T16:16:03.631Z"
    }
  ],
  "count": 9,
  "pagination": {}
}
Container Software Packages

Use the Software Packages endpoint to retrieve a list of all Halo-identified software packages in a set of container images.

- **Object Representation**
- **List software packages**

### Object Representation

**software package object location**

```
api.cloudpassage.com/v1
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The ID of the software package.</td>
</tr>
<tr>
<td>customer_id</td>
<td>(not used)</td>
</tr>
<tr>
<td>image_id</td>
<td>The Halo ID of the container image that includes this package.</td>
</tr>
<tr>
<td>name</td>
<td>The package name of the package.</td>
</tr>
<tr>
<td>platform</td>
<td>The kernel (such as <code>x86_64</code>) of the OS that the package runs on.</td>
</tr>
<tr>
<td>cves</td>
<td>An array of Common Vulnerability and Exposures (CVEs) detected in this package; the value is <code>null</code> if none was detected.</td>
</tr>
<tr>
<td>cves_count</td>
<td>The number of CVEs detected in this package.</td>
</tr>
<tr>
<td>version</td>
<td>The version number of the package.</td>
</tr>
<tr>
<td>max_cvss</td>
<td>The maximum CVSS score detected in the CVEs of the package.</td>
</tr>
<tr>
<td>remotely_exploitable</td>
<td><code>true</code> if any CVE in the package can be exploited remotely (without physical access to the server); otherwise <code>false</code>.</td>
</tr>
</tbody>
</table>

### List software packages

Returns JSON-formatted results listing all software packages, whether vulnerable or not, in the account's container images.

**GET** `https://api.cloudpassage.com/v1/software_packages/`

### Response
[  
  {  
    "id": "d1574b8a-9d28-11e7-b3b3-06d3dc655420",
    "customer_id": "e5b955f6-863b-11e7-acf6-06d3dc655420",
    "image_id": "7c3104ab-7f6f-4e88-b460-00bdc0c84b4c",
    "name": "MAKEDEV",
    "platform": "x86_64",
    "cves": null,
    "cves_count": 0,
    "version": "3.24-6.el6",
    "max_cvss": 0,
    "remotely_exploitable": false
  },
  {  
    "id": "e1514228-9d28-11e7-81dc-06d3dc655420",
    "customer_id": "e5b955f6-863b-11e7-acf6-06d3dc655420",
    "image_id": "d5f2b418-572d-40eb-a161-ff3c4c5cb439",
    "name": "MAKEDEV",
    "platform": "x86_64",
    "cves": null,
    "cves_count": 0,
    "version": "3.24-6.el6",
    "max_cvss": 0,
    "remotely_exploitable": false
  },
  ...
  {  
    "id": "c53e65e7-9d28-11e7-a92b-06d3dc655420",
    "customer_id": "e5b955f6-863b-11e7-acf6-06d3dc655420",
    "image_id": "1f9ee338-126a-49ba-88c4-91e20bb63e2d",
    "name": "apt",
    "platform": "amd64",
    "cves": null,
    "cves_count": 0,
    "version": "1.0.1ubuntu2.17",
    "max_cvss": 0,
    "remotely_exploitable": false
  }
],
"count": 10045,
"pagination": {  
}  
]
You can use the csp_accounts endpoint to view and manage the cloud service provider (CSP) accounts that are in Halo. With this endpoint, you can list all CSP accounts, get details about a specific account, get a list of accounts that meet specific criteria, create a new account, update an account, and delete an account.

- Object Representation
- Create a CSP Account
- Get a List of All CSP Accounts
- Get a List of Specific CSP Accounts
- Update a CSP Account
- Delete a CSP Account
- Reactivate or Deactivate a CSP Account
- Scan an Account Manually

Object Representation

CSP Accounts Object Location

```
api.cloudpassage.com/v1/csp_accounts
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The internal ID of the account in Halo. Example: <code>81e275a5-57e9-4471-aa91-a0e4d6850afa</code></td>
</tr>
<tr>
<td>csp_account_type</td>
<td>The type of cloud service provider; that is, AWS or Azure.</td>
</tr>
<tr>
<td>csp_region_type</td>
<td>The region type of the CSP Account: <code>aws_commercial</code>, <code>aws_govcloud</code>, <code>aws_china</code>, <code>azure_commercial</code>.</td>
</tr>
<tr>
<td>csp_account_id</td>
<td>The UUID of the AWS account or Azure subscription; Example: <code>856192027328</code>.</td>
</tr>
<tr>
<td>azure_directory_id</td>
<td>The Directory ID of the Azure tenant.</td>
</tr>
<tr>
<td>csp_account_alias</td>
<td>The Azure subscription name or AWS account alias.</td>
</tr>
<tr>
<td>account_display_name</td>
<td>Defaults to the csp_account_alias value, unless otherwise updated.</td>
</tr>
<tr>
<td>created_at</td>
<td>The timestamp (in ISO-8601 format) of when this account was created. Example: <code>2017-12-25T00:55:39.000090+0000</code></td>
</tr>
<tr>
<td>updated_at</td>
<td>The timestamp (in ISO-8601 format) of when this account was last updated. Example: <code>2017-12-25T00:55:39.000090+0000</code></td>
</tr>
<tr>
<td>user_id</td>
<td>The Halo ID of the user who created this account.</td>
</tr>
<tr>
<td>group_id</td>
<td>The Halo ID of the group to which you want to assign the account. Example: <code>f8b93a7026e211e8b1754d7d60172183</code></td>
</tr>
<tr>
<td>monitoring_state</td>
<td>The current monitoring state of the account: active, inactive, or suspended.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>aws_access_key</td>
<td>For AWS China or AWS GovCloud region types only. Used with aws_secret to authenticate requests in AWS.</td>
</tr>
<tr>
<td>aws_secret</td>
<td>For AWS China or AWS GovCloud region types only. Used with aws_access_key to authenticate requests in AWS. The value is obfuscated.</td>
</tr>
<tr>
<td>aws_role_arn</td>
<td>The role Amazon resource name (ARN), which is generated by AWS. Example: arn:aws:iam::550429930677:role/Halo-Service-Role</td>
</tr>
<tr>
<td>aws_external_id</td>
<td>In AWS, a unique identifier that is used in an IAM role trust policy to designate who can assume the role. <strong>Note:</strong> This identifier is used to prevent the &quot;confused deputy problem.&quot; For more information, click here.</td>
</tr>
<tr>
<td>azure_application_id</td>
<td>In Azure, the unique identifier assigned to the application. Used with azure_application_key to authenticate requests.</td>
</tr>
<tr>
<td>azure_application_key</td>
<td>In Azure, used with azure_application_id to authenticate requests.</td>
</tr>
<tr>
<td>initial_scan_completed</td>
<td>Indicates whether the initial scan, which is performed when a CSP account is first added, is completed: true or false.</td>
</tr>
<tr>
<td>initial_rules_run_completed</td>
<td>Indicates whether the rules have been run for the CSP account being scanned; used only when the CSP account is first provisioned: true or false.</td>
</tr>
<tr>
<td>initial_scan_summary</td>
<td>A summary of the initial scan, which is performed when a CSP account is first added. Can be used as a basis for comparison; once the initial scan completes, the values in this summary remain static until the CSP account is deleted and re-added.</td>
</tr>
<tr>
<td>scan_status</td>
<td>The status of the latest scan.</td>
</tr>
<tr>
<td>error_detail</td>
<td>The current state of the scan process: In progress, Fail, and Complete.</td>
</tr>
<tr>
<td>time_of_last_scan</td>
<td>The timestamp (in ISO-8601 format) of when this account was last scanned by Halo. Example: 2017-12-25T00:55:39.000090+0000</td>
</tr>
<tr>
<td>aws_sns_status</td>
<td>Used with AWS SNS subscriptions; indicates whether SNS notifications are being delivered: SNS OK, SNS Fail, or -.</td>
</tr>
<tr>
<td>aws_sns_arn</td>
<td>The SNS Amazon resource name (ARN), which is generated by AWS. Example: arn:aws:sns:us-east-2:451776696422:CSPFindings</td>
</tr>
<tr>
<td>aws_sns_error_detail</td>
<td>Used with AWS SNS subscriptions; indicates the reason for an SNS notification failure. Used in conjunction with aws_sns_status.</td>
</tr>
</tbody>
</table>

### Create a CSP Account

Creates a new CSP account entity with the account parameters that you specify. Only site administrators can create a new CSP account.

**Note:** Before you can create a CSP account using the API, you must first obtain the information necessary to formulate the request. The instructions that explain how to obtain this information can be found in Halo in the Add CSP Account dialog. For more information, see Add a CSP Account in the Cloud Secure Guide.

**To create a new CSP account, follow these steps:**

1. **Obtain the information required to formulate the request.** You can find instructions that explain how to get this information in Halo; see Add a CSP Account in the Cloud Secure Guide.
2. **Formulate a standard request JSON for a POST call:**

   **AWS commercial example:**

   ```json
   {
     "aws_external_id": "3bbf6d14-e9b4-4370-8b5d-24034c9bacc0",
     "aws_role_arn": "arn:aws:iam::088344982111:role/cielo-2",
     "group_id": "f8b93a7026e211e8b1754d7d60172183",
     "csp_account_type": "AWS",
   }
   ```
"csp_region_type": "aws_commercial"
}

AWS non-commercial example (AWS GovCloud shown):

```
{
  "aws_access_key": "AKIAJRHL2342JG5Z25AQ",
  "aws_secret_key": "iuw9wsd211e8b1754d7d6sdf2444",
  "group_id": "f8b93a7026e211e8b1754d7d60172183",
  "csp_account_type": "AWS",
  "csp_region_type": "aws_govcloud"
}
```

*Note:* All of the object fields in the examples above are required, with the exception of `aws_sns_arn`, which is optional.

Azure example:

```
{
  "azure_directory_id": "dcbd3a15-128b-4253-b682-cdaf472f57c2",
  "azure_application_id": "2726a898-e0e2-4717-8c1e-77ac04fac7ba",
  "azure_application_key": "P2ByZwbifApMHVTXXqk2SRch1R3M9+8CSzT6KV8NoZQ",
  "csp_account_id": "c84251d7-2730-41e0-a62e-23a330d2d956",
  "csp_account_type": "Azure",
  "csp_region_type": "azure_commercial"
}
```

*Note:* All of the object fields in the example above are required.

3. Post your request to the csp_accounts endpoint:

   POST https://api.cloudpassage.com/v1/csp_accounts

Response

**Status:** 201

```
{
  "87ad14a3-7913-439c-a25b-083e0072e05b"
}
```

Get a List of all CSP Accounts

Returns JSON-formatted results that list all CSP accounts.

GET https://api.cloudpassage.com/v1/csp_accounts

Response

**Status:** 200

```
{
  "csp_accounts": [
    {
      "id": "19d28b5f-8be3-4b99-8372-eab60ccc976a",
      "csp_account_type": "aws",
      "csp_region_type": "aws_govcloud",
      "csp_account_id": "495640807753",
      "azure_directory_id": null,
      "csp_account_alias": "495640807753",
```

59
Get a List of Specific CSP Accounts

Returns JSON-formatted results listing details about all of the CSP accounts that were specified in the query.

GET https://api.cloudpassage.com/v1/csp_accounts/{query parameters}

Example:

GET https://api.cloudpassage.com/v1/csp_accounts/{id}

Response

Status: 200

```json
{
    "csp_account": {
        "id": "6cd26487-9db0-4608-adca-0738056934a1",
        "csp_account_type": "aws",
        "csp_region_type": "aws_commercial",
        "csp_account_id": "357679622600",
        "azure_directory_id": null,
        "csp_account_alias": "357679622600",
        "created_at": "2019-01-09T17:06:51.000405+0000",
        "updated_at": "2019-01-15T10:07:15.000382+0000",
        "user_id": "dfab29fc688311e8ba617f1da6be51c6",
        "group_id": "dfc1296e68311e8ba617f1da6be51c6",
        "monitoring_state": "active",
        "aws_access_key": null,
        "aws_secret": null,
        "aws_role_arn": "arn:aws:iam::357679622600:role/jan9-tejas",
        "azure_application_id": "7bbf1e22-0255-42e0-a014-77a45e68c385",
        "azure_application_key": null,
        "initial_scan_completed": true,
        "initial_rules_run_completed": true,
        "initial_scan_summary": {
            "s3": "Processing rules complete...",
            "rds": "Processing rules complete...",
            "route53": "Processing rules complete...",
            "lambda": "Processing rules complete...",
            "iam": "Processing rules complete...",
            "ec2": "Processing rules complete...",
            "vpc": "Processing rules complete...",
            "cloud_trail": "Processing rules complete...",
            "api_gateway": "Processing rules complete...",
            "cloudformation": "Processing rules complete..."
        },
        "scan_status": "completed_with_errors",
        "error_detail": "Failed to process Policy: ",
        "time_of_last_scan": "2019-01-18T09:05:00.000107+0000",
        "aws_sns_status": null,
        "aws_sns_arn": null,
        "aws_sns_error_detail": null
    }
}
```
Update a CSP Account

Site administrators can use this call to update individual attributes of a CSP account that is specified by ID.

In the request body, include only the attributes that you want modified; other attributes of the group will remain unchanged.

PUT https://api.cloudpassage.com/v1/csp_accounts/{id}

Request Body

```
{
  "account_display_name": "WAS-acctg-west",
  "aws_role_arn": "arn:aws:iam::065368812710:role/trusted-Newark"
}
```

Response

204

Delete a CSP Account

Site administrators can use this call to delete a CSP account that is specified by ID. Once deleted, the account is deactivated from monitoring and all data is removed from the account in Halo.

DELETE https://api.cloudpassage.com/v1/csp_accounts/{id}

Response

204

Reactivate or Deactivate a CSP Account

Site administrators can use this call to disable scanning of a particular AWS account without deleting the account data from Halo. Deactivating an account temporarily disables scanning, but keeps the data intact for up to 90 days. After 90 days, the data is deleted.
The account is specified by ID.

When you reactivate a deactivated account, it immediately enables scanning. Since scanning occurs periodically, new results will not be available until after the next scan.

PUT https://api.cloudpassage.com/v1/csp_accounts/{id}

Request Body Reactivate

```json
{
  "monitoring_state": "active"
}
```

Request Body Deactivate

```json
{
  "monitoring_state": "inactive"
}
```

Response

204

Scan an Account Manually

Use this call to scan an account manually outside of its existing schedule. When you scan an account on demand, the existing schedule is not affected. If you want to change the scanning schedule, see CSP Scanner Settings.

POST https://api.cloudpassage.com/v1/csp_accounts/{id}/scan_now

Response

201
CSP Resources

You can use the csp_resources endpoint to view a single resource or an inventory of all of your CSP account resources. You can sort, group, and filter the results to refine the set.

- Object Representation
- View all CSP Resources
- View the Details of a Single CSP Resource

Object Representation

CSP Resources Object Location

api.cloudpassage.com/v1
csp_resources
  id

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The internal ID of the resource in Halo. Example: 000885b7-2cb8-4532-93ea-1a37a0dcf986</td>
</tr>
<tr>
<td>csp_arn</td>
<td>The ARN of the cloud resource in the CSP account. Value may be null.</td>
</tr>
<tr>
<td>csp_account_type</td>
<td>The type of cloud service account; that is, AWS or Azure.</td>
</tr>
<tr>
<td>csp_tags</td>
<td>The list of tags assigned to the asset in the cloud service provider account. Value may be null.</td>
</tr>
<tr>
<td>created_at</td>
<td>The timestamp (in ISO-8601 format) of when this account was created. Example: 2017-12-25T00:55:39.000090+0000</td>
</tr>
<tr>
<td>csp_resource_type</td>
<td>The type of cloud resource; for example, Policy, Role, User, and so on.</td>
</tr>
<tr>
<td>halo_agent_id</td>
<td>The internal ID of the Halo agent. Value may be null.</td>
</tr>
<tr>
<td>deleted_at</td>
<td>The timestamp (in ISO-8601 format) of when Halo detected the resource was deleted. Only populated if a resource was deleted; otherwise, the value is null.</td>
</tr>
<tr>
<td>url</td>
<td>The URL to view the resource's details.</td>
</tr>
<tr>
<td>halo_agent_display_name</td>
<td>The user-assigned display name of the Halo agent. Value may be null.</td>
</tr>
<tr>
<td>csp_region</td>
<td>The region of the CSP account; for example, AP South 1, AP Northeast 1, CA Central 1, EU West 1, and so on. Value may be null.</td>
</tr>
<tr>
<td>csp_service_type</td>
<td>The type of cloud service; for example, IAM, S3, EC2, and so on.</td>
</tr>
<tr>
<td>updated_at</td>
<td>The timestamp (in ISO-8601 format) of when this account was last updated. Example: 2017-12-25T00:55:39.000090+0000</td>
</tr>
<tr>
<td>group_id</td>
<td>The Halo ID of the group to which the CSP resource belongs.</td>
</tr>
<tr>
<td>instance_state</td>
<td>The current state of an instance; for example, Pending, Running, Terminated, and so on. Value may be null.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>csp_resource_status</td>
<td>The current status of the cloud resource; for example: Deleted.</td>
</tr>
<tr>
<td>csp_resource_name</td>
<td>The Azure subscription name or AWS account alias. Value may be null.</td>
</tr>
<tr>
<td>csp_account_id</td>
<td>The UUID of the AWS account or Azure subscription; Example: 856192027328.</td>
</tr>
<tr>
<td>csp_account_display_name</td>
<td>Defaults to the same value as the &quot;account_display_name&quot; field in the csp_accounts endpoint.</td>
</tr>
<tr>
<td>last_seen_at</td>
<td>The timestamp (in ISO-8601 format) of when this resource was last detected by Halo. Example: 2017-12-25T00:55:39.000090+0000</td>
</tr>
<tr>
<td>csp_resource_id</td>
<td>The ID of the cloud resource in the CSP account. Value may be null.</td>
</tr>
<tr>
<td>resource_json</td>
<td>The resource details in JSON format. The array that appears under this object is provided by the cloud service provider and varies depending on the type of resource. Note: Because fields are provided by the cloud service provider, they do not correlate with fields of the same name in our API (e.g., &quot;platform&quot;).</td>
</tr>
</tbody>
</table>

**Sorting, grouping, and filtering resources**

By default, results are grouped and sorted in ascending order by name. You can use the `sort_by` and `group_by` parameters to specify that the search results are to be alphanumerically sorted (in either ascending or descending order, using the `.asc` and `.desc` filter suffixes) or grouped according to the value of the following object fields:

- csp_account_id
- csp_resource_type
- csp_service_type
- csp_account_type
- csp_resource_id
- csp_account_display_name
- csp_tags
- created_at
- halo_agent_id

Any of the object fields listed above can also be used to filter the result set. When you filter, you can provide either a single value or a comma-separated list of values. If you do provide multiple values, they are OR'd in a search, meaning that the search passes for that filter if any of its supplied values match.

Examples:

*Return resources with a service type of "EC2":*

GET https://api.cloudpassage.com/v1/csp_resources?csp_service_type=EC2

*Return resources that were created before a specific date:*

Note: Insert inequality operators by adding these extensions to created_at: `_gt`, `_lt`, `_gte`, and `_lte.`


Note: The results may be paginated. See Pagination of Results for information on how to set up and retrieve paginated results from the Halo API.

**View All CSP Resources**

Use this call to get a list of CSP resources and view each resource's details. See Sorting, grouping, and filtering resources for information about working with the results to refine the set.

GET https://api.cloudpassage.com/v1/csp_resources
Response

Status: 200

```json
{
    "csp_resources": [
        {
            "csp_arn": "/subscriptions/ed4a1d31-e968-45c2-b763-35440a47d632/resourceGroups/...",
            "csp_account_type": "azure",
            "csp_tags": [
                {
                    "key": "owner",
                    "value": "mariachen"
                }
            ],
            "created_at": ":2019-05-27T09:02:38.194Z",
            "csp_resource_type": "virtual_machine",
            "halo_agent_id": null,
            "deleted_at": null,
            "halo_agent_display_name": null,
            "csp_region": "southafricanorth",
            "csp_service_type": "compute",
            "updated_at": ":2019-06-03T09:04:12.323Z",
            "group_id": "dd40c2f8-6d38-11e8-a66a-2b6deccf7d71",
            "instance_state": "running",
            "csp_resource_status": "not_deleted",
            "csp_resource_name": "cpg-ins-flag",
            "csp_account_id": "ed4a1d31-e968-45c2-b763-35440a47d632",
            "csp_account_display_name": "DEV: 01 content.cloudpassage.xyz",
            "id": "8533c7bb-04bf-4294-bfed-dff88aba41d3",
            "last_seen_at": ":2019-06-03T09:04:12.323Z"
        },
        ...
    ]
}
```

---

View the Details of a Single CSP Resource

Use this call to view the details of a single CSP resource. To make this call, you need the ID number from a View All CSP Resources response.

GET `https://api.cloudpassage.com/v1/csp_resources/{id}`

Response

Status: 200

```json
{
    "csp_resource": {
        "csp_arn": "/subscriptions/ed4a1d31-e968-45c2-b763-35440a47d632/resourceGroups/...",
        "csp_account_type": "azure",
        "resource_json": {
            "halo_agent_display_name": null,
            "computer_name": "cpg-ins-flag",
            "vm_id": "9aaec96f-9479-4324-b9d1-0b68be469d67",
            "boot_diagnostics_enabled": true,
            "disks": [],
            "instance_view": {},
            "name": "cpg-ins-flag",
            "location": "southafricanorth",
            "id": "/subscriptions/ed4a1d31-e968-45c2-b763-35440a47d632/resourceGroups/...",
            "state": "running",
            "halo_agent_id": null
        },
        "csp_tags": [
            {
                "key": "owner",
                "value": "mariachen"
            }
        ],
        "created_at": ":2019-05-27T09:02:38.194Z",
```

65
Search for an AWS Instance or Azure Virtual Machine by IP Address

You can search for an AWS instance or an Azure virtual machine by any IP address associated the instance or virtual machine.

The following call is an example:

GET https://api.cloudpassage.com/v1/csp_resources/?private_ip_address=172.31.18.23
CSP Findings

You can use the `csp_findings` endpoint to view a summary of findings for each rule. You can sort, group, and filter those findings to refine the result set.

- Object Representation
- View a Summary of Findings for Each Rule
- View a Findings Summary for a Specific Rule
- View all Results for a Specific Rule

Object Representation

CSP Findings Object Location

```
api.cloudpassage.com/v1/csp_findings
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>csp_rule_id</td>
<td>The user-readable ID of the rule. Example: <strong>CIS:1.1</strong></td>
</tr>
<tr>
<td>policy_id</td>
<td>The Halo ID (unique identifier) of this policy.</td>
</tr>
<tr>
<td>pass_percent</td>
<td>The percentage of objects that passed the rule.</td>
</tr>
<tr>
<td>rule_name</td>
<td>The name of the rule that was applied; for example <strong>Ensure MFA is enabled for the &quot;root&quot; account.</strong></td>
</tr>
<tr>
<td>pass</td>
<td>The total number of objects that passed the rule.</td>
</tr>
<tr>
<td>criticality</td>
<td>The criticality of a finding: <strong>critical</strong> or <strong>non-critical</strong>.</td>
</tr>
<tr>
<td>policy_name</td>
<td>The name of the policy that was applied; for example, <strong>CIS-Benchmark</strong>.</td>
</tr>
<tr>
<td>csp_resource_type</td>
<td>The type of cloud resource; for example, <strong>Policy, Role, User</strong>, and so on.</td>
</tr>
<tr>
<td>error</td>
<td>The number of errors.</td>
</tr>
<tr>
<td>rule_id</td>
<td>The UUID number of the rule that was applied; for example, <strong>280d33b6ef3411e88ad765862e629d59</strong></td>
</tr>
<tr>
<td>result</td>
<td>The result of the scan: <strong>pass</strong>, <strong>fail</strong>, or <strong>error</strong>.</td>
</tr>
<tr>
<td>fail</td>
<td>The total number of objects that failed the rule.</td>
</tr>
<tr>
<td>total</td>
<td>The total number of objects examined.</td>
</tr>
<tr>
<td>csp_service_type</td>
<td>The type of cloud service; for example, <strong>IAM, S3, EC2</strong>, and so on.</td>
</tr>
</tbody>
</table>

Sorting, grouping, and filtering findings

By default, results are grouped and sorted in ascending order by `csp_rule_id`. You can use the `sort_by` and `group_by` parameters to specify that the search results are to be alphanumerically sorted (in either ascending or descending order, using the `.asc` and `.desc` filter suffixes) or grouped according to the value of the following object fields:
Any of the object fields listed above can also be used to filter the result set. When you filter, you can provide either a single value or a comma-separated list of values. If you do provide multiple values, they are OR'd in a search, meaning that the search passes for that filter if any of its supplied values match.

Examples:

Return finding summaries for a resource type of "policy":

GET https://api.cloudpassage.com/v1/csp_findings?csp_resource_type=policy

Return finding summary for rule ID "CIS:3.5":

GET https://api.cloudpassage.com/v1/csp_findings?csp_rule_id~CIS:3.5

Note: The results may be paginated. See Pagination of Results for information on how to set up and retrieve paginated results from the Halo API.

View a Summary of Findings for Each Rule

Use this call to get a list of all rules that have a finding summary. See Sorting, grouping, and filtering findings for information about working with the results to refine the set.

GET https://api.cloudpassage.com/v1/csp_findings

Response

Status: 200

```json
{
  "count": 91,
  "csp_findings": [
    {
      "csp_rule_id": "CIS:1.1",
      "policy_id": "9c6e6b5c68b211e8ba5027ac22fb850c",
      "pass_percent": 100,
      "rule_name": "Avoid the use of the \"root\" account (Scored)",
      "pass": 3,
      "criticality": "critical",
      "csp_resource_type": "user",
      "error": 0,
      "rule_id": "280d33b6ef3411e88ad765862e629d59",
      "result": "pass",
      "fail": 0,
      "total": 3,
      "csp_service_type": "iam"
    },
    ...
  ]
}
```

View a Finding Summary for a Specific Rule

Use this call to view a finding summary for a specific rule using the csp_rule_id number from a View a Summary of Findings for Each
Rule response.

GET https://api.cloudpassage.com/v1/csp_findings?csp_rule_id={ID}

Example:
https://api.cloudpassage.com/v1/csp_findings?csp_rule_id=CIS:1.1

Response

Status: 200

```
{
  "csp_findings": [
    {
      "csp_rule_id": "CIS:1.1",
      "policy_id": "27f98c30ef3411e88ad765862e629d59",
      "pass_percent": 80,
      "rule_name": "Avoid the use of the \"root\" account (Scored)",
      "pass": 4,
      "criticality": "critical",
      "policy_name": "CIS AWS Foundations Benchmark v1.1 2018-11-23 15:26:32-Copy",
      "csp_resource_type": "user",
      "error": 0,
      "rule_id": "280d33b6ef3411e88ad765862e629d59",
      "result": "fail",
      "fail": 1,
      "total": 5,
      "csp_service_type": "iam"
    },
    ...,
  ]
}
```

View all Results for a Specific Rule

Use this call to view all finding summaries for a specific rule using the rule_id from the response of the View a Summary of Findings for Each Rule call.

GET https://api.cloudpassage.com/v1/csp_findings?rule_id={rule ID}

Example:
GET https://api.cloudpassage.com/v1/csp_findings?rule_id=6800dfccefb111e88ad765862e629d59

Response

Status: 200

```
{
  "count": 5,
  "csp_findings": [
    {
      "csp_rule_id": "CIS:1.1",
      "csp_arn": "arn:aws:iam::980294400423:root",
      "criticality": "critical",
      "created_at": "2019-02-12T09:40:22.086Z",
      "rule_id": "6800dfccefb111e88ad765862e629d59",
      "result": "fail",
      "csp_region": null,
      "rules_run_id": "38643166-3534-3238-2d38-3164332d3433",
      "csp_account_id": "980294400423",
      "csp_resource_name": "",
      "csp_account_display_name": "980294400423",
      "id": "83a7033b-4770-4510-83ff-9588bdf9e66f",
...
```
"csp_resource_id": null
},
{
"csp_rule_id": "CIS:1.1",
"csp_arn": "arn:aws:iam::856192027328:root",
"criticality": "critical",
"created_at": "2019-02-12T10:05:47.451Z",
"rule_id": "6800dfccef811e88ad765862e629d59",
"result": "pass",
"csp_region": null,
"rules_run_id": "63343434-6137-3434-2d65-6432652d3465",
"csp_account_id": "856192027328",
"csp_resource_name": "",
"csp_account_display_name": "cloudpassage-production-test",
"id": "ddd67dd4-f920-498b-a43e-c2cbea68333",
"csp_resource_id": null
},
...
CSP Scanner Settings

You can use the csp_scanner_settings endpoint to view and update the CSP scan settings, which are the intervals at which your CSP accounts are scanned. The settings are separated by service, which enables you to set a different interval for each service.

If you want to scan an account manually outside of the intervals specified in the settings, see Scan an Account Manually.

- Object Representation
- View the CSP Scanner Settings
- Update the CSP Scanner Settings

Object Representation

CSP Resources Object Location

```text
api.cloudpassage.com/v1
csp_scanner_settings
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rds</td>
<td>Relational Database Service; an AWS service.</td>
</tr>
<tr>
<td>ec2</td>
<td>Elastic Compute Cloud; an AWS service.</td>
</tr>
<tr>
<td>azure_application_gateway</td>
<td>Application Gateway; an Azure service.</td>
</tr>
<tr>
<td>s3</td>
<td>Simple Storage Service; an AWS service.</td>
</tr>
<tr>
<td>route53</td>
<td>Route 53; an AWS service.</td>
</tr>
<tr>
<td>lambda</td>
<td>Lambda; an AWS service.</td>
</tr>
<tr>
<td>vpc</td>
<td>Virtual Private Cloud; an AWS service.</td>
</tr>
<tr>
<td>ecs</td>
<td>Elastic Container Service; an AWS service.</td>
</tr>
<tr>
<td>aws_kms</td>
<td>Key Management Service; an AWS service.</td>
</tr>
<tr>
<td>cloudFormation</td>
<td>CloudFormation; an AWS service.</td>
</tr>
<tr>
<td>azure_network</td>
<td>Virtual Network; an Azure service.</td>
</tr>
<tr>
<td>iam</td>
<td>Identity and Access Management; an AWS service.</td>
</tr>
<tr>
<td>azure_compute</td>
<td>Compute; an Azure service.</td>
</tr>
<tr>
<td>azure_storage_account</td>
<td>Storage; an Azure service.</td>
</tr>
<tr>
<td>cloudTrail</td>
<td>CloudTrail; an AWS service.</td>
</tr>
<tr>
<td>azure_sql_server</td>
<td>SQL Servers; an Azure service.</td>
</tr>
<tr>
<td>azure_active_directory</td>
<td>Identity and Access Management, an Azure service.</td>
</tr>
</tbody>
</table>

Intervals
<table>
<thead>
<tr>
<th>Enumerable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Every 15 minutes</td>
</tr>
<tr>
<td>60</td>
<td>Every 60 minutes (hourly)</td>
</tr>
<tr>
<td>12</td>
<td>Every 12 hours</td>
</tr>
<tr>
<td>24</td>
<td>Every 24 hours (daily)</td>
</tr>
<tr>
<td>7</td>
<td>Every 7 days (weekly)</td>
</tr>
</tbody>
</table>

**View the CSP Scanner Settings**

Use this call to get the current CSP scan settings. The result displays the scan interval currently set for each service. For a definition of the intervals, see **Intervals**. To change the interval for any service, see **Update CSP Scanner Settings**.

**GET** https://api.cloudpassage.com/v1/csp_scanner_settings

**Response**

```json
{
   "schedules": {
                  "rds": 24,
                  "ec2": 24,
                  "azure_application_gateway": 24,
                  "s3": 24,
                  "route53": 24,
                  "lambda": 24,
                  "vpc": 24,
                  "ecs": 24,
                  "aws_kms": 24,
                  "cloud_formation": 24,
                  "azure_network": 24,
                  "iam": 24,
                  "azure_compute": 24,
                  "azure_storage_account": 24,
                  "cloud_trail": 24,
                  "azure_sql_server": 24,
                  "azure_active_directory": 24
               }
}
```

**Update CSP Scanner Settings**

Use this call to update the current settings for any service. In the request body, enter a new interval to represent the scan interval.

**PUT** https://api.cloudpassage.com/v1/csp_scanner_settings

**Request Body**

```json
{
   "schedules": {
                  "rds": 24,
                  "ec2": 12,
                  "azure_application_gateway": 24,
                  "s3": 12,
                  "route53": 24,
                  "lambda": 24,
                  "vpc": 12,
                  "ecs": 24,
                  "aws_kms": 24,
                  "cloud_formation": 24,
                  "azure_network": 24,
                  "iam": 24,
                  "azure_compute": 24,
                  "azure_storage_account": 24,
                  "cloud_trail": 24,
                  "azure_sql_server": 24,
                  "azure_active_directory": 24
               }
}
```
"azure_network": 24,
"iam": 24,
"azure_compute": 24,
"azure_storage_account": 24,
"cloud_trail": 24,
"azure_sql_server": 12,
"azure_active_directory": 12
}

Response

201
Groups

Use the Server Groups endpoint to create and manage groupings of your servers. You can list, create, delete, and modify groups, including editing their attributes, assigning or removing policies, and listing any defined software vulnerability exceptions.

- **Object Representation**
- **List groups**
- **Search for groups that use a specific configuration policy**
- **Get a single group**
- **List a group's children**
- **Create a new group**
- **Update group attributes**
- **Get a group's scanner settings**
- **Move a group**
- **Assign one or more policies to a group**
- **Remove policies of a given module and platform from a group**
- **Remove specific individual policies from a group**
- **Delete a group without any servers**
- **Delete a group and move the group's servers into its parent group**

**Object Representation**

**Group object location**

```
api.cloudpassage.com/v1

groups

id
```

**Group object fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The Halo ID (a unique string identifier) for this group.</td>
</tr>
<tr>
<td>url</td>
<td>The URL to the group object.</td>
</tr>
<tr>
<td>name</td>
<td>A unique name for this group.</td>
</tr>
<tr>
<td>description</td>
<td><em>Optional.</em> Additional descriptive information, such as the group's purpose, composition, owner, and so on.</td>
</tr>
<tr>
<td>tag</td>
<td><em>Optional.</em> A unique tag assigned to this group. The tag is used to assign servers to the group. Servers started with a given tag will be assigned to the group with that tag. The tag should start with a letter and contain only letters, numbers, . (dot), - (dash), and _ (underscore).</td>
</tr>
<tr>
<td>firewall_policy_id</td>
<td>DEPRECATED. Halo ID of the Linux firewall policy assigned to this group.</td>
</tr>
<tr>
<td>linux_firewall_policy_id</td>
<td>Halo ID of the Linux firewall policy assigned to this group.</td>
</tr>
<tr>
<td>windows_firewall_policy_id</td>
<td>Halo ID of the Windows firewall policy assigned to this group.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>server_counts</td>
<td>An array of name/value pairs, listing the number of servers in the group for each server status: active, missing, deactivated, and total.</td>
</tr>
<tr>
<td>policy_ids</td>
<td>An array of zero or more Halo IDs of Linux configuration policies assigned to this group.</td>
</tr>
<tr>
<td>windows_policy_ids</td>
<td>An array of zero or more Halo IDs of Windows configuration policies assigned to this group.</td>
</tr>
<tr>
<td>cve_exception_ids</td>
<td>An array of zero or more Halo IDs of active CVE exceptions defined for this group. To view the details of any of those exceptions, call the Get a single CVE exception method of the CVE Exceptions API endpoint.</td>
</tr>
<tr>
<td>fim_policy_ids or linux_fim_policy_ids</td>
<td>An array of zero or more Halo IDs of Linux file integrity policies assigned to this group.</td>
</tr>
<tr>
<td>windows_fim_policy_ids</td>
<td>An array of zero or more Halo IDs of Windows file integrity policies assigned to this group.</td>
</tr>
<tr>
<td>alert_profile_ids</td>
<td>An array of zero or more Halo IDs of alert profiles assigned to this group.</td>
</tr>
<tr>
<td>server_events_policy_id</td>
<td>The Halo ID of the special events policy assigned to this group. <strong>Note:</strong> If you update the value of this field using the Update group attributes method, your request JSON must use special_events_policy_id as the field name, instead of server_events_policy_id.</td>
</tr>
<tr>
<td>lids_policy_ids</td>
<td>An array of zero or more Halo IDs of log-based intrusion detection policies assigned to this group.</td>
</tr>
<tr>
<td>km_policy_ids</td>
<td>(currently not used)</td>
</tr>
<tr>
<td>parent_id</td>
<td>The Halo ID of this group's parent group. If this value is null, this group is the root group.</td>
</tr>
<tr>
<td>has_children</td>
<td>true if this group has one or more child groups; false if it has no children.</td>
</tr>
<tr>
<td>children_groups_url</td>
<td>This field is present only if has_children is true. It contains a search URL that you can use in an HTTPS GET call to obtain a list of this group's child groups. (Returns direct children only, not further descendants.)</td>
</tr>
</tbody>
</table>

**Note:** The field firewall_policy_id may appear in example response bodies below. It is a deprecated field; you should use linux_firewall_policy_id instead.

### List groups

Returns the names and details, including group ID, of all of your currently defined groups.

**Note:** The results of this call may be paginated. See Pagination of Results for information on how to set up and retrieve paginated results from the Halo API.

**GET** https://api.cloudpassage.com/v1/groups

### Response

**Status:** 200

```
{
  "count": 20,
  "groups": [
    {
      "id": "0962bfa087bc01323e360670140ec224",
      "url": "https://api.cloudpassage.com/v1/groups/0962bfa087bc01323e360670140ec224",
      "name": "hq-functional",
      "description": "Corporate HQ Outfacing",
      "tag": "corp-func",
      "firewall_policy_id": "21ca3bd0c1e70132afea06f62520010a",
      "linux_firewall_policy_id": "21ca3bd0c1e70132afea06f62520010a",
      "windows_firewall_policy_id": "291f1420abe7013295e406ba9a9c633c",
      "server_counts": {
        "active": 19,
        "missing": 0,
        "deactivated": 45,
        "total": 64
      },
      "policy_ids": [
        "ac3ef580905e01323e650670140ec224",
        "38c89b381f6611e59cb40db4c60bae5"
      ]
    }
  ]
```

75
Search for groups that use a specific configuration policy

Returns a list of groups that that have a specific assigned configuration policy, defined by policy ID.

*Note:* The results of this call may be paginated. See [Pagination of Results](#) for information on how to set up and retrieve paginated results from the Halo API.

**GET** https://api.cloudpassage.com/v1/groups?search[policy_id]={policy_id}

**Response**

**Status:** 200
Get a single group

Returns information describing a single group specified by group ID.

GET https://api.cloudpassage.com/v1/groups/{id}

Response

Status: 200

```json
{
  "group": {
    "id": "0962bfa087bc01323e360670140ec224",
    "url": "https://api.cloudpassage.com/v1/groups/0962bfa087bc01323e360670140ec224",
    "name": "hq-functional",
    "description": "Corporate HQ Outfacing",
    "tag": "corp-func",
    "firewall_policy_id": "21ca3bd0c1e70132af6a06f62520010a",
    "linux_firewall_policy_id": "21ca3bd0c1e70132af6a06f62520010a",
    "windows_firewall_policy_id": "291f1420abe7013295e406ba9a9c633c",
    "server_counts": {
      "active": 19,
      "missing": 0,
      "deactivated": 45,
      "total": 64
    },
    "policy_ids": [
      "ac3ef580905e01323e650670140ec224",
      "38c89b381f6611e59cb40db4c6c0bae5"
    ],
    "windows_policy_ids": [
      "375fa690ae4b01323f180670140ec224"
    ],
    "cve_exception_ids": [],
    "fim_policy_ids": [],
    "windows_fim_policy_ids": [
      "0aea4620b3b6013295e406ba9a9c633c"
    ],
    "alert_profile_ids": [
      "aa62a890a5bc013295e406ba9a9c633c"
    ],
    "server_events_policy_id": "0972b4f087bc01323e360670140ec224",
    "lids_policy_ids": [
      "f3541070d582013295e406ba9a9c633c",
      "2a480fbca981e59765b6f5a2220ad"
    ],
    "km_policy_ids": [],
    "parent_id": null,
    "has_children": false,
    "children_groups_url": "https://api.cloudpassage.com/v1/groups?parent_id=0962bfa087bc01323e360670140ec224"
  },
  ...
}
```
List a group's children

Returns a list of child groups belonging to the group specified by ID in the call URL. The call returns only direct children, not further descendants.

From the response JSON of the List groups or Get a single group method, copy and execute the contents of the children_groups_url field. For example:

https://api.cloudpassage.com/v1/groups?parent_id=0962bfa087bc01323e360670140ec224

Response

```json
{
  "count": 1,
  "groups": [
    {
      "id": "2dd0c6380df511e5a2894925c0df5203",
      "url": "https://portal.cloudpassage.com/v1/groups/2dd0c6380df511e5a2894925c0df5203",
      "name": "GroupA",
      "description": null,
      "ag": null,
      "firewall_policy_id": "7a47c3e43f8811e5a1e719324121e97",
      "linux_firewall_policy_id": "7a47c3e43f8811e5a1e719324121e97",
      "windows_firewall_policy_id": null,
      "server_counts": {
        "active": 0,
        "missing": 0,
        "deactivated": 0,
        "total": 0
      },
      "policy_ids": [],
      "windows_policy_ids": [],
      "cve_exception_ids": [],
      "fim_policy_ids": [],
      "windows_fim_policy_ids": [],
      "alert_profile_ids": [],
      "server_events_policy_id": "0972b4f087bc01323e360670140ec224",
      "lids_policy_ids": [],
      "km_policy_ids": [],
      "parent_id": "999465a0d0e40132c0c606bf4fdbc353",
      "has_children": true,
      "children_groups_url": "https://portal.cloudpassage.com/v1/groups?parent_id=2dd0c6380df511e5a2894925c0df5203"
    }
  ]
}
```
Create a new group

Creates a new group with default values that you specify, and returns its information, including URL and group ID, in the response body.

The minimum attributes that you must supply are the group's name, in the name field, and the Halo ID of its parent group, in the parent_id field. However, if the API key you supply is the root group's key, or if you are not using hierarchical groups, you can omit the parent_id field, and the group will be created as a child of the root group.

Note: You cannot specify a parent group that is outside of the scope of the current group (the group to which the supplied API key belongs); only that group or one of its descendants can be specified as the parent of the group you are creating.

POST https://api.cloudpassage.com/v1/groups

Request Body

```json
{
    "group": {
        "name": "Load Balancers",
        "parent_id": "0962bfa087bc01323e360670140ec224",
        "linux_firewall_policy_id": null,
        "windows_firewall_policy_id": null,
        "policy_ids": ["dac1c0f082e301318c503c764e10b50e"],
        "tag": "load_balancers"
    }
}
```

Response

Status: 201
Location: https://api.cloudpassage.com/v1/groups/aeddc2607f300132a1c73c764e10b50e

```json
{
    "group": {
        "id": "aeddc2607f300132a1c73c764e10b50e",
        "url": "https://api.cloudpassage.com/v1/groups/aeddc2607f300132a1c73c764e10b50e",
        "name": "Load Balancers",
        "tag": "load_balancers",
        "firewall_policy_id": null,
        "linux_firewall_policy_id": null,
        "windows_firewall_policy_id": null,
        "server_counts": {
            "active": 0,
            "missing": 0,
            "deactivated": 0,
            "total": 0
        },
        "policy_ids": ["dac1c0f082e301318c503c764e10b50e"],
        "windows_policy_ids": [],
        "cve_exception_ids": [],
        "fim_policy_ids": [],
        "windows_fim_policy_ids": [],
        "alerts_profile_ids": [],
        "server_events_policy_id": "091577e0e2a7013095903c764e10b50e",
        "lids_policy_ids": [],
        "has_children": false,
        "parent_id": "0962bfa087bc01323e360670140ec224",
        "has_children": false,
    }
}
```
Update group attributes

Use this call to update individual attributes of the group that you specify by group ID. In the request body, you need to include only the attributes that you want modified; other attributes of the group will remain unchanged.

*Note:* If you use this method to update the value of the `server_events_policy_id` field, your request JSON must use `special_events_policy_id` as the field name, instead of `server_events_policy_id`.

**PUT** https://api.cloudpassage.com/v1/groups/{id}

**Request Body**

```json
{
  "group": {
    "name": "Test Groups",
    "tag": "load_balancers"
  }
}
```

**Response**

**Status:** 204

Get a group's scanner settings

Returns the scanner settings of the group specified by ID in the call URL.

In the Halo portal, these scanner settings appear under **Settings > Agent Settings** for the specified group, and they override the global scanner settings that are defined under **Settings > Agent Settings** in Site Administration.

**GET** https://api.cloudpassage.com/v1/groups/{id}/scanner_settings

**Response**

**Status:** 200

```json
{
  "scanner_settings": {
    "firewall_enforce": false,
    "fim_scan_time_limit": 0,
    "csm_scan_time_limit": 0,
    "svm_scan_time_limit": 0
  }
}
```
**Move a group**

Removes an existing group (specified by ID in the call URL) from its current parent group (which may be the root group or any other group) and assigns it as a child of the group that you specify by ID in the request JSON.

**PUT** https://api.cloudpassage.com/v1/groups/{id}

**Request Body**

```json
{
  "group": {
    "parent_id": "4471fe40a65501323ed60670140ec224"
  }
}
```

**Response**

**Status:** 204

**Assign one or more policies to a group**

To the group that you specify by group ID in the call URL, Halo assigns the policy or policies that you specify by policy ID in the request body. Existing assigned policies of the same module type and platform type (Windows or Linux) are replaced by the specified policy or policies.

*Note:* Alert profiles also are assigned using this method.

**PUT** https://api.cloudpassage.com/v1/groups/{id}

**Request Body (for firewall policy)**

```json
{
  "group": {
    "linux_firewall_policy_id": "96cb9470a9b9012e0e56442c030d794c"
  }
}
```

**Request Body (for configuration policies)**

```json
{
  "group": {
    "policy_ids": ["96cb9470a9b9012e0e56442c030d794d", "96cb9470a9b9012e0e56442c030d794f"]
  }
}
```

**Request Body (for file integrity policies)**

```json
{
}
```
Request Body (for log-based intrusion detection policies)

```json
{
  "group": {
    "lids_policy_ids": [
      "96cb9470a9b9012e0e56442c030d794d",
      "96cb9470a9b9012e0e56442c030d794f"
    ]
  }
}
```

Request Body (for special events policy)

```json
{
  "group": {
    "special_events_policy_id": "dffd09e0ebe60130662b3c764e101158"
  }
}
```

Request Body (for alert profiles)

```json
{
  "group": {
    "alert_profile_ids": [
      "dfe38eb0ebe60130662b3c764e101158",
      "dfe81370ebe60130662b3c764e101158"
    ]
  }
}
```

Response

**Status: 204**

Remove policies of a given module and platform from a group

This call uses a PUT request. From the group that you specify by group ID in the call URL, Halo removes the policy or policies of the module type for which you pass a policy ID value of null in the request body. If the module supports separate Windows and Linux policies, you remove them separately.

**PUT https://api.cloudpassage.com/v1/groups/{id}**

Request Body (for firewall policy)

*Note:* When a firewall policy is removed from a group, servers in that group keep that firewall until a new policy is assigned to the group (or the firewall is manually changed at the server).

```json
{
  "group": {
    "linux_firewall_policy_id": null,
    "windows_firewall_policy_id": null
  }
}
```
Response
Status: 204

Remove specific individual policies from a group

This call uses a DELETE request. From the group that you specify by group ID in the call URL, Halo removes the log-based intrusion detection policies for which you pass valid policy ID values in the request body.

DELETE https://api.cloudpassage.com/v1/groups/{id}

Request Body (for log-based intrusion detection policies)

```json
{
  "group": {
    "lids_policy_ids": ["96cb9470a9b9012e0e56442c030d794d", "96cb9470a9b9012e0e56442c030d794f"]
  }
}
```

Response
Status: 204

Delete a group without any servers

Deletes the group that you specify by group ID. The group must be empty (have no assigned servers); if it is not empty, the call fails with a 422 response status code (unprocessable entity). If the call is successful, the group is deleted from the Halo database and cannot be retrieved.

DELETE https://api.cloudpassage.com/v1/groups/{id}

Response
Status: 202

Delete a group and move the group's servers into its parent group

Deletes the group that you specify by group ID, regardless of whether or not it is empty. If you have not implemented group hierarchy, any servers assigned to the group are moved into the root group; if your groups are organized hierarchically, the servers are moved to the group's parent group. If the call is successful, your specified group is deleted from the Halo database and cannot be retrieved.

DELETE https://api.cloudpassage.com/v1/groups/{id}?move_to_parent=true

Response
Status: 202
Servers

Use the Servers endpoint to manage individual server resources. Any physical or virtual server on which you have installed a Halo agent is represented in the API by a server object.

You can use this API endpoint to list your servers, move servers among groups, and inspect security issues related to your servers.

- **Object Representation**
- List servers
- List servers in a specific group
- List servers that have a specific user account
- Get a single server
- Move a server into a group
- Remove a server from a group
- Retire a server
- Delete a server
- List server issues

### Object Representation

**Server object location**

```plaintext
api.cloudpassage.com/v1
  └ servers
      └ id
```

**Server object fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>created_at</td>
<td>The date-time at which the server's Halo agent first started and registered with Halo.</td>
</tr>
<tr>
<td>id</td>
<td>A unique identifier of the server.</td>
</tr>
<tr>
<td>url</td>
<td>The API URL to the server object.</td>
</tr>
<tr>
<td>hostname*</td>
<td>A calculated hostname of the server.</td>
</tr>
<tr>
<td>server_label*</td>
<td>A user-assigned label or description for the server.</td>
</tr>
<tr>
<td>reported_fqdn*</td>
<td>The internal fully qualified domain name of the server.</td>
</tr>
<tr>
<td>primary_ip_address</td>
<td>The primary IP address of the server (the first routable address in the server's sorted list of supported interfaces and addresses).</td>
</tr>
<tr>
<td>connecting_ip_address</td>
<td>The last reported IP address of the server.</td>
</tr>
<tr>
<td><strong>state</strong></td>
<td>The current state of the server’s Halo agent: <strong>active</strong>, <strong>deactivated</strong>, <strong>missing</strong>, or <strong>retired</strong>.</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>daemon_version</strong></td>
<td>The version number of the currently installed Halo agent.</td>
</tr>
<tr>
<td><strong>read_only</strong></td>
<td><strong>true</strong> if the Halo agent is running in read-only mode; otherwise <strong>false</strong>.</td>
</tr>
<tr>
<td><strong>platform</strong></td>
<td>Family of the currently installed operating system: <strong>windows</strong>, <strong>linux</strong>, or a Linux distribution name.</td>
</tr>
<tr>
<td><strong>platform_version</strong></td>
<td><strong>Linux</strong>: The version number of the O.S. distribution. <strong>Windows</strong>: same as <strong>os_version</strong>.</td>
</tr>
<tr>
<td><strong>os_version</strong></td>
<td>The full version number of the operating system.</td>
</tr>
<tr>
<td><strong>kernel_name</strong></td>
<td><strong>Windows</strong>: The full name of the operating system, such as <strong>Microsoft Windows Server 2008 Dat acenter</strong>. <strong>Linux</strong>: Same as <strong>platform</strong>.</td>
</tr>
<tr>
<td><strong>kernel_machine</strong></td>
<td>The general chip architecture, such as <strong>32-bit</strong>, <strong>64-bit</strong>, or <strong>x86_64</strong>.</td>
</tr>
<tr>
<td><strong>self_verification.failed</strong></td>
<td><strong>true</strong> if the most recent agent self-verification test failed; otherwise <strong>false</strong>.</td>
</tr>
<tr>
<td><strong>connecting_ip_fqdn</strong></td>
<td>The fully qualified domain name of the server, using the connecting IP address as the hostname.</td>
</tr>
<tr>
<td><strong>last_state_change</strong></td>
<td>The date-time (in ISO-8601 format) of the last change in server status (to <strong>active</strong>, <strong>deactivated</strong>, or <strong>missing</strong>).</td>
</tr>
<tr>
<td><strong>docker_inspection</strong></td>
<td>Indicates whether the halo agent on this server has Docker inspection enabled.</td>
</tr>
<tr>
<td><strong>group_id</strong></td>
<td>The Halo ID of the group to which the server belongs.</td>
</tr>
<tr>
<td><strong>group_name</strong></td>
<td>The name of the group to which the server belongs.</td>
</tr>
<tr>
<td><strong>group_path</strong></td>
<td>The full path (in the group hierarchy) to the group to which the server belongs.</td>
</tr>
<tr>
<td><strong>firewall_policy</strong></td>
<td>The current firewall policy installed on the server (if any). <em>Only shown in single server listing details.</em></td>
</tr>
<tr>
<td><strong>proxy</strong></td>
<td>The IP address or FQDN, port number, and name of the proxy server, if this server is configured to use a proxy.</td>
</tr>
<tr>
<td><strong>interfaces</strong></td>
<td>A list of reported network interfaces that are present on the server. Each interface is an array of the following subfields:</td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>The name of the interface.</td>
</tr>
<tr>
<td><strong>ip_address</strong></td>
<td>The IP address of the interface.</td>
</tr>
<tr>
<td><strong>netmask</strong></td>
<td>The netmask of the interface’s network.</td>
</tr>
<tr>
<td><strong>mac_address</strong></td>
<td>The MAC (media access control) address of the interface.</td>
</tr>
<tr>
<td><strong>display_name</strong></td>
<td>The interface name that displays in the Windows UI. (For Windows servers only.)</td>
</tr>
<tr>
<td><strong>csp_provider</strong></td>
<td>The cloud service provider; i.e., <strong>aws_ec2</strong>, <strong>azure</strong>, <strong>gcp</strong> (For cloud servers only.)</td>
</tr>
<tr>
<td><strong>csp_account_id</strong></td>
<td>The ID of the cloud service provider account. (For cloud servers only.)</td>
</tr>
<tr>
<td><strong>csp_availability_zone</strong></td>
<td>The availability zone in which the instance launched; for example, <strong>us_west_1</strong>. (For cloud servers only.)</td>
</tr>
<tr>
<td><strong>csp_image_id</strong></td>
<td>The ID of the Amazon Machine Image from which the workload was instantiated. (For cloud servers only.)</td>
</tr>
<tr>
<td><strong>csp_instance_id</strong></td>
<td>The cloud service provider’s ID of the instance. (For cloud servers only.)</td>
</tr>
<tr>
<td><strong>csp_instance_type</strong></td>
<td>The type of hardware the host computer used for the instance. (For cloud servers only.)</td>
</tr>
<tr>
<td><strong>csp_kernel_id</strong></td>
<td>The ID of the kernel image launched with this instance. (For cloud servers only.)</td>
</tr>
<tr>
<td><strong>csp_private_ip</strong></td>
<td>The private IP address of the instances. In cases where multiple network interfaces are present, this refers to the eth0 device. (For cloud servers only.)</td>
</tr>
<tr>
<td><strong>csp_region</strong></td>
<td>The cloud provider region in which the instance was launched; for example, <strong>AP South 1</strong>, <strong>AP Northe ast 1</strong>, <strong>CA Central 1</strong>, <strong>EU West 1</strong>, and so on. (For cloud servers only.)</td>
</tr>
<tr>
<td><strong>csp_security_groups</strong></td>
<td>The security groups assigned to the cloud instance. (For cloud servers only.)</td>
</tr>
<tr>
<td><strong>csp_instance_tags</strong></td>
<td>Key value pairs assigned to the instance within the cloud service provider account. When available, these are retrieved by the Halo agent.</td>
</tr>
<tr>
<td><strong>csp_tags</strong></td>
<td>The list of tags, in key value pairs, that is assigned to the asset in the cloud service provider account.</td>
</tr>
</tbody>
</table>
List servers

Returns a list of all of your active Halo-protected servers.

**Note:** The results of this call may be paginated. See [Pagination of Results](#) for information on how to set up and retrieve paginated results from the Halo API.

GET https://api.cloudpassage.com/v1/servers?state={state_list}

You can modify the search by applying many filters, and you can also specify how the returned results are to be sorted.

**Search Filters**

You can apply any of the following filters to restrict the set of servers returned. For any of the filters, you can provide either a single value or a comma-separated list of values. If you do provide multiple values, they are OR'd in a search, meaning that the search passes for that filter if any of its supplied values matches.

**Server state:**

Add the `state` filter parameter with any comma-separated combination of the values `active`, `deactivated`, `missing`, and `retrired`. If you do not use the `state` parameter, only active servers are returned. For example:

GET https://api.cloudpassage.com/v1/servers

(default call returns all active servers)

GET https://api.cloudpassage.com/v1/servers?state=active

returns all active servers)

GET https://api.cloudpassage.com/v1/servers?state=missing,deactivated,retrired

returns all servers that are not active)

GET https://api.cloudpassage.com/v1/servers?state=active&last_state_change_gte=timestamp

returns all servers that were activated at or after the specified date-time)

**NOTE:** Insert inequality operators by adding these extensions to `last_state_change: _gt, _lt, _gte, and _lte`
Server identity:

GET https://api.cloudpassage.com/v1/servers?hostname=WEB-2743
    (returns servers whose host name matches or contains "WEB-2743")

GET https://api.cloudpassage.com/v1/servers?connecting_ip_address=127.63.31.15
    (returns the server at that IP address)

GET https://api.cloudpassage.com/v1/servers?reported_fqdn=ts-pg-build
    (returns server whose internal fully qualified domain name matches or contains "ts-pg-build")

    (returns servers whose connecting-IP-address-based fully qualified domain name matches or contains "c-127-63-31-15.west.acme.com")

    (returns servers whose agents registered with halo at or more recently than "2017-02-13T23:07:37Z")

    (returns servers whose agents registered with halo at or earlier than "2017-02-13T23:07:37Z")

GET https://api.cloudpassage.com/v1/servers?group_id=id1,id2,id3
    (returns servers that are in any of the specified groups)

    (returns servers whose group name matches or contains "US-HQ-balancers")

GET https://api.cloudpassage.com/v1/servers?server_label=my-webserver
    (returns servers whose server label matches or contains "my-webserver")

GET https://api.cloudpassage.com/v1/servers?ec2_availability_zone=eu-central-1
    (returns AWS servers whose availability zone is "eu-central-1")

GET https://api.cloudpassage.com/v1/servers?ec2_security_group=acme-db
    (returns AWS servers whose EC2 security group matches or contains "acme-db")

Platform and operating system:

GET https://api.cloudpassage.com/v1/servers?platform=windows
    (returns only windows servers)

GET https://api.cloudpassage.com/v1/servers?platform_version=5.6
    (returns only servers whose platform version number matches or contains "5.6")

GET https://api.cloudpassage.com/v1/servers?kernel_name=Microsoft%20Windows%20Server%202008%20R2%20Datacenter
    (returns only servers whose O.S. name matches exactly "Microsoft Windows Server 2008 R2 Datacenter")
    Note: when used in a search filter, this value must be URL-encoded

GET https://api.cloudpassage.com/v1/servers?os_version=2.6.18-238.19.1.el5.centos.plusxen
    (returns only servers whose O.S. version number matches or contains "2.6.18-238.19.1.el5.centos.plusxen")

GET https://api.cloudpassage.com/v1/servers?kernel_machine=64-bit
    (returns only servers with that general chip architecture)

Halo agent:
GET https://api.cloudpassage.com/v1/servers?daemon_version=2.7.9
  (returns only servers with that version of the Halo agent)

GET https://api.cloudpassage.com/v1/servers?self_verification_failed=true
  (returns only servers whose agent has failed its self-verification test)

GET https://api.cloudpassage.com/v1/servers?read_only=true
  (returns only servers whose agent is running in audit mode)

Vulnerability information:

GET https://api.cloudpassage.com/v1/servers?package_name=Internet+Explorer
  (returns only servers that have a package with that name)
  Note: when used in a search filter, this value must be URL-encoded

  (returns only servers that have a package with that version number)

  (returns only servers that have a package containing the specified CVE)

  (returns only servers that have a package containing one or more of the specified CVEs)

GET https://api.cloudpassage.com/v1/servers?kb=KB2485376
  (returns only Windows servers that have been patched to comply with the Microsoft Knowledge Base article with that ID)

GET https://api.cloudpassage.com/v1/servers?missing_kb=KB2485376
  (returns only Windows servers that have not yet been patched to comply with the Microsoft Knowledge Base article with that ID)

Cloud service information:

GET https://api.cloudpassage.com/v1/servers?csp_account_id=856192027328
  (returns only servers with that specific CSP account ID)

GET https://api.cloudpassage.com/v1/servers?csp_image_id=ami-059e7901352ebaef8
  (returns only servers with that specific CSP image ID)

GET https://api.cloudpassage.com/v1/servers?csp_instance_id=i-0d0995f78cd6edd9f
  (returns only servers with that specific CSP instance ID)

  (returns only servers with a specific provider type)

Sorting the results

You can specify that the search results are to be alphanumerically sorted (in either ascending or descending order) according to the values of any of the following server-object fields:

- hostname
- connecting_ip_fqdn
- platform
- platform_version
- server_group_name
- state
- daemon_version

89
For example:

**GET** https://api.cloudpassage.com/v1/servers?platform=linux&sort_by=server_label.asc

**GET** https://api.cloudpassage.com/v1/servers?server_group_name=web-US&sort_by=hostname.desc

*Note:* If the server is configured to use a proxy, information about the proxy is also returned.

**Response**

**Status:** 200

```json
{
  "servers": [
    {
      "created_at": "2019-06-21T10:42:00.404Z",
      "id": "33177a8c94111e9b0353d9f1714ccd7",
      "url": "https://portal.cloudpassage.com/v1/servers/33177a8c94111e9b0353d9f1714ccd7",
      "hostname": "EC2AMAZ-NDR9IBP",
      "server_label": null,
      "reported_fqdn": "EC2AMAZ-NDR9IBP",
      "primary_ip_address": "172.25.16.1",
      "connecting_ip_address": "172.218.253.104",
      "state": "active",
      "daemon_version": "4.2.2",
      "read_only": false,
      "platform": "windows",
      "os_version": "10.0.17763",
      "kernel_name": "Microsoft Windows Server 2019 Datacenter",
      "kernel_machine": "64-bit",
      "self_verification_failed": false,
      "connecting_ip_fqdn": "ec2-54-218-253-104.us-west-2.compute.amazonaws.com",
      "last_state_change": "2019-06-21T10:42:00.404Z",
      "docker_inspection": "Disabled",
      "group_id": "9b5c583655fc11e9afd41154f44a4b54",
      "group_name": "api automation",
      "group_path": "qa-automation-100/api automation",
      "interfaces": [
        {
          "name": "vEthernet (nat)",
          "ip_address": "172.25.16.1",
          "netmask": "255.255.240.0",
          "mac_address": null,
          "display_name": "vEthernet (nat)"
        },
        {
          "name": "Ethernet",
          "ip_address": "172.31.20.172",
          "netmask": "255.255.240.0",
          "mac_address": null,
          "display_name": "Ethernet"
        }
      ],
      "aws_ec2": {
        "ec2_instance_id": "i-08453cfd2eb547acf",
        "ec2_account_id": "357679622600",
        "ec2_kernel_id": null,
        "ec2_image_id": "ami-0fd06ccdd116000c4",
        "ec2_availability_zone": "us-west-2a",
        "ec2_region": "us-west-2",
        "ec2_private_ip": "172.31.20.172",
        "ec2_instance_type": "t2.micro",
        "ec2_security_groups": [
          "22-udp"
        ]
      },
      "csp_provider": "aws_ec2",
      "csp_account_id": "357679622600",
      "csp_availability_zone": "us-west-2a",
      "csp_image_id": "ami-0fd06ccdd116000c4",
      "csp_instance_id": "i-08453cfd2eb547acf",
      "csp_instance_type": "t2.micro",
      "csp_kernel_id": null,
      "csp_private_ip": "172.31.20.172"
    }
  ]
}
```
List servers in a specific group

Returns a list of all active servers in the group specified by group ID. You can expand or further restrict the results to specific server states by adding the state filter parameter with any comma-separated combination of the values active, deactivated, and missing. If you do not use the state parameter, only active servers are returned. (For example usages, see List servers.)

Note: The results of this call may be paginated. See Pagination of Results for information on how to set up and retrieve paginated results from the Halo API.

GET https://api.cloudpassage.com/v1/servers?group_id={group_id}

GET https://api.cloudpassage.com/v1/servers?group_id={group_id}&state={state}

Response

Status: 200

{  "servers": [    {      "created at": "2019-06-21T10:42:00.404Z",      "id": "33177a8c94111e9b0353d9f1714ccd7",      "url": "https://portal.cloudpassage.com/v1/servers/33177a8c94111e9b0353d9f1714ccd7",      "hostname": "EC2AMAZ-NDR9IBP",      "server label": null,      "reported_fqdn": "EC2AMAZ-NDR9IBP",      "primary ip address": "172.25.16.1",      "connecting_ip_address": "54.218.253.104",      "state": "active",      "daemon version": "4.2.2",      "read only": false,      "platform": "windows",      "platform version": "10.0.17763",      "os version": "10.0.17763",      "kernel name": "Microsoft Windows Server 2019 Datacenter",      "kernel machine": "64-bit",      "self verification failed": false,      "connecting ip fqdn": "ec2-54-218-253-104.us-west-2.compute.amazonaws.com",      "last state change": "2019-06-21T10:42:00.404Z",      "docker inspection": "Disabled",      "group id": "9b5c583655fc11e9afdfd41154f44a4b54",      "group name": "api automation",      "group path": "qa-automation-100/api automation",      "interfaces": [        {          "name": "(3D4EBF7F-33AF-4084-8746-334B6630045C)",          "ip address": "172.25.16.1",          "netmask": "255.255.240.0",          "mac address": null,          "display name": "vEthernet (nat)"        },        {          "name": "(57458FBC-3C60-4E41-8A30-CA6D0716E393)"        }      ]    }  ]
List servers that have a specific user account

Returns a list of all active servers that have the local user account specified by username or uid. Account information for the specified user is also returned. All groups are searched.

You can expand or further restrict the results to specific server states by adding the `state` filter parameter with any comma-separated combination of the values `active`, `deactivated`, and `missing`. If you do not use the `state` parameter, only active servers are returned. (For example usages, see List servers.)

The results show the details of both the server and the account for each server that the account exists on.


GET https://api.cloudpassage.com/v1/servers?search[username]={username}&state={state_list}


GET https://api.cloudpassage.com/v1/servers?search[uid]={uid}&state={state_list}

Response

Status: 200
"servers": [{
    "created_at": "2018-06-29T18:15:43.728Z",
    "id": "6ffc6b907bc811e896c42d7881e8c8b6",
    "url": "https://portal.cloudpassage.com/v2/servers/6ffc6b907bc811e896c42d7881e8c8b6",
    "hostname": "ip-10-0-1-248",
    "server_label": null,
    "reported_fqdn": "ip-10-0-1-248.us-west-1.compute.internal",
    "primary_ip_address": "10.0.1.248",
    "connecting_ip_address": "13.57.221.240",
    "state": "active",
    "daemon_version": "4.2.2",
    "read_only": false,
    "platform": "redhat",
    "platform_version": "7.5",
    "os_version": "3.10.0-862.el7.x86_64",
    "kernel_name": "Linux",
    "kernel_machine": "x86_64",
    "self_verification_failed": false,
    "connecting_ip_fqdn": "ec2-13-57-221-240.us-west-1.compute.amazonaws.com",
    "last_state_change": "2018-06-29T18:15:43.729Z",
    "docker_inspection": "Disabled",
    "group_id": "cb67c496bac311e7a99a25a5439f4006",
    "group_name": "DEV20845",
    "group_path": "qa-automation-100/DEV20845",
    "interfaces": [{
        "name": "eth0",
        "ip_address": "FE80::407:F0FF:FE9F:8FA8/64",
        "netmask": ",",
        "mac_address": null,
        "display_name": "vEthernet (nat)"
    },
    {
        "name": "eth0",
        "ip_address": "10.0.1.248",
        "netmask": "255.255.0.0",
        "mac_address": null,
        "display_name": "Ethernet"
    }]
},
"aws_ec2": {
    "ec2_instance_id": "i-0ba3524709b352ef9",
    "ec2_account_id": "856192027328",
    "ec2_kernel_id": null,
    "ec2_image_id": "ami-18726478",
    "ec2_availability_zone": "us-west-1b",
    "ec2_region": "us-west-1",
    "ec2_private_ip": "10.0.1.248",
    "ec2_instance_type": "t2.micro",
    "ec2_security_groups": ["default"]
},
"csp_provider": "aws_ec2",
"csp_account_id": "856192027328",
"csp_availability_zone": "us-west-1b",
"csp_image_id": "ami-18726478",
"csp_instance_id": "i-0ba3524709b352ef9",
"csp_instance_type": "t2.micro",
"csp_kernel_id": null,
"csp_private_ip": "10.0.1.248",
"csp_region": "us-west-1",
"csp_security_groups": null,
"csp_instance_tags": {
    "csp_tags": [{
        "key": "owner",
        "value": "bobgonzales"
    },
    {
        "key": "customer",
        "value": "acme"
    }]
}
],
"accounts": []
}
Get a single server

Returns the server information (including firewall policy information) for the server specified by server ID.

GET https://api.cloudpassage.com/v1/servers/{server_id}/

Response

Status: 200

```json
{
  "server": {
    "created_at": "2019-06-21T10:42:00.404Z",
    "url": "https://portal.cloudpassage.com/v1/servers/33177a8c941111e9b0353d9f1714ccd7",
    "hostname": "EC2AMAZ-NDR9IBP",
    "reported_fqdn": "EC2AMAZ-NDR9IBP",
    "primary_ip_address": "172.25.16.1",
    "connecting_ip_address": "54.218.253.104",
    "state": "active",
    "daemon_version": "4.2.2",
    "read_only": false,
    "platform": "windows",
    "platform_version": "10.0.17763",
    "os_version": "10.0.17763",
    "kernel_name": "Microsoft Windows Server 2019 Datacenter",
    "kernel_machine": "64-bit",
    "self_verification_failed": false,
    "connecting_ip_fqdn": "ec2-54-218-253-104.us-west-2.compute.amazonaws.com",
    "last_state_change": "2019-06-21T10:42:00.404Z",
    "docker_inspection": "Disabled",
    "group_id": "9b5c583655fc11e9afd41154f44a4b54",
    "group_name": "api automation",
    "group_path": "qa-automation-100/api automation",
    "firewall_policy": null,
    "interfaces": [
      {
        "name": "{3D4EBF7F-33AF-4084-8746-334B6630045C}",
        "ip_address": "172.25.16.1",
        "netmask": "255.255.240.0",
        "mac_address": null,
        "display_name": "vEthernet (nat)"
      },
      {
        "name": "{57458FBC-3C60-4E41-8A30-CA6D0716E393}",
        "ip_address": "172.31.20.172",
        "netmask": "255.255.240.0",
        "mac_address": null,
        "display_name": "Ethernet"
      }
    ],
    "aws_ec2": {
      "ec2_instance_id": "i-08453cfd2eb547acf",
      "ec2_account_id": "357679622600",
      "ec2_kernel_id": null,
      "ec2_image_id": "ami-0fd06ccdd116000c4",
      "ec2_availability_zone": "us-west-2a",
      "ec2_region": "us-west-2",
      "ec2_private_ip": "172.31.20.172",
      "ec2_instance_type": "t2.micro",
      "ec2_security_groups": [
        "22-udp"
      ]
    },
    "csp_provider": "aws ec2",
    "csp_account_id": "357679622600",
    "csp_availability_zone": "us-west-2a",
    "csp_image_id": "ami-0fd06ccdd116000c4",
    "csp_instance_id": "i-08453cfd2eb547acf",
    "csp_instance_type": "t2.micro",
    "csp_kernel_id": null,
    "csp_private_ip": "172.31.20.172",
    "csp_region": "us-west-2",
    "csp_security_groups": [
      "22-udp"
    ],
    "csp_instance_tags": [],
    "csp_tags": [
      ...
```

94
Move a server into a group

Moves the server specified by server ID in the call URL into the group specified by group ID in the request body. This is equivalent to deleting the server from its previous group and adding it to the specified group.

**Note:** Retiring a server is no longer considered a move. See Retire a server.

**PUT** https://api.cloudpassage.com/v1/servers/{server_id}

**Request Body**

```json
{
  "server": {
    "group_id": "94a90ae07284012e23f3442c031a719c"
  }
}
```

**Response**

**Status:** 204

Remove a server from a group

Removing an active server from a group means moving it to another group, such as the root group. If you want to move a server to the root group, first obtain the group ID for the root group by submitting a List groups request:

**GET** https://api.cloudpassage.com/v1/groups

Then move the server to the root group by submitting a Move server into a group request and supplying the root group’s ID:

**PUT** https://api.cloudpassage.com/v1/servers/{server_id}

**Request Body**

```json
{
  "server": {
    "group_id": "{root_group_id}"
  }
}
```

**Response**

**Status:** 204
Retire a server

Retires the server that you specify by server ID in the request URL. The server must be inactive. If the call is successful, the server has the state retired and remains assigned to its group, although it is by default no longer visible in the Halo portal.

PUT https://api.cloudpassage.com/v1/servers/{server_id}

Request Body

```json
{
    "server": {
        "retire": true
    }
}
```

Response

Status: 204

Delete a server

Deletes the server that you specify by server ID. The server must be inactive. If the call is successful, the server is permanently removed from Halo and cannot be retrieved.

DELETE https://api.cloudpassage.com/v1/servers/{server_id}

Response

Status: 204

List server issues

For the active server specified by server ID, this call returns a list of security issues detected on that server from the most recent configuration and vulnerability scans. Critical issues appear first, followed by non-critical issues.

Note: The "issues" described here are scan findings, and they differ in detail from the Halo issues returned by calls to the Issues API endpoint (which are also the issues seen in the Issues view of the Halo portal).

In the response JSON to this call, the findings field and its subfields describe scan results. See the the Server Scans endpoint for explanations of those fields.

Note: In the response JSON, any reported issues involving Windows Local Security policy are displayed with the abbreviated names used by the Windows secedit tool; see Valid Values for Local Security Policy Settings for a full list of the abbreviations.

GET https://api.cloudpassage.com/v1/servers/{server_id}/issues

Response
json format:

```json
{
  "id": "272c13d4a503fa7a851e5373ddcb8c1",
  "hostname": "ip-10-171-139-167",
  "connecting_ip_address": "184.72.3.57",
  "state": "active",
  "csm": {
    "status": "completed_with_errors",
    "critical_findings_count": 2,
    "non_critical_findings_count": 23,
    "policies": ["AllChief-4053", "ami, centos, rhel, fedora core v2"],
    "findings": [
      {
        "critical": true,
        "status": "bad",
        "details": {
          "type": "configuration",
          "status": "bad",
          "target": "/etc/hosts",
          "expected": "gleeb",
          "actual": "localhost  localhost.localdomain",
          "scan_status": "ok",
          "config_key": "127.0.0.1",
          "config_key_value_delimiter": "",
        }
      },
      {
        "type": "configuration",
        "status": "bad",
        "target": "/proc/sys/net/ipv4/ip_forward",
        "expected": "42",
        "actual": "0",
        "scan_status": "ok",
        "config_key": "",
        "config_key_value_delimiter": ""
      },
      {
        "type": "port_white",
        "status": "bad",
        "target": "*",
        "expected": "22",
        "actual": "68/UDP",
        "scan_status": "ok",
        "requested_target": "eth0",
        "bound_process": "dhclient",
        "port_scan_status": "unroutable"
      },
      {
        "type": "port_white",
        "status": "bad",
        "target": "*",
        "expected": "22",
        "actual": "631/UDP",
        "scan_status": "ok",
        "requested_target": "eth0",
        "bound_process": "portreserve",
        "port_scan_status": "unroutable"
      },
      {
        "type": "port_white",
        "status": "good",
        "target": "*",
        "expected": "22",
        "actual": "22/TCP",
        "scan_status": "ok",
        "requested_target": "eth0",
        "bound_process": "sshd",
        "port_scan_status": "unroutable"
      }
    ]
  }
}
```

---

**Status:** 200

```json
{
  "id": "272c13d4a503fa7a851e5373ddcb8c1",
  "hostname": "ip-10-171-139-167",
  "connecting_ip_address": "184.72.3.57",
  "state": "active",
  "csm": {
    "status": "completed_with_errors",
    "critical_findings_count": 2,
    "non_critical_findings_count": 23,
    "policies": ["AllChief-4053", "ami, centos, rhel, fedora core v2"],
    "findings": [
      {
        "critical": true,
        "status": "bad",
        "details": {
          "type": "configuration",
          "status": "bad",
          "target": "/etc/hosts",
          "expected": "gleeb",
          "actual": "localhost  localhost.localdomain",
          "scan_status": "ok",
          "config_key": "127.0.0.1",
          "config_key_value_delimiter": ""
        }
      },
      {
        "type": "configuration",
        "status": "bad",
        "target": "/proc/sys/net/ipv4/ip_forward",
        "expected": "42",
        "actual": "0",
        "scan_status": "ok",
        "config_key": "",
        "config_key_value_delimiter": ""
      },
      {
        "type": "port_white",
        "status": "bad",
        "target": "*",
        "expected": "22",
        "actual": "68/UDP",
        "scan_status": "ok",
        "requested_target": "eth0",
        "bound_process": "dhclient",
        "port_scan_status": "unroutable"
      },
      {
        "type": "port_white",
        "status": "bad",
        "target": "*",
        "expected": "22",
        "actual": "631/UDP",
        "scan_status": "ok",
        "requested_target": "eth0",
        "bound_process": "portreserve",
        "port_scan_status": "unroutable"
      },
      {
        "type": "port_white",
        "status": "good",
        "target": "*",
        "expected": "22",
        "actual": "22/TCP",
        "scan_status": "ok",
        "requested_target": "eth0",
        "bound_process": "sshd",
        "port_scan_status": "unroutable"
      }
    ]
  }
}
```
"status": "bad",
"cve_entries": [
    {
        "cve_entry": "CVE-2008-3962",
        "cvss_score": 4.9,
        "suppressed": false
    },
    {
        "cve_entry": "CVE-2008-7258",
        "cvss_score": 5.2,
        "suppressed": false
    }
]
Server Accounts

Use the Server Accounts endpoint to manage local user accounts on your Linux or Windows servers. You can list user accounts, get account details, search for specific users, and (for Linux accounts) reset passwords, update SSH keys, and create, disable, or remove accounts.

Note: You can also use the API to launch a server account scan of an individual server. See Launch scan of a server in the Server Scans API endpoint for details.

- Object Representation
  - List server accounts
  - Get server account details
  - Create a new server account
  - Reset password for a server account
  - Disable a server account
  - Enable a server account
  - Update SSH keys for a server account
  - Remove a server account

Object Representation

Server account object location

\[
\text{api.cloudpassage.com/v1/servers/\_server\_id/accounts/\_username}
\]

Server account object fields

Two levels of server-account information are available.

Core server account fields

Core account fields are accessed through, for example, the List server accounts method.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>A username of the server account.</td>
</tr>
<tr>
<td>url</td>
<td>The API URL to the server account object.</td>
</tr>
<tr>
<td>id</td>
<td>[Linux only] A user ID of the server account.</td>
</tr>
<tr>
<td>geed</td>
<td>[Linux only] A group ID of the server account.</td>
</tr>
<tr>
<td>seed</td>
<td>[Windows only] The security ID of the server account.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>admin</td>
<td><em>true</em> if this account has administrative privileges; otherwise <em>false</em>.</td>
</tr>
<tr>
<td>comment</td>
<td>A user-defined comment or description of the account.</td>
</tr>
<tr>
<td>home</td>
<td>The home directory of the server account.</td>
</tr>
<tr>
<td>shell</td>
<td>[<em>Linux only</em>] A server's account shell.</td>
</tr>
<tr>
<td>last_login_at</td>
<td>The last time the server account logged on, in UTC time (if available)</td>
</tr>
<tr>
<td>last_login_from</td>
<td>[<em>Linux only</em>] The last domain and port the account logged on from (if available)</td>
</tr>
<tr>
<td>active</td>
<td><em>true</em> if this account is active; otherwise <em>false</em>.</td>
</tr>
<tr>
<td>locked</td>
<td>[<em>Windows only</em>] <em>true</em> if this account is locked; otherwise <em>false</em>.</td>
</tr>
</tbody>
</table>

**Server account details fields**

Account details fields are accessed through the **Get server account details** method.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username*</td>
<td>The username of the server account.</td>
</tr>
<tr>
<td>url</td>
<td>The API URL to the server account object.</td>
</tr>
<tr>
<td>id</td>
<td>[<em>Linux only</em>] The user id of the server account.</td>
</tr>
<tr>
<td>geed</td>
<td>[<em>Linux only</em>] The group id of the server account.</td>
</tr>
<tr>
<td>seed</td>
<td>[<em>Windows only</em>] The security ID of the server account.</td>
</tr>
<tr>
<td>admin</td>
<td><em>true</em> if this account has administrative privileges; otherwise <em>false</em>.</td>
</tr>
<tr>
<td>comment</td>
<td>A user-defined comment or description of the account.</td>
</tr>
<tr>
<td>home</td>
<td>The home directory of the server account.</td>
</tr>
<tr>
<td>shell</td>
<td>[<em>Linux only</em>] The server's account shell.</td>
</tr>
<tr>
<td>last_login_at</td>
<td>The last time the server account logged on, in UTC time (if available)</td>
</tr>
<tr>
<td>last_login_from</td>
<td>[<em>Linux only</em>] The last domain and port the account logged on from (if available)</td>
</tr>
<tr>
<td>active</td>
<td><em>true</em> if this account is active; otherwise <em>false</em>.</td>
</tr>
<tr>
<td>locked</td>
<td>[<em>Windows only</em>] <em>true</em> if the file is currently locked; <em>false</em> if not.</td>
</tr>
<tr>
<td>groups</td>
<td>A list of the names of the groups to which the account belongs, if any.</td>
</tr>
<tr>
<td>home_exists</td>
<td>[<em>Linux only</em>] Whether or not the server account's home directory exists or not</td>
</tr>
<tr>
<td>expires</td>
<td>[<em>Windows only</em>] The date on which this account expires; <em>never</em> if the account does not expire.</td>
</tr>
<tr>
<td>password_required</td>
<td>[<em>Windows only</em>] <em>true</em> if the account requires a password; <em>false</em> if not.</td>
</tr>
<tr>
<td>password_changeable</td>
<td>[<em>Windows only</em>] <em>true</em> if the account password can be updated; <em>false</em> if not.</td>
</tr>
<tr>
<td>password_expires</td>
<td>[<em>Windows only</em>] The date on which the account's current password will expire; <em>null</em> if the password never expires.</td>
</tr>
<tr>
<td>password_expired</td>
<td>[<em>Windows only</em>] <em>true</em> if the password has expired; <em>false</em> if not.</td>
</tr>
<tr>
<td>last_password_change</td>
<td>[<em>Windows only</em>] <em>true</em> if the password was last changed (if available).</td>
</tr>
<tr>
<td>minimum_days_between_password_changes</td>
<td>[<em>Linux only</em>] The date before which the account's password may be changed (if available)</td>
</tr>
<tr>
<td>maximum_days_between_password_changes</td>
<td>[<em>Linux only</em>] The date before which the account's password must be changed (if available)</td>
</tr>
<tr>
<td>days_warn_before_password_expiration</td>
<td>[<em>Linux only</em>] How long before password expiration the account is warned about it (if available).</td>
</tr>
<tr>
<td>disabled_after_days_inactive</td>
<td>[<em>Linux only</em>] How many days of inactivity before the account is disabled (if available).</td>
</tr>
<tr>
<td>days_since_disabled</td>
<td>[<em>Linux only</em>] How many days since the account was disabled (if available).</td>
</tr>
<tr>
<td>ssh Authorized_keys</td>
<td>[<em>Linux only</em>] An array of any authorized SSH keys belonging to the account (if available).</td>
</tr>
<tr>
<td>ssh acl</td>
<td>[<em>Linux only</em>] The access control settings for the SSH folder.</td>
</tr>
</tbody>
</table>
*These fields, when used as search filters, support partial match.

### List server accounts

Returns summary information (core fields) for all local user accounts on the server specified by server ID.

**Note:** The results of this call may be paginated. See Pagination of Results for information on how to set up and retrieve paginated results from the Halo API.

**GET** https://api.cloudpassage.com/v1/servers/{server_id}/accounts

**Response**

**Status:** 200

```json
{
    "accounts": [
        {
            "username": "root",
            "url": "https://api.cloudpassage.com/v1/servers/0cd6df5416f811e7b78441efec4abe5d/accounts/root",
            "id": "0",
            "geed": true,
            "admin": true,
            "comment": "root",
            "home": "/root",
            "shell": "/bin/bash",
            "last_login_at": null,
            "active": true,
            "last_login_from": null
        },
        {
            "username": "daemon",
            "url": "https://api.cloudpassage.com/v1/servers/0cd6df5416f811e7b78441efec4abe5d/accounts/daemon",
            "id": "1",
            "geed": false,
            "admin": false,
            "comment": "daemon",
            "home": "/usr/sbin",
            "shell": "/usr/sbin/nologin",
            "last_login_at": null,
            "active": true,
            "last_login_from": null
        },
        ...
        {
            "username": "ubuntu",
            "url": "https://api.cloudpassage.com/v1/servers/0cd6df5416f811e7b78441efec4abe5d/accounts/ubuntu",
            "uid": "1000",
            "gid": "1000",
            "admin": false,
            "comment": "Ubuntu",
            "home": "/home/ubuntu",
            "shell": "/bin/bash",
            "last_login_at": "2017-04-01T16:26:27.000Z",
            "active": true,
            "last_login_from": "73.162.184.135 pts/0"
        }
    ],
    "count": 31
}
```

### Get server account details

102
For the server specified by server ID, returns detailed information (both core account and account details fields) for the server account specified by username.

GET https://api.cloudpassage.com/v1/servers/{server_id}/accounts/{username}

Response

Status: 200

```
{"account": {
    "username": "proxy",
    "url": "https://api.cloudpassage.com/v1/servers/0cd6df5416f811e7b78441efec4abe5d/accounts/proxy",
    "uid": "13",
    "gid": "13",
    "admin": false,
    "comment": "proxy",
    "home": "/bin",
    "shell": "/usr/sbin/nologin",
    "last_login_at": null,
    "active": true,
    "last_login_from": null,
    "groups": "proxy",
    "home_exists": false,
    "last_password_change": "2017-02-21T00:00:00.000Z",
    "minimum_days_between_password_changes": 0,
    "maximum_days_between_password_changes": 99999,
    "days_warn_before_password_expiration": 7,
    "disabled_after_days_inactive": 0,
    "days_since_disabled": 0,
    "ssh_authorized_keys": null,
    "ssh_acl": null,
    "sudo_access": "None"
}}
```

Create a new server account

**Note:** This capability is available for Linux accounts only.

On the server specified by server ID in the call URL, creates a new server account with the initial values specified in the request body. The minimum required fields to supply are username and password requirements. The initial password for the account is returned upon command completion.

Creating a new server account occurs asynchronously. Successful execution results in a response status 202 (Accepted) and returns information about the command in the response body. You may use the Get command details call to poll for completion of the command; see the discussion in the Server Commands API endpoint.

If the create account command completes successfully, the new password is returned in the password field under result in the response body of Get command details. The password will remain valid for 2 hours.

POST https://api.cloudpassage.com/v1/servers/{server_id}/accounts

**Request Body**

```
{"account": {
    "username": "bob",
    "comment": "User Bob",
    "groups": "users",
    "password": {
        "length": 10,
        "include_special": true,
        "include_numbers": true,
        "include_uppercase": false
    }
}}
```
Reset password for a server account

*Note:* This capability is available for Linux accounts only.

In the server account specified by username and on the server specified by server ID in the call URL, this call resets (invalidates) the account's password, sets the password requirements to the values specified in the request body, and returns a new password for the account upon command completion.

Resetting a server account's password occurs asynchronously. Successful execution results in a response status 202 (Accepted) and returns information about the command in the response body. You may use the [Get command details](#) call to poll for completion of the command; see the discussion in the Server Commands API endpoint.

If the password-reset command completes successfully, the new password is returned in the `password` field under `result` in the response body of Get command details. The password will remain valid for 2 hours.

**PUT** https://api.cloudpassage.com/v1/servers/{server_id}/accounts/{username}/password

**Request Body**

```
{
  "password": {
    "length": 10,
    "include_special": true,
    "include_numbers": true,
    "include_uppercase": false
  }
}
```

**Response**

```
{
  "command": {
    "id": "ac49ce6e06448012e21a713ce62c039c",
    "url": "https://api.cloudpassage.com/v1/servers/bd49ce6e06448012e21a713ce62c039c/commands/ac49ce6e06448012e21a713ce62c039c",
    "name": "Create Account",
    "status": "queued",
    "created_at": "2011-10-10T10:10:10Z",
    "updated_at": "2011-10-10T10:10:10Z"
  }
}
```

---

**Response**

```
Location: https://api.cloudpassage.com/v1/servers/bd49ce6e06448012e21a713ce62c039c/commands/ac49ce6e06448012e21a713ce62c039c

Status: 202
```

```
{
}
```
Disable a server account

Note: This capability is available for Linux accounts only.

Disables the account specified by username on the server specified by server ID. The account is marked as disabled and cannot be used, but it is not removed from the server.

Disabling a server account occurs asynchronously. Successful execution results in a response status 202 (Accepted) and returns information about the command in the response body. You may use the Get command details call to poll for completion of the command; see the discussion in the Server Commands API endpoint.

PUT https://api.cloudpassage.com/v1/servers/{server_id}/accounts/{username}

Request Body

```
{  
  "account": {  
    "active": false  
  }
}
```

Response

Status: 202

```
{  
  "command": {  
    "id": "ac49ce6e06448012e21a713ce62c039c",  
    "url": "https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c039c",  
    "name": "Reset Password",  
    "status": "queued",  
    "created_at": "2011-10-10T10:10:10Z",  
    "updated_at": "2011-10-10T10:10:10Z"
  }
}
```

Enable a server account

Note: This capability is available for Linux accounts only.

Enables the account specified by username on the server specified by server ID. Use this call to re-enable a previously disabled account on the server.

Enabling a server account occurs asynchronously. Successful execution results in a response status 202 (Accepted) and returns information about the command in the response body. You may use the Get command details call to poll for completion of the command; see the discussion in the Server Commands API endpoint.
PUT https://api.cloudpassage.com/v1/servers/{server_id}/accounts/{username}

Response

Status: 202

```
{
    "command": {
        "id": "ac49ce6e06448012e21a713ce62c039c",
        "url": "https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c039c",
        "name": "Enable Account",
        "status": "queued",
        "created_at": "2011-10-10T10:10:10Z",
        "updated_at": "2011-10-10T10:10:10Z"
    }
}
```

**Update SSH keys for a server account**

*Note:* This capability is available for Linux accounts only.

Adds the SSH keys specified in the request body to the server account specified by server ID and username in the call URL.

Adding SSH keys to an account is done asynchronously. Successful execution results in a response status 202 (Accepted) and returns information about the command in the response body. You may use the Get command details call to poll for completion of the command; see the discussion in the Server Commands API endpoint.

*Important:* This action completely replaces the existing keys file and all of its keys. If, for example, the existing keys are in the file `authorized_keys2`, that file is deleted and replaced with the file (`authorized_keys` in this example) specified in the request body. If you pass an empty array for the value of "ssh Authorized_keys", all SSH keys are removed from this account on this server.

PUT https://api.cloudpassage.com/v1/servers/{server_id}/accounts/{username}

Request Body

```
{
    "account": {
        "active": true
    }
}
```

If you want to add a comment to a key, you can put it after the end-delimiter in the request. For example:

```
"ssh-dsa AAAAe06448012e21a713e06448012e21a713e06448012e21a713e06448012e21a713== username@host"
```
To completely remove all existing keys, pass a request body like this:

```json
{
    "account": {
        "ssh Authorized_keys": []
    }
}
```

**Response**

**Status:** 202  
**Location:** `https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c039c`

```json
{
    "command": {
        "id": "ac49ce6e06448012e21a713ce62c039c",
        "url": "https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c039c",
        "name": "Update Account SSH Keys",
        "status": "queued",
        "created_at": "2011-10-10T10:10:10Z",
        "updated_at": "2011-10-10T10:10:10Z"
    }
}
```

**Remove a server account**

Removes the account specified by username from the server specified by server ID.

Removing a server account is done asynchronously. Successful execution results in a response status 202 (Accepted) and returns information about the command in the response body. You may use the [Get command details](#) call to poll for completion of the command; see the discussion in the Server Commands API endpoint.

**DELETE** `https://api.cloudpassage.com/v1/servers/{server_id}/accounts/{username}`

**Response**

**Status:** 202  
**Location:** `https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c039c`

```json
{
    "command": {
        "id": "ac49ce6e06448012e21a713ce62c039c",
        "url": "https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c039c",
        "name": "Remove Account",
        "status": "queued",
        "created_at": "2011-10-10T10:10:10Z",
        "updated_at": "2011-10-10T10:10:10Z"
    }
}
```
Server Commands

The Server Commands endpoint allows you to access the details of previously executed commands. You can use this endpoint to monitor the progress of asynchronously executed calls, such as Create server account in the Server Accounts API endpoint and Launch scan of a server in the Server Scans API endpoint. You might employ a calling sequence like the following:

1. Make one of the asynchronous calls in the Server Accounts API endpoint. Retrieve the command ID from the id field in the response body. The initial command status (the value of the status field in the response) is likely to be "queued".

2. Periodically call the Get command details call of this API endpoint, passing the command ID in the call URL. Then examine the status field in the response body. If its value is "completed", the call successfully accomplished its task. If it is still "queued" or if it is "pending" or "started", call Get command details again after some time has elapsed. If it is an error status ("failed"), your call has failed.

For any of the above server account calls, the results of your changes will be visible in the Halo Portal after the next server access scan occurs.

- Object Representation
- Get command details

Object Representation

Server command object location

api.cloudpassage.com/v1

servers

server_id

commands

id

Server command object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique identifier of the server command.</td>
</tr>
<tr>
<td>name</td>
<td>A name of the command.</td>
</tr>
<tr>
<td>status</td>
<td>A status of the command. Possible values queued, pending, completed, failed.</td>
</tr>
<tr>
<td>created_at</td>
<td>A timestamp when command was created.</td>
</tr>
<tr>
<td>updated_at</td>
<td>A timestamp when command was last updated.</td>
</tr>
<tr>
<td>result</td>
<td>A result of the command execution once command is finished.</td>
</tr>
</tbody>
</table>
Get command details

Returns the details of the individual server command specified by command ID and executed on the server specified by server ID.

GET https://api.cloudpassage.com/v1/servers/{server_id}/commands/{id}

Response

Status: 200

```
{
  "command": {
    "id": "ac49ce6e06448012e21a713ce62c039c",
    "url": "https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c039c",
    "name": "Remove Account",
    "status": "completed",
    "created_at": "2011-10-10T10:10:10Z",
    "updated_at": "2011-10-10T10:11:12Z",
    "result": "done"
  }
}
```

If the command returns a password (see Create Server Account and Reset password for server account), the password is returned in a subfield of the result field:

Status: 200

```
{
  "command": {
    "id": "df0715804bce01302a5518fe9446aaba",
    "url": "http://test.host/v1/servers/3f11b34710360a2e354662cd6998428/commands/df0715804bce01302a5518fe9446aaba",
    "name": "Reset Password",
    "status": "completed",
    "created_at": "2013-01-28T23:17:55Z",
    "updated_at": "2013-01-28T23:17:55Z",
    "result": {
      "password": "uhgdf7sdfd$$"
    }
  }
}
```
Server Connections

Use the Server Connections v1 endpoint to view the details of all of the recently established connections (inbound or outbound) to or from a server, plus all of the server’s recently opened listening ports. You can also view all of the unique connections (in, out, and listening) established across all of the servers of a group. You can then use that information to design Halo firewall policies for protecting your servers and groups.

For more information on how Traffic Discovery works and how it can help you to design host firewalls, see the Traffic Discovery User Guide.

- Object Representation
- List a server’s connections
- List a group’s connections

Object Representation

Server connections object location

api.cloudpassage.com/v1

    servers
       id
          connections

Server connections object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent_id</td>
<td>The Halo ID of this server when the connection was detected.</td>
</tr>
<tr>
<td>protocol</td>
<td>The network protocol used by the connection.</td>
</tr>
<tr>
<td>listen</td>
<td>true if the connection is open and listening, regardless of whether an external entity has established a connection through it.</td>
</tr>
<tr>
<td>direction</td>
<td>The direction of the connection request: in or out.</td>
</tr>
<tr>
<td>user</td>
<td>The username running the local process that initiated or received the connection.</td>
</tr>
<tr>
<td>process_name</td>
<td>The name of the local process that initiated or received the connection.</td>
</tr>
<tr>
<td>local_address</td>
<td>The IP address of this server.</td>
</tr>
<tr>
<td>local_port</td>
<td>The port number on this server used for the connection.</td>
</tr>
<tr>
<td>local_location</td>
<td>The geolocation (country code) of the local server's address. RFC 1918 addresses will not include this information.</td>
</tr>
<tr>
<td>remote_address</td>
<td>The IP address of the remote server.</td>
</tr>
<tr>
<td>remote_port</td>
<td>The port number on the remote server used for the connection.</td>
</tr>
<tr>
<td>remote_location</td>
<td>If known, the remote server's geolocation (country code).</td>
</tr>
<tr>
<td>remote_server_id</td>
<td>If known, the Halo ID of the remote server, based on its address. (Must be a Halo-protected server.)</td>
</tr>
</tbody>
</table>
List a server's connections

Returns a list of all recently detected connections on the server whose server ID is specified in the call URL.

Note: The results of this call may be paginated. See Pagination of Results for information on how to set up and retrieve paginated results from the Halo API.

GET https://api.cloudpassage.com/v1/servers/{id}/connections

Response

```
Status: 200
{
  "connections": [
    {
      "agent_id": "728b17f64ce311e5953b11e86205f2df",
      "protocol": "tcp",
      "listen": true,
      "direction": "in",
      "user": "root",
      "process_name": "master",
      "local_address": "127.0.0.1",
      "local_port": 25,
      "local_location": "unknown",
      "remote_address": "unknown",
      "remote_port": "unknown",
      "remote_location": "unknown",
      "remote_server_id": "unknown",
      "remote_fqdn": "unknown",
      "remote_context_type": "unknown",
      "remote_context_id": "unknown",
      "remote_context_name": "unknown",
      "created_at": "2016-09-22T14:51:48.839Z",
      "updated_at": "2016-09-22T14:51:48.839Z",
      "local_group_id": "e4f2a600b67511e58c19053e7ab32284",
      "local_hostname": "ip-10-2-20-204",
      "local_fqdn": "--unknown--"
    },
    {
      "agent_id": "728b17f64ce311e5953b11e86205f2df",
      "protocol": "tcp",
      "listen": "unknown",
      "direction": "out",
      "user": "root",
      "process_name": "cphalow",
      "local_address": "10.2.20.204",
      "local_port": 56622,
      "local_location": "unknown",
      "remote_address": "54.241.18.169",
      "remote_port": 13128,
      "remote_location": "usa",
      "remote_server_id": "ae64715a4ce311e5953b11e86205f2df",
      "remote_fqdn": "--unknown--"
    }
  ]
}```
You can restrict the results by applying any of the object fields as filters, and you can also group the results into bundles with distinct values of several fields. For example, to retrieve only outbound connections in which the user is root, construct the method call like this:

GET https://api.cloudpassage.com:10443/v1/servers/212ac5aecea311e58021271e7dd7e385/connections?direction=out&user=root

Response

Status: 200

"connections": [
  {
    "agent_id": "728b17f64ce311e5953b11e86205f2df",
    "protocol": "tcp",
    "listen": "unknown",
    "direction": "out",
    "user": "root",
    "process_name": "cphalow",
    "local_address": "10.2.20.204",
    "local_port": 56622,
    "local_location": "unknown",
    "remote_address": "54.241.18.169",
    "remote_port": 13128,
    "remote_location": "usa",
    "remote_server_id": "ae64f71sa4ce311e5953b11e86205f2df",
    "remote_fqdn": "unknown",
    "remote_context_type": "group",
    "remote_context_id": "60bde96e89dc11e5b482655825511ab5",
    "remote_context_name": "eric-test2333333333333",
    "created_at": "2016-08-30T12:51:49.205Z",
    "updated_at": "2016-08-30T12:51:49.205Z",
    "local_group_id": "e4f2a600b67511e58c19053e7ab32284",
    "local_hostname": "ip-10-2-20-204",
    "local_fqdn": "--unknown--"
  },
  {
    "agent_id": "728b17f64ce311e5953b11e86205f2df",
    "protocol": "tcp",
    "listen": "unknown",
    "direction": "in",
    "user": "sshd",
    "process_name": "sshd",
    "local_address": "10.2.20.204",
    "local_port": 22,
    "local_location": "unknown",
    "remote_address": "222.186.34.83",
    "remote_port": 3680,
    "remote_location": "chn",
    "remote_server_id": "unknown",
    "remote_fqdn": "unknown",
    "remote_context_type": "unknown",
    "remote_context_id": "unknown",
    "remote_context_name": "unknown",
    "created_at": "2016-08-30T12:51:49.205Z",
    "updated_at": "2016-08-30T12:51:49.205Z",
    "local_group_id": "e4f2a600b67511e58c19053e7ab32284",
    "local_hostname": "ip-10-2-20-204",
    "local_fqdn": "--unknown--"
  }
],

"count": 80
List a group's connections

Returns a list of all recently detected inbound and outbound connections on the servers of the group specified by ID in the call URL.

GET https://api.cloudpassage.com/v1/groups/{group_id}/connections/

Response

Status: 200

{  "connections": [  {   "agent_id": "ddb649f4d5ac11e594662388268169a7",   "protocol": "tcp",   "listen": "unknown",   "direction": "in",   "user": "unknown",   "process_name": "svchost.exe",   "local_address": "172.31.24.114",   "local_port": 3389,   "local_location": "unknown",   "remote_address": "182.71.211.169",   "remote_port": 51615,   "remote_location": "ind",   "remote_server_id": "unknown",   "remote_fqdn": "unknown",   "remote_context_type": "unknown",   "remote_context_id": "unknown",   "remote_context_name": "unknown",   "created_at": "2016-09-23T17:15:24.059Z",   "updated_at": "2016-09-23T17:15:24.059Z",   "local_group_id": "57e9a244d5ac11e5ab1551c1f46706b3",   "local_hostname": "ip-AC1F1872",   "local_fqdn": "ip-AC1F1872"  }  ]  ]

"count": 2
Several call URL parameters are available to refine this method call:

- Use the `group_by` parameter to specify the object fields that should appear in the results. These are the fields that uniquely define the resource. For example, to list distinct operating systems, group by `os_name` (or `distribution_name`) and `os_version`.
- Optionally use any of the other filter operators defined for the List servers method in the Servers API endpoint.
- Optionally use the pagination parameters to define page size and the page number of the results to be returned. See Pagination of Results for details.

**Inbound connections:**
GET https://api.cloudpassage.com/v1/groups/{group_id}/connections?&direction=in&
group_by=local_port,protocol,user,process_name,remote_location,remote_address,remote_fqdn

**Outbound connections:**
GET https://api.cloudpassage.com/v1/groups/{group_id}/connections?direction=out&
group_by=remote_location,remote_address,remote_fqdn,remote_port,protocol,user,process_name

**Listening ports:**
GET https://api.cloudpassage.com/v1/groups/{group_id}/connections?listen=true&
group_by=local_port,protocol,user,process_name

(See above for additional parameters you can add to the call URL.)

Specify `direction=in` or `out` to retrieve inbound or outbound connections, respectively; specify `listen=true` to retrieve listening ports. The response JSON includes values for each of the fields that define the type of connection you are retrieving.

**Note:** Making calls similar to the above can directly help you to approximate firewall policies for a group:

- Use `direction=in&group_by=local_port` to determine all ports that are receiving connections. That will tell you which ports you might need to have open in that group's firewall policy.
- Then get more specific by adding `group_by=remote_address` to learn which remote addresses are connecting to which ports.

**Example call**
GET https://api.cloudpassage.com/v1/groups/0962bfa087bc01323e360670140ec224/connections?group_by=direction,local_port

**Response**

```
Status: 200
{
```
In the results, the inbound connections are listed first, outbound afterward. The only information returned for each grouping is its port number and a count of how many connections passed through that port.
Server Processes

Use the Server Processes endpoint to retrieve information about each running process on a specified Linux or Windows server.

*Note:* Halo gathers the process information by automatically scanning all active servers every hour.

Historical scan data is not saved; only the most recent scan results are available

- Object Representation
- List server processes

Object Representation

Server process object location

```
api.cloudpassage.com/v1

servers

server_id

processes

process_name
```

Server process object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process_name</td>
<td>The name of the process.</td>
</tr>
<tr>
<td>pid</td>
<td>The process ID of the process.</td>
</tr>
<tr>
<td>ppid</td>
<td>The process ID of the process's parent process.</td>
</tr>
<tr>
<td>user</td>
<td>The username of the account that launched the process.</td>
</tr>
<tr>
<td>state</td>
<td>The state of the process. Supported values include:</td>
</tr>
<tr>
<td></td>
<td><em>(Windows)</em> Running, Not Responding, or Unknown</td>
</tr>
<tr>
<td></td>
<td><em>(Linux)</em> R = running or runnable (on run queue) D = uninterruptible sleep (usually I/O) S = interruptible sleep (waiting for an event to complete) Z = defunct/zombie, terminated but not reaped by its parent T = stopped by a job control signal or because it is being traced W = paging X = dead</td>
</tr>
<tr>
<td>command</td>
<td>The full path of the command that launched the process.</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>memory_usage</td>
<td>Current memory usage of the process (in bytes)</td>
</tr>
<tr>
<td>cpu_usage</td>
<td>Windows only: Current CPU usage of the process (in cumulative processor time)</td>
</tr>
<tr>
<td>cpu_percent</td>
<td>Linux only: Current CPU usage of the process (in percentage of total CPU capacity)</td>
</tr>
<tr>
<td>memory_percent</td>
<td>Linux only: Current memory usage of the process (in percentage of total RAM)</td>
</tr>
</tbody>
</table>

**List server processes**

Returns summary information for all running processes on the server specified by server ID. In the response JSON, the list of processes is sorted alphabetically by process name.

*Note:* The results of this call may be paginated. See Pagination of Results for information on how to set up and retrieve paginated results from the Halo API.

**GET** https://api.cloudpassage.com/v1/servers/{server_id}/processes

**Response (Linux)**

**Status: 200**

```json
{
  "processes": [
    {
      "process_name": "bash",
      "pid": "1",
      "ppid": "0",
      "user": "root",
      "state": "S",
      "command": "/bin/bash /start.sh",
      "memory_usage": "11352",
      "cpu_percent": "0.0",
      "memory_percent": "0.0"
    },
    {
      "process_name": "cphalo",
      "pid": "24",
      "ppid": "1",
      "user": "root",
      "state": "S",
      "command": "/opt/cloudpassage/bin/cphal",
      "memory_usage": "27136",
      "cpu_percent": "0.0",
      "memory_percent": "0.0"
    },
    {
      "process_name": "cphalow",
      "pid": "26",
      "ppid": "24",
      "user": "root",
      "state": "S",
      "command": "/opt/cloudpassage/bin/cphal",
      "memory_usage": "928940",
      "cpu_percent": "0.0",
      "memory_percent": "0.3"
    },
    {
      "process_name": "ps",
      "pid": "1334",
      "ppid": "26",
      "user": "root",
      "state": "R",
      "command": "/bin/ps -eo pid,ppid,user,s",
      "memory_usage": "13372",
      "cpu_percent": "0.0",
      "memory_percent": "0.0"
    },
    {
      "process_name": "tail",
      "pid": "32",
    }
  ]
}
```
Response (Windows)

Status: 200

```json
{
    "processes": [
        {
            "process_name": "conhost.exe",
            "pid": "2516",
            "ppid": "",
            "user": "NT AUTHORITY\SYSTEM",
            "state": "Unknown",
            "command": "",
            "memory_usage": "2,704",
            "cpu_usage": "0:00:00"
        },
        {
            "process_name": "cphalow.exe",
            "pid": "1184",
            "ppid": "484",
            "user": "NT AUTHORITY\SYSTEM",
            "state": "Unknown",
            "command": "C:\Program Files\CloudPassage\bin\cphalow.exe",
            "memory_usage": "12,568",
            "cpu_usage": "0:02:32"
        },
        {
            "process_name": "csrss.exe",
            "pid": "344",
            "ppid": "336",
            "user": "NT AUTHORITY\SYSTEM",
            "state": "Running",
            "command": "%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winrv:UserServerDllInitialization,3 ServerDll=winrv:ConServerDllInitialization,2 ServerDll=swssrv,4 ProfileControl=Off MaxRequestThreads=16",
            "memory_usage": "4,100",
            "cpu_usage": "0:00:29"
        },
        ...
    ]
}
```
Server Scans

Use the Server Scans API endpoint to launch a configuration scan, file integrity scan, vulnerability scan, server access scan, or agent self-verification test on a specified server. Use it also to view the results of the most recent configuration, file integrity, vulnerability, or self-verification scan on the server.

- Object Representation
- Launch a scan of a server
- List server configuration scan results
- List server file integrity scan results
- List server vulnerability scan results
- List server access scan results

Object Representation

Server scan object location

```
api.cloudpassage.com/v1/servers/server_id/module or scans*
```

*Use the "scans" URL endpoint to launch a scan; use the module endpoint to retrieve scan results.

Server scan object fields

The server scan object represents the most recent scan of a given type (configuration, file integrity, vulnerability, or server access) on the specified server. The server scan results object contains information about the scan as a whole. The findings objects contain information about the scan results (configuration issues, file integrity issues, or CVE entries).

Scan fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique identifier for the server.</td>
</tr>
</tbody>
</table>
| module  | The type of scan to execute or get results for:  
  - csm = configuration scan  
  - svm = vulnerability scan  
  - sam = server access scan (for launching a scan)  
  - accounts = server access scan (for retrieving scan results)  
  - fim = file integrity scan  
  - sv = agent self-verification test |
Note: Scan results are not available for an agent self-verification test. There is no available method on this endpoint for returning self-verification test results.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique identifier for the server.</td>
</tr>
<tr>
<td>hostname</td>
<td>Server host name.</td>
</tr>
<tr>
<td>server_label</td>
<td>Optional. A label that identifies the server.</td>
</tr>
<tr>
<td>connecting_ip_address</td>
<td>Server IP address.</td>
</tr>
<tr>
<td>state</td>
<td>Halo agent state: active, deactivated, or missing.</td>
</tr>
<tr>
<td>scan</td>
<td>Information for the scan. Includes the following sub-fields:</td>
</tr>
<tr>
<td>id</td>
<td>A unique identifier for the scan.</td>
</tr>
<tr>
<td>url</td>
<td>The URL to the scan object. Note that the object is accessed through the Scan History API endpoint.</td>
</tr>
<tr>
<td>module</td>
<td>The type of scan: csm, svm, sam, or fim.</td>
</tr>
<tr>
<td>status</td>
<td>Overall scan status: <em>completed_clean</em>: The scan was successful, and (for a configuration scan) no rule checks failed.</td>
</tr>
<tr>
<td></td>
<td><em>completed_with_errors</em>: The scan was successful, some rule checks failed. (Applies to configuration scans only.)</td>
</tr>
<tr>
<td></td>
<td><em>failed</em>: The scan was not successful.</td>
</tr>
<tr>
<td>created_at</td>
<td>When the scan started.</td>
</tr>
<tr>
<td>completed_at</td>
<td>When the scan ended.</td>
</tr>
<tr>
<td>server_id</td>
<td>Halo server ID for the server.</td>
</tr>
<tr>
<td>server_hostname</td>
<td>Server host name.</td>
</tr>
<tr>
<td>server_url</td>
<td>API URL to the server object.</td>
</tr>
<tr>
<td>critical_findings_count</td>
<td>The number of scan results considered to be critical issues.</td>
</tr>
<tr>
<td>non_critical_findings_count</td>
<td>The number of scan results considered to be non-critical issues.</td>
</tr>
<tr>
<td>ok_findings_count</td>
<td>The number of scan results considered to be non-issues.</td>
</tr>
<tr>
<td>indeterminate_findings_count</td>
<td>The number of scan results considered to be indeterminate.</td>
</tr>
<tr>
<td>requested_by</td>
<td>For a manual scan, the Halo user who requested it.</td>
</tr>
<tr>
<td>findings</td>
<td>A list of results for each item examined. See tables below.</td>
</tr>
</tbody>
</table>

Configuration scan findings fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>critical</td>
<td>true if failure of this rule is a critical issue; otherwise false.</td>
</tr>
<tr>
<td>status</td>
<td>the result for this rule: good ( = passed), indeterminate, or bad ( = failed).</td>
</tr>
<tr>
<td>rule_operator</td>
<td>AND if all checks must pass for the rule to pass; OR if the rule passes if at least one check passes.</td>
</tr>
<tr>
<td>details</td>
<td>A list of results for each configuration check in this rule. Includes the following sub-fields:</td>
</tr>
<tr>
<td>type</td>
<td>The rule check that was applied.</td>
</tr>
<tr>
<td>status</td>
<td>the result for this check: good ( = passed), indeterminate, or bad ( = failed).</td>
</tr>
<tr>
<td>check_id</td>
<td>The Halo ID assigned to this check.</td>
</tr>
<tr>
<td>target</td>
<td>The item examined by this check.</td>
</tr>
</tbody>
</table>
expected | The target value expected by this check.
---|---
actual | The target value detected by this check.
scan_status | Scan-completion status: ok if the target was found; not_found if it was not.
config_key | The key (called "configuration-file item" in the Halo portal UI) of a key-value pair in the configuration file.
config_key_value_delimiter | The character that separates the key from its value in key-value pairs. Default = space.

File integrity scan findings summary fields

For a file integrity scan, the server scan object includes only summary information for the findings. Complete information is contained in the file integrity scan findings object, accessed by calling the Get file integrity scan findings details method of the Scan History API endpoint.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
id | A unique identifier for the file integrity scan findings details object. |
url | The API URL to the file integrity scan findings object. |
rule | A description of this file integrity rule (target). Includes the following sub-fields: |
critical | true if failure of this rule is a critical issue; otherwise false. |
recurse | true if this directory target should be scanned recursively; otherwise false. |
target | The file path to the object to be examined by this check. |
alert | true if failure of this rule generates an alert; otherwise false. |
log | true if failure of this rule should be logged as an event; otherwise false. |
status | Scan-completion status: good if no objects in this target changed; otherwise bad. |
counts | Counts of results for all objects checked by this rule. Includes the following sub-fields: |
ok | This many objects were unchanged. |
missing | This many objects were removed. |
added | This many new objects were added. |
changed | This many objects had changes to their content or metadata. |
reference_identifiers | A comma-separated list of IDs used to mark this rule for compliance purposes. Each identifier is a name-value pair with this JSON format: {"name":"value"} — for example, {"USB":"67"},{"CIS":"1.1.2"}

Vulnerability scan findings fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
package_name | The name of the software package examined. |
package_version | The version number of the software package. |
critical | true if detection of a vulnerability in this package is considered to be a critical issue; otherwise false. |
status | bad if this package contains one or more vulnerabilities; otherwise good. |
cve_entries | A list of the CVE's present in this package. Includes the following sub-fields: |
cve_entry | The ID of this CVE. |
cvss_score | The NIST-assigned numerical severity score for this CVE. |
suppressed | true if reporting of this CVE has been suppressed; otherwise false. |
vendor | (Windows only) The name of the vendor of this package. |
install_date | (Windows only) The date on which this package was installed on this server. |
cpe | (Windows only) The Common Platform Enumeration (CPE) designation for this package (program and version). |
Server access scan findings fields *(accounts object)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>The name of the software package examined.</td>
</tr>
<tr>
<td>url</td>
<td>The version number of the software package.</td>
</tr>
<tr>
<td>uid</td>
<td><code>true</code> if detection of a vulnerability in this package is considered to be a critical issue; otherwise <code>false</code>.</td>
</tr>
<tr>
<td>gid</td>
<td><code>bad</code> if this package contains one or more vulnerabilities; otherwise <code>good</code>.</td>
</tr>
<tr>
<td>comment</td>
<td>A list of the CVE's present in this package. Includes the following sub-fields:</td>
</tr>
<tr>
<td>home</td>
<td>The ID of this CVE.</td>
</tr>
<tr>
<td>shell</td>
<td>The NIST-assigned numerical severity score for this CVE.</td>
</tr>
<tr>
<td>last_login_at</td>
<td><code>true</code> if reporting of this CVE has been suppressed; otherwise <code>false</code>.</td>
</tr>
<tr>
<td>last_login_from</td>
<td>(Windows only) The name of the vendor of this package.</td>
</tr>
<tr>
<td>active</td>
<td>(Windows only) The date on which this package was installed on this server.</td>
</tr>
</tbody>
</table>

Launch a scan of a server

Launches a one-time scan of the server specified by ID in the call URL. The server must have a valid policy for the requested scan type *(module)* or the request will be ignored. If *module* is not provided or if it is of an unknown type, an error is returned.

These are the supported values and meanings for *module*:

- **csm.** A configuration scan.
- **svm.** A vulnerability scan.
- **sam.** A server access scan.
- **fim.** A file integrity scan.
- **sv.** An agent self-verification test.

Scanning occurs asynchronously. Successful execution of this call results in a response status 202 (Accepted) and returns information about the scan command in the response body. You may use the *Get command details* call to poll for completion of the scan; see the discussion in the Server Commands API endpoint.

POST https://api.cloudpassage.com/v1/servers/{server_id}/scans

Request Body

```
{
    "scan": {
        "module": "sam"
    }
}
```

Response

Status: 202
Location: https://api.cloudpassage.com/v1/servers/5ad1f4534b49ee59335d150cebec4099/commands/154e98905860013022d83c0754715774

```json
{
}
```
List server configuration scan results

For the server specified in the call URL, returns all results (policy-rule passes, indeterminates, and failures) reported from the most recent configuration scan on that server.

In the results, failures are listed first, followed by indeterminate results, followed by passes.

GET https://api.cloudpassage.com/v1/servers/{server_id}/sca

Response

Status: 200

```json
{
    "id": "c827779463036a0b90faf16283927dc2",
    "hostname": "AMAZONA-CN1DVU6",
    "connecting_ip_address": "107.21.199.187",
    "state": "active",
    "scan": {
        "module": "csm",
        "status": "completed_with_errors",
        "created_at": "2013-07-25T20:57:29Z",
        "completed_at": "2013-07-25T20:57:30Z",
        "server_id": "c827779463036a0b90faf16283927dc2",
        "server_hostname": "AMAZONA-CN1DVU6",
        "server_url": "https://api.cloudpassage.com/v1/servers/c827779463036a0b90faf16283927dc2",
        "critical_findings_count": 0,
        "non_critical_findings_count": 1,
        "ok_findings_count": 12,
        "indeterminate_findings_count": null,
        "findings": [
            {
                "critical": true,
                "status": "indeterminate",
                "rule_operator": "AND",
                "details": [
                    {
                        "type": "windows_service_started",
                        "status": "indeterminate",
                        "check_id": 11223,
                        "target": "workstation",
                        "expected": true,
                        "actual": false,
                        "scan_status": "not_found"
                    },
                    {
                        "type": "windows_service_started",
                        "status": "indeterminate",
                        "target": "server",
                        "expected": true,
                        "actual": false,
                        "scan_status": "not_found"
                    },
                    {
                        "type": "windows_service_started",
                        "status": "indeterminate",
                        "target": "iis",
                        "expected": true,
                        "actual": false,
                        "scan_status": "not_found"
                    },
                    {
                        "type": "windows_service_started",
                        "status": "indeterminate",
                        "target": "iis",
                        "expected": true,
                        "actual": false,
                        "scan_status": "not_found"
                    }
                ]
            }
        ]
    }
}
```
List server file integrity scan results

For the server specified in the call URL, returns summaries of all results (target content changes, ownership/permissions changes, additions, and deletions) reported from the most recent file integrity scan on that server.

In the results, failures are listed first, followed by indeterminate results, followed by passes.

Note: For complete details of all scan results, call the Get file integrity scan findings details method of the Scan History API endpoint.

GET https://api.cloudpassage.com/v1/servers/{server_id}/fim

Response

Status: 200

```json
{
  "id": "28389050a6f2013193473c764e101158",
  "hostname": "ip-10-170-202-36",
  "server_label": "chrisj-appserv-16",
  "connecting_ip_address": "184.169.248.7",
  "state": "active",
  "scan": {
    "id": "b73713b0c28301319a393c764e101158",
    "url": "https://api.cloudpassage.com/v1/scans/b73713b0c28301319a393c764e101158",
    "module": "fim",
    "status": "completed_clean",
    "created_at": "2014-05-20T19:34:42Z",
    "completed_at": "2014-05-20T19:36:29Z",
    "server_id": "28389050a6f2013193473c764e101158",
    "server_hostname": "ip-10-170-202-36",
    "server_url": "https://api.cloudpassage.com/v1/servers/28389050a6f2013193473c764e101158",
    "critical_findings_count": 23,
    "non_critical_findings_count": 566,
    "ok_findings_count": null,
    "requested_by": "chrisj-halo-2",
    "findings": [
      {
        "id": "05f48316-e056-11e3-834d-01b01b432ddc",
        "url": "https://api.cloudpassage.com/v1/scans/b73713b0c28301319a393c764e101158/findings/05f48316-e056-11e3-834d-01b01b432ddc",
        "rule": {
          "critical": false,
          "recursive": true,
          "target": "/home/ec2",
          "alert": true,
          "log": true
        },
        "status": "bad",
        "counts": {
          "ok": 709,
          "missing": 66,
          "added": 6,
          "changed": 17
        },
        "reference_identifiers": []
      }
    ]
}
List server vulnerability scan results

For the server specified in the call URL, returns all results (vulnerable software packages and non-vulnerable packages) detected by the most recent vulnerability scan on that server. For each vulnerable package, all of its known vulnerabilities (CVE's) are listed as well.

In the results, vulnerable packages are listed first, followed by non-vulnerable packages.

GET https://api.cloudpassage.com/v1/servers/{server_id}/svm

Response

Status: 200

```json
{
  "id": "63a61dda4d369b3da0761638652ac29",
  "hostname": "ip-10-197-5-10",
  "connecting_ip_address": "54.215.114.114",
  "state": "active",
  "scan": {
    "module": "svm",
    "status": "completed_clean",
    "created_at": "2013-07-28T16:35:46Z",
    "completed_at": "2013-07-28T16:35:49Z",
    "server_id": "63a61dda4d369b3da0761638652ac29",
    "server_hostname": "ip-10-197-5-10",
    "server_url": "https://api.cloudpassage.com/v1/servers/63a61dda4d369b3da0761638652ac29",
    "critical_findings_count": 2,
    "non_critical_findings_count": 5,
    "findings": [
      {
        "package_name": "curl.x86_64",
        "package_version": "7.27.0-10.fc18",
        "critical": true,
        "status": "bad",
        "cve_entries": [
          {
            "cve_entry": "CVE-2013-0249",
            "cvss_score": 7.3,
            "suppressed": false
          },
          {
            "cve_entry": "CVE-2013-1944",
            "cvss_score": 5.5,
            "suppressed": false
          }
        ]
      },
      {
        "package_name": "libcurl.x86_64",
        "package_version": "7.27.0-10.fc18",
        "critical": true,
        "status": "bad",
        "cve_entries": [
          {
            "cve_entry": "CVE-2013-0249",
            "cvss_score": 5.1,
            "suppressed": false
          }
        ]
      }
    ]
  }
}...
List server access scan results

For the server specified in the call URL, returns a list of the local user accounts found by the most recent access scan on that server. For each account, results include the account's name, IDs, important attributes, recent login history, and status (active or deactivated).

Note: For this call, the module designator is not, as might be expected, sam; it is accounts.

GET https://api.cloudpassage.com/v1/servers/{server_id}/accounts

Response

Status: 200

{    "accounts": [        {            "username": "root",            "url": "https://api.cloudpassage.com/v1/servers/8088416e097511e5988067ded7bb0e03/accounts/root",            "uid": "0",            "gid": "0",            "comment": "root",            "home": "/root",            "shell": "/bin/bash",            "last_login_at": null,            "last_login_from": null,            "active": true        },        {            "username": "bin",            "url": "https://api.cloudpassage.com/v1/servers/8088416e097511e5988067ded7bb0e03/accounts/bin",            "uid": "587023",            "gid": "1",            "comment": "root",            "home": "/root",            "shell": "/bin/bash",            "last_login_at": null,            "last_login_from": null,            "active": true        },        {            "username": "daemon",            "url": "https://api.cloudpassage.com/v1/servers/8088416e097511e5988067ded7bb0e03/accounts/daemon",            "uid": "2",            "gid": "2",            "comment": "daemon",            "home": "/sbin",            "shell": "/sbin/nologin",            "last_login_at": null,            "last_login_from": null,            "active": true        },        {            "username": "adm",            "url": "https://api.cloudpassage.com/v1/servers/8088416e097511e5988067ded7bb0e03/accounts/adm",            "uid": "1",            "gid": "1",            "comment": "adm",            "home": "/sbin",            "shell": "/sbin/nologin",            "last_login_at": null,            "last_login_from": null,            "active": true        }    ]}
"url": "https://api.cloudpassage.com/v1/servers/8088416e097511e5988067ded7bb0e03/accounts/adm",
"uid": "3",
"gid": "4",
"comment": "adm",
"home": "/var/adm",
"shell": "/sbin/nologin",
"last_login_at": null,
"last_login_from": null,
"active": true

...,
{
"username": "myaccount",
"url": "https://api.cloudpassage.com/v1/servers/8088416e097511e5988067ded7bb0e03/accounts/myaccount",
"uid": "938475",
"gid": "59914",
"comment": "",
"home": "/log",
"shell": "/bin/bash",
"last_login_at": null,
"last_login_from": null,
"active": true
}
{
"username": "pw_gen_opts_fix5",
"url": "https://api.cloudpassage.com/v1/servers/8088416e097511e5988067ded7bb0e03/accounts/pw_gen_opts_fix5",
"uid": "482360",
"gid": "59920",
"comment": "",
"home": "/home/pw_gen_opts_fix5",
"shell": "/bin/bash",
"last_login_at": null,
"last_login_from": null,
"active": true
}
"count": 81
}
Server Local Firewall

Use the Server Local Firewall Logs endpoint to retrieve information about the firewall installed locally on a specified Linux or Windows server. The firewall need not be a Halo firewall.

- **Object Representation**
- **Get local firewall**

**Object Representation**

Firewall object location

```plaintext
api.cloudpassage.com/v1
  - servers
    - server_id
      - firewall
```

Local Firewall object fields

The `firewall` object for a server includes the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>managed_by_halo</td>
<td><code>true</code> if it is a successfully installed Halo firewall, <code>false</code> if not. Note that there may be a time lag of several minutes between assigning a new Halo firewall policy to a server's group, and seeing the <code>true</code> value displayed in this field.</td>
</tr>
<tr>
<td>first_collected_at</td>
<td>The date-time (in ISO 8601 format) at which this firewall policy was first detected.</td>
</tr>
<tr>
<td>last_seen_at</td>
<td>The date-time (in ISO 8601 format) at which the firewall policy was last detected on this server.</td>
</tr>
<tr>
<td>installed_policy</td>
<td>The text of the firewall policy (unformatted). Note that the presence of firewall rules in this field plus a value of <code>true</code> in the <code>managed_by_halo</code> field indicate that the policy is active; if no rules appear, the policy is either missing or not active.</td>
</tr>
</tbody>
</table>

**Get local firewall**

Returns the content and selected metadata for the local firewall policy installed on the server specified in the call URL, regardless of whether it is a Halo firewall policy or some other kind of firewall policy.

**GET** https://api.cloudpassage.com/v1/servers/{id}/firewall

**Response**

**Status: 200**
Note: Pasting the raw JSON of the **installed_policy** field into a text file allows you to view it as minimally formatted text:

```
\r\nDomain Profile Settings: \r\n---------------------------------------------------
\r\nState ON\r\nFirewall Policy AllowInbound, AllowOutbound\r\nLocalFirewallRules N/A (GPO-store only)\r\nLocalConSecRules N/A (GPO-store only)\r\nInboundUserNotification Disable\r\nRemoteManagement Not Configured\r\nUnicastResponseToMulticast Enable\r\n\r\nLogging:\r\nLogAllowedConnections Disable\r\nLogDroppedConnections Disable\r\nFileName C:\\Windows\\system32\\LogFiles\\Firewall\\pfirewall.log\r\nMaxFileSize 4096\r\n\r\nPrivate Profile Settings: \r\n---------------------------------------------------
\r\nState ON\r\nFirewall Policy AllowInbound, AllowOutbound\r\nLocalFirewallRules N/A (GPO-store only)\r\nLocalConSecRules N/A (GPO-store only)\r\nInboundUserNotification Disable\r\nRemoteManagement Not Configured\r\nUnicastResponseToMulticast Enable\r\n\r\nLogging:\r\nLogAllowedConnections Disable\r\nLogDroppedConnections Disable\r\nFileName C:\\Windows\\system32\\LogFiles\\Firewall\\pfirewall.log\r\nMaxFileSize 4096\r\n\r\nPublic Profile Settings: \r\n----------------------------------------------------------------------
\r\nState ON\r\nFirewall Policy AllowInbound, AllowOutbound\r\nLocalFirewallRules N/A (GPO-store only)\r\nLocalConSecRules N/A (GPO-store only)\r\nInboundUserNotification Disable\r\nRemoteManagement Not Configured\r\nUnicastResponseToMulticast Enable\r\n\r\nLogging:\r\nLogAllowedConnections Disable\r\nLogDroppedConnections Disable\r\nFileName C:\\Windows\\system32\\LogFiles\\Firewall\\pfirewall.log\r\nMaxFileSize 4096\r\n```

...
Server Firewall Logs

Use the Server Firewall Logs endpoint to retrieve information about firewall updates on a specified Linux or Windows server. Firewall creation, deletion, and updates made to a server's local iptables or Windows firewall are logged. Firewall policy changes made within Halo are not logged.

*Note:* Each server's firewall logs maintain a record of all changes since the server's initial startup.

- Object Representation
- Get firewall logs

Object Representation

Firewall logs object location

```
api.cloudpassage.com/v1
   ---
   servers
   ---
    server_id
    ---
    agent_firewall_logs
```

Firewall log object fields

The `agent_firewall_logs` object is an array of individual log entries. Each entry includes the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent_id</td>
<td>The Halo ID of the Halo agent installed on the server.</td>
</tr>
<tr>
<td>change_detected_at</td>
<td>The date-time (in ISO 8601 format) at which a change to the server's firewall was detected.</td>
</tr>
<tr>
<td>last_installed_at</td>
<td>The date-time (in ISO 8601 format) at which the server's firewall policy was installed.</td>
</tr>
<tr>
<td>raw_policy_installed</td>
<td>The content (in text format) of the server's current firewall policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In the response JSON for Linux, you can format this policy for improved readability by inserting returns/newlines where indicated by &quot;\n&quot;. The examples shown below have been reformatted in that manner.</td>
</tr>
<tr>
<td>raw_policy_monitored</td>
<td>The content (in text format) of the server's expected firewall policy, based on the most recent policy installation or update received from the Halo analytics engine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In the response JSON for Linux, you can format this policy for improved readability by inserting returns/newlines where indicated by &quot;\n&quot;. The Linux examples shown below have been reformatted in that manner.</td>
</tr>
</tbody>
</table>
Get firewall logs

Returns all firewall-change entries logged for the server specified by ID in the call URL. The entries report firewall installations and deletions, plus updates detected as departures from the server's current Halo firewall policy. The returned logs information covers the server's entire history of firewall changes from initial startup until the time the method is called.

*Note:* The results of this call may be paginated. See [Pagination of Results](#) for information on how to set up and retrieve paginated results from the Halo API.

GET https://api.cloudpassage.com/v1/servers/{server_id}/firewall_logs

(Note that the call URL ends with "firewall_logs", even though the firewall logs object is named "agent_firewall_logs").

Response (Linux)

**Status:** 200

```
{
    "agent_firewall_logs": [
    {
        "agent_id": "aaa6979cb40211e5b4891leda6605b06",
        "change_detected_at": "2016-01-05T23:34:52.647+00:00",
        "last_installed_at": "2016-01-05T23:18:54.289+00:00",
        "raw_policy_installed": "Chain INPUT (policy ACCEPT)
        target     prot opt source               destination
        ACCEPT     tcp -- 174.36.18.228        0.0.0.0/0           tcp spt:443 state RELATED,ESTABLISHED
        ACCEPT     tcp -- 174.36.20.154        0.0.0.0/0           tcp spt:443 state RELATED,ESTABLISHED
        ...
```

Response (Linux) — after server start, with no Halo firewall policy installed:

```
{
    "agent_id": "ee61e39ca8f411e5a56547a7263f0c91",
    "change_detected_at": null,
    "last_installed_at": null,
    "raw_policy_installed": null,
    "raw_policy_monitored": null
}
```

Response (Linux) — after initial installation of a Halo firewall policy:

```
{
    "agent_id": "aaa6979cb40211e5b4891leda6605b06",
    "change_detected_at": null,
    "last_installed_at": "2016-01-05T23:18:54.289+00:00",
    "raw_policy_installed": "Chain INPUT (policy ACCEPT)
    target     prot opt source               destination
    ACCEPT     tcp -- 174.36.18.228        0.0.0.0/0           tcp spt:443 state RELATED,ESTABLISHED
    ACCEPT     tcp -- 174.36.20.154        0.0.0.0/0           tcp spt:443 state RELATED,ESTABLISHED
    ACCEPT     udp -- 0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED udp spt:53
    ACCEPT     tcp -- 0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED tcp spt:53
    ACCEPT     all -- 0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    LOG        all -- 172.17.0.89          0.0.0.0/0           state NEW,RELATED,ESTABLISHED LOG flags 0
    level 4
    LOG        all -- 172.17.0.90          0.0.0.0/0
    LOG        all -- 172.17.0.91          0.0.0.0/0
    LOG        all -- 172.17.0.92          0.0.0.0/0
    LOG        all -- 172.17.0.94          0.0.0.0/0
    LOG        all -- 172.17.0.95          0.0.0.0/0
    LOG        all -- 172.17.0.96          0.0.0.0/0
    LOG        all -- 172.17.0.97          0.0.0.0/0
    LOG        all -- 52.8.189.5           0.0.0.0/0           state NEW,RELATED,ESTABLISHED
    ACCEPT     all -- 172.17.0.89          0.0.0.0/0
    ACCEPT     all -- 172.17.0.90          0.0.0.0/0
    ACCEPT     all -- 172.17.0.91          0.0.0.0/0
    ACCEPT     all -- 172.17.0.92          0.0.0.0/0
    ACCEPT     all -- 172.17.0.93          0.0.0.0/0
    ACCEPT     all -- 172.17.0.94          0.0.0.0/0
```

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>172.17.0.95</td>
<td>0.0.0.0/0</td>
<td>state NEW,RELATED,ESTABLISHED</td>
</tr>
<tr>
<td>TCP</td>
<td>52.8.189.5</td>
<td>0.0.0.0/0</td>
<td>state NEW,RELATED,ESTABLISHED</td>
</tr>
</tbody>
</table>

**Chain FORWARD (policy ACCEPT)**

- **target**: default (policy ACCEPT)
- **protocol**: all
- **options**: state NEW,RELATED,ESTABLISHED

**reject-with icmp-port-unreachable**

**Chain OUTPUT (policy ACCEPT)**

- **target**: default (policy ACCEPT)
- **protocol**: all
- **options**: state RELATED,ESTABLISHED

**Response (Linux) — after modification of local iptables firewall:**

Note that three TCP rules at the beginning of the policy-specified firewall ("raw_policy_monitored") have been removed from the firewall as it now exists on the local server ("raw_policy_installed").

```json
{
  "agent_id": "aaa6979cb4021e5b48911eda6605b06",
  "change_detected_at": "2016-01-05T23:34:52.647+00:00",
  "last_installed_at": "2016-01-05T23:18:54.289+00:00",
  "raw_policy_installed": "Chain INPUT (policy ACCEPT)
  target     prot opt source               destination
  ACCEPT     tcp  --  174.36.18.228        0.0.0.0/0           tcp spt:443 state RELATED,ESTABLISHED
  ACCEPT     tcp  --  174.36.20.154        0.0.0.0/0           tcp spt:443 state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            172.17.0.94         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            172.17.0.95         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
  LOG        all  --  172.17.0.89          0.0.0.0/0           state NEW,RELATED,ESTABLISHED LOG flags 0 level 4
  LOG        all  --  172.17.0.90          0.0.0.0/0           state NEW,RELATED,ESTABLISHED LOG flags 0 level 4
  LOG        all  --  172.17.0.91          0.0.0.0/0           state NEW,RELATED,ESTABLISHED LOG flags 0 level 4
  LOG        all  --  172.17.0.92          0.0.0.0/0           state NEW,RELATED,ESTABLISHED LOG flags 0 level 4
  LOG        all  --  172.17.0.93          0.0.0.0/0           state NEW,RELATED,ESTABLISHED LOG flags 0 level 4
  LOG        all  --  172.17.0.94          0.0.0.0/0           state NEW,RELATED,ESTABLISHED LOG flags 0 level 4
  LOG        all  --  172.17.0.95          0.0.0.0/0           state NEW,RELATED,ESTABLISHED LOG flags 0 level 4
  LOG        all  --  52.8.189.5           0.0.0.0/0           state NEW,RELATED,ESTABLISHED LOG flags 0 level 4
  Chain FORWARD (policy ACCEPT)
  target     prot opt source               destination
  ACCEPT     tcp  --  174.36.18.228        174.36.20.154        tcp dpt:443
  ACCEPT     tcp  --  174.36.20.154        174.36.18.228        tcp dpt:443
  ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:53
  ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:53
  ACCEPT     all  --  0.0.0.0/0            172.17.0.94         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            172.17.0.95         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.94          172.17.0.95         state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.95          172.17.0.94         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.94          172.17.0.95         state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.95          172.17.0.94         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.94          172.17.0.95         state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.95          172.17.0.94         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.94          172.17.0.95         state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.95          172.17.0.94         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.94          172.17.0.95         state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.95          172.17.0.94         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

  Chain OUTPUT (policy ACCEPT)
  target     prot opt source               destination
  ACCEPT     tcp  --  0.0.0.0/0            174.36.18.228        tcp dpt:443
  ACCEPT     tcp  --  0.0.0.0/0            174.36.20.154        tcp dpt:443
  ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:53
  ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:53
  ACCEPT     all  --  0.0.0.0/0            172.17.0.94         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            172.17.0.95         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.94          172.17.0.95         state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.95          172.17.0.94         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.94          172.17.0.95         state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.95          172.17.0.94         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.94          172.17.0.95         state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.95          172.17.0.94         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.94          172.17.0.95         state RELATED,ESTABLISHED
  ACCEPT     all  --  172.17.0.95          172.17.0.94         state RELATED,ESTABLISHED
  ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
},
```

133
Response (Windows)

(Excerpted, manually formatted)

Status: 200

{  
  agent_firewall_logs: [  
  
    {      
      agent_id: "ef349dd6064b11e5be930f1780293383",  
      change_detected_at: "2015-12-17T19:55:31.423+00:00",  
      last_installed_at: "2015-12-15T05:54:33.469+00:00",  
      raw_policy_installed: "  
      "  
    }  
  ]  
}
FileName C:\Windows\System32\LogFiles\Firewall\pfirewall.log MaxFileSize 4096 Ok. Rule Name: CloudPassage - 292a2760abe7013295e406ba9a9c633c


---

raw_policy_monitored: " Domain Profile Settings:

<table>
<thead>
<tr>
<th>State</th>
<th>Firewall Policy</th>
<th>BlockInbound, BlockOutbound</th>
<th>LocalFirewallRules</th>
<th>N/A (GPO-store only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalConSecRules</td>
<td>N/A (GPO-store only)</td>
<td>InboundUserNotification</td>
<td>Disable</td>
<td>RemoteManagement</td>
</tr>
<tr>
<td>UnicastResponseToMulticast</td>
<td>Enable Logging</td>
<td>LogAllowedConnections</td>
<td>Disable</td>
<td>LogDroppedConnections</td>
</tr>
</tbody>
</table>

FileName C:\Windows\System32\LogFiles\Firewall\pfirewall.log MaxFileSize 4096 Private Profile Settings:

<table>
<thead>
<tr>
<th>State</th>
<th>Firewall Policy</th>
<th>BlockInbound, BlockOutbound</th>
<th>LocalFirewallRules</th>
<th>N/A (GPO-store only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalConSecRules</td>
<td>N/A (GPO-store only)</td>
<td>InboundUserNotification</td>
<td>Disable</td>
<td>RemoteManagement</td>
</tr>
<tr>
<td>UnicastResponseToMulticast</td>
<td>Enable Logging</td>
<td>LogAllowedConnections</td>
<td>Disable</td>
<td>LogDroppedConnections</td>
</tr>
</tbody>
</table>

FileName C:\Windows\System32\LogFiles\Firewall\pfirewall.log MaxFileSize 4096 Public Profile Settings:

<table>
<thead>
<tr>
<th>State</th>
<th>Firewall Policy</th>
<th>BlockInbound, BlockOutbound</th>
<th>LocalFirewallRules</th>
<th>N/A (GPO-store only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalConSecRules</td>
<td>N/A (GPO-store only)</td>
<td>InboundUserNotification</td>
<td>Disable</td>
<td>RemoteManagement</td>
</tr>
<tr>
<td>UnicastResponseToMulticast</td>
<td>Enable Logging</td>
<td>LogAllowedConnections</td>
<td>Disable</td>
<td>LogDroppedConnections</td>
</tr>
</tbody>
</table>

FileName C:\Windows\System32\LogFiles\Firewall\pfirewall.log MaxFileSize 4096 Ok. Rule Name: Google Chrome (mDNS-In)


---

135

135
Local User Accounts

Use the Local User Accounts endpoint to retrieve the set of local user accounts across an entire Halo account, in a specified group, or on an individual server. The information can be retrieved filtered, sorted or grouped by a number of parameters.

Note: Some of the methods documented here are not performed on this API endpoint, but on the Server Accounts endpoint.

- Object Representation
- List all local user accounts
- List a group's local user accounts
- List a server's local user accounts
- Get local user account details

Object Representation

User account object location

api.cloudpassage.com/v1

  local_accounts

username

User account summary object fields

These fields are returned by the List all local user accounts method. Note that some fields apply only to Linux servers, others only to Windows servers, and still others apply to both.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>The username assigned to this local user account.</td>
</tr>
<tr>
<td>url</td>
<td>The API URL to the account object.</td>
</tr>
<tr>
<td>uid</td>
<td>[Linux only] The account's user ID.</td>
</tr>
<tr>
<td>gid</td>
<td>[Linux only] The group ID of the account's owner group.</td>
</tr>
<tr>
<td>admin</td>
<td>true if the account has root or sudo access; otherwise, false.</td>
</tr>
<tr>
<td>comment</td>
<td>An optional user-defined name or description of the account.</td>
</tr>
<tr>
<td>home</td>
<td>The home directory of the account.</td>
</tr>
<tr>
<td>shell</td>
<td>[Linux only] The path to the command shell used by the account.</td>
</tr>
<tr>
<td>last_login_at</td>
<td>Timestamp (in ISO-8601 format) of the last successful login into the account.</td>
</tr>
<tr>
<td>locked</td>
<td>[Windows only] true if the account is currently locked; otherwise, false.</td>
</tr>
<tr>
<td>server_id</td>
<td>The Halo ID of the server on which this local user account was created.</td>
</tr>
<tr>
<td>server_name</td>
<td>A (by default) calculated hostname of the server.</td>
</tr>
</tbody>
</table>
server_label | A user-assigned label or description for the server.
group_id | The Halo ID of the group containing the server on which this local user account was created.
os_type | The platform (linux or windows) of the server on which this user account was created.

User account details object fields

These fields are returned by the Get local user account details method. They include the summary fields noted above, plus additional account details and information for user groups to which the account belongs.

Note that some fields apply only to Linux servers, others only to Windows servers; most fields apply to both.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>The username assigned to this local user account.</td>
</tr>
<tr>
<td>full_name</td>
<td>[Windows only] The full user name of this account.</td>
</tr>
<tr>
<td>url</td>
<td>The API URL to the account object.</td>
</tr>
<tr>
<td>uid</td>
<td>[Linux only] The account's user ID.</td>
</tr>
<tr>
<td>sid</td>
<td>[Windows only] The security identifier (SID) of the account.</td>
</tr>
<tr>
<td>gid</td>
<td>[Linux only] The group ID of the account's owner group.</td>
</tr>
<tr>
<td>admin</td>
<td>true if the account has root or sudo access; otherwise, false.</td>
</tr>
<tr>
<td>comment</td>
<td>An optional user-defined name or description of the account.</td>
</tr>
<tr>
<td>home</td>
<td>The home directory of the account.</td>
</tr>
<tr>
<td>shell</td>
<td>[Linux only] The path to the command shell used by the account.</td>
</tr>
<tr>
<td>last_login_at</td>
<td>Timestamp (in ISO-8601 format) of the last successful login into the account.</td>
</tr>
<tr>
<td>last_login_from</td>
<td>[Linux only] The domain and port from which the account last logged into the server (if available).</td>
</tr>
<tr>
<td>active</td>
<td>true if the account is active; false if it is deactivated.</td>
</tr>
<tr>
<td>locked</td>
<td>[Windows only] true if the file is currently locked, false if not.</td>
</tr>
<tr>
<td>groups</td>
<td>An array of comma-separated group names, showing each user group that the account belongs to.</td>
</tr>
<tr>
<td>home_exists</td>
<td>[Linux only] true if the account's home directory has been specified; false if not.</td>
</tr>
<tr>
<td>password_required</td>
<td>[Windows only] true if the account requires a password; false if not.</td>
</tr>
<tr>
<td>password_changeable</td>
<td>[Windows only] true if the account password can be updated; false if not.</td>
</tr>
<tr>
<td>last_password_change</td>
<td>The timestamp (in ISO 8061 format) of the last change to the account's password.</td>
</tr>
<tr>
<td>expires</td>
<td>The date on which this account expires; never or null if the account does not expire.</td>
</tr>
<tr>
<td>minimum_days_between_password_changes</td>
<td>[Linux only] The number of days after a successful password change that must elapse before the password can be changed again. Also called minimum password life.</td>
</tr>
<tr>
<td>maximum_days_between_password_changes</td>
<td>[Linux only] The number of days after password creation or a successful password change that the password will remain valid. Also called password life.</td>
</tr>
<tr>
<td>days_warn_before_password_expired</td>
<td>[Linux only] The number of days before password expiration that the system will start alerting the account user that the password will soon expire.</td>
</tr>
<tr>
<td>password_expires</td>
<td>[Windows only] The date on which the account's current password expires; null if the password never expires.</td>
</tr>
<tr>
<td>password_expired</td>
<td>[Windows only] true if the password has expired; false if it never expires.</td>
</tr>
</tbody>
</table>
| disabled_after_days_inactive | [Linux only] The number of consecutive days with no account activity after which the account...
Call parameters for local user accounts

When you make API calls that return a list of local user accounts, you can apply any of the following parameters to restrict the results, to change the sorting of the results, and to aggregate the results into groups based on individual values of certain object fields.

Search filters

Use the following filters and operators to restrict the set of local user accounts returned. For any of the filters, you can provide either a single value or a comma-separated list of values. If you do provide multiple values, they are OR’d in a search, meaning that the search passes for that filter if any of its supplied values matches.

- os_type
- username
- admin
- active
- last_login_at
- never_logged_in
- password_required
- password_expired
- comment
- group_id
- server_id
- server_name
- server_label
- group_name
- locked
- gid
- sid
- uid
- sort_by
- group_by

Note: You can search for time ranges by adding any of the suffixes _lt, _lte, _gt, or _gte to the field name last_login_at. (For example, created_at_lt means "return all local user accounts that have not logged in since the specified date-time").

Sorting the results

You can use the sort_by parameter to specify that the search results are to be alphanumerically sorted (in either ascending or descending order, using the .asc and .desc filter suffixes) according to the values of the following user account object fields:

- os_type
- username
- admin
- active
- last_login_at
- password_required
- password_expired

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh_authorized_keys</td>
<td>[Linux only] An array of any authorized SSH keys belonging to the account (if available).</td>
</tr>
<tr>
<td>ssh_acl</td>
<td>[Linux only] The access control settings for the SSH folder.</td>
</tr>
<tr>
<td>sudo_access</td>
<td>A list of sudo access rules for the account, both as a member of a group and as a user (if available).</td>
</tr>
</tbody>
</table>
you can use the group_by parameter to specify that the search results are to be aggregated according to the values in one or more user account object fields. for example, if you search a server's accounts and aggregate by os_type, all windows accounts are listed together, and all linux accounts are listed together. if you search a group's local user accounts and sort by account name, the results will group together all instances of each account name within the group. these are the fields by which you can group local user accounts:

- os_type
- username

list all local user accounts

returns json-formatted results listing summary information for all local accounts within the scope of the api key used for the api session.

get https://api.cloudpassage.com/v1/local_accounts

you can modify the results of this call by applying a variety of parameters to the url (see call parameters for local user accounts, above).

response

status: 200

```json
{
  "accounts": [
    {
      "username": "kilau23",
      "comment": "",
      "home": "/",
      "last login at": null,
      "admin": false,
      "group_id": "1f429fb6165311e7b4660fadc3c5dfce",
      "os type": "linux",
      "gid": "502",
      "uid": "502",
      "shell": "/bin/bash",
      "active": true,
      "server_name": "ip-10-3-30-29",
      "server_label": null,
      "url": "https://api.cloudpassage.com/v1/servers/e28a9550165311e78a121b96b1ed2b89/accounts/kilau23",
      "server_id": "e28a9550165311e78a121b96b1ed2b89"
    },
    {
      "username": "madmaxwell",
      "comment": "maxwell-sales",
      "server_id": "e28a9550165311e78a121b96b1ed2b89"
    }
  ]
}
Other example call URLs:

Returns all local accounts on Linux servers:

GET https://api.cloudpassage.com/v1/local_accounts?os_type=linux

Returns all local accounts that have never logged in:

GET https://api.cloudpassage.com/v1/local_accounts?never_logged_in=true

Returns all Linux accounts with the username root:

GET https://api.cloudpassage.com/v1/local_accounts?os_type=linux&username=root

List a group's local user accounts

Returns JSON-formatted results listing summary information for all local accounts on the servers of the group specified by ID in the call URL.

GET https://api.cloudpassage.com/v1/local_accounts?group_id={id}

You can modify the results of this call by applying a variety of parameters to the URL (see Call parameters for local user accounts, above).

Response

Status: 200

```json
{
    "accounts": [
        {
            "username": "Administrator",
            "comment": "Built-in account for administering the computer/domain",
            "home": "C:\Users\Administrator",
            "last_login_at": "2017-03-30T09:10:19.000Z",
            "admin": true,
            "locked": false,
            "group_id": "ce1d4a3014011e7adf41191abf97f6a",
            "os_type": "windows",
            "active": true,
            "sid": "S-1-5-21-3101936619-1018315348-248917622-500",
            "server_name": "WIN-73-20-4",
            "server_label": "2012-r2-1kusertest",
            "url": "https://api.cloudpassage.com/v1/servers/c615e96e144c11e79f262166426a0a65/accounts/madmaxwell",
            "server_id": "c615e96e144c11e79f262166426a0a65"
        }
    ],
    "count": 4253,
    "pagination": {
        "next": "https://api.cloudpassage.com/v1/local_accounts?page=2&per_page=1000"
    }
}
```
Returns all local Linux accounts in the specified group:

GET https://api.cloudpassage.com/v1/local_accounts?group_id=d771e98e...0f176dc198&os_type=linux

Returns all administrative (high-privileged) local accounts in the specified group:

GET https://api.cloudpassage.com/v1/local_accounts?group_id=d771e98e...0f176dc198&admin=true

List a server's local user accounts

Returns JSON-formatted results listing summary information for all local accounts on the server specified by ID in the call URL.

GET https://api.cloudpassage.com/v1/local_accounts?server_id={server_id}

Note: Another way to make this call is to use the Server Accounts endpoint instead of this endpoint (Local User Accounts. However, the response JSON returned from that call may be slightly different from that shown here.

You can modify the results of this call by applying a variety of parameters to the URL (see Call parameters for local user accounts, above).
Response
Status: 200

```json
{
  "accounts": [
    {
      "username": "adm",
      "comment": "adm",
      "home": "/var/adm",
      "last_login_at": null,
      "admin": false,
      "group_id": "ce1d4a3014011e7adf4191abf97f6a",
      "os_type": "linux",
      "uid": "3",
      "gid": "4",
      "shell": "/sbin/nologin",
      "active": true,
      "server_name": "ip-10-3-30-27",
      "server_label": null,
      "url": "https://api.cloudpassage.com/v1/servers/558ab6c8156b11e7b11d53f8844a2f57/accounts/adm",
      "server_id": "558ab6c8156b11e7b11d53f8844a2f57"
    },
    {
      "username": "bin",
      "comment": "bin",
      "home": "/bin",
      "last_login_at": null,
      "admin": false,
      "group_id": "ce1d4a3014011e7adf4191abf97f6a",
      "os_type": "linux",
      "uid": "1",
      "gid": "1",
      "shell": "/sbin/nologin",
      "active": true,
      "server_name": "ip-10-3-30-17",
      "server_label": null,
      "url": "https://api.cloudpassage.com/v1/servers/558ab6c8156b11e7b11d53f8844a2f57/accounts/bin",
      "server_id": "558ab6c8156b11e7b11d53f8844a2f57"
    },
    ...
    {
      "username": "uucp",
      "comment": "uucp",
      "home": "/var/spool/uucp",
      "last_login_at": null,
      "admin": false,
      "group_id": "ce1d4a3014011e7adf4191abf97f6a",
      "os_type": "linux",
      "uid": "14",
      "gid": "10",
      "shell": "/sbin/nologin",
      "active": true,
      "server_name": "ip-10-3-30-31",
      "server_label": null,
      "url": "https://api.cloudpassage.com/v1/servers/558ab6c8156b11e7b11d53f8844a2f57/accounts/uucp",
      "server_id": "558ab6c8156b11e7b11d53f8844a2f57"
    }
  ],
  "count": 25
}
```

Other example call URLs:

- **Returns all local accounts on Windows servers:**
  
  **GET** https://api.cloudpassage.com/v1/local_accounts?os_type=windows

- **Returns all local accounts that have never logged in:**
  
  **GET** https://api.cloudpassage.com/v1/local_accounts?never_logged_in=true

- **Returns all root-access Linux accounts (those with a GID of zero):**
  
  **GET** https://api.cloudpassage.com/v1/local_accounts?os_type=linux&gid=0
Get local user account details

Returns the details of the local user account specified by username in the call URL.

GET https://api.cloudpassage.com/v1/servers/{id}/accounts/{username}

Note: You make this call to the Server Accounts endpoint, not to this endpoint (Local User Accounts).

Response for a Linux server

Status: 200

```json
{
  "account": {
    "username": "www-data",
    "url": "https://api.cloudpassage.com/v1/servers/b0ea882e152811e79c5f755722aea3ce/accounts/www-data",
    "uid": "33",
    "gid": "33",
    "admin": false,
    "comment": "www-data",
    "home": "/var/www",
    "shell": "/usr/sbin/nologin",
    "last_login_at": null,
    "active": true,
    "last_login_from": null,
    "groups": "www-data",
    "home_exists": false,
    "last_password_change": "2016-10-20T00:00:00.000Z",
    "minimum_days_between_password_changes": 0,
    "maximum_days_between_password_changes": 99999,
    "days_warn_before_password_expiration": 7,
    "disabled_after_days_inactive": 0,
    "days_since_disabled": 0,
    "ssh_authorized_keys": null,
    "ssh_acl": null,
    "sudo_access": "None"
  }
}
```

Response for a Windows server

Status: 200

```json
{
  "account": {
    "username": "Administrator",
    "url": 
    "https://api.cloudpassage.com/v1/servers/e1968478152811e7b00e491118052707/accounts/Administrator",
    "sid": "S-1-5-21-3101936619-1018315348-2489197622-500",
    "comment": "Built-in account for administering the computer/domain",
    "home": "C:\Users\Administrator",
    "last_login_at": "2017-03-30T09:10:19.000Z",
    "active": true,
    "admin": true,
    "locked": false,
    "last_password_change": "2017-03-30T09:10:00.000Z",
    "password_required": true,
    "password_changeable": true,
    "password_expires": null,
    "password_expired": false,
    "full_name": "",
    "expires": "never",
    "groups": "Administrators"
  }
}
```
Local User Groups

Use the Local User Groups endpoint to retrieve the set of local user groups on an individual server, in a group, or across an entire Halo account. The information can be retrieved filtered, sorted and grouped by a number of parameters.

- Object Representation
- List all local user groups
- List a group's local user groups
- List a server's local user groups
- Get a single local user group

Object Representation

User group object location

api.cloudpassage.com/v1

local_groups

id

User group object fields

These fields are returned by the List all local user groups method and all other methods on this endpoint.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the local user group.</td>
</tr>
<tr>
<td>comment</td>
<td>An optional user-defined name or description of the user group.</td>
</tr>
<tr>
<td>os_type</td>
<td>The type of operating system (windows or linux) of the group's server.</td>
</tr>
<tr>
<td>group_id</td>
<td>The Halo ID of the local user group.</td>
</tr>
<tr>
<td>sid</td>
<td>[Windows only] The security identifier (SID) of the user group.</td>
</tr>
<tr>
<td>gid</td>
<td>[Linux only] The group ID of the user group.</td>
</tr>
<tr>
<td>server_label</td>
<td>A user-assigned label or description for the server.</td>
</tr>
<tr>
<td>server_name</td>
<td>A (by default) calculated hostname of the server.</td>
</tr>
<tr>
<td>url</td>
<td>The API URL to the user group object.</td>
</tr>
<tr>
<td>server_id</td>
<td>The Halo ID of the server on which this local user group was created.</td>
</tr>
<tr>
<td>members</td>
<td>A comma-separated array listing the names of the group's members.</td>
</tr>
</tbody>
</table>

Call parameters for local user groups

When you make API calls that return a list of local user groups, you can apply any of the following parameters to restrict the results, to change the sorting of the results, or to aggregate the results into categories based on individual values of certain object fields.
Search filters

Use the following filters and operators to restrict the set of local user groups returned. For any of the filters, you can provide either a single value or a comma-separated list of values. If you do provide multiple values, they are OR'd in a search, meaning that the search passes for that filter if any of its supplied values matches.

- os_type
- comment
- members
- member_name
- group_id
- server_id
- server_name
- server_label
- name
- gid
- sid
- sort_by
- group_by

Sorting the results

You can use the sort_by parameter to specify that the search results are to be alphanumerically sorted (in either ascending or descending order, using the .asc and .desc filter suffixes) according to the values of any of the following user group object fields:

- server_id
- os_type
- group_id
- name
- comment
- sid
- gid
- server_name
- server_label

Example: sort_by=server_name.asc

Aggregating the results

You can use the group_by parameter to specify that the search results are to be categorized according to the values in one or more user group object fields. For example, if you search a server's user groups and aggregate by os_type, all Windows user groups are listed together, and all Linux user groups are listed together. If you search a group's accounts and sort by account name, the results will aggregate together all instances of each user group name within the group. These are the fields by which you can group local user groups:

- os_type
- name

List all local user groups

Returns JSON-formatted results listing summary information for all local user groups within the scope of the API key used for the API session.
GET https://api.cloudpassage.com/v1/local_groups

You can modify the results of this call by applying a variety of parameters to the URL (see Call parameters for local user groups, above).

Response

Status: 200

```json
{
    "local_groups": [
        {
            "members": [],
            "os_type": "windows",
            "sid": "S-1-5-32-579",
            "comment": "Members of this group can remotely query authorization attributes and permissions for resources on this computer."
        },
        {
            "members": [],
            "os_type": "windows",
            "sid": "S-1-5-32-579",
            "comment": "Members of this group can remotely query authorization attributes and permissions for resources on this computer."
        },
        {
            "members": [],
            "os_type": "linux",
            "gid": "1",
            "name": "daemon",
            "group_id": "ee2f43814661e7bdcf452e5f825898",
            "server_label": null,
            "server_name": "sam-redhat2",
            "url": "https://api.cloudpassage.com/v1/local_groups/45a18ed6147011e79f262166426a0a65:1",
            "server_id": "45a18ed6147011e79f262166426a0a65"
        },
        {
            "members": [],
            "os_type": "windows",
            "sid": "S-1-5-21-1812932179-979827559-110896304-4159",
            "comment": "",
            "name": "group1159",
            "group_id": "aad1e04014ac11e7bf984f13e2e0df4d",
            "server_label": null,
            "server_name": "WINDOWS 2012R2-26",
            "url": "https://api.cloudpassage.com/v1/local_groups/7407c31c14e311e788904107d814b2dd:S-1-5-21-1812932179-979827559-110896304-4159",
            "server_id": "7407c31c14e311e788904107d814b2dd"
        }
    ],
    "count": 1409,
    "pagination": {
        "next": "https://api.cloudpassage.com/v1/local_groups?page=2&per_page=1000"
    }
}
Other example call URLs:

- Returns all local groups created on Windows servers:
  
  GET https://api.cloudpassage.com/v1/local_groups?os_type=windows

- Returns all Local Windows user groups with the name **Administrators**:
  
  GET https://api.cloudpassage.com/v1/local_groups?os_type=windows&name=Administrators

- Returns all local Linux user groups, aggregated by user-group name. Note that the results show the number of local user groups that have each group name:
  
  GET https://api.cloudpassage.com/v1/local_groups?os_type=linux&group_by=name

  Example response JSON:

  ```json
  {
  "local_groups": [
  {
    "name": "vcsa",
    "count": 1
  },
  {
    "name": "tcpdump",
    "count": 1
  },
  .....
  {
    "name": "mailnull",
    "count": 5
  },
  {
    "name": "chrony",
    "count": 5
  },
  .....
  {
    "name": "audio",
    "count": 19
  },
  {
    "name": "adm",
    "count": 19
  }
  ],
  "count": 94
  }
  ```

**List a group's local user groups**

Returns JSON-formatted results listing all local user groups on the servers of the server group specified by ID in the method URL.

GET https://api.cloudpassage.com/v1/local_groups?group_id={group_id}

You can modify the results of this call by applying a variety of parameters to the URL (see [Call parameters for local user groups](#), above).

**Response**

**Status: 200**
Other example call URLs:

- Returns all local user groups within a group, grouped by platform:

  GET https://api.cloudpassage.com/v1/local_groups?group_id={group_id}&group_by=os_type

  Example response JSON:

  ```json
  {
    "local_groups": [{
      "os_type": "windows",
      "count": 115
    }, {
      "os_type": "linux",
      "count": 408
    }],
    "count": 2
  }
  ```

  (The above counts show that the group includes two platforms, 115 Windows user groups, and 408 Linux user groups.)

- Returns all local user groups of a given name within a group (this field supports partial match):

  GET https://api.cloudpassage.com/v1/local_groups?group_id={group_id}&name={name}
List a server's local user groups

Returns JSON-formatted results listing all local user groups on the server specified by ID in the method URL.

**GET** https://api.cloudpassage.com/v1/local_groups?server_id={id}
You can modify the results of this call by applying a variety of parameters to the URL (see Call parameters for local user groups, above).

### Response

**Status: 200**

```
{
  "local_groups": [
    {
      "members": [],
      "os_type": "windows",
      "sid": "S-1-5-32-579",
      "comment": "Members of this group can remotely query authorization attributes and permissions for resources on this computer."
    },
    {
      "members": [],
      "os_type": "windows",
      "sid": "S-1-5-32-579",
      "comment": "Members of this group can remotely query authorization attributes and permissions for resources on this computer."
    },
    {
      "members": [],
      "os_type": "windows",
      "sid": "S-1-5-32-579",
      "comment": "Members of this group can remotely query authorization attributes and permissions for resources on this computer."
    },
    {
      "members": [],
      "os_type": "windows",
      "sid": "S-1-5-32-579",
      "comment": "Members of this group can remotely query authorization attributes and permissions for resources on this computer."
    }
  ],
  "count": 23
}
```

**Other example call URLs:**

- Returns all local user groups on the specified server that have a specific comment field (partial matches on this field are supported):
  
  GET https://api.cloudpassage.com/v1/local_groups?server_id={id}&comment=US Administrators

- Get a single local user group

  Returns the details of the local user group specified by server ID and GID in the call URL. Note that this call returns the same group information as that returned from other calls to this endpoint, such as List all local user groups.

  GET https://api.cloudpassage.com/v1/local_groups?server_id={id}&gid={gid}
Response
Status: 200

```json
{
  "local_groups": [
    {
      "members": [
        "daemon",
        "pollinate"
      ],
      "os_type": "linux",
      "gid": "1",
      "name": "daemon",
      "group_id": "ee2fb438146611e7bdcf452e5f825898",
      "server_label": null,
      "server_name": "sam-redhat2",
      "url": "https://api.cloudpassage.com/v1/local_groups/45a18ed6147011e79f262166426a0a65:1",
      "server_id": "45a18ed6147011e79f262166426a0a65"
    }
  ],
  "count": 1
}
```
Scan History

Use the Scan History endpoint to retrieve summary information for historical scans.

- Object Representation
- List historical scans
- Get scan details
- Get file integrity scan findings details

Object Representation

Scan object location

```
api.cloudpassage.com/v1

/scan

id
```

Scan object fields

These fields are returned by the List historical scans call. The Get scan details call also returns additional fields for the findings, or issues—such as vulnerabilities—detected by the scan. Those fields are documented with the Server Scans endpoint.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The ID of this scan.</td>
</tr>
<tr>
<td>url</td>
<td>The API URL to the scan object.</td>
</tr>
<tr>
<td>module</td>
<td>The type of scan performed: csm, fim, svm, or sam.</td>
</tr>
<tr>
<td>status</td>
<td>The status of the scan: queued, pending, running, completed_clean, completed_with_errors, or failed.</td>
</tr>
<tr>
<td>created_at</td>
<td>When the scan started. (ISO-8601 format)</td>
</tr>
<tr>
<td>completed_at</td>
<td>When the scan finished. (ISO-8601 format)</td>
</tr>
<tr>
<td>analysis_started_at</td>
<td>When analysis of the scan data started. (ISO-8601 format)</td>
</tr>
<tr>
<td>analysis_completed_at</td>
<td>When analysis of the scan data finished. (ISO-8601 format)</td>
</tr>
<tr>
<td>agent_started_at</td>
<td>When the agent started scanning. (ISO-8601 format)</td>
</tr>
<tr>
<td>agent_completed_at</td>
<td>When the agent finished scanning. (ISO-8601 format)</td>
</tr>
<tr>
<td>policies</td>
<td>An array of the name and Halo ID of each policy that was applied to this scan.</td>
</tr>
<tr>
<td>server_id</td>
<td>The server's Halo ID.</td>
</tr>
<tr>
<td>server_hostname</td>
<td>The server's hostname.</td>
</tr>
<tr>
<td>server_url</td>
<td>The API URL to the server object.</td>
</tr>
<tr>
<td>critical_findings_count</td>
<td>Number of critical issues reported. (Not reported for server access scans.)</td>
</tr>
<tr>
<td>non_critical_findings_count</td>
<td>Number of non-critical issues reported. (Not reported for server access scans.)</td>
</tr>
</tbody>
</table>
File integrity scan findings object fields

These fields are returned by the Get file integrity scan findings details call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique identifier for this findings object.</td>
</tr>
<tr>
<td>url</td>
<td>The API URL to this findings object.</td>
</tr>
<tr>
<td>rule</td>
<td>An array describing the policy rule (target) for this findings object.</td>
</tr>
<tr>
<td>critical</td>
<td>true if failure of this rule is a critical issue; otherwise false.</td>
</tr>
<tr>
<td>recurse</td>
<td>true if this rule is recursive; otherwise false.</td>
</tr>
<tr>
<td>target</td>
<td>The full file path to this rule's target object.</td>
</tr>
<tr>
<td>alert</td>
<td>true if failure of this rule should generate an alert; otherwise false.</td>
</tr>
<tr>
<td>log</td>
<td>true if failure of this rule should be logged as an event; otherwise false.</td>
</tr>
<tr>
<td>description</td>
<td>A user-provide description of this rule.</td>
</tr>
<tr>
<td>policy_id</td>
<td>The Halo ID of the policy that this rule belongs to.</td>
</tr>
<tr>
<td>status</td>
<td>The status of the file integrity scan results of this target. Possible values are good if the rule passed, and bad if the rule failed.</td>
</tr>
<tr>
<td>counts</td>
<td>Counts of results for all objects checked by this rule.</td>
</tr>
<tr>
<td>ok</td>
<td>This many objects were unchanged.</td>
</tr>
<tr>
<td>missing</td>
<td>This many objects were removed.</td>
</tr>
<tr>
<td>added</td>
<td>This many objects were added.</td>
</tr>
<tr>
<td>changed</td>
<td>This many objects had changes to their content or metadata.</td>
</tr>
<tr>
<td>reference_identifiers</td>
<td>A comma-separated list of IDs used to mark this rule for compliance purposes. Each identifier is a name-value pair with this JSON format: {&quot;name&quot;:&quot;value&quot;} — for example, {&quot;USB&quot;:&quot;67&quot;},{&quot;CIS&quot;:&quot;1.1.2&quot;}</td>
</tr>
<tr>
<td>findings</td>
<td>An array of scan results, one finding for each examined object within this target. Includes the following sub-fields:</td>
</tr>
<tr>
<td>file</td>
<td>The full file path to the object that was examined.</td>
</tr>
<tr>
<td>status</td>
<td>The status of the file integrity scan of this object.</td>
</tr>
<tr>
<td>detail</td>
<td>An array of the detailed results of the scan of this object.</td>
</tr>
<tr>
<td>meta</td>
<td>An array of values for this object's metadata.</td>
</tr>
<tr>
<td>dev</td>
<td>Linux only: The device number of this object (in decimal).</td>
</tr>
<tr>
<td>type</td>
<td>The type of this object. Possible values are file, dir, and link for Linux, and file, dir, link, and regkey for Windows.</td>
</tr>
<tr>
<td>user</td>
<td>Linux only: The usename of this object's user owner.</td>
</tr>
<tr>
<td>owner</td>
<td>Windows only: The usename of this object's owner.</td>
</tr>
<tr>
<td>ctime</td>
<td>Linux only: The date-time at which the metadata or content of this object was last modified. In Unix epoch format.</td>
</tr>
<tr>
<td>nlink</td>
<td>Linux only: The link count—the number of hard links that point to this object's inode.</td>
</tr>
<tr>
<td>atime</td>
<td>Linux only: The date-time at which the object was last accessed. In Unix epoch format.</td>
</tr>
<tr>
<td>ino</td>
<td>Linux only: The inode number of this object.</td>
</tr>
<tr>
<td>mtime</td>
<td>Linux only: The date-time at which the content of this object was last modified. In Unix epoch format.</td>
</tr>
<tr>
<td>gid</td>
<td>Linux only: The group ID of this object's group owner.</td>
</tr>
<tr>
<td><strong>group</strong></td>
<td>Linux only: The name of this object's group owner.</td>
</tr>
<tr>
<td><strong>mode</strong></td>
<td>Linux only: The set of permissions on this object.</td>
</tr>
<tr>
<td><strong>perm</strong></td>
<td>Windows only: The set of permissions on this object.</td>
</tr>
<tr>
<td><strong>uid</strong></td>
<td>Linux only: The user ID of this object's user owner.</td>
</tr>
<tr>
<td><strong>size</strong></td>
<td>Linux only: The size of this object in bytes.</td>
</tr>
<tr>
<td><strong>sha256</strong></td>
<td>The cryptographic signature (SHA 256 hash) of this object's content.</td>
</tr>
<tr>
<td><strong>status</strong></td>
<td>A comma-separated list of status values (added, missing, or changed), one for each baseline applied to the object. If there is only one baseline, this value is the same as the value in the status field for the entire scan (see above).</td>
</tr>
<tr>
<td><strong>expected</strong></td>
<td>A comma separated list of sets of name-value pairs. Each set lists the expected values for the signature and metadata of this object, as specified in one of the baselines applied to the object. If there is only one baseline, only one set of pairs appears here.</td>
</tr>
</tbody>
</table>

### List historical scans

Returns JSON-formatted results listing all configuration scans, file-integrity scans, software vulnerability scans, and server-access scans conducted on all servers.

**GET** https://api.cloudpassage.com/v1/scans/

This call supports many optional parameters:

- By using the filter parameters `since` (inclusive) and `until` (exclusive), you can restrict the retrieved scans to a time/date range. The value for each parameter is an ISO 8601 formatted timestamp string (for example `YYYY-MM-DD`, or `YYYY-MM-DDThh:mmZ` for Zulu time zone). For example:


- By using the filter parameters `module`, `server_id`, `server_hostname`, and `status`, you can restrict the results to scans of a specified kind, or occurring in a specified server, or with a specified scan status. For example:

  GET https://api.cloudpassage.com/v1/scans?module=fim,csm

  GET https://api.cloudpassage.com/v1/scans?server_id=c827779463036a0b90faf16283927dc2


- By using the filter parameters `ec2_instance_id` and `ec2_account_id`, you can restrict the results of scans (on AWS servers only) to specific AWS EC2 workload instances or customer accounts. For example:

  GET https://api.cloudpassage.com/v1/scans?ec2_instance_id=i-039b9cfc7671567bb

  (Note that these filters are available but are not fields in the scan or scan findings objects.)

You can combine any of the above parameters in your **List historical scans** calls. Note also:

- Scan objects in the response JSON are listed in reverse chronological order, based on the value in the `completed_at` field.
- The response JSON includes a `count` parameter following the array of scan objects. It displays the total number of objects returned from the call.
- The response is paginated, with a page size of 10 items by default. The response JSON also includes the full URL for retrieving the next or previous page of results.

    "pagination": {
    "previous": "https://api.cloudpassage.com/v1/scans?page=2&per_page=100"
    "next": "https://api.cloudpassage.com/v1/scans?page=4&per_page=100"
    }
You can use the `per_page` parameter to specify custom page sizes up to 100 objects, and you can use the `page` parameter to specify which page to retrieve. See Pagination of Results for further explanation and examples.

**Response**

**Status: 200**

```json
{
  "scans": [
    {
      "id": "15d7158a328b11e6aa531f56fb0a298c",
      "url": "https://api.cloudpassage.com/v1/scans/15d7158a328b11e6aa531f56fb0a298c",
      "module": "fim",
      "status": "completed_clean",
      "created_at": "2016-06-14T23:52:42.963Z",
      "completed_at": "2016-06-14T23:53:39.511Z",
      "analysis_started_at": "2016-06-14T23:53:39.511Z",
      "analysis_completed_at": "2016-06-14T23:53:39.511Z",
      "agent_started_at": "2016-06-14T23:53:11.000Z",
      "agent_completed_at": "2016-06-14T23:53:11.000Z",
      "server_id": "8f7883b4325a11e6941d3d82fcef9dc7",
      "server_hostname": "7fe5d75afbf5",
      "server_url": "https://api.cloudpassage.com/v1/servers/8f7883b4325a11e6941d3d82fcef9dc7",
      "critical_findings_count": 0,
      "non_critical_findings_count": 2,
      "ok_findings_count": 213
    },
    {
      "id": "b6d6db5e326411e69df771040bc89c8",
      "url": "https://api.cloudpassage.com/v1/scans/b6d6db5e326411e69df771040bc89c8",
      "module": "svm",
      "status": "completed_clean",
      "created_at": "2016-06-14T19:18:02.659Z",
      "completed_at": "2016-06-14T19:25.914Z",
      "analysis_started_at": "2016-06-14T19:18:02.980Z",
      "analysis_completed_at": "2016-06-14T19:25.914Z",
      "agent_started_at": "2016-06-14T19:18:00.000Z",
      "agent_completed_at": "2016-06-14T19:18:00.000Z",
      "server_id": "fa1a4920319a11e6855d45c77a8b1042",
      "server_hostname": "ip-172-31-30-247",
      "server_url": "https://api.cloudpassage.com/v1/servers/fa1a4920319a11e6855d45c77a8b1042",
      "critical_findings_count": 17,
      "non_critical_findings_count": 0,
      "ok_findings_count": 221
    },
    {
      "id": "2553edc0326411e6903e61c10a77163c",
      "url": "https://api.cloudpassage.com/v1/scans/2553edc0326411e6903e61c10a77163c",
      "module": "sam",
      "status": "completed_clean",
      "created_at": "2016-06-14T19:13:58.529Z",
      "completed_at": "2016-06-14T19:13:58.837Z",
      "analysis_started_at": "2016-06-14T19:13:58.836Z",
      "analysis_completed_at": "2016-06-14T19:13:58.837Z",
      "agent_started_at": "2016-06-14T19:13:57.000Z",
      "agent_completed_at": "2016-06-14T19:13:57.000Z",
      "server_id": "728b17f64ce311e5953b11e86205f2df",
      "server_hostname": "ip-10-2-20-204",
      "server_url": "https://api.cloudpassage.com/v1/servers/728b17f64ce311e5953b11e86205f2df"
    },
    {
      "id": "fa0482122adc11e6adb93f2202004769",
      "url": "https://api.cloudpassage.com/v1/scans/fa0482122adc11e6adb93f2202004769",
      "module": "csm",
      "status": "completed_clean",
      "created_at": "2016-06-05T05:18:45.681Z",
      "completed_at": "2016-06-05T05:18:45.960Z",
      "analysis_started_at": "2016-06-05T05:18:45.960Z",
      "analysis_completed_at": "2016-06-05T05:18:45.979Z",
      "agent_started_at": "2016-06-05T05:19:02.000Z",
      "agent_completed_at": "2016-06-05T05:19:02.000Z",
      "server_id": "e2cf334e0dc211e6a0941953c38af63d",
      "server_hostname": "ip-10-2-20-226",
      "server_url": "https://api.cloudpassage.com/v1/servers/e2cf334e0dc211e6a0941953c38af63d",
      "critical_findings_count": 0,
      "non_critical_findings_count": 0,
      "ok_findings_count": 0,
      "indeterminate_findings_count": 0
    }
  ]
}
```
Get scan details

Returns the details of the configuration scan, file-integrity scan, software vulnerability scan, or server-access scan specified by scan ID in the call URL.

Note: For a file integrity scan, this call returns only only summary findings information. For full details of each target’s findings, call the Get file integrity scan findings details method.

GET https://api.cloudpassage.com/v1/scans/{scan_id}

Response

Status: 200

{ "scan": { "id": "62c34430936001318cc03c764e10b50e", "url": "https://api-ninja.cloudpassage.com:10443:10443/v1/scans/62c34430936001318cc03c764e10b50e", "module": "svm", "status": "completed_clean", "created_at": "2014-03-21T19:53:24Z", "completed_at": "2014-03-21T19:53:29Z", "server_id": "e337150082df01318c4c3c764e10b50e", "server_hostname": "westninja-1", "server_url": "https://api.cloudpassage.com/v1/servers/e337150082df01318c4c3c764e10b50e", "critical_findings_count": 0, "non_critical_findings_count": 19, "findings": [ { "package_name": "perl.x86_64", "package_version": "4:5.10.1-136.el6", "critical": false, "status": "bad", "cve_entries": [ { "cve_entry": "CVE-2011-0761", "suppressed": false } ], "cpe": "not_found" }, { "package_name": "openssl.x86_64", "package_version": "1.0.1e-16.el6_5.4", "critical": false, "status": "bad", "cve_entries": [ { "cve_entry": "CVE-2013-4353", "suppressed": false }, { "cve_entry": "CVE-2013-6449", "suppressed": false }, { "cve_entry": "CVE-2013-6450", "suppressed": false } ], "cpe": "not_found" } ] }
Get file integrity scan findings details

For the file integrity scan specified by scan ID in the call URL, returns full details of the individual target's findings specified by findings ID in the call URL.

GET https://api.cloudpassage.com/v1/scans/{scan_id}/findings/{id}

Response

Response for Linux:

Status: 200

```json
{
  "id": "cea6aacc-9768-11e4-97d0-61bdcab12d11",
  "url": "https://api.cloudpassage.com/v1/scans/ba91cb807996013202b43c764e101158/findings/cea6aacc-9768-11e4-97d0-61bdcab12d11",
  "rule": {
    "critical": true,
    "recurse": false,
    "target": "/opt/cloudpassage/bin/cphalo",
    "alert": true,
    "log": true
  },
  "status": "bad",
  "counts": {
    "ok": 0,
    "missing": 0,
    "added": 1,
    "changed": 0
  },
  "reference_identifiers": [],
  "findings": [
    {
      "file": "/opt/cloudpassage/bin/cphalo",
      "status": "added",
      "detail": {
        "meta": {
          "dev": 64819,
          "type": "regular",
          "user": "root",
          "ctime": 1420671706,
          "nlink": 1,
          "atime": 1420671706,
          "ino": 404948,
          "mtime": 1394771786,
          "gid": 0,
          "group": "root",
          "mode": "r-x------",
          "uid": 0,
          "size": 4000416
        },
        "sha256": "b4f6c2208f93e811a5ba3339a5bc857e633c7ec2be6407b2b401ef9732eec90b",
        "status": [
          "added",
          "added",
          "added",
          "added"
        ],
        "expected": []
      }
    }
  ]
}
```
Response for Windows:

Status: 200

```json
{
    "id": "3ab09910-8ae6-11e4-bf4c-670ce7af26b1",
    "url": "https://api.cloudpassage.com/v1/scans/0007b870613013201934c1013546e101158/findings/3ab09910-8ae6-11e4-bf4c-670ce7af26b1",
    "rule": {
        "critical": true,
        "recurse": true,
        "target": "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems",
        "alert": false,
        "log": true
    },
    "status": "bad",
    "counts": {
        "ok": 0,
        "missing": 0,
        "added": 1,
        "changed": 0
    },
    "reference_identifiers": [],
    "findings": [
        {
            "file": "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems",
            "status": "added",
            "detail": {
                "meta": {
                    "perm": "S-1-5-32-545:0:16:131097:BUILTIN\Users,S-1-5-32-545:0:26:2147483648:BUILTIN\Users,S-1-5-32-544:0:16:983103:BUILTIN\Administrators,S-1-5-32-544:0:26:268435456:BUILTIN\Administrators,S-1-5-18:0:16:983103:NT AUTHORITY\SYSTEM,S-1-5-18:0:26:268435456:NT AUTHORITY\SYSTEM,S-1-3-0:0:26:268435456:C\CREATOR OWNER",
                    "type": "regkey",
                    "owner": "S-1-5-32-544:BUILTIN\Administrators"
                },
                "sha256": "68120f34a2f76d955a13546abca5aa9aeff670f2daca040a4843485c8785ecd",
                "status": "added",
                "expected": []
            }
        }
    },
    "starting_at": "https://api.cloudpassage.com/v1/scans/327598/findings/3ab09910-8ae6-11e4-bf4c-670ce7af26b1?per_page=100&starting_at=",
    "per_page": 100,
    "next": ""
}
```
Issues

Use the v3/issues endpoint to retrieve issues for all assets monitored by Halo. v3/issues retrieves issues from Cloud Secure, Container Secure, and Server Secure in a single endpoint.

Note: The v1/issues endpoint is deprecated. We recommend that you use v3/issues. For reference purposes only, you can view v1/issues documentation here.

- Object Representation
- List all Active Issues
- Get a Specific Issue
- Filter Issues
- Resolve a Specific Issue

Object Representation

Issue object location

api.cloudpassage.com/v3

   └── issues
       ├── id

Issue object fields

Note: In some cases, a field may not appear if it does not apply to a specific issue.

<table>
<thead>
<tr>
<th>Field</th>
<th>Searchable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>N</td>
<td>The unique Halo ID of the issue affecting a single asset.</td>
</tr>
<tr>
<td>url</td>
<td>N</td>
<td>The Halo uniform resource locator of the issue.</td>
</tr>
<tr>
<td>name</td>
<td>Y</td>
<td>The display name of the issue in Halo; for example, Vulnerable package: systemd.x86_64.</td>
</tr>
<tr>
<td>type</td>
<td>Y</td>
<td>The type of issue in Halo. Includes: FW, LIDS, SVA, CSM, SAM, Agent, FIM, and SVA.</td>
</tr>
<tr>
<td>status</td>
<td>Y</td>
<td>The status of the issue: active or resolved.</td>
</tr>
<tr>
<td>critical</td>
<td>Y</td>
<td>true if the issue is considered critical; otherwise false.</td>
</tr>
<tr>
<td>source</td>
<td>Y</td>
<td>The product that generated the issue in Halo; that is, server_secure, cloud_secure, container_secure.</td>
</tr>
<tr>
<td>created_at</td>
<td>Y</td>
<td>The date-time (in ISO 8601 format) when the issue was created in the Halo issues service.</td>
</tr>
<tr>
<td>updated_at</td>
<td>Y</td>
<td>The last date-time (in ISO 8601 format) when the issue was updated in the Halo issues service.</td>
</tr>
<tr>
<td>first_seen_at</td>
<td>Y</td>
<td>The date-time (in ISO 8601 format) when the issue was first detected/observed by the monitoring tool.</td>
</tr>
<tr>
<td>last_seen_at</td>
<td>Y</td>
<td>The last date-time (in ISO 8601 format) when the issue was detected by the monitoring tool.</td>
</tr>
<tr>
<td>Field</td>
<td>Required</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>policy_id</td>
<td>N</td>
<td>The Halo ID of the policy whose rule violation caused the issue to be created.</td>
</tr>
<tr>
<td>policy_name</td>
<td>Y</td>
<td>The name of the policy whose rule violation caused the issue to be created; for example, <strong>CIS Benchmark for Windows Server 2016</strong>.</td>
</tr>
<tr>
<td>cp_rule_id</td>
<td>Y</td>
<td>The friendly name of the CloudPassage CSM rule; for example, <strong>CIS:1.1</strong>. <strong>Note:</strong> This is preferred over csp_rule_id.</td>
</tr>
<tr>
<td>csp_rule_id</td>
<td>Y</td>
<td>The user-readable ID of the rule; for example, <strong>CIS:1.1</strong>. <strong>Note:</strong> Deprecated; use cp_rule_id.</td>
</tr>
<tr>
<td>rule_id</td>
<td>Y</td>
<td>The UUID number of the rule that was applied; for example, 280d33b6ef3411e88ad765862e629d59.</td>
</tr>
<tr>
<td>rule_name</td>
<td>N</td>
<td>The name of the rule that was applied; for example, <strong>Ensure MFA is enabled for the &quot;root&quot; account.</strong></td>
</tr>
<tr>
<td>last_finding_urls</td>
<td>N</td>
<td>Provides a link to the latest finding for additional details, if needed.</td>
</tr>
<tr>
<td>extended_attributes</td>
<td>N</td>
<td>Attributes that are specific to both the type of issue and the type of the affected asset. For example, Container Secure SVA issues.</td>
</tr>
<tr>
<td>asset_id</td>
<td>Y</td>
<td>The Halo ID of the affected asset.</td>
</tr>
<tr>
<td>asset_url</td>
<td>N</td>
<td>The Halo uniform resource locator of the affected asset.</td>
</tr>
<tr>
<td>asset_type</td>
<td>Y</td>
<td>The type of the asset affected; for example: <strong>user, ami, instance, policy, virtual machine, security_group, server</strong>, and so on.</td>
</tr>
<tr>
<td>asset_name</td>
<td>Y</td>
<td>The Halo display name of the affected asset; for example, <strong>server-1</strong>.</td>
</tr>
<tr>
<td>group_id</td>
<td>Y</td>
<td>The Halo ID of the group to which the asset belongs.</td>
</tr>
<tr>
<td>group_name</td>
<td>Y</td>
<td>The Halo display name of the group to which the asset belongs; for example, <strong>Docker Hosts</strong>.</td>
</tr>
<tr>
<td>group_path</td>
<td>Y</td>
<td>The uniform resource locator path of the group to which the asset belongs.</td>
</tr>
<tr>
<td>resolved_at</td>
<td>Y</td>
<td>The date-time (in ISO 8601 format) when the issue was marked as resolved in the Halo issues service. The value is <strong>null</strong> for active issues.</td>
</tr>
<tr>
<td>resolved_by</td>
<td>N</td>
<td>The username of the Halo user who resolved the issue. If the issue was resolved automatically, the value of this field is <strong>system</strong>. If the issue is not yet resolved, the value is <strong>null</strong>.</td>
</tr>
<tr>
<td>resolution_comment</td>
<td>N</td>
<td>The reason the issue was marked as resolved.</td>
</tr>
<tr>
<td>time_to_resolution</td>
<td>N</td>
<td>The amount of time it took for the issue to be resolved by Halo after it was first detected.</td>
</tr>
<tr>
<td>csp_account_id</td>
<td>Y</td>
<td>The UUID of the AWS account or Azure subscription; for example: 856192027328.</td>
</tr>
<tr>
<td>csp_account_type</td>
<td>Y</td>
<td>The type of cloud service provider; that is, <strong>AWS</strong> or <strong>Azure</strong>.</td>
</tr>
<tr>
<td>csp_account_name</td>
<td>Y</td>
<td>For Cloud Secure customers. The Halo display name of the cloud service provider account.</td>
</tr>
<tr>
<td>csp_region</td>
<td>Y</td>
<td>The region in which the cloud service provider account exists; for example, <strong>eastus</strong>.</td>
</tr>
<tr>
<td>csp_service_type</td>
<td>Y</td>
<td>For Cloud Secure customers. The type of cloud service; for example, <strong>IAM, S3, EC2</strong>, and so on.</td>
</tr>
<tr>
<td>csp_resource_id</td>
<td>Y</td>
<td>The ID of the cloud resource in the CSP account. Value may be <strong>null</strong>.</td>
</tr>
<tr>
<td>csp_tags</td>
<td>Y</td>
<td>The key-value pairs used to identify and/or categorize the asset in the CSP account. <strong>Note:</strong> If a change is made to CSP tags in the IaaS platform, it will not be available until after the asset is scanned again.</td>
</tr>
<tr>
<td>csp_resource_uri</td>
<td>Y</td>
<td>For Cloud Secure customers. The uniform resource identifier of the asset in the CSP account.</td>
</tr>
<tr>
<td>csp_image_id</td>
<td>Y</td>
<td>For Server Secure customers. The machine image from which an instance/vm was created.</td>
</tr>
<tr>
<td>package_name</td>
<td>N</td>
<td>For SVA issues, the name of the vulnerable software package.</td>
</tr>
<tr>
<td>package_version</td>
<td>N</td>
<td>For SVA issues, the version of the vulnerable software package.</td>
</tr>
<tr>
<td>cve_ids</td>
<td>Y</td>
<td>For SVA issues, the list of CVEs affecting the package. <strong>Note:</strong> When you search on a single CVE, use cve_id.</td>
</tr>
<tr>
<td>max_cvss</td>
<td>Y</td>
<td>For SVA issues, the maximum CVSS score of all CVEs found for the package.</td>
</tr>
<tr>
<td>remotely_exploitable</td>
<td>Y</td>
<td>For SVA issues, whether any of the CVEs affecting the package are remotely exploitable.</td>
</tr>
</tbody>
</table>
List all Active Issues

Retrieves all active issues in your Halo account. By default, the method returns all active issues if a status is not specified.

```
GET https://api.cloudpassage.com/v3/issues/
```

Because the above call returns all active issues in your Halo account, we recommend that you use filters to narrow down your results. See Filtering issues for instructions and examples. See also Sorting and grouping results and Pagination of Results for information about how to work with your results.

Response

**Status: 200**

```
{
  "issues": [
    {
      "id": "7642abdb-d40c-11e9-9ea5-0242ac110007",
      "url": "https://api.cloudpassage.com/v3/issues/7642abdb-d40c-11e9-9ea5-0242ac110007",
      "name": "AWS EC2 Instance Naming Conventions",
      "type": "csm",
      "status": "active",
      "critical": true,
      "source": "cloud secure",
      "created_at": "2019-09-10T20:49:20.030638Z",
      "updated_at": "2019-09-11T10:33:25.019243Z",
      "first_seen_at": "2019-09-10T20:49:20.000027Z",
      "last_seen_at": "2019-09-11T10:33:25.000014Z",
      "policy_id": "56a5918e-bcfa-11e9-9a08-3db3c8ca5fc8",
      "policy_name": "CloudPassage AWS EC2 Best Practices v1.0 2019-08-12 12:11:39-Copy",
      "cp_rule_id": "CP:EC2:12",
      "csp_rule_id": "CP:EC2:12",
      "rule_id": "56d507b6-bcfa-11e9-9a08-3db3c8ca5fc8",
      "rule_name": "AWS EC2 Instance Naming Conventions",
      "last_finding_urls": [
        "https://api.cloudpassage.com/v1/csp_findings/96d6979f-2dfc-4db4-b90f-e...
      ],
      "extended_attributes": {},
      "asset_id": "9c226eaa-a050-44b1-af19-a1541e2b6b1d",
      "asset_url": "https://api.cloudpassage.com/v1/csp_resources/9c226eaa-a050-44b1-af19-a1541e2b6b1d",
      "asset_type": "instance",
      "asset_name": "ris-win2008r2-policy-test",
      "group_id": "80112640-d40c-11e9-81c4-2535d26e72cf",
      "group_name": "aws-account",
      "group_path": "CloudPassage/aws-account",
      "csp_account_id": "849489318606",
      "csp_account_type": "aws",
      "csp_account_name": "cloudpassage-qa",
      "csp_region": "ap-south-1",
      "csp_service_type": "ec2",
      "csp_resource_id": "i-0f015ea6a4f742fd8"
    }
  ]
```
Filter Issues

You can filter the v3/issues endpoint by formulating a call that includes filter attributes. Refer to the Searchable column in the Object Representation table to determine which object fields can be used as filter attributes. The result is a response that retrieves all issues for the particular class of attributes you specified. You can see an example of the response in List all active issues.

Note: For any of the filters, you can provide either a single value or a comma-separated list of values. If you do provide multiple values, they are OR'd in a search, meaning that the search passes for that filter if any of its supplied values match.

Examples of common filters:

<table>
<thead>
<tr>
<th>Find issues by</th>
<th>Call</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created in last 24 hrs</td>
<td>GET <a href="https://api.cloudpassage.com/v3/issues?created_at_gte=2019-09-08&amp;created_at_lte=2019-09-09">https://api.cloudpassage.com/v3/issues?created_at_gte=2019-09-08&amp;created_at_lte=2019-09-09</a></td>
</tr>
<tr>
<td>CVE that is remotely exploitable</td>
<td>GET <a href="https://api.cloudpassage.com/v3/issues?remotely_exploitable=true">https://api.cloudpassage.com/v3/issues?remotely_exploitable=true</a></td>
</tr>
<tr>
<td>Halo group</td>
<td>GET <a href="https://api.cloudpassage.com/v3/issues?group_id=dd40c2f8-6d38-11e8-a66a-2b6deccf7d71">https://api.cloudpassage.com/v3/issues?group_id=dd40c2f8-6d38-11e8-a66a-2b6deccf7d71</a></td>
</tr>
<tr>
<td>Policy rule</td>
<td>GET <a href="https://api.cloudpassage.com/v3/issues?rule_id=8f8fb10b14521e8a74421f47e52225c">https://api.cloudpassage.com/v3/issues?rule_id=8f8fb10b14521e8a74421f47e52225c</a></td>
</tr>
<tr>
<td>Type</td>
<td>GET <a href="https://api.cloudpassage.com/v3/issues?type=sva">https://api.cloudpassage.com/v3/issues?type=sva</a></td>
</tr>
</tbody>
</table>

Note: All of the above method calls support several optional parameters that can sort and group your results. For more information, see Sorting and grouping results.

Sorting and grouping results

When you make API calls that return a list of issues, you can apply any of the parameters listed in this section to sort and group the results based on individual values of certain object fields.

Sorting results

By default, results are sorted in ascending order by created_date. You can use the sort_by parameter to specify that the search results are to be alphanumerically sorted (in either ascending or descending order, using the .asc and .desc filter suffixes) according to the value of the object fields listed below.

This example sorts by asset type in descending order:

You can sort by:

- asset_type
- critical
- group_id
- image_sha
- name
- os_type
- policy_name
- repository_id
- repository_name
- status
- type

**Grouping results**

You can also use the `group_by` parameter to group results according to the value of the object fields listed below. When you use the `group_by` parameter, the call does not return complete issue objects; instead, it lists a count of issue objects that fit into your request. You can use the call to show, for example, how many similar issues exist across all of your groups.

You can group by:

- asset_id
- asset_type
- critical
- group_id
- image_sha
- name
- os_type
- policy_name
- registry_id
- repository_id
- repository_name
- status
- type

For example, the following call groups results by status and asset type:

GET https://api.cloudpassage.com/v3/issues?status=active&status=resolved&group_by=status,asset_type

The response will be grouped by asset type and status, along with a count of the issues that meet the criteria:
Get a Specific Issue

Retrieves details about a specific issue, which is specified by issue ID in the request URL. The details include a link to the scan findings that led to the creation of the issue.

**GET** https://api.cloudpassage.com/v3/issues/{id}

**Response**

**Status: 200**

{ 
  "issue": {
    "id": "08084354-ba9e-11e9-b9f9-0d426754a8d5",
    "url": "https://api.cloudpassage.com/v3/issues/08084354-ba9e-11e9-b9f9-0d426754a8d5",
    "name": "util-linux",
    "type": "sva",
    "status": "active",
    "critical": true,
    "source": "container_secure",
    "created_at": "2019-08-09T12:05:51.390185Z",
    "updated_at": "2019-08-09T12:05:51.390185Z",
    "first_seen_at": "2019-08-09T12:05:51.388906Z",
    "last_seen_at": "2019-08-09T12:05:51.388906Z",
    "extended_attributes": {
      "cve_info": [
        {
          "id": "CVE-2016-2779",
          "score": 7.2
        },
        {
          "id": "CVE-2016-5011",
          "score": 0
        },
        {
          "id": "CVE-2017-2616",
          "score": 4.7
        }
      ]
    }
  },
  "asset_id": "d3c59855-b52b-452e-be66-8032732f8efa",
  "asset_url": "https://api.cloudpassage.com/v1/images/d3c59855-b52b-452e-be66-8032732f8efa",
  "asset_type": "container_image",
  "asset_name": "new-hotfix-1:xenial",
  "group_id": "cdbca790-ba6f-11e9-bd0d-05db4973d6d",
  "group_name": "CloudPassage",
  "group_path": "CloudPassage",
  "package_name": "util-linux",
  "package_version": "2.27.1-6ubuntu3.6",
  "cve_ids": [
    "CVE-2016-2779",
    "CVE-2016-5011",
    "CVE-2017-2616"
  ]
}
Resolve a Specific Issue

You can use the Issues API endpoint to manually resolve active issues.

If you have remediated an issue, Halo will (except in the case of LIDS and some SAM issues) automatically mark the issue as resolved when the next scan of that server does not report the finding that caused the issue to be created. However, you can also use the Halo portal or the Halo API to manually mark an issue as resolved.

To resolve an issue through the API, make the following PUT call, passing the issue ID in the URL and passing the new value for the status field as JSON in the request body.

PUT https://api.cloudpassage.com/v3/issues/{issue_id}

Request Body

```json
{
  "status": "resolved",
  "resolution_comment": "Resolved issue by replacing the file",
}
```

Should you ever need to manually reactivate a resolved issue, make the same call but set the status value to active in the request JSON.

Response

Status: 204
**Configuration Policies**

Use the Configuration Policies endpoint to retrieve core information and details about all defined configuration policies (used in configuration security monitoring scans), and to create or delete a policy. To assign a policy to a group, call **Assign several configuration policies to a group** in the Server Groups API endpoint.

*Note:* You can use the API to launch a configuration scan of an individual server. See **Launch scan of a server** in the Server Scans API endpoint for details.

- **Object Representation**
- **List configuration policies**
- **Get configuration policy details**
- **Create a new configuration policy**
- **Delete a configuration policy**
- **Update a configuration policy**
- **Defined Configuration Checks**

---

**Object Representation**

**Configuration policy object location**

```plaintext
gapi.cloudpassage.com/v1
  policies
    id
```

**Configuration policy object fields**

Two levels of configuration-policy information are available: core policy fields (accessed through, for example, the **List configuration policies** call), and policy detail fields (accessed through, for example, the **Get configuration policy details** call).

**Core configuration policy fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>A name given to the configuration policy.</td>
</tr>
<tr>
<td>description</td>
<td>A description of the configuration policy.</td>
</tr>
<tr>
<td>module</td>
<td>The Halo security module that uses this policy. For configuration security policies, this value is <code>csm</code>.</td>
</tr>
<tr>
<td>platform</td>
<td>The OS platform of the configuration policy. Either <code>windows</code> or <code>linux</code>. Default = <code>linux</code>.</td>
</tr>
<tr>
<td>template</td>
<td><code>true</code> if this policy is a policy template; otherwise, false.</td>
</tr>
<tr>
<td>group_id</td>
<td>The Halo ID of the group that owns this policy.</td>
</tr>
<tr>
<td>group_name</td>
<td>The name of the group that owns this policy.</td>
</tr>
<tr>
<td>created_by</td>
<td>The Halo username of the user who created this policy.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>rules</td>
<td>A list of the rules in the policy. Each rule includes the following sub-fields:</td>
</tr>
<tr>
<td>active</td>
<td>true if the rule is active; false if it is inactive (not used by the policy).</td>
</tr>
<tr>
<td>alert</td>
<td>true if failure of the rule generates an email alert; false if not.</td>
</tr>
<tr>
<td>comment</td>
<td>An optional comment or description for the rule.</td>
</tr>
<tr>
<td>critical</td>
<td>true if an event logged by the failure of the rule should be classified as critical; false if not.</td>
</tr>
<tr>
<td>rule_operator</td>
<td>AND if all checks in the rule must pass for the rule to pass; OR if the rule will pass if any of its checks passes.</td>
</tr>
<tr>
<td>log</td>
<td>true if failure of the rule is logged as an event; false if not.</td>
</tr>
<tr>
<td>name</td>
<td>A name for the rule.</td>
</tr>
<tr>
<td>taxonomy</td>
<td>The general category of the rule (from the Edit Configuration Policy page of the Halo Portal), such as system_configuration or other.</td>
</tr>
<tr>
<td>checks</td>
<td>A list of the checks used in this rule. Each check includes the appropriate sub-fields for its definition. See the Configuration Rule Checks appendix of the Configuration Security Monitoring Setup Guide for descriptions of each check's specific fields. Also, the following fields are returned for all checks:</td>
</tr>
<tr>
<td>object_type</td>
<td>The name of the check, as documented in the Configuration Rule Checks appendix.</td>
</tr>
<tr>
<td>active</td>
<td>true if the check is active; false if it is inactive (not used by the rule).</td>
</tr>
<tr>
<td>exportable</td>
<td>true if the check is API-exportable (its failures are to be included in the results returned by the List issues for an individual server method of the API); false if not.</td>
</tr>
<tr>
<td>suggestion</td>
<td>An optional remediation suggestion for failures of this check.</td>
</tr>
<tr>
<td>reference_identifiers</td>
<td>An optional comma-separated list of IDs applied to this rule for compliance purposes. Each identifier is a name-value pair with this JSON format: {&quot;name&quot;:&quot;value&quot;} — for example, {&quot;USB&quot;:&quot;67&quot;},{&quot;CIS&quot;:&quot;1.1.2&quot;}</td>
</tr>
</tbody>
</table>

### List configuration policies

Returns a list of defined configuration policies, with summary information for each policy.

*Note:* The results of this call may be paginated. See [Pagination of Results](#) for information on how to set up and retrieve paginated results from the Halo API.

**GET https://api.cloudpassage.com/v1/policies**

You can use this call to, for example, obtain the ID of an individual policy so that you can view or manipulate it by calling any of the other methods described here.

You can add parameters to the call to filter the results by the values of individual fields. For example:
GET https://api.cloudpassage.com/v1/policies?platform=windows
GET https://api.cloudpassage.com/v1/policies?template=true
GET https://api.cloudpassage.com/v1/policies?retired=true
GET https://api.cloudpassage.com/v1/policies?name={policy name} (partial name matches are supported)

Response
Status: 200

```json
{
  "count": 193,
  "policies": [
    {
      "name": "CSM Linux policy-2790",
      "description": "API based Linux CSM policy",
      "module": "csm",
      "platform": "linux",
      "template": false,
      "group_id": "0962bfa087bc01323e360670140ec224",
      "group_name": "NW-functional",
      "created_by": "ui_automation",
      "updated_by": "ui_automation",
      "created_at": "2016-03-31T05:20:11.345Z",
      "updated_at": "2016-03-31T05:20:11.767Z",
      "url": "https://NW.cloudpassage.com/v1/policies/3dcb3e52f70011e59c1f57970d44218e",
      "id": "3dcb3e52f70011e59c1f57970d44218e",
      "shared": false,
      "retired": false,
      "used_by": []
    },
    {
      "name": "CSM Linux policy-3100",
      "description": "API based Linux CSM policy",
      "module": "csm",
      "platform": "linux",
      "template": false,
      "group_id": "0962bfa087bc01323e360670140ec224",
      "group_name": "SW-functional",
      "created_by": "ui_automation",
      "updated_by": "ui_automation",
      "created_at": "2016-03-31T05:20:12.656Z",
      "updated_at": "2016-03-31T05:20:12.983Z",
      "url": "https://api.cloudpassage.com/v1/policies/3e934bfef70011e59c1f57970d44218e",
      "id": "3e934bfef70011e59c1f57970d44218e",
      "shared": false,
      "retired": false,
      "used_by": []
    },
    ...
    {
      "name": "windows_csm-database",
      "description": "",
      "module": "csm",
      "platform": "windows",
      "template": false,
      "group_id": "0962bfa087bc01323e360670140ec224",
      "group_name": "SW-functional",
      "created_by": "autobot15@acme.com",
      "updated_by": "autobot15@acme.com",
      "created_at": "2016-03-30T16:26:50.019Z",
      "updated_at": "2016-03-30T21:32:04.562Z",
      "url": "https://api.cloudpassage.com/v1/policies/3472d8eaf69411e55b54533e7d3c8057d",
      "id": "3472d8eaf69411e55b54533e7d3c8057d",
      "shared": false,
      "retired": false,
      "used_by": []
    }
  ]
}```
Get configuration policy details

Returns detailed information—including all policy rules and all configuration checks—for the configuration policy specified by ID in the call URL.

GET https://api.cloudpassage.com/v1/policies/{policy_id}

Response

Status: 200

```
{
  "policy": {
    "name": "windows_csm-database",
    "description": "",
    "module": "csm",
    "platform": "windows",
    "template": false,
    "group_id": "0962bfa087bc01323e360670140ec224",
    "group_name": "SW-functional",
    "created_by": "autobot15@acme.com",
    "updated_by": "ehhedstrom3@acme.com",
    "created_at": "2016-03-30T16:26:50.019Z",
    "updated_at": "2016-04-01T11:32:04.562Z",
    "url": "https://api.cloudpassage.com/v1/policies/3472d8eaf69411e5b54533e7d3c8057d",
    "id": "3472d8eaf69411e5b54533e7d3c8057d",
    "shared": false,
    "retired": false,
    "used_by": [],
    "rules": []
  }
}
```

Create a new configuration policy

Creates a new configuration policy with the initial values and rules specified in the request body. The minimum required fields to supply are name and module.

If you do not specify a platform attribute or if you specify linux, a Linux configuration policy is created. To create a Windows policy, you must specify windows for the platform attribute.

To create rules and rule checks, supply the request JSON in the format as shown below. See Defined Configuration Checks for a complete list of all supported check names (object_type values) and the defined fields (attribute values) for each one.

If the call is successful, the response body contains the created policy in JSON format.
POST https://api.cloudpassage.com/v1/policies/

Request Body

```
{
  "policy": {
    "name": "Configuration Settings",
    "description": "Verifies important limits and restrictions",
    "platform": "linux",
    "rules": [
      { "active": true, "alert": false, "comment": "", "critical": false, "log": false, "name": "System settings", "taxonomy": "system_configuration", "checks": [
        { "object_type": "configuration_file_setting", "active": true, "exportable": true, "suggestion": "restore proper value", "config_file_path": "/etc/php5/apache2/php.ini", "config_file_section": "", "config_item": "post_max_size", "desired_value": "1K", "comment_character": "", "delimiter": "=" }, { "object_type": "file_presence", "active": true, "exportable": true, "suggestion": "investigate file removal", "files": "/home/ccruz/.profile", "present": true }
      ]
    }
  }
}
```

Response

Status: 201
Location: https://api.cloudpassage.com/v1/firewall_policies/812b7500b27b012ec6c4404096c01709

```
{
  "policy": {
    "name": "Configuration Settings",
    "description": "Verifies important limits and restrictions",
    "platform": "linux",
    "url": "https://api.cloudpassage.com/v1/policies/b095e280ecd5013095ba3c764e10b50e",
    "id": "b095e280ecd5013095ba3c764e10b50e",
    "used_by": [],
    "rules": [
      { "active": true, "alert": false, "comment": "", "critical": false, "log": false, "name": "System settings", "taxonomy": "system_configuration",
      ... }
    ]
  }
}
```
Delete a configuration policy

Completely removes from Halo the record of the configuration policy specified by Halo policy ID.

DELETE https://api.cloudpassage.com/v1/policies/{policy_id}

Response

Status: 204

Update a configuration policy

Updating an existing configuration policy through the Halo API involves obtaining the policy in JSON format, modifying the JSON as needed, and making a PUT request to upload the modified policy back to the API. Follow these steps:

1. Determine the ID of the policy that you want to update, perhaps by calling the List configuration policies method:

   GET https://api.cloudpassage.com/v1/policies?name={policy name}

   where {policy_name} can be a full or partial policy name.

2. Pass the policy's ID in the Get configuration policy details method to retrieve the policy in JSON format.

3. Modify the policy JSON as desired. Do not change the policy's ID or URL.

4. To upload the updated policy, make this PUT request to the API, with your modified JSON object in the request body.

   PUT https://api.cloudpassage.com/v1/policies/

   IMPORTANT: Unlike with some PUT requests to the Halo API, you must include the entire policy JSON in the request body. The JSON you upload will completely replace the contents of the existing policy.

Request Body

```json
{
   "policy": {
      "name": "Windows configuration policy",
      "description": "Basic default windows checks",
      "platform": "windows",
      "url": "https://api.cloudpassage.com/v1/policies/ae22b360ecd5013095ba3c764e10b50e",
      "id": "ae22b360ecd5013095ba3c764e10b50e",
      "used_by": [],
      "rules": [
         {
            "active": true,
            "alert": true,
            "comment": null,
            "critical": true,
            "log": false,
            "name": "system-level checks",
            "taxonomy": "system_configuration",
            "checks": [
               {
                  "object_type": "file_presence",
                  "active": true,
                  "exportable": true,
                  "suggestion": "Replace file if missing",
                  "files": "C:\Windows\System32\wininit.exe",
                  "present": true
               },
               {
                  "object_type": "registry_key_value_setting",
                  "active": true,
                  "exportable": true,
                  "suggestion": "",
                  "registry_key": "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer",
```
Response
Status: 204

Defined Configuration Checks

The following tables list the API identifiers for the defined configuration rule checks for Linux and Windows, as well as the identifiers for all defined fields—both optional and required—in each check. Use the spellings here to specify checks and fields in the request JSON that you construct when creating a policy through the API.

Linux checks

<table>
<thead>
<tr>
<th>Object type (= check name)</th>
<th>Attribute values (= defined fields)</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration_file_setting</td>
<td>active, comment_character, config_file_path, config_file_section, config_item, delimiter, desired_value, exportable, suggestion</td>
</tr>
<tr>
<td>directory_acl</td>
<td>acls, active, exportable, files, suggestion</td>
</tr>
<tr>
<td>directory_group_ownership</td>
<td>active, exportable, files, owned_by, suggestion</td>
</tr>
<tr>
<td>directory_presence</td>
<td>active, exportable, folders, present, suggestion</td>
</tr>
<tr>
<td>directory_user_ownership</td>
<td>active, exportable, folders, owned_by, suggestion</td>
</tr>
<tr>
<td>file_acl</td>
<td>acls, active, exportable, files, suggestion</td>
</tr>
<tr>
<td>file_group_ownership</td>
<td>active, exportable, files, owned_by, suggestion</td>
</tr>
<tr>
<td>file_presence</td>
<td>active, exportable, files, present, suggestion</td>
</tr>
<tr>
<td>file_setgid</td>
<td>active, exportable, files, setgid, suggestion</td>
</tr>
<tr>
<td>file_setuid</td>
<td>active, exportable, files, setuid, suggestion</td>
</tr>
<tr>
<td>file_string_presence</td>
<td>active, exportable, files, patterns, present, suggestion</td>
</tr>
<tr>
<td>file_user_ownership</td>
<td>active, exportable, files, owned_by, suggestion</td>
</tr>
<tr>
<td>geolocation_by_country</td>
<td>active, allowed, countries, exportable, suggestion</td>
</tr>
<tr>
<td>group_gid</td>
<td>active, exportable, gid, group, suggestion</td>
</tr>
<tr>
<td>group_has_password</td>
<td>active, exportable, groups, suggestion</td>
</tr>
<tr>
<td>group_members</td>
<td>active, exportable, group, suggestion, users</td>
</tr>
<tr>
<td>home_directory_exists</td>
<td>active, exportable, suggestion, users</td>
</tr>
<tr>
<td>home_directory_file_presence</td>
<td>active, exportable, files, present, suggestion, users</td>
</tr>
<tr>
<td>home_directory_files_have_no_invalid_umask_commands</td>
<td>active, exportable, files, suggestion, umask, users</td>
</tr>
<tr>
<td>home_directory_files_have_no_unsafe_path_statements</td>
<td>active, exportable, files, suggestion, users</td>
</tr>
<tr>
<td><strong>Object type</strong></td>
<td><strong>Attribute values ( = defined fields)</strong></td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>home_directory_files_owned_by_correct_group</td>
<td>active, exportable, suggestion, users</td>
</tr>
<tr>
<td>home_directory_files_owned_by_correct_user</td>
<td>active, exportable, suggestion, users</td>
</tr>
<tr>
<td>home_directory_has_no_device_files</td>
<td>active, exportable, suggestion, users</td>
</tr>
<tr>
<td>home_directory_has_no_setgid_files</td>
<td>active, exportable, suggestion, users</td>
</tr>
<tr>
<td>home_directory_has_no_setuid_files</td>
<td>active, exportable, suggestion, users</td>
</tr>
<tr>
<td>home_directory_owned_by_correct_group</td>
<td>active, exportable, suggestion, users</td>
</tr>
<tr>
<td>home_directory_owned_by_correct_user</td>
<td>active, exportable, suggestion, users</td>
</tr>
<tr>
<td>mount_point</td>
<td>active, exportable, mount_point, mounted, target, suggestion</td>
</tr>
<tr>
<td>network_service_accessibility</td>
<td>active, exportable, interfaces, ports, suggestion</td>
</tr>
<tr>
<td>network_service_processes</td>
<td>active, exportable, interface_port, process, suggestion</td>
</tr>
<tr>
<td>no_recent_account_login</td>
<td>active, days, exportable, suggestion, users</td>
</tr>
<tr>
<td>password_does_not_match_user_name</td>
<td>active, exportable, suggestion, users</td>
</tr>
<tr>
<td>password_is_not_expired</td>
<td>active, exportable, suggestion, users</td>
</tr>
<tr>
<td>process_group_ownership</td>
<td>active, exportable, owned_by, processes, suggestion</td>
</tr>
<tr>
<td>process_presence</td>
<td>active, exportable, process, present, suggestion</td>
</tr>
<tr>
<td>process_user_ownership</td>
<td>active, exportable, owned_by, processes, suggestion</td>
</tr>
<tr>
<td>recent_account_login</td>
<td>active, days, exportable, suggestion, users</td>
</tr>
<tr>
<td>user_account_uid</td>
<td>active, exportable, suggestion, uid, user</td>
</tr>
<tr>
<td>user_group_membership</td>
<td>active, exportable, groups, suggestion, user</td>
</tr>
<tr>
<td>user_has_password</td>
<td>active, exportable, suggestion, users</td>
</tr>
<tr>
<td>world_writable_directories_have_sticky_bit_set</td>
<td>active, exclude_directories, exportable, suggestion</td>
</tr>
</tbody>
</table>

**Windows checks**

<table>
<thead>
<tr>
<th><strong>Object type ( = check name)</strong></th>
<th><strong>Attribute values ( = defined fields)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>advanced_audit_policy_setting</td>
<td>active, audit_subcategory, desired_value, exportable, suggestion</td>
</tr>
<tr>
<td>directory_presence</td>
<td>active, exportable, folders, present, suggestion</td>
</tr>
<tr>
<td>file_presence</td>
<td>active, exportable, files, present, suggestion</td>
</tr>
<tr>
<td>geolocation_by_country</td>
<td>active, allowed, countries, exportable, suggestion</td>
</tr>
<tr>
<td>local_security_policy_settings</td>
<td>active, desired_value, exportable, setting, suggestion</td>
</tr>
<tr>
<td>local_user_rights_assignment</td>
<td>active, desired_value, exportable, setting, suggestion</td>
</tr>
<tr>
<td>process_presence</td>
<td>active, desired_value, exportable, processes, present, ok, suggestion</td>
</tr>
<tr>
<td>registry_key_value_setting</td>
<td>active, expected_data, exportable, registry_key, suggestion, value_name</td>
</tr>
<tr>
<td>service_started</td>
<td>active, exportable, services, started, suggestion</td>
</tr>
</tbody>
</table>
File Integrity Policies

Use the File Integrity Policies endpoint to create and manage the policies that define your file integrity monitoring implementation. You can use the API to list policies, get the details of a policy (including its rules and exclusions), and create, update, or delete policies.

Note: You can also use the API to launch a file integrity scan of an individual server. See Launch scan of a server in the Server Scans API endpoint for details.

File integrity policies have associated baselines. To manipulate baselines through the CloudPassage API, use the File Integrity Baselines API endpoint.

- Object Representation
- List File Integrity policies
- Get a single File Integrity policy
- Create a new File Integrity policy
- Update a File Integrity policy
- Delete a File Integrity policy

Object Representation

File integrity policy object location

api.cloudpassage.com/v1

├── fim_policies

└── id

File integrity policy object fields

This endpoint expresses a file integrity policy with three kinds of objects. The policy object contains general information about the policy and includes an array of rule objects. The rule object contains all information about a single rule, and may include an array of exclusion or inclusion objects. The exclusion/exclusion object contains a filename or wildcard string specifying a file or class of files that should (or should not) be scanned.

Policy fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique identifier for the policy</td>
</tr>
<tr>
<td>name</td>
<td>The name of the policy</td>
</tr>
<tr>
<td>description</td>
<td>The description given to the policy</td>
</tr>
<tr>
<td>platform</td>
<td>The OS platform of the policy (linux or windows)</td>
</tr>
<tr>
<td>template</td>
<td>true if this policy is a policy template, false if not</td>
</tr>
<tr>
<td>url</td>
<td>The URL of the policy object</td>
</tr>
<tr>
<td>active</td>
<td>true if this policy has at least one active baseline, false if not</td>
</tr>
</tbody>
</table>
rules An array of rules that make up the policy

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>The path or wildcard for monitoring</td>
</tr>
<tr>
<td>description</td>
<td>The description of this rule</td>
</tr>
<tr>
<td>active</td>
<td><em>true</em> if this rule is active, <em>false</em> if it is inactive (deactivated)</td>
</tr>
<tr>
<td>recurse</td>
<td><em>true</em> if Halo should recursively scan all subdirectories of this target</td>
</tr>
<tr>
<td>critical</td>
<td><em>true</em> if this rule should be marked as critical</td>
</tr>
<tr>
<td>alert</td>
<td><em>true</em> if this rule should generate an alert when matched</td>
</tr>
<tr>
<td>patterns</td>
<td>An array of files or wildcards to include or exclude from monitoring (see below)</td>
</tr>
<tr>
<td>reference_identifiers</td>
<td>A comma-separated list of IDs used to mark this rule for compliance purposes. Each identifier is a name-value pair with this JSON format: {&quot;name&quot;: &quot;value&quot;} — for example, {&quot;USB&quot;: &quot;67&quot;}, {&quot;CIS&quot;: &quot;1.1.2&quot;}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pattern</td>
<td>The file or wildcard for including or excluding from the rule's target</td>
</tr>
<tr>
<td>description</td>
<td>The description for this pattern</td>
</tr>
<tr>
<td>inclusion</td>
<td><em>true</em> if the pattern is an inclusion, <em>false</em> if it is an exclusion</td>
</tr>
</tbody>
</table>

List file integrity policies

Returns a list of all defined file integrity policies. Includes the details of all rules and exclusions in each policy.

*Note*: The results of this call may be paginated. See [Pagination of Results](#) for information on how to set up and retrieve paginated results from the Halo API.

**GET** https://api.cloudpassage.com/v1/fim_policies

You can use this call to, for example, obtain the ID of an individual policy so that you can view or manipulate it by calling any of the other methods described here.

You can add parameters to the call to filter the results by the values of individual fields. For example:

**GET** https://api.cloudpassage.com/v1/fim_policies?platform=windows

**GET** https://api.cloudpassage.com/v1/fim_policies?template=true

**GET** https://api.cloudpassage.com/v1/fim_policies?retired=true

Response

**Status: 200**

```json
{
  "fim_policies": [{
    "id": "78eb8ea0053442c031a719c501307981",
    "url": "https://api.cloudpassage.com/v1/fim_policies/78eb8ea0053442c031a719c501307981",
    "name": "My FIM Policy",
    "platform": "linux",
    "rules": [{
      "target": "/var/www",
    }]
  }]
}
Get a single file integrity policy

Returns the details of the file integrity policy specified by policy ID. Includes the details of all rules and exclusions in the policy.

**GET** https://api.cloudpassage.com/v1/fim_policies/{id}

**Response**

**Status:** 200

```json
{
  "fim_policy": {
    "id": "78eb8ea0053442c031a719c501307981",
    "url": "https://api.cloudpassage.com/v1/fim_policies/78eb8ea0053442c031a719c501307981",
    "name": "My Linux FIM Policy",
    "description": "This is my Linux FIM policy",
    "platform": "linux",
    "rules": [{
      "target": "/var/www",
      "description": "web files",
      "recurse": false,
      "critical": true,
      "alert": true
    },
    {"target": "/etc",
     "description": "etc files",
     "recurse": true,
     "critical": false,
     "alert": false,
     "patterns": [{
       "pattern": "nginx.conf",
       "description": "Changes too much",
       "include": false
     }]
    }]
  }
}
```
Create a new file integrity policy

Creates a new file integrity policy with the attributes specified in the request body. The request can include rules and exclusions. Returns the created policy details, including its policy ID, in the response body.

**POST** https://api.cloudpassage.com/v1/fim_policies

**Request Body**

```
{
  "fim_policy": {
    "name": "My new policy",
    "description": "Something about policy",
    "platform": "linux",
    "rules": [{
      "target": "/etc",
      "description": "All etc files",
      "recurse": true,
      "patterns": [{
        "pattern": "hosts",
        "description": "Ignore the hosts file",
        "inclusion": false},
      {"pattern": "*.conf",
        "description": "all conf files",
        "inclusion": true
      }]
    }]
  }
}
```

**Response**

```
{
  "fim_policy": {
    "id": "2343sh34h23254543543hgf5",
    "url": "https://api.cloudpassage.com/v1/fim_policies/2343sh34h23254543543hgf5",
    "name": "My new policy",
    "description": "Something about policy",
    "platform": "linux",
    "rules": [{
      "target": "/etc",
      "description": "All etc files",
      "recurse": true,
      "critical": false,
      "alert": false,
      "patterns": [{
        "pattern": "hosts",
        "description": "Ignore the hosts file",
        "inclusion": false},
      {"pattern": "*.conf",
        "description": "all conf files",
        "inclusion": true
      }]
    }]
  }
}
```

Update a file integrity policy

For the existing file integrity policy specified by ID in the call URL, updates the values of the attributes specified in the request body.

*Important:* If the request body includes any rules, those rules will replace all existing rules in the policy.
PUT https://api.cloudpassage.com/v1/fim_policies/{id}

Request Body

```json
{
  "fim_policy": {
    "name": "New policy name",
    "rules": [{
      "target": "/var/lib",
      "description": "watch lib files instead",
      "recurse": true,
      "critical": false,
      "alert": false
    }]
  }
}
```

Response

Status: 204

Delete a file integrity policy

Deletes the file integrity policy specified by policy ID. If the call is successful, the policy is removed from Halo and cannot be retrieved.

DELETE https://api.cloudpassage.com/v1/fim_policies/{id}

Response

Status: 204
File Integrity Baselines

Use the File Integrity Baselines endpoint to manage the baselines associated with file integrity policies. You can use the API to list all of a policy's baselines, get the details of a baseline, and create, update, or delete a baseline.

For this API endpoint, a "baseline" is defined as the results of a file integrity scan on a file integrity policy's baseline server. Updating a baseline (or "re-baselining") means re-running the scan on the same server. When a baseline expires, it is no longer valid and cannot be used in scans; updating the baseline will restore its validity. Deleting a baseline means deleting the results of a particular baseline scan; it does not mean removing or changing a baseline server.

- Object Representation
- List all baselines for a file integrity policy
- Get a single baseline
- Show baseline details
- Create a new baseline
- Update/Request a re-baseline
- Delete a file integrity baseline

Object Representation

File integrity baseline object location

```
api.cloudpassage.com/v1
├── fim_policies
│   └── policy_id
│       └── baselines
│               └── id
```

File integrity baseline object fields

Two levels of file integrity baseline information are available: core baseline fields (accessed through, for example, the List all baselines for a file integrity policy call), and baseline detail fields (accessed through the Show baseline details call).

Core file integrity baseline fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique identifier for the baseline.</td>
</tr>
<tr>
<td>url</td>
<td>The API URL to the baseline object.</td>
</tr>
<tr>
<td>server_id</td>
<td>The id of the server used for the baseline.</td>
</tr>
<tr>
<td>comment</td>
<td>Any comments associated with the baseline.</td>
</tr>
<tr>
<td>status</td>
<td>The current status of the baseline, for example Pending, Active, Expired, or Invalid.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>effective_at</td>
<td>When the baseline takes effect.</td>
</tr>
<tr>
<td>expires_at</td>
<td>When the baseline will expire (or null if there is no expiration).</td>
</tr>
<tr>
<td>policy_name</td>
<td>The name of the file integrity policy that this baseline is assigned to.</td>
</tr>
<tr>
<td>server_name</td>
<td>The host name of the baseline server.</td>
</tr>
<tr>
<td>platform</td>
<td>The platform family (windows or linux) of the baseline server.</td>
</tr>
<tr>
<td>details</td>
<td>Appears only in Show baseline details call. See table below.</td>
</tr>
</tbody>
</table>

**File integrity baseline details fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total_objects</td>
<td>The total number of target objects scanned in the baseline scan.</td>
</tr>
<tr>
<td>targets</td>
<td>A list of the scanned target objects. Includes the following subfields:</td>
</tr>
<tr>
<td>target</td>
<td>Full path to the target, as specified in the file integrity policy.</td>
</tr>
<tr>
<td>inclusions</td>
<td>A pattern specifying which objects within the target directory should be scanned.</td>
</tr>
<tr>
<td>exclusions</td>
<td>A pattern specifying which objects within the target directory should not be scanned.</td>
</tr>
<tr>
<td>number_of_objects</td>
<td>the number of individual objects within this target specification that were scanned.</td>
</tr>
<tr>
<td>objects</td>
<td>Details about each of the scanned objects. Includes the following sub-fields:</td>
</tr>
<tr>
<td>name</td>
<td>Full path to the scanned object.</td>
</tr>
<tr>
<td>type</td>
<td>The kind of object scanned, such as file, directory, or registry (key).</td>
</tr>
<tr>
<td>owner</td>
<td>The username of the owner of the object.</td>
</tr>
<tr>
<td>permissions</td>
<td>The set of permissions on the object.</td>
</tr>
<tr>
<td>contents</td>
<td>The signature (SHA-256 hash) of the object's contents.</td>
</tr>
</tbody>
</table>

**List all baselines for a file integrity policy**

Returns a list of all baselines, including all core baseline fields, for the file integrity policy specified by policy ID.

**GET https://api.cloudpassage.com/v1/fim_policies/{policy_id}/baselines**

**Response**

**Status: 200**

```json
{
  "baselines": [  
  
    
    "id": "42b43bb07f90013062c2404096c01709",
    "url": "https://api.cloudpassage.com/v1/fim_policies/3310d1707f90013062be404096c01709/baselines/42b43bb07f9001306",
    "server_id": "04a50e1aeac5e25fe2cf7d23f020f47a",
    "comment": "",
    "status": "Active",
    "effective_at": "2013-04-04T20:01:29Z",
    "expires_at": "2013-08-11T23:59:59Z",
    "policy_name": "Core Registry Keys (Windows 2008) BETA Copy",
    "server_name": "ATOM7D80",
    "platform": "windows"
  ],
  
  "id": "78eb8ea0053442c031a719c501307981",
  "url": "https://api.cloudpassage.com/v1/fim_policies/2343sh34h23254543543hgf5/baselines/78eb8ea0053442c031a719c501",
  "server_id": "hsjfs323212342jh343"
}
```
Get a single baseline

For the policy specified by policy ID, returns core information for the baseline specified by baseline ID.

GET https://api.cloudpassage.com/v1/fim_policies/{policy_id}/baselines/{id}

Response
Status: 200

```
{
  "baseline": {
    "id": "cac345d0698a013027cd404096c01709",
    "url":
      "https://api.cloudpassage.com/v1/fim_policies/9cf3e42068c201302754404096c01709/baselines/cac345d0698a013027cd404096c01709",
    "server_id": "a6417fd57197858f0dd685f94ce52f8",
    "comment": "This one will not expire",
    "status": "Active",
    "effective_at": "2012-10-22T05:28:19.148087Z",
    "expires_at": null,
    "policy_name": "OS Core (Windows 2012) BETA Copy",
    "server_name": "ATOM7D81",
    "platform": "windows"
  }
}
```

Show baseline details

For the policy specified by policy ID, returns detailed information for the baseline specified by baseline ID. The baseline details include a list of all objects analyzed in the baseline scan.

GET https://api.cloudpassage.com/v1/fim_policies/{policy_id}/baselines/{id}/details

Response
Status: 200

```
{
  "baseline": {
    "id": "42b43bb07f90013062ca04096c01709",
    "url":
      "https://api.cloudpassage.com/v1/fim_policies/3310d1707f90013062ca04096c01709/baselines/42b43bb07f90013062ca04096c01709",
    "server_id": "04a50e1ae4bdc5fe2df7d23f020f47a",
    "comment": "",
    "status": "Active",
    "effective_at": "2013-03-07T19:29:16Z",
    "expires_at": "2013-03-08T23:59:59Z",
    "policy_name": "Core System Files (Windows 2012) BETA - IMPORTED",
    "server_name": "US-WIN2008",
    "platform": "windows"
  }
}
```
Create a new baseline

Creates a baseline (runs a baseline scan) on the server specified in the request body, and assigns the baseline to the policy specified by ID in the call URL. The `expires` attribute should be an integer number of days (from creation) to expiration of the baseline. If the baseline should never expire, specify `null`. The response body from this call lists the new baseline’s details, including its baseline ID.

**Note:** Make sure that the server you specify for the baseline and the policy that you assign it to have the same general operating system (Linux or Windows).

**POST** https://api.cloudpassage.com/v1/fim_policies/{policy_id}/baselines

**Request Body**

```
"details": {
  "total_objects": 122,
  "targets": [
    {
      "name": "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole",
      "inclusions": "None",
      "exclusions": "None",
      "number_of_objects": 1,
      "objects": [
        {
          "name": "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole",
          "type": "registry",
          "owner": "BUILTIN\Administrators",
          "permissions": ["BUILTIN\Users: (CI) (IO) (I) (Allow) (KR)", "BUILTIN\Users: (I) (Allow) (CC, SW, RP, RC)", "BUILTIN\Administrators: (CI) (IO) (I) (Allow) (KA)", "BUILTIN\Administrators: (I) (Allow) (CC, DC, LC, SW, RP, WP, SD, RC, WD, WO)", "NT AUTHORITY\SYSTEM: (CI) (IO) (I) (Allow) (KA)", "NT AUTHORITY\SYSTEM: (I) (Allow) (CC, DC, LC, SW, RP, WP, SD, RC, WD, WO)", "NT SERVICE\TrustedInstaller: (CI) (IO) (I) (Allow) (KA)", "NT SERVICE\TrustedInstaller: (I) (Allow) (CC, DC, LC, SW, RP, WP, SD, RC, WD, WO)"
        ],
        "contents": "33bfbf90ce5f4f88169a8daba94ac2d1d01816f6a5bf99d532cbddd4f41641b6dc"
      }
    },
    ...
    {
      "name": "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems",
      "inclusions": "None",
      "exclusions": "None",
      "number_of_objects": 1,
      "objects": [
        {
          "name": "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems",
          "type": "registry",
          "owner": "BUILTIN\Administrators",
          "permissions": ["CREATOR OWNER: (CI) (IO) (I) (Allow) (KA)", "NT AUTHORITY\SYSTEM: (CI) (IO) (I) (Allow) (KA)", "NT AUTHORITY\SYSTEM: (I) (Allow) (CC, DC, LC, SW, RP, WP, SD, RC, WD, WO)", "BUILTIN\Administrators: (CI) (IO) (I) (Allow) (KA)", "BUILTIN\Administrators: (I) (Allow) (CC, DC, LC, SW, RP, WP, SD, RC, WD, WO)", "BUILTIN\Users: (CI) (IO) (I) (Allow) (KR)", "BUILTIN\Users: (I) (Allow) (CC, SW, RP, RC)"
        ],
        "contents": "3dcd88d48c0039de469d390c9b48a8a490490f939378eb78c8090b1428d1966"
      }
    }
  ]
}
```
Update / Request a re-baseline

Updates the baseline (re-runs the baseline scan) specified by baseline ID and policy ID in the call URL, on the server specified in the request body.

**PUT** https://api.cloudpassage.com/v1/fim_policies/{policy_id}/baselines/{id}

**Request Body**

```
{
  "baseline": {
    "server_id": "8343jb3hbv233834g32hgh34"
  }
}
```

**Response**

**Status: 202**

**Location:** https://api.cloudpassage.com/v1/fim_policies/2343sh34h23254543543hgf5/baselines/78eb8ea053442c031a719c501307981

```
{
  "baseline": {
    "id": "78eb8ea0053442c031a719c501307981",
    "url": "https://api.cloudpassage.com/v1/fim_policies/2343sh34h23254543543hgf5/baselines/78eb8ea0053442c031a719c501307981",
    "server_id": "83734bh3bv347iy343bh3423",
    "effective_at": null,
    "expires_at": null,
    "comment": "This one will not expire",
    "status": "Pending"
  }
}
```
Delete a file integrity baseline

Deletes the baseline specified by baseline ID from the policy specified by policy ID. If the call is successful, The baseline is removed from the policy (and from Halo), and cannot be retrieved.

DELETE https://api.cloudpassage.com/v1/fim_policies/{policy_id}/baselines/{id}

Response

Status: 204
CVE Details

You can use the CVE Details endpoint to retrieve complete information on one Common Vulnerability and Exposure (CVE), as defined by the National Institute of Standards and Technology (NIST).

For further discussion of software vulnerabilities, see *Software Vulnerability Assessment Setup Guide.*

- Object Representation
- Get CVE Details

Object Representation

CVE details object location

```
api.cloudpassage.com/v1
```

CVE details object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>published</td>
<td>Date and time when this details document was published.</td>
</tr>
<tr>
<td>last_modified</td>
<td>Date and time when this details document was last modified.</td>
</tr>
<tr>
<td>cwe_id</td>
<td>The Common Weakness Enumeration (CWE) identifier for this CVE.</td>
</tr>
<tr>
<td>summary</td>
<td>A brief description of this CVE.</td>
</tr>
<tr>
<td>CVE</td>
<td>The identifier (number) of this CVE.</td>
</tr>
<tr>
<td>CVSS Metrics</td>
<td>An array of the following subfields, which describe the nature of the CVE and its overall risk severity.</td>
</tr>
<tr>
<td>score</td>
<td>The Common Vulnerability Scoring System (CVSS) numerical severity score for this vulnerability. By default, Halo flags all vulnerabilities with a score higher than 5.0 as &quot;Critical&quot;.</td>
</tr>
<tr>
<td>access_vector</td>
<td>How remote an attacker can be; for example &quot;LOCAL&quot; or &quot;NETWORK&quot;.</td>
</tr>
<tr>
<td>access_complexity</td>
<td>How common the conditions are that allow this vulnerability to be exploited. A value of &quot;LOW&quot; means very common.</td>
</tr>
<tr>
<td>authentication</td>
<td>Whether and how many times an attacker must authenticate to the target system to perform the exploit. A value of &quot;NONE&quot; means that no authentication is required.</td>
</tr>
<tr>
<td>confidentiality_impact</td>
<td>The impact that a successful exploit could have on the confidentiality of the target; for example, &quot;NONE&quot;, &quot;PARTIAL&quot;, or &quot;COMPLETE&quot;.</td>
</tr>
<tr>
<td>integrity_impact</td>
<td>The impact that a successful exploit could have on the integrity of the target; for example, &quot;NONE&quot;, &quot;PARTIAL&quot;, or &quot;COMPLETE&quot;.</td>
</tr>
<tr>
<td>availability_impact</td>
<td>The impact that a successful exploit could have on the availability of the target; for example, &quot;NONE&quot;, &quot;PARTIAL&quot;, or &quot;COMPLETE&quot;.</td>
</tr>
<tr>
<td>source</td>
<td>The URL to the NIST National Vulnerability Database.</td>
</tr>
</tbody>
</table>
Get CVE details

Retrieves the details of the Common Vulnerability and Exposure specified by CVE number in the call URL.

GET https://api.cloudpassage.com/v1/cve_details/{CVE}

Response

Status: 200

```json
{
  "published": "2015-09-05T02:59:03.000Z",
  "last_modified": "2015-10-24T01:59:24.000Z",
  "cwe_id": "CWE-20",
  "summary": "buffer.c in named in ISC BIND 9.x before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) by creating a zone containing a malformed DNSSEC key and issuing a query for a name in that zone."
  "CVE": "CVE-2015-5722",
  "CVSS Metrics": {
    "score": 7.8,
    "access_vector": "NETWORK",
    "access_complexity": "LOW",
    "authentication": "NONE",
    "confidentiality_impact": "NONE",
    "integrity_impact": "NONE",
    "availability_impact": "COMPLETE",
    "source": "http://nvd.nist.gov",
    "generated_on": "2015-09-08T13:53:29.000Z"
  }
  "References": [
    "https://kb.isc.org/article/AA-01287",
    "https://support.apple.com/HT205376"
  ],
  "Vulnerable packages": [
    "cpe:/a:isc:bind:9.10.2:p3",
    "cpe:/a:isc:bind:9.9.7:p2"
  ]
}
Halo software exceptions are defined by Halo users for the purpose of ignoring software vulnerabilities detected by Halo. You can use the CVE Exceptions endpoint to retrieve information on one or all defined software exceptions, and you can also use the endpoint to create, update, and delete exceptions. For further discussion of software exceptions, see Specify Exceptions in the Software Vulnerability Assessment Setup Guide.

- Object Representation
- List CVE exceptions
- Get a single CVE exception
- Create a CVE exception
- Update a CVE exception
- Delete a CVE exception

Object Representation

CVE exception object location

```
api.cloudpassage.com/v1
cve_exceptions
  id
```

CVE exception object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>The API URL to the CVE exception object.</td>
</tr>
<tr>
<td>id</td>
<td>Unique identifier for this CVE exception.</td>
</tr>
<tr>
<td>username</td>
<td>The name of the Halo user who created this CVE exception.</td>
</tr>
<tr>
<td>package_name</td>
<td>The name of the vulnerable package to be excepted.</td>
</tr>
<tr>
<td>package_version</td>
<td>The version number of the vulnerable package.</td>
</tr>
<tr>
<td>comment</td>
<td>A text description or comment entered when the exception was created.</td>
</tr>
<tr>
<td>created_at</td>
<td>Date/time at which the exception was created. Formatted in ISO 8601.</td>
</tr>
<tr>
<td>expires_at</td>
<td>Date/time at which the exception expires. Formatted in ISO 8601.</td>
</tr>
</tbody>
</table>

**NOTE:** when creating or updating a software exception, you supply a `length` field instead of an `expires_at` field in the request JSON. See Create a CVE exception, below.

server_id

Unique ID of the server to which this exception applies. If this field is empty or null, the exception applies to all servers in the group (if the `group_id` field is populated), or to all servers in the account (if the `group_id` field is empty).

**NOTE:** when creating or updating a software exception, you supply a `scope` field instead of a `server-id` field in the request JSON. See Create a CVE exception, below.
group_id

The ID of the group containing the server to which this exception applies. If this field is empty or null, the exception applies to a single server (if the server_id field is populated), or to all servers in the account (if the server_id field is empty).

**NOTE:** when creating or updating a software exception, you supply a scope field instead of a group-id field in the request JSON. See Create a CVE exception, below.

cve_entries

An array of CVE reference numbers, by default listing all of the package’s known vulnerabilities.

**NOTE:** when creating or updating a software exception, you can optionally use this field to list the specific CVEs in this package that you want suppressed. In that case, the package may still appear as vulnerable in later scan results (if the package contains other, unsuppressed CVEs), but the CVEs in this list will not appear.

To ensure that all detected CVEs will appear in the scan results, enter an asterisk (*) in this field.

---

### List CVE exceptions

Retrieves all defined software exceptions from the Halo database.

**Note:** The results of this call may be paginated. See Pagination of Results for information on how to set up and retrieve paginated results from the Halo API.

**GET** https://api.cloudpassage.com/v1/cve Exceptions/

**Response**

**Status:** 200

```json
{
  "count": 27,
  "pagination": {
    "next": "https://api.cloudpassage.com/v1/cve Exceptions?page=2&per_page=10"
  },
  "cve Exceptions": [
    {
      "url": "https://api.cloudpassage.com/v1/cve Exceptions/413651102bea0132cc573c764e101158",
      "id": "413651102bea0132cc573c764e101158",
      "username": "jstrauss29",
      "package_name": "nfs-utils.i686",
      "package_version": "1:1.2.3-39.el6",
      "comment": "",
      "created_at": "2014-10-01T22:43:15.194Z",
      "expires_at": "2014-10-31T23:59:59.999Z",
      "server_id": null,
      "group_id": null,
      "cve entries": [
        "CVE-2013-1923"
      ]
    },
    {
      "url": "https://api.cloudpassage.com/v1/cve Exceptions/aa82f6108b4901306fc3404096c01709",
      "id": "aa82f6108b4901306fc3404096c01709",
      "username": "ericaj",
      "package_name": "freetype.x86_64",
      "package_version": "2.3.11-6.el6_2.9",
      "comment": "-1",
      "created_at": "2013-04-19T18:05:39.169Z",
      "expires_at": null,
      "server_id": null,
      "group_id": "eb2a1720add1012fc92f404096c01709",
      "cve entries": [
        "CVE-2010-2497",
        "CVE-2010-2498",
        "CVE-2010-2499",
        "CVE-2010-2500"
      ]
    }
  ]
}
```
Get a single CVE exception

Retrieves the software exception specified by ID in the call URL.

GET https://api.cloudpassage.com/v1/cve_exceptions/{id}

Response

Status: 200

```json
{
  "cve_exception": {
    "url": "https://api.cloudpassage.com/v1/cve_exceptions/413651102bea0132cc573c764e101158",
    "id": "413651102bea0132cc573c764e101158",
    "username": "jstrauss29",
    "package_name": "nfs-utils.i686",
    "package_version": "1:1.2.3-39.el6",
    "created_at": "2014-10-01T22:43:15.194Z",
    "expires_at": "2014-10-31T23:59:59.999Z",
    "server_id": "2152f490be98013199b83c764e101158",
    "group_id": null,
    "cve_entries": [ "CVE-2013-1923"
                    ]
  }
}
```

Create a CVE exception

Creates a new software exception with the attributes passed in the request JSON. Minimum required attributes to supply are `package_name`, `package_version`, and `scope`.

Two attributes that you can supply in the request JSON do not appear in the response as fields of the `cve_exception` object:

- **length**. The lifetime of the exception (in days). In the response JSON, the `expires_at` field contains an expiration date that corresponds to the value you submit for `length`. If you do not include this attribute in the request, the exception never expires.

- **scope**. A designation of how widely this exception is to be applied. Possible values are `server`, `group` and `all`. If you pass the value `server` in this field, the request JSON must also include a server ID in the `server_id` field. If you pass the value `group` in
this field, the request JSON must also include a group ID in the group_id field. If you pass all, the exception applies to all servers across your entire Halo account.

POST https://api.cloudpassage.com/v1/cve_exceptions/

Request Body

```
{
    "cve_exception": {
        "package_name": "nfs-utils.i686",
        "package_version": "41:1.2.3-39.el6",
        "scope": "server",
        "server_id": "c82779463036a0b90faf16283927dc2",
        "comment": "package not used",
    }
}
```

Response

Status: 201

```
{
    "cve_exception": {
        "url": "https://api.cloudpassage.com/v1/cve_exceptions/557074f4c61811e6a18033e5064599cb",
        "id": "557074f4c61811e6a18033e5064599cb",
        "username": "e8270c54(test one)",
        "package_name": "nfs-utils.i686",
        "package_version": "41:1.2.3-39.el6",
        "comment": "package not used",
        "created_at": "2016-12-19T18:24:09.632Z",
        "expires_at": "2017-01-18T23:59:59.999Z",
        "server_id": "c82779463036a0b90faf16283927dc2",
        "group_id": "c4e9e062c0f111e6972e199079951bd9",
        "cve_entries": []
    }
}
```

Update a CVE exception

Modifies the software exception specified in the call URL with the attributes passed in the request JSON. Pass only the attributes to be updated.

When updating an exception, instead of suppressing it entirely you can opt to suppress only certain CVEs within the package. To do that, list the CVEs to be suppressed in the cve_entries field of your request JSON. To stop suppressing any CVEs in the package, pass an asterisk (*) in the cve_entries field of your request JSON.

PUT https://api.cloudpassage.com/v1/cve_exceptions/{id}

Request Body

```
{
    "cve_exception": {
        "scope": "group",
        "group_id": "",
        "cve_entries": [{
            "CVE-2017-297"
        }]
    }
}
```
Delete a CVE exception

Removes the software exception specified in the call URL. Once it has been deleted, the exception cannot be restored.

DELETE https://api.cloudpassage.com/v1/cve_exceptions/{id}
Firewall Policies

Use the Firewall Policies endpoint to create and manage the policies that define your server firewalls. You can list policies, view policy rules, and create, update, and delete policies.

With this endpoint you can manipulate general information and settings for a policy, and you can also view the rules in a policy and create rules when you create a policy. To manage firewall policy rules in more depth, use the Firewall Rules endpoint. You also use separate endpoints to manage firewall interfaces, services, and zones.

- Object Representation
- List firewall policies
- Get firewall policy details including firewall rules
- Create a new firewall policy
- Update name or description for a firewall policy
- Delete a firewall policy

Object Representation

Firewall policy object location

api.cloudpassage.com/v1

firewall_policies

id

Firewall policy object fields

The firewall policy object includes general information and settings for the policy. Note that several fields apply only to Windows firewalls. Firewall rules fields are described in Firewall Rules.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique identifier of the firewall policy.</td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>A unique name given to the firewall policy.</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td>Optional. A description of the firewall policy.</td>
<td></td>
</tr>
<tr>
<td>platform</td>
<td>Optional. The OS platform of the firewall policy. Either &quot;windows&quot; or &quot;linux&quot;.</td>
<td>linux</td>
</tr>
<tr>
<td>used_by</td>
<td>Read-only. The identifiers and names of groups that use the firewall policy.</td>
<td></td>
</tr>
<tr>
<td>ignore Forwarding rules</td>
<td>Linux-only. true if the iptables default forwarding rules should be ignored; otherwise false.</td>
<td>false</td>
</tr>
<tr>
<td>log_allowed</td>
<td>Windows-only. Whether to log allowed connections or not by default.</td>
<td>false</td>
</tr>
<tr>
<td>log_dropped</td>
<td>Windows-only. Whether to log dropped connections or not by default.</td>
<td>false</td>
</tr>
<tr>
<td>block_inbound</td>
<td>Windows-only. Whether to block all inbound connections by default.</td>
<td>true</td>
</tr>
<tr>
<td>block_outbound</td>
<td>Windows-only. Whether to block all outbound connections by default.</td>
<td>false</td>
</tr>
</tbody>
</table>
List firewall policies

Lists core information, including firewall ID, for all of your defined firewall policies.

*Note:* The results of this call may be paginated. See [Pagination of Results](#) for information on how to set up and retrieve paginated results from the Halo API.

**GET** https://api.cloudpassage.com/v1/firewall_policies/

**Response**

**Status:** 200

```json
{
  "count": 5,
  "firewall_policies": [
    {
      "id": "d3448a70ae5c01323f190670140ec224",
      "url": "https://api.cloudpassage.com/v1/firewall_policies/d3448a70ae5c01323f190670140ec224",
      "name": "database-rhel",
      "description": "",
      "platform": "linux",
      "used_by": [
        {
          "id": "511ed0d0a5b4013295b806ba9a9c633c",
          "name": "HQ group"
        }
      ],
      "ignore_forwarding_rules": true
    },
    {
      "id": "291f1420abe7013295e406ba9a9c633c",
      "url": "https://api.cloudpassage.com/v1/firewall_policies/291f1420abe7013295e406ba9a9c633c",
      "name": "http-win",
      "description": "",
      "platform": "windows",
      "used_by": [
        {
          "id": "23ba3420abe0013295e406ba9a9c633c",
          "name": "web-asia-pac"
        }
      ],
      "log_allowed": false,
      "log_dropped": false,
      "block_inbound": false,
      "block_outbound": false
    },
    {
      "id": "8eb1b050abe2013295e406ba9a9c633c",
      "url": "https://api.cloudpassage.com/v1/firewall_policies/8eb1b050abe2013295e406ba9a9c633c",
      "name": "loadbalancers-linux",
      "description": "",
      "platform": "linux",
      "used_by": [
        {
          "id": "23ba3420abe0013295e406ba9a9c633c",
          "name": "web-US"
        }
      ],
      "ignore_forwarding_rules": false
    },
    ..., // More firewall policies...
]}
```
Get firewall policy details including firewall rules

Lists policy details, including rule details, for an individual firewall policy specified by ID.

GET https://api.cloudpassage.com/v1/firewall_policies/{id}

Response:

Status: 200

```
{
  "firewall_policy": {
    "id": "d3448a70ae5c01323f190670140ec224",
    "url": "https://api.cloudpassage.com/v1/firewall_policies/d3448a70ae5c01323f190670140ec224",
    "name": "database-rhel",
    "description": "",
    "platform": "linux",
    "used_by": [
      {
        "id": "511ed0d0a5b4013295b806ba9a9c633c",
        "name": "HQ Group"
      }
    ],
    "ignore_forwarding_rules": true,
    "firewall_rules": [
      {
        "id": "d34cb2e0ae5c01323f190670140ec224",
        "url": "https://api.cloudpassage.com/v1/firewall_policies/d3448a70ae5c01323f190670140ec224/firewall_rules/d34cb2e",
        "chain": "INPUT",
        "action": "ACCEPT",
        "active": true,
        "connection_states": null,
        "log": false,
        "log_prefix": "",
        "comment": "",
        "firewall_service": {
          "id": "5a89cfe06ac7012ea3c240403472c9f3",
          "url": "https://api.cloudpassage.com/v1/firewall_services/5a89cfe06ac7012ea3c240403472c9f3",
          "name": "ssh",
          "protocol": "TCP",
          "port": "22",
          "system": true
        }
      },
      {
        "id": "d34e6b00ae5c01323f190670140ec224",
        "url": "https://api.cloudpassage.com/v1/firewall_policies/d3448a70ae5c01323f190670140ec224/firewall_rules/d34e6b0",
        "chain": "OUTPUT",
        "action": "ACCEPT",
        "active": true,
        "connection_states": null,
        "log": false,
        "log_prefix": "",
        "comment": ""
      }
    ]
  }
}
```

Create a new firewall policy

Creates a new firewall policy with the initial values and rules specified in the request body. The minimum required field to supply is `name`.

Rule order in the new policy will reflect the order in the request body, although you can later change the order with the Move firewall rule to a desired position call. If you do not specify a platform attribute or if you specify `linux`, a Linux firewall policy is created.
To create a Windows policy, you must specify `windows` for the `platform` attribute. If the call is successful, the call returns the created policy in JSON format in the response body.

POST https://api.cloudpassage.com/v1/firewall_policies

Request Body

```json
{  "firewall_policy": {    "name": "policy one",    "description": "my new policy",    "platform": "linux",    "ignore_forwarding_rules": false,    "firewall_rules": [{      "chain": "INPUT",      "active": true,      "firewall_interface": null,      "firewall_source": {        "id": "c26c6a50b190012ec6b4404096c01709",        "type": "FirewallZone"      },      "firewall_service": "7b6409a072b1012ec681404096c01709",      "connection_states": "NEW, ESTABLISHED",      "action": "ACCEPT",      "log": false    },    {      "chain": "INPUT",      "active": true,      "firewall_interface": "7b881ca072b1012ec681404096c01709",      "firewall_source": null,      "firewall_service": null,      "connection_states": null,      "action": "REJECT",      "log": true,      "comment": "Default reject-all"    },    {      "chain": "OUTPUT",      "active": true,      "firewall_interface": "7b881ca072b1012ec681404096c01709",      "firewall_destination": null,      "firewall_service": null,      "connection_states": null,      "action": "ACCEPT",      "log": false    }]  }  }
```

Response

Status: 201
Location: https://api.cloudpassage.com/v1/firewall_policies/812b7500b27b012ec6c4404096c01709

```
{  "firewall_policy": {    "id": "812b7500b27b012ec6c4404096c01709",    "url": "https://api.cloudpassage.com/v1/firewall_policies/812b7500b27b012ec6c4404096c01709",    "name": "policy one",    "description": "my new policy",    "ignore_forwarding_rules": false,    "firewall_rules": [{      "firewall_service": {        "port": "53",        "protocol": "TCP",        "name": "dns AXFR",        "system": true        },      "firewall_source": {        "id": "c26c6a50b190012ec6b4404096c01709",        "type": "FirewallZone"      },      "log": false,      "connection_states": "NEW, ESTABLISHED",      "action": "ACCEPT",      "firewall_interface": "7b881ca072b1012ec681404096c01709",      "active": true,      "firewall_destination": null,      "firewall_rule": null      }]  }  }
```
Update name or description for a firewall policy

In the policy specified by firewall ID, updates specified core firewall fields with the values contained in the request body. To update a policy’s firewall rules, use the Firewall Rules endpoint. Likewise, to update firewall interfaces, services, or zones, use the Firewall Interfaces, Firewall Services, and Firewall Zones endpoints, respectively.

**PUT** https://api.cloudpassage.com/v1/firewall_policies/{id}

**Request Body**

```json
{  "firewall_policy": {    "name": "policy one"  }
}
```

**Response**

**Status:** 204

Delete a firewall policy
Deletes an existing firewall policy from Halo. If the policy is assigned to one or more groups, the call fails and a response status 422 is returned. Remove the policy from all groups before attempting to delete it again.

DELETE https://api.cloudpassage.com/v1/firewall_policies/{id}

Response

Status: 204
Firewall Rules

Use the Firewall Rules endpoint to view and manipulate individual rules in your firewall policies. You can list the rules in a policy, view all rule details, and add, delete, update, and reposition rules.

- Object Representation
- List firewall rules in a firewall policy
- Get firewall rule details
- Add a new firewall rule to a firewall policy
- Add a new firewall rule with a source or target
- Delete a firewall rule
- Update a firewall rule
- Move a firewall rule to a desired position

Object Representation

Firewall rule object location

api.cloudpassage.com/v1

firewall_policies

 policy_id

firewall_rules

 id

Firewall rule object fields

Two levels of firewall-rule information are available: core firewall rule fields (accessed through, for example, the List firewall rules in a firewall policy call), and a single firewall rule details field (accessed through the Get firewall rule details call). Note that several core fields are Linux-only. The fields of firewall interfaces, zones, and services are described with those API endpoints.

Core firewall rule fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique identifier of the firewall rule.</td>
</tr>
<tr>
<td>url</td>
<td>The API URL to the firewall rule object.</td>
</tr>
<tr>
<td>chain</td>
<td>Whether the firewall rule covers INPUT or OUTPUT connections. Allowed values are INPUT and OUTPUT.</td>
</tr>
<tr>
<td>active</td>
<td>Whether the firewall rule is active or not.</td>
</tr>
<tr>
<td>firewall_interface</td>
<td>Linux-only. The specified firewall interface for this rule. Specify the ID of the interface you wish to use.</td>
</tr>
<tr>
<td>firewall_source</td>
<td>The specified source/zone for an INPUT rule. You must specify the ID* and type of source you wish to use. Allowed values for type are FirewallZone, Group, User, or UserGroup. Note: When using UserGroup you must specify the name, and not the ID of the source. Currently, only &quot;All</td>
</tr>
</tbody>
</table>
"GhostPorts users" is a valid **UserGroup**. Please see example below.

"All Active Servers" is a special group that has no ID, so you must specify it by **name**.

<table>
<thead>
<tr>
<th><strong>firewall_target</strong></th>
<th>The specified source/zone for an OUTPUT rule. You must specify the ID and type of destination you wish to use. Allowed values for <strong>type</strong> are <strong>FirewallZone</strong> or <strong>Group</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>firewall_service</strong></td>
<td>The specified firewall service for this rule. Specify the ID of the service you wish to use.</td>
</tr>
<tr>
<td><strong>connection_states</strong></td>
<td><strong>Linux-only</strong>. The specified firewall connection state(s) for this rule. <strong>NEW</strong>, <strong>RELATED</strong>, and <strong>ESTABLISHED</strong> are allowed.</td>
</tr>
<tr>
<td><strong>action</strong></td>
<td>The specified action to take if this rule is matched. Allowed values are <strong>ACCEPT</strong>, <strong>DROP</strong>, and <strong>REJECT</strong> (<strong>REJECT</strong> is <strong>Linux-only</strong>).</td>
</tr>
<tr>
<td><strong>log</strong></td>
<td><strong>Linux-only</strong>. Whether matches to this rule are logged or not.</td>
</tr>
<tr>
<td><strong>log_prefix</strong></td>
<td><strong>Linux-only</strong>. A user-defined string (max. 29 characters) to attach to the beginning of the log message whenever this rule is matched and logged. The purpose of attaching a prefix is to help Log-Based Intrusion Detection to detect occurrences of matches to this rule in the firewall log file.</td>
</tr>
<tr>
<td><strong>comment</strong></td>
<td>An optional description of this rule.</td>
</tr>
</tbody>
</table>

**Fields present only in firewall rule details**

| **position** | The position order of the rule in the chain. |

**List firewall rules in a firewall policy**

Lists, in policy order, all rules and their core field values (including rule ID) in the firewall policy specified by policy ID. Also lists the fields and values for any firewall interfaces, services, and zones used by the rule.

**GET** https://api.cloudpassage.com/v1/firewall_policies/{firewall_policy_id}/firewall_rules/

**Response**

**Status: 200**

```json
{
  "firewall_rules": [ 
    {
      "id": "f99fc8b0c2da012f11ab40403472c9f3",
      "url": "https://api.cloudpassage.com/v1/firewall_policies/f99222d0c2da012f11ab40403472c9f3/firewall_rules/f99fc8b0c2da012f11ab40403472c9f3",
      "chain": "INPUT",
      "action": "ACCEPT",
      "active": true,
      "connection_states": null,
      "log": false,
      "log_prefix": null,
      "comment": "Accept HTTP connections on port 80",
      "firewall_service": { 
        "id": "5a8c53106ac7012ea3c24043472c9f3",
        "url": "https://api.cloudpassage.com/v1/firewall_services/5a8c53106ac7012ea3c24043472c9f3",
        "name": "http",
        "protocol": "TCP",
        "port": "80",
        "system": true
      },
      "firewall_source": { 
        "type": "Group",
        "name": "All active servers"
      }
    },
    {
      "id": "f9d431e0c2da012f11ab40403472c9f3",
      "url": "https://api.cloudpassage.com/v1/firewall_policies/f99222d0c2da012f11ab40403472c9f3/firewall_rules/f9d431e0c2da012f11ab40403472c9f3",
      "chain": "INPUT",
```
Get firewall rule details

For the firewall policy specified by policy ID, lists both core and detail field values for the firewall rule specified by rule ID. Also lists the fields and values for any firewall interfaces, services, and zones used by the rule. This call returns one more field (position) per rule than does the call List firewall rules in a firewall policy.

GET https://api.cloudpassage.com/v1/firewall_policies/{firewall_policy_id}/firewall_rules/{id}

Response

Status: 200

```
{
  "firewall_rule": {
    "id": "81304d50b27b012ec6c4404096c01709",
    "url": "https://api.cloudpassage.com/v1/firewall_policies/812b7500b27b012ec6c4404096c01709/firewall_rules/81304d50b27b012ec6c4404096c01709",
    "chain": "OUTPUT",
    "action": "ACCEPT",
    "active": true,
    "connection_states": null,
    "log": false,
    "log_prefix": null,
    "comment": "",
    "position": 1,
    "firewall_interface": {
      "name": "eth0",
      "system": false,
      "url": "https://api.cloudpassage.com/v1/firewall_interfaces?id=7b881ca072b1012ec681404096c01709",
      "id": "7b881ca072b1012ec681404096c01709"
    }
  }
}
```

Add a new firewall rule to a firewall policy

Creates a new firewall rule based on information in the request body and assigns it (at the indicated position) to the firewall policy specified in the call URL. The minimum required fields to supply are action, chain, connection states, and position (for Linux; not required for Windows).

The firewall rule ID is returned in the response body, along with the rest of the rule fields, expanded to show the fields within any
firewall interfaces, services, and zones.

Note:

- If you are specifying a source or target in the rule you are creating, see the next call description: **Add new firewall rule with a source or target**.

- Use **position** to place the rule in proper execution order relative to other rules. Rule numbering starts from 1 (at the top, or first-processed) for each chain (**INPUT** and **OUTPUT**). To add a new rule at the very end of either chain, set the value of the position attribute to **last**.

- If you specify a position number that is already occupied by an existing rule, the position numbers of that existing rule and all higher-numbered rules are incremented to accommodate the insertion of the new rule.

```plaintext
POST https://api.cloudpassage.com/v1/firewall_policies/{firewall_policy_id}/firewall_rules

Request Body

```json
{
    "firewall_rule": {
        "chain": "INPUT",
        "active": true,
        "firewall_interface": "7b881ca072b1012ec681404096c01709",
        "firewall_service": "7b6409a072b1012ec681404096c01709",
        "connection_states": "NEW, ESTABLISHED",
        "action": "ACCEPT",
        "log": true,
        "log_prefix": "East-3 input-accept",
        "comment": "All servers in group East-3 must include this rule"
        "position": 4
    }
}
```

Response

Status: 201
Location: https://api.cloudpassage.com/v1/firewall_policies/812b7500b27b012ec6c4404096c01709/firewall_rules/99b71970b27c012ec6c4404096c01709

```json
{
    "firewall_rule": {
        "firewall_service": {
            "port": "53",
            "protocol": "TCP",
            "name": "dns AXFR",
            "system": true,
            "url": "https://api.cloudpassage.com/v1/firewall_services/7b6409a072b1012ec681404096c01709",
            "id": "7b6409a072b1012ec681404096c01709"
        },
        "log": true,
        "log_prefix": "East-3 input-accept",
        "comment": "All servers in group East-3 must include this rule",
        "active": true,
        "position": 4,
        "firewall_interface": {
            "name": "eth0",
            "system": true,
            "url": "https://api.cloudpassage.com/v1/firewall_interfaces?id=7b881ca072b1012ec681404096c01709",
            "id": "7b881ca072b1012ec681404096c01709"
        },
        "action": "ACCEPT",
        "chain": "INPUT",
        "url": "https://api.cloudpassage.com/v1/firewall_policies/812b7500b27b012ec6c4404096c01709/firewall_rules/99b71970b27c012ec6c4404096c01709",
        "connection_states": "NEW, ESTABLISHED"
    }
}
```
Add a new firewall rule with a source or target

As noted in the Object Representation table for the Firewall Rules endpoint, when you specify a source or target that is of type Firew allZone, User, or Group, you must specify both its ID and its type. (The group "All Servers" is a special case; it has no ID, so you must specify it by name and type.) Also, you can specify a source or target of type UserGroup (such as "All GhostPorts users"), and again you must specify both its ID and its type.

Note: UserGroup is a special Halo designation for a particular kind of group defined for firewall purposes. It is different from the standard meaning of Group as a named set of users that may be assigned privileges. "All GhostPorts Users" is currently the only usergroup supported for Halo firewall rules.

The first request body below shows how to specify a firewall source whose type is firewall zone. The second shows how too specify a firewall source whose type is usergroup.

POST https://api.cloudpassage.com/v1/firewall_policies/{firewall_policy_id}/firewall_rules

Request Body (specifying a FirewallZone)

```
{
  "firewall_rule" : {
    "chain" : "INPUT",
    "active" : true,
    "firewall_source" : {
      "id" : "7b881ca072b1012ec681404096c01709",
      "type" : "FirewallZone"
    },
    "firewall_interface" : "7b881ca072b1012ec681404096c01709",
    "connection_states" : "NEW, ESTABLISHED",
    "action" : "ACCEPT",
    "log" : false,
    "position": 4
  }
}
```

Request Body (specifying a GhostPorts UserGroup)

```
{
  "firewall_rule" : {
    "chain" : "INPUT",
    "active" : true,
    "firewall_source" : {
      "name" : "All GhostPorts users",
      "type" : "UserGroup"
    },
    "firewall_interface" : "7b881ca072b1012ec681404096c01709",
    "connection_states" : "NEW, ESTABLISHED",
    "action" : "ACCEPT",
    "log" : false,
    "position": 4
  }
}
```

Firewall source or target elements

The examples below illustrate further how to specify various kinds of source or target elements.

All active servers

```
"firewall_source" : {
  "name" : "All Active Servers",
  "type" : "Group"
}
```
**Servers belonging to specific group**

```
"firewall_source" : { 
  "id" : "2e809ca072b1012ec681204096c01665, 
  "type" : "Group"
}
```

**Servers with IP matching a specific firewall zone**

```
"firewall_source" : { 
  "id" : "7b881ca072b1012ec681404096c01709", 
  "type" : "FirewallZone"
}
```

**All GhostPorts enabled users**

```
"firewall_source" : { 
  "name" : "All GhostPorts users", 
  "type" : "UserGroup"
}
```

**One specific GhostPorts user**

```
"firewall_source" : { 
  "id" : "7b881ca072098bec681404096c01709", 
  "type" : "User"
}
```

**Delete a firewall rule**

Removes the rule (specified by rule ID) from the policy specified by policy ID. If the call is successful, the rule no longer exists and cannot be retrieved.

DELETE https://api.cloudpassage.com/v1/firewall_policies/{firewall_policy_id}/firewall_rules/{id}

**Response**

**Status:** 204

**Update a firewall rule**

Updates the firewall rule specified by rule ID with the values of the attributes specified in the request body.

- If specifying the source or destination, remember that you also need to specify whether the zone type is FirewallZone, Group, User, or UserGroup.
- To move a rule to a new position, change the value of its `position` attribute; for an example, see [Move firewall rule to a desired position](#).

PUT https://api.cloudpassage.com/v1/firewall_policies/{firewall_policy_id}/firewall_rules/{id}

**Request Body**

```
{
  "firewall_rule" : {
```

205
Response

Status: 204

Move a firewall rule to a desired position

You can control the processing order of the rules within a firewall policy. To view the current order, call the Get firewall policy details including firewall rules method. In the response, the rules will be listed in order. Positions are whole numbers with 1 being the first position in either the INPUT or OUTPUT chain. Alternatively, you can use "position" : "last" for the rule to be moved to the last position.

Note: If you specify a position number that is already occupied by an existing rule, the position numbers of that existing rule and all higher-numbered rules are incremented to accommodate the insertion of the new rule.

PUT https://api.cloudpassage.com/v1/firewall_policies/{firewall_policy_id}/firewall_rules/{id}

Request Body

```
{"firewall_rule":{
  "position":{position}
}}
```

Response

Status: 204
Firewall Interfaces

Use the Firewall Interfaces endpoint to manage the identification of physical network interfaces (such as eth0) used in your firewall policies. You can use the API to list interfaces, get interface detail, and create or delete interfaces.

- Object Representation
- List firewall interfaces
- Get firewall interface details
- Create a new firewall interface
- Delete a firewall interface

Object Representation

Firewall interface object location

```
api.cloudpassage.com/v1

firewall_interfaces

id
```

Firewall interface object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique identifier of the firewall interface.</td>
</tr>
<tr>
<td>name</td>
<td>A unique name given to the firewall interface.</td>
</tr>
<tr>
<td>system</td>
<td>Denotes whether the firewall interface is built-in/system or not. System interfaces cannot be deleted.</td>
</tr>
</tbody>
</table>

List firewall interfaces

Returns a list of all of your defined firewall interfaces.

```
GET https://api.cloudpassage.com/v1/firewall_interfaces/
```

Response

Status: 200

```
{
  "firewall_interfaces": [
    {
      "name": "eth0",
      "system": true,
      "url": "https://api.cloudpassage.com/v1/firewall_interfaces?id=5a9a36906ac7012ea3c240403472c9f3",
      "id": "5a9a36906ac7012ea3c240403472c9f3"
    }
  ]
}
```
Get firewall interface details

Returns detailed information for the firewall interface specified by interface ID.

**GET** https://api.cloudpassage.com/v1/firewall_interfaces/{id}

**Response**

**Status:** 200

```
{
    "firewall_interface": {
        "name": "eth0:15",
        "system": false,
        "url": "https://api.cloudpassage.com/v1/firewall_interfaces?id=5a9b5b406ac7012ea3c240403472c9f3",
        "id": "5a9b5b406ac7012ea3c240403472c9f3"
    }
}
```

Create a new firewall interface

Creates the firewall interface specified in the request body. Returns the details of the created interface, including interface ID, in the response body.

**POST** https://api.cloudpassage.com/v1/firewall_interfaces

**Request Body**

```
{
    "firewall_interface": {
        "name": "eth0:16"
    }
}
```

**Response**

**Status:** 201

**Location:** https://api.cloudpassage.com/v1/firewall_interfaces/2e542e3f344a07288012e22c031a719c

```
{
    "firewall_interface": {
        "name": "eth0:16",
        "system": false,
        "url": "https://api.cloudpassage.com/v1/firewall_interfaces?id=648e7d40ae4f012ea3f340403472c9f3",
        "id": "648e7d40ae4f012ea3f340403472c9f3"
    }
}
```
Delete a firewall interface

Deletes the firewall interface specified by ID. If the call is successful, the interface is removed from Halo and cannot be retrieved.

Only non-system firewall interfaces that are not used by any firewall policy can be deleted. Attempting to delete a system firewall interface or a firewall interface that is used by a firewall policy results in a 422 response status.

DELETE https://api.cloudpassage.com/v1/firewall_interfaces/{id}

Response

Status: 204
Firewall Services

Use the Firewall Services endpoint to manage the descriptions of the software services, protocols, and ports (such as \texttt{http\,(tcp/80\,)}) used in your firewall policies. You can use the API to list firewall services, view service details, and create or delete firewall services.

- **Object Representation**
- **List firewall services**
- **Get a single firewall service**
- **Create a new firewall service**
- **Delete a firewall service**

Object Representation

Firewall service object location

\[
\text{api.cloudpassage.com/v1/firewall_services/\,id}
\]

Firewall service object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique identifier of the firewall service.</td>
</tr>
<tr>
<td>url</td>
<td>The API URL to the firewall service object.</td>
</tr>
<tr>
<td>name</td>
<td>A unique name given to the firewall service.</td>
</tr>
<tr>
<td>protocol</td>
<td>The specified protocol of the firewall service.</td>
</tr>
<tr>
<td>port</td>
<td>The specified port(s) of the firewall service.</td>
</tr>
<tr>
<td>system</td>
<td>Denotes whether the firewall service is built-in/system or not. System firewall services cannot be deleted.</td>
</tr>
</tbody>
</table>

List firewall services

Returns a list of all defined firewall services.

\text{GET https://api.cloudpassage.com/v1/firewall_services/}

Response

Status: 200
Get a single firewall service

Returns the details of the firewall service specified by service ID.

GET https://api.cloudpassage.com/v1/firewall_services/{id}

Response

Status: 200

```
{
  "firewall_service": {
    "port": "5432",
    "protocol": "TCP",
    "name": "postgres",
    "system": false,
    "url": "https://api.cloudflare.com/v1/firewall_services/5a8e66606ac7012ea3c240403472c9f3",
    "id": "5a8e66606ac7012ea3c240403472c9f3"
  }
}
```

Create a new firewall service

Creates a firewall service with the information specified in the request body. Returns the details of that service, including its ID, in the response body.

POST https://api.cloudflare.com/v1/firewall_services

Request Body

```
{
  "firewall_service": {
    "name": "rails",
    "protocol": "TCP",
    "port": "3000"
  }
}
```
Response
Status: 201
Location: https://api.cloudpassage.com/v1/firewall_service/d9887180ae4e012ea3f340403472c9f3

```
{
    "firewall_service": {
        "port": "3000",
        "protocol": "TCP",
        "name": "rails",
        "system": false,
        "url": "https://api.cloudpassage.com/v1/firewall_services/d9887180ae4e012ea3f340403472c9f3",
        "id": "d9887180ae4e012ea3f340403472c9f3"
    }
}
```

Delete a firewall service

Deletes the firewall service specified by ID. If the call is successful, the service is removed from Halo and cannot be retrieved.

Only non-system firewall services that are not used by any firewall policy can be deleted. Attempting to delete a system firewall service or a firewall service that is used by firewall policies will result in a 422 response status.

DELETE https://api.cloudpassage.com/v1/firewall_services/{id}

Response
Status: 204
Firewall Zones

Use the Firewall Zones endpoint to manage the descriptions of the IP Zones (sets of IP addresses or CIDR blocks, such as 127.0.0.0/24) used in your firewall policies. You can use the API to list firewall zones, get zone details, and create, clone, update, or delete firewall zones.

Note: The Halo API uses the term "firewall zone" for what the Halo Portal calls "IP zone". The terms are interchangeable.

- Object Representation
- List firewall zones
- Get firewall zone details
- Create a new firewall zone
- Clone a firewall zone
- Update a firewall zone
- Delete a firewall zone

Object Representation

Firewall zone object location

api.cloudpassage.com/v1

```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique identifier of the firewall zone.</td>
</tr>
<tr>
<td>name</td>
<td>A unique name given to the firewall zone.</td>
</tr>
<tr>
<td>ip_address</td>
<td>The specified IP address(es) of the firewall zone.</td>
</tr>
<tr>
<td>system</td>
<td>Denotes whether the firewall zone is built-in/system or not. System zones can not be updated or deleted.</td>
</tr>
<tr>
<td>used_by</td>
<td><em>Read-only</em>. The list of firewall policies that use this firewall zone.</td>
</tr>
</tbody>
</table>
```

List firewall zones

Returns a list of all defined firewall zones.

```
GET https://api.cloudpassage.com/v1/firewall_zones/
```
Get firewall zone details

Returns details of the firewall zone specified by ID. The details include information on which firewall policies are using the zone.

GET https://api.cloudpassage.com/v1/firewall_zones/{id}

Create a new firewall zone

Creates a new firewall zone with the attributes specified in the request body. Returns the firewall zone details, including its ID, in the response body.

POST https://api.cloudpassage.com/v1/firewall_zones

Request Body

```json
{
  "firewall_zone": {
    "name": "databases",
    "ip_address": "10.10.10.1, 10.10.10.2, 10.10.10.3"
  }
}
```
Response

Status: 201 Location: https://api.cloudpassage.com/v1/firewall_zones/002736c0ae4b012ea3f240403472c9f3

{
  "firewall_zone": {
    "ip_address": "10.10.10.1, 10.10.10.2, 10.10.10.3",
    "used_by": [],
    "name": "databases",
    "system": false,
    "url": "https://api.cloudpassage.com/v1/firewall_zones/002736c0ae4b012ea3f240403472c9f3",
    "id": "002736c0ae4b012ea3f240403472c9f3"
  }
}

Clone a firewall zone

To clone a firewall zone, first call the Get firewall zone details method for the zone you want to clone. Then make the Create a new firewall zone call, passing a modified name and possibly new IP address(es).

Update a firewall zone

For the firewall zone specified by ID in the call URL, updates the attributes specified in the request body.

PUT https://api.cloudpassage.com/v1/firewall_zones/{id}

Request Body

```
{
  "firewall_zone": {
    "ip_address": "10.10.10.4"
  }
}
```

Response

Status: 204

Delete a firewall zone

Deletes the firewall zone specified by ID. If the call is successful, the zone is removed from Halo and cannot be retrieved.

Only non-system firewall zones that are not used by any firewall policy can be deleted. Attempting to delete a system firewall zone or a firewall zone that is used by firewall policies will result in a 422 response status.

DELETE https://api.cloudpassage.com/v1/firewall_zones/{id}
Response

Status: 204
Log-Based Intrusion Detection Policies

Use the Log-Based Intrusion Detection Policies endpoint to create and manipulate log-based intrusion detection policies.

To assign a log-based intrusion detection policy to a group, call the Assign one or more log-based intrusion detection policies to a group method of the Server Groups API endpoint.

- Object Representation
- List log-based intrusion detection policies
- Get a single log-based intrusion detection policy
- Create a new log-based intrusion detection policy
- Update a log-based intrusion detection policy
- Delete a log-based intrusion detection policy

Object Representation

Log-based intrusion detection policy object location

api.cloudpassage.com/v1

```plaintext
lids_policies
  id
```

Log-based intrusion detection policy object fields

Two levels of log-based intrusion detection policy information are available: core policy fields (accessed through, for example, the List log-based intrusion detection policies call), and rule fields (accessed through, for example, the Get a single log-based intrusion detection policy call).

Core log-based intrusion detection policy object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The Halo ID (unique identifier) of the log-based intrusion detection policy.</td>
</tr>
<tr>
<td>url</td>
<td>The full URL (including policy ID) to the log-based intrusion detection policy object.</td>
</tr>
<tr>
<td>name</td>
<td>A name given to the log-based intrusion detection policy.</td>
</tr>
<tr>
<td>description</td>
<td>Optional. A description of the log-based intrusion detection policy.</td>
</tr>
<tr>
<td>platform</td>
<td>The OS platform of the log-based intrusion detection policy. Either windows or linux.</td>
</tr>
<tr>
<td>template</td>
<td>true if this policy is a policy template; otherwise false.</td>
</tr>
<tr>
<td>retired</td>
<td>true if this policy is retired; otherwise false.</td>
</tr>
<tr>
<td>used_by</td>
<td>A list of IDs of the groups that use the log-based intrusion detection policy.</td>
</tr>
<tr>
<td>rules</td>
<td>An array of the rules that make up the policy. (Appears only in policy details.)</td>
</tr>
</tbody>
</table>

Log-based intrusion detection policy rule object fields
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>A name or description for the rule.</td>
</tr>
<tr>
<td>kind</td>
<td>windows_channel (Windows only) or text (Windows or Linux).</td>
</tr>
<tr>
<td>search_pattern</td>
<td>The search pattern to match against the log message. If the pattern matches, an event is created. See Search Expression Syntax in the Halo Operations Guide for the supported pattern syntax.</td>
</tr>
<tr>
<td>critical</td>
<td>true if an event logged by a match of this rule should be classified as critical; false if not.</td>
</tr>
<tr>
<td>active</td>
<td>true if this rule is active; false if it is inactive (not used by the policy).</td>
</tr>
<tr>
<td>alert</td>
<td>true if failure of this rule generates an email alert; false if not.</td>
</tr>
<tr>
<td>windows_event_channel</td>
<td>If the rule kind is windows_channel, this is the name of the event channel.</td>
</tr>
<tr>
<td>windows_event_id</td>
<td>If the rule kind is windows_channel, this is the ID of the target event.</td>
</tr>
<tr>
<td>file_path</td>
<td>If the rule kind is text, this is the full path to the log file to examine for this rule.</td>
</tr>
</tbody>
</table>

**List log-based intrusion detection policies**

Retrieves and displays core information for all defined log-based intrusion detection policies and policy templates.

*Note:* The results of this call may be paginated. See Pagination of Results for information on how to set up and retrieve paginated results from the Halo API.

GET https://api.cloudpassage.com/v1/lids_policies/

You can use this call to, for example, obtain the ID of an individual policy so that you can view or manipulate it by calling any of the other methods described here.

You can add parameters to the call to filter the results by the values of individual fields. For example:

GET https://api.cloudpassage.com/v1/lids_policies?platform=windows

GET https://api.cloudpassage.com/v1/lids_policies?template=true

GET https://api.cloudpassage.com/v1/lids_policies?retired=true

**Response**

**Status:** 200

```json
{
    "lids_policies": [
    {
        "id": "9bfb3cf01cbf01315e713c764e101158",
        "url": "https://api.cloudpassage.com/v1/lids_policies/9bfb3cf01cbf01315e713c764e101158",
        "name": "linux top 10 alerts template-1",
        "description": "Enter customization descriptions here",
        "platform": "linux",
        "template": true,
        "retired": false,
        "used_by": [
        
        ],
    },
    {
        "id": "0a622ea01c6a01315e6f3c764e101158",
        "url": "https://api.cloudpassage.com/v1/lids_policies/0a622ea01c6a01315e6f3c764e101158",
        "name": "Red Hat/Apache Intrusion Detection",
        "description": "See 'Acme Intrusion Detection Module Run Guide' for a description of this policy",
        "platform": "linux",
        "template": false,
        "retired": false,
        "used_by": [
        
        ],
        "name": "appservers-RHEL",
    }
    ]
}
Get a single log-based intrusion detection policy

Returns the details of the log-based intrusion detection policy specified by policy ID. Includes the details of all rules in the policy.

GET https://api.cloudpassage.com/v1/lids_policies/{id}

Response

Status: 200

```json
{
    "lids_policy": {
        "id": "cc9e87d01cb901315e703c764e101158",
        "url": "https://api.cloudpassage.com/v1/lids_policies/cc9e87d01cb901315e703c764e101158",
        "name": "winserver_critical_events",
        "description": "All events here are critical and generate alerts",
        "platform": "windows",
        "template": false,
        "retired": false,
        "used_by": [{
            "name": "webservers-1",
            "id": "7bbea00072b1012ec681404096c01709"
        },
        {
            "name": "windows-dbservers",
            "id": "6814047b0072b1012ec68140bea1406c"
        }],
        "rules": [
            {
                "name": "job start failure",
                "kind": "windows_channel",
                "search_pattern": "fail",
                "critical": true,
                "active": true,
                "alert": true,
                "windows_event_channel": "Microsoft-Windows-TaskScheduler/Operational",
                "windows_event_id": 101
            },
            ...
            {
                "name": "test",
                "kind": "text",
                "search_pattern": "fail",
                "critical": true,
                "active": true,
                "alert": true,
                "file_path": "C:\Program files\Acme\acme_log.txt"
            }
        ]
    }
}
```
Create a new log-based intrusion detection policy

Create a new log-based intrusion detection policy with the attributes and rules specified in the request body. Returns the created policy details, including its policy ID, in the response body.

**POST** https://api.cloudpassage.com/v1/lids_policies

**Request Body**

```json
{
  "lids_policy": {
    "name": "winserver_subcritical_events",
    "description": "These events are less critical and do not generate alerts",
    "platform": "windows",
    "template": false,
    "rules": [
      {
        "name": "job start failure",
        "kind": "windows_channel",
        "search_pattern": "fail",
        "critical": true,
        "active": true,
        "alert": false,
        "windows_event_channel": "Microsoft-Windows-TaskScheduler/Operational",
        "windows_event_id": 101
      }
    ]
  }
}
```

**Response**

**Status:** 201

**Location:** https://api.cloudpassage.com/v1/lids_policies/2343sh34h23254543543hgf5

```json
{
  "lids_policy": {
    "id": "2343sh34h23254543543hgf5",
    "url": "https://api.cloudpassage.com/v1/lids_policies/2343sh34h23254543543hgf5",
    "name": "winserver_subcritical_events",
    "description": "These events are less critical and do not generate alerts",
    "platform": "windows",
    "template": false,
    "retired": false,
    "used_by": []
    "rules": [
      {
        "name": "job start failure",
        "kind": "windows_channel",
        "search_pattern": "fail",
        "critical": true,
        "active": true,
        "alert": false,
        "windows_event_channel": "Microsoft-Windows-TaskScheduler/Operational",
        "windows_event_id": 101
      }
    ]
  }
}
```
Update a log-based intrusion detection policy

Use this call to add or update individual attributes and rules of the log-based intrusion detection policy that you specify by policy ID. In the request body, include only the attributes and rules that you want added or modified; other parts of the policy will remain unchanged.

PUT https://api.cloudpassage.com/v1/lids_policies/{policy_id}

Request Body

```json
{
  "lids_policy": {
    "rules": [
      {
        "name": "new rule added",
        "kind": "text",
        "search_pattern": "fail",
        "critical": true,
        "active": true,
        "alert": true,
        "file_path": "C:\Program files\Acme\acme_log.txt"
      }
    ]
  }
}
```

Response

Status: 204

Delete a log-based intrusion detection policy

Deletes an existing log-based intrusion detection policy from Halo. The policy can be deleted regardless of whether it is assigned to a group.

DELETE https://api.cloudpassage.com/v1/lids_policies/{policy_id}

Response

Status: 204
Special Events Policies

Use the Special Events Policies endpoint to retrieve a list of all defined special-events policies. You can use the List special events policies call to, for example, obtain a policy ID to use as input to the Assign a special events policy to a group method of the Server Groups endpoint.

- Object Representation
- List special events policies
- Get a single special events policy

Object Representation

Special events policy object location

```
api.cloudflare.com/v1
special_events_policies/
id
```

Special events policy object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The Halo ID (a unique identifier) of the special-events policy.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the special events policy.</td>
</tr>
<tr>
<td>module</td>
<td>The Halo security module that this policy applies to. For a special events policy, it is se.</td>
</tr>
<tr>
<td>group_id</td>
<td>The Halo ID of the policy's owning group.</td>
</tr>
<tr>
<td>group_name</td>
<td>The name of the policy's owning group.</td>
</tr>
<tr>
<td>description</td>
<td>An optional description of the policy.</td>
</tr>
<tr>
<td>global</td>
<td>true if this policy is the Global Events Policy; otherwise false.</td>
</tr>
<tr>
<td>shared</td>
<td>true if this policy is shared to descendants of the owning group; otherwise false.</td>
</tr>
<tr>
<td>read_only</td>
<td>true if this policy cannot be edited; otherwise false.</td>
</tr>
<tr>
<td>retired</td>
<td>true if this policy is retired; otherwise false.</td>
</tr>
<tr>
<td>created_at</td>
<td>The timestamp (in ISO-8601 format) of this policy's creation.</td>
</tr>
<tr>
<td>updated_at</td>
<td>The timestamp (in ISO-8601 format) of this policy's last update.</td>
</tr>
<tr>
<td>created_by</td>
<td>The Halo username of the user who created this policy.</td>
</tr>
<tr>
<td>updated_by</td>
<td>The Halo username of the user who last updated this policy.</td>
</tr>
<tr>
<td>used_by</td>
<td>An array of the groups that use this special events policy. Includes the following sub-fields:</td>
</tr>
</tbody>
</table>
List special events policies

Returns a list of all defined special events policies, including the default Global Events Policy. The results for each policy include Halo ID and other basic information for each profile. The results do not include details such as the policy's event settings.

GET https://api.cloudpassage.com/v1/special_events_policies/

Response

Status: 200

```
{
"special_events_policies": [
{
"id": "0c53e1c0292411e6a70f5d1eba4a88dd",
"name": "QA1 SE Policy",
"module": "se",
"group_id": "0962bfa087bc01323e360670140ec224",
"group_name": "qa-functional",
"description": "",
"global": false,
"shared": true,
"read_only": false,
"retired": false,
"created_at": "2016-06-03T00:42:28.376Z",
"updated_at": "2016-06-03T00:42:47.939Z",
"created_by": "jherz",
"updated_by": "jherz",
"used_by": [
{
"id": "e85953544e3f11e6a61bd5598aed2",
"name": "selinite"
}
]
},
{
"id": "08a5491c291d11e68b4821439f895476",
"name": "QA2 SE Policy",
"module": "se",
"group_id": "0962bfa087bc01323e360670140ec224",
"group_name": "qa-functional",
"description": "",
"global": false,
"shared": false,
"read_only": false,
"retired": false,
"created_at": "2016-06-02T00:42:28.376Z",
"updated_at": "2016-06-02T00:42:47.939Z",
"created_by": "cheadley+qa@acme.com",
"updated_by": "cheadley+qa@acme.com",
"used_by": []
}
]
}
```

Get a single special events policy

Returns the special events policy specified by ID in the call URL. The results do not include details such as the policy's event settings.

GET https://api.cloudpassage.com/v1/special_events_policies/{id}

Response

Status: 200

```
{

```
"id": "0972b4f087bc01323e360670140ec224",
"name": "Global Events Policy",
"module": "se",
"group_id": "0962bfa087bc01323e360670140ec224",
"group_name": "qa-functional",
"description": "This is the default Special Events policy ...",
"global": true,
"shared": true,
"read_only": false,
"retired": false,
"created_at": "2015-01-26T19:04:11.764Z",
"updated_at": "2016-03-15T15:58:09.510Z",
"created_by": null,
"updated_by": null,
"used_by": []}
Events

Use the Events endpoint to retrieve any of the security events and audit events that Halo logs. You can, for example, develop a tool that uses the API to obtain the events in JSON format, reformats them if necessary, and then passes them on to a third-party log analyzer or SIEM application.

- Object Representation
- List events
- Supported Event Types

Object Representation

Event object location

api.cloudpassage.com/v1/events

Event object fields

Note: The fields that appear vary depending on the type of event. The following table includes all possible fields; no single event includes all of the fields listed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Identifier for this event.</td>
</tr>
<tr>
<td>type</td>
<td>The name of the event type, as used by the CloudPassage API. See Supported Event Types, below.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the event, as displayed in the Halo Portal.</td>
</tr>
<tr>
<td>message</td>
<td>The event message as displayed to the user.</td>
</tr>
<tr>
<td>critical</td>
<td>Criticality of the event. true if critical, false if not.</td>
</tr>
<tr>
<td>created_at</td>
<td>Event creation timestamp. Formatted in ISO 8601.</td>
</tr>
<tr>
<td>policy_name</td>
<td>Name of the policy that triggered the event.</td>
</tr>
<tr>
<td>server_hostname</td>
<td>Server's hostname.</td>
</tr>
<tr>
<td>server_ip_address</td>
<td>Server's connecting IP address.</td>
</tr>
<tr>
<td>server Reported fqdn</td>
<td>The internal fully qualified domain name of the server.</td>
</tr>
<tr>
<td>server_label</td>
<td>A user-assigned label or description for the server.</td>
</tr>
<tr>
<td>server_display_name</td>
<td>(In priority order) either server_label, server Reported fqdn, or server_hostname.</td>
</tr>
<tr>
<td>server_primary_ip_address</td>
<td>Server's primary IP address (the first routable address in the server's sorted list of supported interfaces and addresses).</td>
</tr>
<tr>
<td>server_id</td>
<td>Server's Halo ID.</td>
</tr>
<tr>
<td>server_platform</td>
<td>Server's platform (Windows or Linux).</td>
</tr>
<tr>
<td>server_group_name</td>
<td>Server's group name.</td>
</tr>
<tr>
<td>tag</td>
<td>The server tag, if any, assigned to the server on which the event occurred.</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>server_group_path</td>
<td>The full path (in the group hierarchy) to the server on which the event occurred.</td>
</tr>
<tr>
<td>csp_provider</td>
<td>The cloud service provider; i.e., <code>aws_ec2</code>, <code>azure</code>, <code>gcp</code>. (For cloud servers only.)</td>
</tr>
<tr>
<td>csp_account_id</td>
<td>The ID of the cloud service provider account. (For cloud servers only.)</td>
</tr>
<tr>
<td>csp_availability_zone</td>
<td>The availability zone in which the instance launched; for example, <code>us_west_1</code>. (For cloud servers only.)</td>
</tr>
<tr>
<td>csp_image_id</td>
<td>The ID of the Amazon Machine Image from which the workload was instantiated. (For cloud servers only.)</td>
</tr>
<tr>
<td>csp_instance_id</td>
<td>The cloud service provider's ID of the instance. (For cloud servers only.)</td>
</tr>
<tr>
<td>csp_instance_type</td>
<td>The type of hardware the host computer used for the instance. (For cloud servers only.)</td>
</tr>
<tr>
<td>csp_kernel_id</td>
<td>The ID of the kernel image launched with this instance. (For cloud servers only.)</td>
</tr>
<tr>
<td>csp_private_ip</td>
<td>The private IP address of the instances. In cases where multiple network interfaces are present, this refers to the <code>eth0</code> device. (For cloud servers only.)</td>
</tr>
<tr>
<td>csp_region</td>
<td>The cloud provider region in which the instance was launched; for example, <code>AP South 1</code>, <code>AP Northeast 1</code>, <code>CA Central 1</code>, <code>EU West 1</code>, and so on. (For cloud servers only.)</td>
</tr>
<tr>
<td>csp_security_groups</td>
<td>The security groups assigned to the cloud instance. (For cloud servers only.)</td>
</tr>
<tr>
<td>csp_instance_tags</td>
<td>User-defined key/value pairs assigned to the instance.</td>
</tr>
<tr>
<td>registry_name</td>
<td>The name of the registry. (For container image events.)</td>
</tr>
<tr>
<td>repository_name</td>
<td>The name of the repository. (For container image events.)</td>
</tr>
<tr>
<td>repository_digest</td>
<td>The full SHA-256 digest of the repository. (For container image events.)</td>
</tr>
<tr>
<td>image_id</td>
<td>The Halo ID of the container image. (For container image events.)</td>
</tr>
<tr>
<td>image_sha</td>
<td>The Docker SHA-256 image representation for this image. (For container image events.)</td>
</tr>
<tr>
<td>image_tag</td>
<td>The primary tag assigned to the image (the first entry in the tags array). (For container image events.)</td>
</tr>
<tr>
<td>container_id</td>
<td>The Halo ID of the container name. (This is also its Docker ID.) (For container events.)</td>
</tr>
<tr>
<td>container_event_type</td>
<td>The type of container event. (For container events.)</td>
</tr>
<tr>
<td>container_name</td>
<td>The name of the container. (For container events.)</td>
</tr>
<tr>
<td>container_created_at</td>
<td>The date and time of the creation (instantiation) of the container. (For container events.)</td>
</tr>
<tr>
<td>original_log_entry</td>
<td>The full text of the triggering log entry (for LIDS events). May be empty, or plain text, XML, or other format.</td>
</tr>
<tr>
<td>server_new_ip_address</td>
<td>Server's new IP address. (For address-change events.)</td>
</tr>
<tr>
<td>server_old_ip_address</td>
<td>Server's old IP address. (For address-change events.)</td>
</tr>
<tr>
<td>actor_key_id</td>
<td>The ID of the API key used. (For key-related events that have an actor.)</td>
</tr>
<tr>
<td>actor_key_label</td>
<td>The label of the API key used. (For key-related events that have an actor.)</td>
</tr>
<tr>
<td>actor_username</td>
<td>Username of the user who requested the change. (For events that have an actor.)</td>
</tr>
<tr>
<td>actor_ip_address</td>
<td>IP address of the user who requested the change. (For events that have an actor.)</td>
</tr>
<tr>
<td>actor_country</td>
<td>Location of the user who requested the change. (For events that have an actor.)</td>
</tr>
<tr>
<td>target_username</td>
<td>Username of the user that is being modified. (For account-related events.)</td>
</tr>
<tr>
<td>daemon_version</td>
<td>Current version of the Halo agent. (For agent-related events.)</td>
</tr>
<tr>
<td>previous_daemon_version</td>
<td>Previous version of the Halo agent. (For agent version-change events.)</td>
</tr>
<tr>
<td>rule_name</td>
<td>Configuration or log-based intrusion detection policy rule that failed.</td>
</tr>
<tr>
<td>rule_reference_identifiers</td>
<td>An optional comma-separated list of IDs applied to this policy rule for compliance purposes. Each identifier is a name-value pair with this JSON format: <code>&quot;name&quot;:&quot;value&quot;</code> — for example, <code>&quot;USB&quot;:&quot;67&quot;</code>, <code>&quot;CIS&quot;:&quot;1.1.2&quot;</code></td>
</tr>
<tr>
<td>server_account_username</td>
<td>Local server account username. (For account-related events.)</td>
</tr>
<tr>
<td>server_account_id</td>
<td>Local server account id. (For account-related events.)</td>
</tr>
<tr>
<td>scan_id</td>
<td>Halo ID of the scan that generated this event. (For FIM events.)</td>
</tr>
</tbody>
</table>
finding_id | Halo ID of the specific scan finding that generated this event. (For FIM events.)
api_key_id | API Key's ID. (For key-related events.)
api_key_label | API Key's name. (For key-related events.)
package_name | The name of the software package in this (vulnerability) event.
package_version | The version number of the software package in this (vulnerability) event.
cves | An array of the CVEs in this (vulnerability) event. Each CVE has the following subfields:
  CVE | The Common Vulnerability and Exposure identifier for this CVE.
  CVSS | The Common Vulnerability Scoring System (CVSS) score for the severity of this CVE.
  cpe | (Windows) The Common Platform Enumeration (CPE) name for the package in this (vulnerability) event.
ec2_instance_id | The AWS EC2 instance ID of the server. (For AWS servers only.)
ec2_account_id | The AWS EC2 ID of the account under which the server instance was created. (For AWS servers only.)
object_name | Name of the FIM object. For a file it is a file path. (For FIM events.)

List events

Retrieves all security events from the Halo database.

GET https://api.cloudpassage.com/v1/events/

This call supports many optional parameters:

- By using the filter parameters since (inclusive) and until (exclusive), you can restrict the retrieved events to a time/date range. The value for each parameter is an ISO 8601 formatted timestamp string (for example YYYY-MM-DD, or YYYY-MM-DDThh:mmZ for Zulu time zone). For example:


- By using the filter parameters type, group_id, server_id, and server_platform, you can restrict the results to events of specified types, or occurring in a specified group or on a specified server, or on a specified server platform family (windows or linux). For example:

  GET https://api.cloudpassage.com/v1/events?type=fim_signature_changed,csm_rule_failed
  (see Supported Event Types below for a list of valid values for the type parameter)

  GET https://api.cloudpassage.com/v1/events?group_id=1f8503e07dc6012f112040403472c9f3

  GET https://api.cloudpassage.com/v1/events?server_id=c827779463036a0b90faf16283927dc2

  GET https://api.cloudpassage.com/v1/events?server_platform=windows

- For all server events, you can restrict the results to AWS servers with a specific AWS EC2 instance ID or account ID by using the filter parameters ec2_instance_id and ec2_account_id:

  GET https://api.cloudpassage.com/v1/events?ec2_account_id=856192027328

- For file integrity events, you can use the filter parameters scan_id and finding_id to view the details of the individual objects in the event target that failed or passed:

  GET https://api.cloudpassage.com/v1/scans/{scan_id}/findings/{finding_id}
  (For more detailed documentation on this call, see Get file integrity scan findings details.)

- The response is paginated, with a page size of 10 items by default. You can specify custom page sizes up to 100 items by using the per_page parameter. You can also specify which page to retrieve by using the page parameter. See Pagination of Results for further explanation and examples.
You can combine any of the above parameters in your List events calls.

Response
Status: 200

Note: The fields that you see in the response vary depending on the type of event. The following is just one example.

```
{
    "events": [
        {
            "id": "94ed5efa03811e8bac34ffea2af23232",
            "type": "lids_rule_failed",
            "name": "Log-based intrusion detection rule matched",
            "message": "Log-based intrusion detection rule rule2 matched on Linux ...",
            "server_id": "6ff6907bc811e896c42d7881e8c8b6",
            "critical": true,
            "server_platform": "Linux",
            "server_hostname": "ip-10-0-1-248",
            "server_group_name": "DEV20845",
            "server_ip_address": "13.57.221.240",
            "server_reported_fqdn": "ip-10-0-1-248.us-west-1.compute.internal",
            "server_label": null,
            "server_primary_ip_address": "10.0.1.248",
            "tag": null,
            "server_group_path": "qa-automation-100/DEV20845",
            "ec2_instance_id": "i-0ba3524709b352ef9",
            "ec2_account_id": "856192027328",
            "csp_provider": "aws ec2",
            "csp_account_id": "856192027328",
            "csp_availability_zone": "us-west-1b",
            "csp_image_id": "ami-18726478",
            "csp_instance_id": "i-0ba3524709b352ef9",
            "csp_instance_type": "t2.micro",
            "csp_kernel_id": null,
            "csp_private_ip": "10.0.1.248",
            "csp_region": "us-west-1",
            "csp_security_groups": null,
            "csp_instance_tags": null,
            "policy_name": "Test",
            "rule_name": "rule2",
            "original_log_entry": "2018-09-24 20:29:44.2 ip-10-0-1-248.us-west-1.compute...",
            "additional_details": true,
            "server_display_name": "ip-10-0-1-248.us-west-1.compute.internal"
        },
        ...
    ]
}
```

Supported Event Types

The leftmost column of the table below lists the values that you can supply for the type parameter in the List events call. The middle column lists the equivalent filter-parameter names displayed in the "event Type" drop-down list on the Security Events History page of the Halo Portal. The rightmost column gives additional explanatory notes for some of the values.

For each event type that you pass in the type parameter for your call, you must provide the exact spelling shown in the left column (except for capitalization, which does not matter). If you pass any other spelling, it is considered an unknown value and the call returns no results.

<table>
<thead>
<tr>
<th>API value</th>
<th>Portal value</th>
</tr>
</thead>
<tbody>
<tr>
<td>activation_link_failed</td>
<td>Halo user activation failed</td>
</tr>
<tr>
<td>agent_key_regenerated</td>
<td>Agent registration key regenerated</td>
</tr>
<tr>
<td>agent_restarted</td>
<td>Agent restarted</td>
</tr>
<tr>
<td>agent_upgrade_failed</td>
<td>Agent upgrade failed</td>
</tr>
<tr>
<td>agent_upgrade_succeeded</td>
<td>Agent upgrade succeeded</td>
</tr>
</tbody>
</table>
lids_policy_created
lids_policy_deleted
lids_policy_exported
lids_policy_modified
lids_policy_unassigned
lids_rule_failed
lids_scan_disabled
lids_scan_enabled
local_account_activate_request
local_account_create_request
local_account_deactivate_request
local_account_update_request
local_account_update_ssh_keys_request
master_account_linked
multiple_root_accounts
new_server
password_changed
password_config_changed
password_recovery_request_failed
password_recovery_requested
password_recovery_success
portal_audit_policy_modified
registry_add
registry_changed
registry_deleted
registry_status_changed
repository_add
repository_delete
repository_modified
sam_scan_requested
sca_policy_assigned
sca_policy_created
sca_policy_deleted
sca_policy_exported
sca_policy_imported
sca_policy_modified
sca_policy_unassigned
sca_rule_failed
sca_scan_terminated
scan_time_limit_modified
server_account_created
server_account_deleted
server_deactivated
server_deleted
server_firewall_modified_locally
server_group_added
server_group_deleted
server_group_moved
server_missing
server_moved
server_reactivated
server_retired
server_unretired
session_timeout
session_timeout_modified
Log-based intrusion detection policy created
Log-based intrusion detection policy deleted
Log-based intrusion detection policy exported
Log-based intrusion detection policy modified
Log-based intrusion detection policy unassigned
Log-based intrusion detection rule matched
Log-based intrusion detection disabled
Log-based intrusion detection enabled
Local account activation requested
Local account creation requested
Local account deactivation requested
Local account modification requested
Local account ssh keys update requested
Master account linked
Multiple root accounts detected (linux only)
New server
Halo password changed
Halo password authentication settings modified
Halo password recovery request failed
Halo password recovery requested
Halo password recovery success
Portal audit policy modified
Image registry added
Image registry changed
Image registry deleted
Image registry status changed
Image repository added
Image repository deleted
Image repository modified
Server account scan requested
Configuration policy assigned
Configuration policy created
Configuration policy deleted
Configuration policy exported
Configuration policy imported
Configuration policy modified
Configuration policy unassigned
Configuration rule matched
Configuration scan terminated
Agent scan time limit modified
Local account created
Local account deleted
Server deactivated
Server deleted
Server firewall modified
Group added
Group deleted
Group moved
Server missing
Server moved to another group
Server reactivated
Server retired
Server un-retired
Halo session timeout
Halo session timeout modified
*The daemon_compromised event is reported only once, when an agent self-verification scan first discovers that the agent has been compromised. Subsequent self-verification scans will not generate duplicate events, as long as the compromised state persists.*
Alert Profiles

Use the Alert Profiles endpoint to retrieve a list of all defined alert profiles. You can use the List alert profiles call to, for example, obtain profile IDs to use as input to the Assign one or more alert profiles to a group method of the Server Groups endpoint.

- Object Representation
- List alert profiles

Object Representation

Alert profile object location

api.cloudpassage.com/v1/alert_profiles

Alert profile object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The Halo ID (a unique identifier) of the alert profile.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the alert profile.</td>
</tr>
<tr>
<td>group_id</td>
<td>The Halo ID of the alert profile's owning group.</td>
</tr>
<tr>
<td>group_name</td>
<td>The name of the alert profile's owning group.</td>
</tr>
<tr>
<td>description</td>
<td>Optional description of the alert profile.</td>
</tr>
<tr>
<td>frequency</td>
<td>How frequently alert notifications are sent out. Ranges from instant to every_week.</td>
</tr>
<tr>
<td>created_at</td>
<td>The timestamp (in ISO-8601 format) of this alert profile's creation.</td>
</tr>
<tr>
<td>updated_at</td>
<td>The timestamp (in ISO-8601 format) of this alert profile's last update.</td>
</tr>
<tr>
<td>created_by</td>
<td>The Halo username of the user who created this alert profile.</td>
</tr>
<tr>
<td>updated_by</td>
<td>The Halo username of the user who last updated this alert profile.</td>
</tr>
<tr>
<td>shared</td>
<td>The Halo username of the user who last updated this alert profile.</td>
</tr>
<tr>
<td>used_by</td>
<td>\textbf{true} if this alert profile is shared to descendant groups of the owning group; \textbf{false} if it is not.</td>
</tr>
<tr>
<td>id</td>
<td>The Halo ID of the group.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the group.</td>
</tr>
</tbody>
</table>

List alert profiles

Returns a list of all defined alert profiles, including the Halo ID and other basic information for each profile. The results do not include details such as a profile's list of alert recipients.

\textbf{GET https://api.cloudpassage.com/v1/alert_profiles/}
Response

Status: 200

```json
{
  "count": 2,
  "alert_profiles": [
    {
      "id": "0226a27af95c11e5a92a471a4310f7c2",
      "name": "script alert(1) profile",
      "group_id": "0962bfa087bc01323e360670140ec224",
      "group_name": "qa-functional",
      "description": "script alerts",
      "frequency": "every_week",
      "created_at": "2016-04-03T05:22:07.306Z",
      "created_by": null,
      "updated_by": "jherz",
      "shared": true,
      "used_by": [
        {
          "id": "e0ae5bf0cac211e5925f353d8d5ee575",
          "name": "C-Group"
        },
        {
          "id": "9d0c0754027f11e6bc0a3b672c145ea8",
          "name": "TestTest11"
        },
        {
          "id": "0a59c07d092ad0132954206ba9a9c633c",
          "name": "chef"
        }
      ]
    },
    {
      "id": "c25d8d4201211e6a3e669ed2e08b040",
      "name": "jh_profile",
      "group_id": "6c76501cfb9611e590696d80e6b442ab",
      "group_name": "ops-functional",
      "description": "",
      "frequency": "instant",
      "created_at": "2016-04-13T02:52:28.280Z",
      "updated_at": "2016-04-13T18:55:57.999Z",
      "created_by": "jherz",
      "updated_by": "jherz",
      "shared": true,
      "used_by": []
    }
  ]
}
```

Using search filters to narrow results

If your organization has a large number of alert profiles, you can narrow the results returned from this method by applying values in any of the following fields as search filters:

- name
- description (partial search supported)
- updated_by
- created_by
- shared (boolean)
- frequency
- used_by

For example:

GET https://api.cloudpassage.com/v1/alert_profiles?created_by=jherz

GET https://api.cloudpassage.com/v1/alert_profiles?shared=true

GET https://api.cloudpassage.com/v1/alert_profiles?used_by=C-Group

GET https://api.cloudpassage.com/v1/alert_profiles?used_by=c25d8d4201211e6a3e669ed2e08b040
Saved Searches

Use the Saved Searches endpoint to create and manage the call URLs used to search and filter Halo servers. You can use the API to list searches, get the details of a search, and create, update, or delete a search.

You can also use the Halo API to execute any of the saved searches. See Executing a saved search.

- Object Representation
- List saved searches
- Get a single saved search
- Create a new saved search
- Update a saved search
- Delete a saved search
- Executing a saved search

Object Representation

Each object in this endpoint represents a saved search of the Halo database, to be performed through the Halo API. Each search queries a single API endpoint. The search object contains six fields, including an array of search criteria (filters).

Halo search object location

api.cloudpassage.com/v1

   searches
      id

Halo search object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A unique identifier for the search.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the search.</td>
</tr>
<tr>
<td>endpoint</td>
<td>The API endpoint that the search accesses.</td>
</tr>
<tr>
<td>criteria</td>
<td>(Optional) An array of one or more search criteria (filters) that, along with the endpoint value, compose the search URL.</td>
</tr>
<tr>
<td>url</td>
<td>(In response JSON only) The URL to the Halo search object. This is the same URL used by the Get a single saved search method.</td>
</tr>
<tr>
<td>search_url</td>
<td>(In response JSON only) A URL to use in a GET request to the Halo API to execute this search.</td>
</tr>
</tbody>
</table>

List saved searches

Returns a list of all stored Halo searches. Includes all fields for each search, including the search criteria.
GET https://api.cloudpassage.com/v1/searches

You can use this call to, for example, obtain the ID of an individual search so that you can view or manipulate it by calling any of the other methods described here.

Response

Status: 200

```
{
  "searches": [
    {
      "id": "118a18a0d7b301319c1e3c764e101158",
      "name": "non-active servers in US-west",
      "endpoint": "servers",
      "criteria": {
        "state": "missing,deactivated",
        "server_label": "US-west"
      },
      "url": "https://api.cloudpassage.com/v1/searches/118a18a0d7b301319c1e3c764e101158"
    },
    {
      "id": "79509a10d7bf01319c1f3c764e101158",
      "name": "servers unpatched for KB2485376",
      "endpoint": "servers",
      "criteria": {
        "missing_kb": "KB2485376"
      },
      "search_url": "https://api.cloudpassage.com/v1/servers?missing_kb=KB2485376",
      "url": "https://api.cloudpassage.com/v1/searches/79509a10d7bf01319c1f3c764e101158"
    },
    ...
    {
      "id": "2171ae70d87d01319c3a3c764e101158",
      "name": "Windows Daemon issues in MSSQL group",
      "endpoint": "events",
      "criteria": {
        "type": "daemon_compromised,daemon_version_change",
        "server_platform": "windows",
        "group_id": "1f8503e07dc6f12040403472c9f3"
      },
      "search_url": "https://api.cloudpassage.com/v1/events?type=daemon_compromised,daemon_version_change&server_platform=windows&group_id=1f8503e07dc6f12040403472c9f3",
      "url": "https://api.cloudpassage.com/v1/searches/2171ae70d87d01319c3a3c764e101158"
    }
  ]
}
```

Get a single saved search

Returns the details of the stored search specified by search ID. Includes the details of all search criteria.

GET https://api.cloudpassage.com/v1/searches/{id}

Response

Status: 200

```
{
  "search": {
    "id": "118a18a0d7b301319c1e3c764e101158",
    "name": "non-active linux servers",
    "endpoint": "servers",
```

237
Create a new saved search

Creates and stores a new search with the attributes specified in the request body. The request body must include values for name and endpoint, and can optionally include any number of search criteria. Note:

- Each search criterion has the form "field" : "value" in the request JSON.
- To include multiple values for a given field, use the form "field" : "value1,value2,..." (no space between the comma and the following value). The values are OR'd in the search.
- The set of available search criteria varies by API endpoint. See the documentation for each API endpoint to learn what searchable fields or other criteria it supports.
- All searches also support the criteria page (page number of the results) and page_size (number of results per page), allowing you to control the pagination of the results when the search is executed.
- Criteria values that can include spaces or special characters must be URL-encoded in the request body. For example, if a criterion specifies the kernel name "Microsoft Windows Server 2008 R2 Datacenter", the request JSON entry should be formatted like this:

  "kernel_name" : "Microsoft+Windows+Server+2008+R2+Datacenter"

The response body includes the details of the new saved search, including its ID, URL, and search URL.

POST https://api.cloudpassage.com/v1/searches

Request Body

```
{  
  "search" : {  
    "name" : "bad win login events",
    "endpoint" : "events",
    "criteria" : {  
      "type" : "halo_login_failure,halo_user_locked",
      "server_platform" : "windows",
      "group_id" : "1f8503e07dc6012f112040403472c9f3"
    }
  }
}
```

Response

Status: 201

```
{
  "search" : {
    "id" : "2171ae70d87d01319c3a3c764e101158",
    "name" : "bad win login events",
    "endpoint" : "events",
    "criteria" : {  
      "type" : "halo_login_failure,halo_user_locked",
      "server_platform" : "windows",
      "group_id" : "1f8503e07dc6012f112040403472c9f3"
    }
  },
  "search_url" : "https://api.cloudpassage.com/v1/events?type=halo_login_failure,halo_user_locked&server_platform=windows&group_id=1f8503e07dc6012f112040403472c9f3",
  "url" : "https://api.cloudpassage.com/v1/searches/2171ae70d87d01319c3a3c764e101158"
}
```
Update a saved search

For the existing saved search specified by ID in the call URL, updates the values of the attributes specified in the request body.

Important: If the request body includes any search criteria, those criteria will replace all existing criteria in the search.

PUT https://api.cloudpassage.com/v1/searches/{id}

Request Body

```json
{
  "search": {
    "name": "bad LINUX login events",
    "endpoint": "events",
    "criteria": {
      "type": ["halo_login_failure", "halo_user_locked"],
      "server_platform": "linux",
      "group_id": "1f8503e07dc6012f112040403472c9f3"
    }
  }
}
```

Response

Status: 204

Delete a saved search

Deletes the Halo search specified by search ID. If the call is successful, the search is removed from Halo and cannot be retrieved.

DELETE https://api.cloudpassage.com/v1/searches/{id}

Response

Status: 204

Executing a saved search

To execute a saved search:

1. Call the List searches or Get a single search method of this API endpoint.
2. Copy the contents of the search_url field in the response.
3. Execute that string as an HTTP GET request to the Halo API.

The search results are by default returned in JSON format. If you are searching the servers endpoint and want the results in PDF or CSV format instead, modify the search URL by appending .csv or .pdf to the endpoint name, like this:

https://api.cloudpassage.com/v1/servers.csv?state=missing,deactivated&platform=linux
Alternatively, you can append a **format** parameter to the search URL, like this:

Global Scanner Settings

Use the Scanner Settings endpoint to view or set the values of selected agent-scanning settings that are global defaults for all groups in the Halo account. These global values can be overridden by group scanner settings defined for individual groups.

Currently, scan time limits are the only global scanner settings exposed in the Halo API.

- Object representation
- List global scanner settings
- Update global scanner settings

Object Representation

Global scanner settings object location

api.cloudpassage.com/v1

scanner_settings

Global scanner_settings object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fim_scan_time_limit</td>
<td>The maximum number of minutes (in CPU time) to allow for a file-integrity scan to complete. Valid values are 1 through 60; a value of null means that there is no time limit. Any scan that has not completed by the time limit is terminated with a scan status of &quot;Failed (terminated)&quot;. and a &quot;fim scan terminated&quot; audit event is created.</td>
</tr>
<tr>
<td>csm_scan_time_limit</td>
<td>The maximum number of minutes (in CPU time) to allow for a configuration scan to complete. Valid values are 1 through 60; a value of null means that there is no time limit. Any scan that has not completed by the time limit is terminated with a scan status of &quot;Failed (terminated)&quot;. and a &quot;csm scan terminated&quot; audit event is created.</td>
</tr>
<tr>
<td>svm_scan_time_limit</td>
<td>The maximum number of minutes (in CPU time) to allow for a vulnerability scan to complete. Valid values are 1 through 60; a value of null means that there is no time limit. Any scan that has not completed by the time limit is terminated with a scan status of &quot;Failed (terminated)&quot;. and an &quot;svm scan terminated&quot; audit event is created</td>
</tr>
</tbody>
</table>
Returns the global default scanner settings for the Halo account. In the Halo portal, these settings appear under **Settings > Agent Settings** in Site Administration. Currently the scan time limits are the only global scanner settings accessible through the Halo API.

These global settings can be overridden on a per-group bases by **group scanner settings** in the Halo API, or under **Settings > Agent Settings** for the specified group in the Halo portal.

**GET** https://api.cloudpassage.com/v1/scanner_settings

**Response**

**Status: 200**

```
{
  "scanner_settings": {
    "fim_scan_time_limit": null,
    "csm_scan_time_limit": 11,
    "svm_scan_time_limit": 34
  }
}
```

**Update global scanner settings**

Updates the global default scanner settings with the values of the scanner settings specified in the request JSON. Currently, only the scan time limits settings can be changed through the API.

Modifying any of the scan-time limits triggers a **scan_time_limit_modified** audit event.

**PUT** https://api.cloudpassage.com/v1/scanner_settings

**Request Body**

```
{
  "scanner_settings": {
    "csm_scan_time_limit": null
  }
}
```

**Response**

**Status: 204**
Group Scanner Settings

Use the Group Scanner Settings endpoint to view or set the values of the agent-scanning settings for a specified group.

- Object representation
- List group scanner settings
- Update group scanner settings

Object Representation

Group scanner settings object location

```
api.cloudpassage.com/v1/groups/id/scanner_settings
```

Group scanner_settings object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>firewall_enforce</td>
<td><code>true</code> if the group's firewall policy is to be applied to all servers of the group, including servers whose agent runs in audit mode (read-only); <code>false</code> if the policy is not applied to read-only servers. Default = <code>false</code>.</td>
</tr>
<tr>
<td>fim_scan_time_limit</td>
<td>The maximum number of minutes (in CPU time) to allow for a file-integrity scan to complete. Valid values are 1 through 60; a value of null means that there is no time limit. Any scan that has not completed by the time limit will be terminated with a status of &quot;Failed (terminated)&quot;. and a &quot;fim scan terminated&quot; audit event is created.</td>
</tr>
<tr>
<td>csm_scan_time_limit</td>
<td>The maximum number of minutes (in CPU time) to allow for a configuration scan to complete. Valid values are 1 through 60; a value of null means that there is no time limit. Any scan that has not completed by the time limit is terminated with a scan status of &quot;Failed (terminated)&quot;. and a &quot;csm scan terminated&quot; audit event is created.</td>
</tr>
<tr>
<td>svm_scan_time_limit</td>
<td>The maximum number of minutes (in CPU time) to allow for a vulnerability scan to complete. Valid values are 1 through 60; a value of null means that there is no time limit. Any scan that has not completed by the time limit is terminated with a scan status of &quot;Failed (terminated)&quot;. and an &quot;svm scan terminated&quot; audit event is created.</td>
</tr>
</tbody>
</table>
List group scanner settings

Returns the scanner settings of the group specified by ID in the call URL.

In the Halo portal, these scanner settings appear under Settings > Agent Settings for the specified group, and they override the global scanner settings that are defined under Settings > Agent Settings in Site Administration.

GET https://api.cloudpassage.com/v1/groups/{id}/scanner_settings

Response

Status: 200

```
{
   "scanner_settings": {
      "firewall_enforce": false,
      "fim_scan_time_limit": null,
      "csm_scan_time_limit": null,
      "svm_scan_time_limit": null
   }
}
```

Update group scanner settings

Updates the scanner settings of the specified group with the values of the scanner settings specified in the request JSON.

Modifying any of the scan-time limits triggers a scan_time_limit_modified audit event.

PUT https://api.cloudpassage.com/v1/groups/{id}/scanner_settings

Request Body

```
{
   "scanner_settings": {
      "firewall_enforce": true,
      "csm_scan_time_limit": 4
   }
}
```

Response

Status: 204
Users

Use the Users API endpoint to retrieve information on all Halo users in your account that are visible to you. Also use it to create new users, update user information, change user roles, or delete users.

- Object Representation
- List Halo users
- Get a single Halo user
- Create a new Halo user
- Update a Halo user account
- Delete a Halo user account

Object Representation

User object location

api.cloudpassage.com/v2

/users/{user_id}

User object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The Halo ID of the user object.</td>
</tr>
<tr>
<td>url</td>
<td>The API URL to the user object.</td>
</tr>
<tr>
<td>username</td>
<td>The user's Halo username.</td>
</tr>
<tr>
<td>firstname</td>
<td>The user's first name.</td>
</tr>
<tr>
<td>lastname</td>
<td>The user's last name.</td>
</tr>
<tr>
<td>email</td>
<td>The email address at which the user receives notifications and other</td>
</tr>
<tr>
<td></td>
<td>communication from CloudPassage.</td>
</tr>
<tr>
<td>active</td>
<td>true if the user is active; false if the user has been deactivated.</td>
</tr>
<tr>
<td>pending</td>
<td>true if the user's registration is still in progress; false if it is</td>
</tr>
<tr>
<td></td>
<td>complete.</td>
</tr>
<tr>
<td>locked</td>
<td>true if the user's account has been locked (typically for excessive login</td>
</tr>
<tr>
<td></td>
<td>attempts); false if it is not locked.</td>
</tr>
<tr>
<td>access</td>
<td>An array of information listing the user's owning group role and roles.</td>
</tr>
<tr>
<td></td>
<td>Includes these subfields:</td>
</tr>
<tr>
<td></td>
<td>- group_id: The Halo ID of the group to which the user belongs (in a</td>
</tr>
<tr>
<td></td>
<td>comma-separated list, if more than one). If the user belongs to the root</td>
</tr>
<tr>
<td></td>
<td>group, the value is root.</td>
</tr>
<tr>
<td></td>
<td>- roles: A comma-separated list of one or more Halo roles that the user</td>
</tr>
<tr>
<td></td>
<td>has. Possible values are: standard, administrator, auditor, and</td>
</tr>
<tr>
<td></td>
<td>ghostport.</td>
</tr>
<tr>
<td>sms_phone_number</td>
<td>The mobile phone number at which the user receives Halo authentication</td>
</tr>
<tr>
<td>yubikey</td>
<td>The ID of the user's Yubikey device.</td>
</tr>
<tr>
<td>last_login_at</td>
<td>The date-time (in ISO 8601 format) of the user's most recent login.</td>
</tr>
</tbody>
</table>
List Halo users

Retrieves information on all Halo users visible to you in your Halo account. The method also returns a total count of users.

GET https://api.cloudpassage.com/v2/users/

Response

Status: 200

```json
{
  "count": 90,
  "users": [
    {
      "id": "0b632047becfa5711e4b2d113204e30c",
      "url": "https://api-qastaging.cloudpassage.com:10443/v2/users/0b632047becfa5711e4b2d113204e30c",
      "username": "mandropov",
      "firstname": "Mikhail",
      "lastname": "Andropov",
      "email": "mandropov@acme.com",
      "active": true,
      "pending": false,
      "locked": false,
      "access": [
        {
          "group_id": "999465a0d0e40132c0c606bf4fdbc353",
          "roles": [
            "standard"
          ]
        }
      ],
      "sms_phone_number": "",
      "yubikey": "",
      "last_login_at": "2016-04-29T01:21:45.475Z",
      "last_login_ip": "108.80.59.84",
      "created_at": "2015-05-14T16:34:08.812Z",
      "otp_verified": false
    },
    {
      "id": "0e441c629e34c1e68179537b8a0b3375",
      "url": "https://api.cloudpassage.com/v2/users/0e441c629e34c1e68179537b8a0b3375",
      "username": "cnicolette",
      "firstname": "Celine",
      "lastname": "Nicolette",
      "email": "cnicolette@acme.com",
      "active": true,
      "pending": false,
      "locked": false,
      "access": [
        {
          "group_id": "0962bfa087bc01323e360670140e224,999465a0d0e40132c0c606bf4fdbc353",
          "roles": [
            "administrator"
          ]
        }
      ],
      "sms_phone_number": null,
      "yubikey": null,
      "last_login_at": "2016-05-10T17:29:15.801Z",
      "last_login_ip": "108.80.59.84",
      "created_at": "2015-05-14T16:34:08.812Z",
      "otp_verified": false
    },
    ...
  ]
}
```
Get a single Halo user

Retrieves details of the Halo user specified by ID in the request URL. The information returned is identical to that returned for the same user from the List Halo users method.

GET https://api.cloudpassage.com/v2/users/{id}

Response

Status: 200

{
  "user": {
    "id": "0b632047becfa5711e4b2d113204e30c",
    "url": "https://api.cloudpassage.com/v2/users/0b632047becfa5711e4b2d113204e30c",
    "username": "mandropov",
    "firstname": "Mikhail",
    "lastname": "Andropov",
    "email": "mandropov@acme.com",
    "active": true,
    "pending": false,
    "locked": false,
    "access": [
      {
        "group_id": "999465a0d0e40132c0c606bf4fdcb353",
        "roles": [
          "standard"
        ]
      }
    ],
    "sms_phone_number": "",
    "yubikey": "ccccccbjsfkj",
    "last_login_at": "2016-04-29T01:21:45.475Z",
    "last_login_ip": "108.80.59.84",
    "created_at": "2015-05-14T16:34:08.812Z",
    "otp_verified": false
  }
}

Create a new Halo user

Creates a Halo user with the attributes specified in the request JSON. Required fields to supply are username, firstname, lastname, email, and access (with its subfields group_id and roles).

The response JSON displays all fields of the user object, including its Halo ID and API URL.

POST https://api.cloudpassage.com/v2/users/

Request body

{
  "user": {
    "username": "mchen",
    "firstname": "Maria",
    "lastname": "Chen",
    "email": "mchen@acme.com",
    "access": [
      {
        "group_id": "d09612c8cc3c1e58e924f90bb8338dd,999465a0d0e40132c0c606bf4fdcb353",
        "roles": [
          "standard"
        ]
      }
    ]
  }
}
Update a Halo user account

To the user specified by ID in the call URL, updates the attributes specified in the request JSON. The JSON should include only the fields that are to be changed.

Besides making minor administrative updates to a user's account, you can use this method to make a number of updates that affect the user's activities, such as:

- **Change roles**: update the \texttt{roles} array.
- **Move between groups**: specify the new group in the \texttt{group_id} field.
- **Add or change authentication method(s)**: update the \texttt{sms_phone_number} and/or \texttt{yubikey} fields.
- **Change username or email address**: update the \texttt{username} or \texttt{email} field.

If the call is successful, the method returns only a status designation; there is no response JSON.

\textbf{PUT} https://api.cloudpassage.com/v2/users/{id}

**Request body**

```
{
  "user": {
    "id": "7b917186212911e6a5b25973552d48ce",
    "url": "https://api-qastaging.cloudpassage.com:10443/v2/users/7b917186212911e6a5b25973552d48ce",
    "username": "mchen",
    "firstname": "Maria",
    "lastname": "Chen",
    "email": "mchen@acme.com",
    "active": true,
    "pending": true,
    "locked": false,
    "access": [
      {
        "group_id": "d09612c8cc3c11e58e924f90bb8338dd,999465a0d0e4132c0c606bf4fdcb353",
        "roles": [
          "auditor"
        ]
      },
      {
        "sms_phone_number": null,
        "yubikey": null,
        "last_login_at": null,
        "last_login_ip": null,
        "created_at": "2016-05-23T21:01:13.194Z"
      }
    ]
  }
}
```
Delete a Halo user account

Deletes the user account specified by ID in the call URL Halo maintains historical information about the user, but the user no longer appears under User Administration in the Halo portal, and login with that user account is no longer possible.

DELETE https://api.cloudpassage.com/v2/users/{id}

Response

Status: 204
System Announcements

Use the System Announcements endpoint to retrieve a list of all stored Halo system announcements (Halo portal banners).

- **Object Representation**
- **List system announcements**

**Object Representation**

System announcement object location

```
api.cloudpassage.com/v1
```

System announcement object fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>announcement</td>
<td>The content of the announcement. May contain HTML source as well as text.</td>
</tr>
<tr>
<td>message_begin_at</td>
<td>The date/time (in ISO 8601 format) when the announcement was posted or will be posted.</td>
</tr>
<tr>
<td>message_expire_at</td>
<td>The date/time (in ISO 8601 format) when the announcement expired and was removed, or will expire.</td>
</tr>
<tr>
<td>announcement_type</td>
<td>The type of announcement. Can be planned_outage or information.</td>
</tr>
<tr>
<td>status</td>
<td>The current status of the announcement. Can be active or expired.</td>
</tr>
<tr>
<td>outage_time_start</td>
<td>For announcements involving an outage, the date/time (in ISO form) at which the outage occurred or will occur.</td>
</tr>
<tr>
<td>outage_time_end</td>
<td>For announcements involving an outage, the date/time (in ISO form) at which the outage ended.</td>
</tr>
</tbody>
</table>

**List system announcements**

Returns information for all system announcements stored in the Halo database.

*Note:* The results of this call may be paginated. See Pagination of Results for information on how to set up and retrieve paginated results from the Halo API.

```
GET https://api.cloudpassage.com/v1/system_announcements/
```

You can optionally filter the results according to the value of the `status` field:

```
GET https://api.cloudpassage.com/v1/system_announcements?status=active
```
Deprecated Endpoints

v1/Issues

Note: The v1/issues endpoint has been deprecated. Please use the v3/Issues endpoint. The following section is for reference purposes only and will remain available for a limited time.

Use the Issues API endpoint to retrieve full or filtered views of the active or resolved issues for your account. Also use it to explicitly
resolve issues that have been remediated.

- List issues
  - Example: List issues for an individual server
  - Example: List issues across a group
- Get details and findings for a single issue
- Manually resolve an issue

Object Representation

**Issue object location**

```plaintext
api.cloudpassage.com/v1
   └──issues
       └──id
```

**Issue object fields**

The Issue object is returned from the List issues method and other methods that retrieve lists of issues.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| name          | The name of the policy rule that was violated. Different modules can have different formats for the rule name. For example:  
  - For CSM, `name` refers to the configuration check that failed. For example, **No Recent Account Login**.  
  - For FIM, `name` refers to the target path specified in the rule. For example, `/opt/cloudpassage/!*/*`.  
  - For LIDS, `name` consists of the word "rule" followed by the sequence number of the rule in the policy. For example, `rule1` refers to the first rule in the policy.  
  - For SVA, `name` is the name of the vulnerable package detected. For example, **polkit.x86_64**. |
| agent_id      | The Halo ID of the server on which the issue was detected.                                                                                                                                                     |
| comment       | For manually resolved issues, an optional user-defined description of the resolution. For automatically resolved issues, the field contains the following message: "Policy does not exist anymore or issue was resolved". |
| os_type       | The platform (linux or windows) of the server on which the issue was detected.                                                                                                                                   |
| created_at    | The date-time (in ISO 8601 format) at which the issue was first detected.                                                                                                                                       |
| last_seen_at  | The date-time (in ISO 8601 format) of the most recent scan in which the issue was detected.                                                                                                                                 |
| resolved_at   | The date-time (in ISO 8601 format) at which the issue was resolved. The value is **null** for active issues.                                                                                                                                                        |
| resolved_by   | The username of the Halo user who resolved the issue. If the issue was resolved automatically, the value of this field is **system**. If the issue is not yet resolved, the value is **null**. |
| rule_key      | An identifier of the rule violation that the issue represents. A string with the format `issue_type::rule_number::rule_name`. For example, `sca::11640::critical_package_presence`.  
  The rule key is a unique identifier for each issue. Two issues that share the same rule key value can be  
  considered to be essentially the same issue. Conversely, two issues that share the same rule name and issue type  
  but are in different rules or policies will have distinct rule keys. |
<p>| issue_type    | The type of the issue: <strong>lids, csm, fim, sva, sam, fw</strong>, or <strong>agent</strong>.                                                                                                                                          |
| status        | The status of the issue: <strong>active</strong> or <strong>resolved</strong>.                                                                                                                                                           |
| critical      | <strong>true</strong> if the issue is considered critical; otherwise <strong>false</strong>.                                                                                                                                             |
| policy_id     | The Halo ID of the policy whose rule violation caused the issue to be created.                                                                                                                                    |
| policy_name   | The name of the policy whose rule violation caused the issue to be created.                                                                                                                                       |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_id</td>
<td>The Halo ID of the group to which this server belongs.</td>
</tr>
<tr>
<td>id</td>
<td>The Halo ID of this issue.</td>
</tr>
<tr>
<td>url</td>
<td>The URL to the issue object.</td>
</tr>
<tr>
<td>agent_url</td>
<td>The URL to the server object on which the issue was detected.</td>
</tr>
<tr>
<td>policy_url</td>
<td>The URL to the policy object whose rule violation caused the issue to be created.</td>
</tr>
</tbody>
</table>

**Issue findings fields (from Issue Details object)**

The Issue Details object (returned from the **Get issue details** method) consists of the Issues object (described above) plus an additional field, **findings**, which is an array of subfields that include links to the descriptions of the scan finding or findings that led to the creation of the issue.

**Field** | **Description**
---|---
findings | An array of one or more sets of subfields, each set describing and linking to a finding object that led to the creation of the issue.
finding | The URL to the finding object.
issue_status | The status (**active** or **resolved**) of the issue created from this finding.
created_at | The creation timestamp of this finding’s issue.

**Call parameters for issues**

When you make API calls that return a list of issues, you can apply any of the following parameters to restrict the results, to change the sorting of the results, and to aggregate the results into groups based on individual values of certain object fields.

**Search filters**

Use the following filters and operators to restrict the set of local user accounts returned. For any of the filters, you can provide either a single value or a comma-separated list of values. If you do provide multiple values, they are OR'd in a search, meaning that the search passes for that filter if any of its supplied values matches.

- name
- agent_id
- os_type
- resolved_by
- created_at
- comment
- last_seen_at
- resolved_at
- rule_key
- issue_type
- status
- critical
- group_id
- policy_id
- policy_name
- sort_by
- group_by

**Note:** You can search for time ranges by adding any of the suffixes _lt, _lte, _gt, or _gte to the field names created_at, last_seen_at, or resolved_at. (For example, created_at_lte means "return all issues whose creation timestamp is less than or equal to the specified value").

**Sorting the results**

253
You can use the sort_by parameter to specify that the search results are to be alphanumerically sorted (in either ascending or descending order) according to the values of the following user account object fields:

- name
- agent_id
- os_type
- created_at
- last_seen_at
- resolved_at
- rule_key
- issue_type
- status
- count
- critical
- policy_id
- policy_name

Aggregating the results

You can use the group_by parameter to specify that the search results are to be aggregated according to the values in one or more user account object fields. Grouping can help you to build custom reports into your reporting tools and dashboards.

For example, if you search a server's accounts and aggregate by by os_type, all Windows accounts are listed together, and all Linux accounts are listed together. If you search a group's local user accounts and sort by account name, the results will group together all instances of each account name within the group. These are the fields by which you can group local user accounts:

- agent_id
- os_type
- rule_key
- issue_type
- status
- critical
- name
- group_id
- policy_id
- policy_name

List issues

Note: The v1/issues endpoint has been deprecated. Please use the v3/Issues endpoint. The following section is for reference purposes only and will remain available for a limited time.

Retrieves all issues in your Halo account. By default, the method returns all active issues plus all resolved issues whose resolved_at date is within the last 90 days. The method also returns a total count of issues.

GET https://api.cloudpassage.com/v1/issues/

The response (see "Response 1", below) may be paginated. You can specify custom page sizes up to 100 items by using the per_page parameter. You can also specify which page to retrieve by using the page parameter. See Pagination of Results for further explanation and examples.

https://api.cloudpassage.com/v1/issues?page={pagenum}&per_page={pagesize}

This method call supports several other optional parameters:
You can restrict the retrieved issues to a time/date range by using the filter parameters `created_at_gte` and `created_at_lte`. The value for each parameter is an ISO 8601 formatted timestamp string (for example `YYYY-MM-DD`, or `YYYY-MM-DDThh:mmZ` for Zulu time zone). For example:

```
```

You can filter the returned results by using several of the issue object fields (such as `critical`, `status`, `issue_type`, `id`, `agent_id`, or `policy_id`) as a filter parameter. For example:

```
GET https://api.cloudpassage.com/v1/issues?issue_type=fim,svm
GET https://api.cloudpassage.com/v1/issues?status=resolved
GET https://api.cloudpassage.com/v1/issues?id=4bafaba464011e585ab1d6c9a2e7cc4
GET https://api.cloudpassage.com/v1/issues?policy_id=f3541070d5820132c0df06bf4fdcb353
```

(See "Response 2", below.)

You can group results into specific categories, by using one or more of the `group_by` parameters listed above. For example:

```
GET https://api.cloudpassage.com/v1/issues?group_by=status,rule_key,issue_type
```

In this case the call does not return complete issue objects; instead, it lists every existing combination of the values of the specified group-by parameters, with a count of how many issue objects fit into each combination. You can use the call to show, for example, how many essentially identical issues (those with the same `rule_key` value) exist across all of your groups, segregated by issue type and by criticality. (See "Response 3", below.)

You can combine any of the above parameters in your `List issues` calls.

**Response 1**

(for GET `https://api.cloudpassage.com/v1/issues/`)

**Status: 200**

```
{
  "issues": [
    {
      "agent_id": "0cd6df5416f811e7b78441efec4abe5d",
      "comment": null,
      "created_at": "2017-04-01T16:30:30.436Z",
      "critical": true,
      "group_id": "bc4cd1601f6e11e7a95c0387f10121b2",
      "issue_type": "fim",
      "last_seen_at": "2017-04-02T21:30:38.764Z",
      "name": "/var/log/",
      "os_type": "Linux",
      "policy_id": "eca57ca0140811e7962e538631243f4e",
      "policy_name": "FIM",
      "resolved_at": null,
      "rule_key": "fim::1835::/var/log/",
      "status": "active",
      "id": "856e038e160911e7b5877189466e776",
      "url": "https://api.cloudpassage.com/v2/issues/856e038e160911e7b5877189466e776",
      "agent_url": "https://api.cloudpassage.com/v1/servers/0cd6df5416f811e7b78441efec4abe5d",
      "policy_url": "https://api.cloudpassage.com/v1/fim_policies/eca57ca0140811e7962e538631243f4e"
    },
    {
      "agent_id": "0350c6d8160911e7b5877189466e776",
      "comment": "Policy does not exist anymore or issue was resolved",
      "created_at": "2017-04-02T16:30:30.436Z",
      "critical": false,
      "group_id": "2d171572160311e788ab393b4f222840",
      "issue_type": "sca",
      "last_seen_at": null,
      "name": "5.2.11 Ensure only approved ciphers are used",
      "os_type": "Linux",
      "policy_id": "3e5a1elee143a1e78c840dd8383e370",
      "policy_name": "CIS Benchmark for Amazon Linux v2",
      "resolved_at": "2017-04-03T15:18:846Z"
    }
  ]
}
```
"rule_key": "sca::11785::5.2.11 Ensure only approved ciphers are used",
"status": "resolved",
"id": "135c558e160d11e7b9ab1b060e773d17",
"url": "https://api.cloudpassage.com/v2/issues/135c558e160d11e7b9ab1b060e773d17",
"agent_url": "https://api.cloudpassage.com/v1/servers/0350c6d8160911e7b85a154596627f29",
"policy_url": "https://api.cloudpassage.com/v1/policies/3e5a1eee143a11e78c840dd8383e370"
],
"count": 1646,
"pagination": {
}
],
"count": 1646,
"pagination": {
}
}

Response 2
(for GET https://api.cloudpassage.com/v1/issues?issue_type=sva&os_type=windows&critical=false, which means "Return all non-critical Windows vulnerability issues")

Status: 200

{
   "issues": [
      {
         "agent_id": "a785bf22745111e8b43039940452108",
         "comment": null,
         "created_at": "2018-09-19T13:49:22.916Z",
         "critical": false,
         "group_id": "66a566807d63012ff31e4040ebe4a8e4",
         "issue_type": "sva",
         "last_seen_at": "2018-11-05T16:50:36.728Z",
         "name": "XML Core Services",
         "os_type": "Windows",
         "policy_id": "null_value",
         "policy_name": null,
         "resolved_at": null,
         "resolved_by": null,
         "rule_key": "sva::Microsoft Corporation::XML Core Services",
         "status": "active",
         "id": "d08d615abc1211e8911c69d73b6d3cc9",
         "url": "https://portal.cloudpassage.com/v1/issues/d08d615abc1211e8911c69d73b6d3cc9",
         "agent_url": "https://portal.cloudpassage.com/v1/servers/a785bf22745111e8b43039940452108",
         "policy_url": "null_value"
      },
      ...
   ]
}

Response 3
(for GET https://api.cloudpassage.com/v1/issues?group_by=critical,name,issue_type, which means "Return the total number of servers containing each issue as specified by its rule name and issue type")

Status: 200

{
   "issues": [
      {
         "critical": true,
         "name": "/var/log/",
         "issue_type": "fim",
         "count": 17
      },
      {
         "critical": true,
         "name": "Self verification failed",
         "issue_type": "agent",
         "count": 14
      },
      {
         "critical": true,
         "name": "Rule",
         "issue_type": "csm",
         "count": 13
      },
      {
         "critical": true,
         
      }
   ]
}
Other examples of retrieving information from a set of issues:

Example: List issues for an individual server

Note: The v1/issues endpoint has been deprecated. Please use the v3/Issues endpoint. The following section is for reference purposes only and will remain available for a limited time.

Returns a list of all issues detected in the server specified by server ID in the call URL. Does not return the findings field of an issue; to view the findings, call the Get a single issue method.

By default both active and resolved issues are returned, but you can filter and group the results of this call by applying the same parameters available for the List issues method, including status.

GET https://api.cloudpassage.com/v1/issues?agent_id={server_id}

Response

Status: 200

{ "issues": [
  { "agent_id": "14a1da6e51c311e5805b4df8b41d6d1e", "rule_key": "csm::11640::auto_package_presence,allowed_to_be,bad", "issue_type": "csm", "status": "active", "critical": false, "resolved_at": null, "created_at": "2015-09-02T22:47:08.883Z", "last_seen_at": "2015-09-02T22:47:08.893Z", "policy_id": "38c89b381f6611e59cb40db40db4c6c0bae5", "id": "8acd856651c411e5bced0562db0e8b21", "url": "https://api.cloudpassage.com/v1/issues/8acd856651c411e5bced0562db0e8b21", "agent_url": "https://api.cloudpassage.com/v1/servers/14a1da6e51c311e5805b4df8b41d6d1e", "policy_url": "https://api.cloudpassage.com/v1/policies/38c89b381f6611e59cb40db4c6c0bae5" },

257
Example: List issues across a group

Note: The v1/issues endpoint has been deprecated. Please use the v3/Issues endpoint. The following section is for reference purposes only and will remain available for a limited time.

GET https://api.cloudpassage.com/v1/issues?group_id={groupID}

Returns a list of all issues detected on all servers of the group specified by group ID in the call URL.

To make this call, first obtain the group ID of the group of interest, and then pass that ID to the API when you call this method. (Note that the issue object does not itself include a group ID field.)

You can filter and group the results of this call by applying the same parameters available for the List issues method.

Response

Status: 200

{ "issues": [ { "agent_id": "14alda6e51c311e5805b4df8b41d6d1e", "rule_key": "fim::147661::::/usr/sbin", "issue_type": "fim", "status": "active", "critical": false, "resolved_at": null, "created_at": "2015-09-02T22:57:30.634Z", "last_seen_at": "2015-09-02T22:57:30.642Z", "policy_id": "ab50af103f8211e5a1e7193241212e97", "id": "fd65296651c511e59a8f7961ff13ecf8", "url": "https://api.cloudpassage.com/v1/issues/fd65296651c511e59a8f7961ff13ecf8", "agent_url": "https://api.cloudpassage.com/v1/servers/14alda6e51c311e5805b4df8b41d6d1e", "policy_url": "https://api.cloudpassage.com/v1/policies/ab50af103f8211e5..." } ] }
Get details and findings for a single issue

**Note:** The v1/issues endpoint has been deprecated. Please use the v3/Issues endpoint. The following section is for reference purposes only and will remain available for a limited time.

Retrieves details of the issue specified by issue ID in the request URL. The details include links to information describing the scan findings that led to the creation of the issue.

GET https://api.cloudpassage.com/v1/issues/{id}

**Response**

`status: 200`

```json
{
  "agent_id": "0cd6df5416f811e7b78441efec4abe5d",
  "comment": null,
  "created_at": "2017-04-01T16:30:30.436Z",
  "critical": true,
  "group_id": "bc4cd1f016ee11e7a95c0387f10121b2",
  "issue_type": "fim",
  "last_seen_at": "2017-04-02T21:30:38.764Z",
  "os_type": "Linux",
  "policy_id": "eca57ca0140811e7962e538631243f4e",
  "policy_name": "FIM",
  "resolved_at": null,
  "rule_key": "fim::1835::::/var/log/",
  "status": "active",
  "id": "856e038e16f811e7ab5877189466e776",
  "findings": [
    {
      "finding": "https://api.cloudpassage.com/v1/scans/0d71c9e216f811e79f6305e8049b67ee/findings...",
      "issue_status": "active",
      "issue_created_at": "2017-04-01T16:30:30.434Z"
    },
    {
      "finding": "https://api.cloudpassage.com/v1/scans/9d4c4c5617eb11e7ab5877189466e776/findings...",
      "issue_status": "active",
      "issue_created_at": "2017-04-02T21:30:38.717Z"
    }
  ],
  "url": "https://api.cloudpassage.com/v2/issues/856e038e16f811e7ab5877189466e776",
  "agent_url": "https://api.cloudpassage.com/v1/servers/0cd6df5416f811e7b78441efec4abe5d",
  "policy_url": "https://api.cloudpassage.com/v1/fim_policies/eca57ca0140811e7962e538631243f4e",
  "name": "/var/log/"
}
```
Use the response JSON to locate and review the finding details for the issue. Make a GET request to each of the URLs that are returned in the individual finding subfields of the findings field in the issue. For example:

GET https://api.cloudpassage.com/v1/scans/02cb1e0a2...605092f8f527d/findings/9c235c0...5809d5f19d06086d

This an abbreviated example of finding details returned for a configuration security issue:

```
{
  "Status": 200,
  "critical": false,
  "status": "bad",
  "rule_operator": "OR",
  "details": [
    {
      "type": "package_presence",
      "status": "good",
      "target": "python",
      "expected": "allowed",
      "actual": "false",
      "scan_status": "ok"
    },
    {
      "type": "package_presence",
      "status": "good",
      "target": "python-urllib3",
      "expected": "allowed",
      "actual": "false",
      "scan_status": "ok"
    },
    ...
    {
      "type": "package_presence",
      "status": "bad",
      "target": "apt",
      "expected": false,
      "actual": true,
      "scan_status": "ok"
    },
    {
      "type": "package_presence",
      "status": "bad",
      "target": "adduser",
      "expected": false,
      "actual": true,
      "scan_status": "ok"
    }
  ],
  "rule_name": "allowed_packages",
  "reference_identifiers": [],
  "id": "9c235c0c308e11e5809d5f19d060865d",
  "url": "https://api.cloudpassage.com/v1/scans/02cb1e0a208a11e5ab1605092f8f527d/findings/9c2..."
}
```

Manually resolve an issue

**Note:** The v1/Issues endpoint has been deprecated. Please use the v3/Issues endpoint. The following section is for reference purposes only and will remain available for a limited time.

You can use the Issues API endpoint to manually resolve active issues.

If you have remediated an issue, Halo will (except in the case of LIDS and some SAM issues) automatically mark the issue as resolved when the next scan of that server does not report the finding that caused the issue to be created. However, you can also use the Halo portal or the Halo API to manually mark an issue as resolved.

To resolve an issue through the API, make the following PUT call, passing the issue ID in the URL and passing the new value for the **status** field as JSON in the request body.
PUT https://api.cloudpassage.com/v1/issues/{issue_id}

**Request Body**

```json
{
  "status": "resolved",
}
```

Should you ever need to manually reactivate a resolved issue, make the same call but set the `status` value to `active` in the request JSON.

**Response**

```
Status: 204
```

---

**Container Image Issues**

*Note: The v1/image_issues endpoint has been deprecated. Please use the v3/Issues endpoint. The following section is for reference purposes only and will remain available for a limited time.*

Image issues are the Halo security issues detected in container images. Use the Image Issues endpoint to list and view the details of the security issues Halo has found in one or more images.

- Object Representation
- List image issues
- Get a single image issue

**Object Representation**

*Image issue object location*

```text
api.cloudpassage.com/v1/image_issues/issue_id
```

*Image issue object fields*

These fields are returned by the **List image issues** call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>comment</td>
<td>A user-added note about the issues.</td>
</tr>
<tr>
<td>created_at</td>
<td>When Halo created the issue. (ISO-8601 format)</td>
</tr>
<tr>
<td>critical</td>
<td><code>true</code> if the issue is critical; <code>false</code> if not.</td>
</tr>
<tr>
<td>customer_id</td>
<td>(not used)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cves</td>
<td>An array of name and score pairs, listing the name and CVSS score of each CVE detected in the package.</td>
</tr>
<tr>
<td>cves_count</td>
<td>The number of CVEs in this issue.</td>
</tr>
<tr>
<td>group_id</td>
<td>The ID of the Halo group that the issue's host server belongs to.</td>
</tr>
<tr>
<td>id</td>
<td>The Halo ID of the image issue.</td>
</tr>
<tr>
<td>image</td>
<td>An array of attributes of the issue's image. Includes the following subfields:</td>
</tr>
<tr>
<td>current</td>
<td><strong>true</strong> if the image is the most recent version; <strong>false</strong> if not.</td>
</tr>
<tr>
<td>id</td>
<td>The Halo ID of the image.</td>
</tr>
<tr>
<td>image_sha</td>
<td>The Docker SHA-256 representation of the image.</td>
</tr>
<tr>
<td>in_use</td>
<td>The number of running or paused containers that were instatiated from the image.</td>
</tr>
<tr>
<td>registry</td>
<td>An object that specifies the name of the registry containing the image.</td>
</tr>
<tr>
<td>registry_id</td>
<td>The Halo ID of the registry containing the image.</td>
</tr>
<tr>
<td>repository</td>
<td>An object that specifies the name of the repository containing the image.</td>
</tr>
<tr>
<td>repository_id</td>
<td>The Halo ID of the repository containing the image.</td>
</tr>
<tr>
<td>tag</td>
<td>The version tag assigned to the image.</td>
</tr>
<tr>
<td>image_id</td>
<td>The Halo ID of the image in which this issue was detected.</td>
</tr>
<tr>
<td>issue_type</td>
<td>The type of the issue: <strong>image_sva</strong> is the currently supported type.</td>
</tr>
<tr>
<td>last_seen_at</td>
<td>The date-time of the most recent scan that detected the issue. (ISO-8601 format)</td>
</tr>
<tr>
<td>max_cvss</td>
<td>The highest criticality score of the findings in the issue.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the issue (vulnerable package).</td>
</tr>
<tr>
<td>name_dc</td>
<td>Alternate name for the issue (vulnerable package).</td>
</tr>
<tr>
<td>os_type</td>
<td>The platform (<strong>linux</strong> or <strong>windows</strong>) on which the image runs.</td>
</tr>
<tr>
<td>policy_id</td>
<td>The ID of the Halo policy that generated the issue.</td>
</tr>
<tr>
<td>policy_name</td>
<td>The name of the Halo policy that generated the issue.</td>
</tr>
<tr>
<td>remotely_exploitable</td>
<td><strong>true</strong> if the issue can be exploited remotely; <strong>false</strong> if not.</td>
</tr>
<tr>
<td>resolved_at</td>
<td>The date-time of the issue's resolution. (ISO-8601 format)</td>
</tr>
<tr>
<td>resolved_by</td>
<td>The username of the Halo user who resolved the issue.</td>
</tr>
<tr>
<td>rule_key</td>
<td>The name of the violated policy rule underlying the issue.</td>
</tr>
<tr>
<td>status</td>
<td>The status of the issue: <strong>active</strong> or <strong>resolved</strong>.</td>
</tr>
<tr>
<td>sweep_timestamp</td>
<td>The date-time at which the issue was first created. (ISO-8601 format)</td>
</tr>
<tr>
<td>updated_at</td>
<td>The date-time at which the issue was last updated. (ISO-8601 format)</td>
</tr>
<tr>
<td>version</td>
<td>The version number of the issue (vulnerable package).</td>
</tr>
<tr>
<td>id</td>
<td>The Halo ID of the image issue.</td>
</tr>
</tbody>
</table>

*Image issue details object fields*

These fields are returned by the Get a single image issue call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>comment</td>
<td>A user-added note about the issues.</td>
</tr>
<tr>
<td>created_at</td>
<td>When Halo created the issue. (ISO-8601 format)</td>
</tr>
<tr>
<td>critical</td>
<td><strong>true</strong> if the issue is critical; <strong>false</strong> if not.</td>
</tr>
<tr>
<td>customer_id</td>
<td>(not used)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cves</td>
<td>An array of name and score pairs, listing the name and CVSS score of each CVE detected in the package.</td>
</tr>
<tr>
<td>group_id</td>
<td>The ID of the Halo group that the issue's host server belongs to.</td>
</tr>
<tr>
<td>id</td>
<td>The Halo ID of the image issue.</td>
</tr>
<tr>
<td>image</td>
<td>An array of attributes of the image. Includes the following subfields:</td>
</tr>
<tr>
<td>current</td>
<td><code>true</code> if the image is the most recent version; <code>false</code> if not.</td>
</tr>
<tr>
<td>id</td>
<td>The Halo ID of the image.</td>
</tr>
<tr>
<td>image_sha</td>
<td>The Docker SHA-256 representation of the image.</td>
</tr>
<tr>
<td>in_use</td>
<td>The number of running or paused containers that were instantiated from the image.</td>
</tr>
<tr>
<td>registry</td>
<td>The name of the registry containing the image.</td>
</tr>
<tr>
<td>repository</td>
<td>The name of the repository containing the image.</td>
</tr>
<tr>
<td>repository_id</td>
<td>The Halo ID of the repository containing the image.</td>
</tr>
<tr>
<td>tag</td>
<td>The Halo ID of the image in which this issue was detected.</td>
</tr>
<tr>
<td>image_id</td>
<td>The version tag assigned to the image.</td>
</tr>
<tr>
<td>issue_type</td>
<td>The type of the issue: <code>image_sva</code> is the currently supported type.</td>
</tr>
<tr>
<td>last_seen_at</td>
<td>The date-time of the most recent scan that detected the issue. (ISO-8601 format)</td>
</tr>
<tr>
<td>max_cvss</td>
<td>The highest criticality score of the findings in the issue.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the issue (vulnerable package).</td>
</tr>
<tr>
<td>os_type</td>
<td>The platform (Linux or Windows) on which the image runs.</td>
</tr>
<tr>
<td>policy_id</td>
<td>The ID of the Halo policy that generated the issue.</td>
</tr>
<tr>
<td>policy_name</td>
<td>The name of the Halo policy that generated the issue.</td>
</tr>
<tr>
<td>remotely_exploitable</td>
<td><code>true</code> if the issue can be exploited remotely; <code>false</code> if not.</td>
</tr>
<tr>
<td>resolved_at</td>
<td>The date-time of the issue's resolution. (ISO-8601 format)</td>
</tr>
<tr>
<td>resolved_by</td>
<td>The username of the Halo user who resolved the issue.</td>
</tr>
<tr>
<td>rule_key</td>
<td><code>true</code> if the issue is critical; <code>false</code> if not.</td>
</tr>
<tr>
<td>status</td>
<td>The status of the issue: <code>active</code> or <code>resolved</code>.</td>
</tr>
<tr>
<td>updated_at</td>
<td>The date-time at which the issue was last updated. (ISO-8601 format)</td>
</tr>
<tr>
<td>version</td>
<td>The version number of the issue (vulnerable package).</td>
</tr>
<tr>
<td>findings</td>
<td>An array of IDs of the scan findings underlying this issue.</td>
</tr>
<tr>
<td>image_sha</td>
<td>(not used)</td>
</tr>
</tbody>
</table>

**Search filters**

You can use any of the following attributes and operators to narrow down the results of a GET call that you make to this endpoint:

- `critical`
- `issue_type`
- `name`
- `created_at_gte`
- `created_at_lte`
- `updated_at_gte`
- `updated_at_lte`
- `image_name`
- `image_tag`
- `image_id`
Sort by
You can use any of the following operators to sort (ascending or descending, respectively) the results of a GET call:

- critical.asc
- critical.desc
- issue_type.asc
- issue_type.desc
- name.asc
- name.desc
- remotely_exploitable.asc
- remotely_exploitable.desc
- max_cvss.asc
- max_cvss.desc
- cves_count.asc
- cves_count.desc
- created_at.asc
- created_at.desc
- updated_at.asc
- updated_at.desc

List image issues

Note: The v1/image_issues endpoint has been deprecated. Please use the v3/Issues endpoint. The following section is for reference purposes only and will remain available for a limited time.

Returns JSON-formatted results listing all Halo security issues detected in scanned image containers.

GET https://api.cloudpassage.com/v1/image_issues/

Response

Status: 200

```json
{
  "image_issues": [
    {
      "comment": "",
      "created_at": "2017-12-20T21:34:27.54Z",
      "critical": true,
      "customer_id": "f4fa0b56e5c611e781ec23c27568c85c",
      "cves": [
        {
          "score": 6.8,
          "name": "cve-2016-9840"
        },
        {
          "score": 7.5,
          "name": "cve-2016-9841"
        },
        {
          "score": 6.8,
          "name": "cve-2016-9842"
        }
      ]
    }
  ]
}```
"score": 7.5,
"name": "cve-2016-9843"
},
"cves_count": 4,
"group_id": "f51e674e-e5c6-11e7-81ec-23c27568c85c",
"image": {
"current": true,
"id": "f4653bf2-9592-4064-9402-e0702abbf262",
"image_sha": "sha256:3b97d11fb15083b4363391859cf0eaa73c5f35ae9dcb3cd8c2fa3e3546b343e6",
"in_use": 1,
"registry": {
"name": "ECR-kishore"
},
"registry_id": "2d76fa60-1540-4f6c-8008-43bf33844bec",
"repository": {
"name": "kishore-vuln"
},
"repository_id": "f11045c5-3342-4163-9865-28d10974f2fc",
"tag": "vuln-2"
},
"image_id": "f4653bf2-9592-4064-9402-e0702abbf262",
"issue_type": "image_sva",
"last_seen_at": "2017-12-20T21:34:27.542Z",
"max_cvss": 7.5,
"name": "zlib1g:amd64",
"name_dc": "zlib1g:amd64",
"os_type": "Linux",
"policy_id": "null_value",
"policy_name": "",
"remotely_exploitable": true,
"resolved_at": null,
"resolved_by": "",
"rule_key": "image_sva:::zlib1g:amd64",
"status": "active",
"sweep_timestamp": "2017-12-20T21:34:27.544Z",
"updated_at": null,
"version": "1:1.2.8.dfsg-2ubuntu4",
"id": "8e3b7d94e5cd11e7b6655529d25d6abf"
}
...

{
"comment": "",
"created_at": "2017-12-20T21:04:59.004Z",
"critical": true,
"customer_id": "f4fa0b56e5c611e781ec23c27568c85c",
"cves": [
{
"score": 6,
"name": "cve-2016-0634"
},
{
"score": 7.2,
"name": "cve-2016-7543"
},
{
"score": 2.1,
"name": "cve-2016-9401"
}
],
"cves_count": 3,
"group_id": "f51e674e-e5c6-11e7-81ec-23c27568c85c",
"image": {
"current": false,
"id": "43c8934a-3db7-471b-aeb5-30334c52971",
"image_sha": "sha256:ff95182c803f9ace90ae7cdda1be3747dd29de805d9d1fa1841dcee00538f9b",
"in_use": 2,
"registry": {
"name": "ECR-kishore"
},
"registry_id": "2d76fa60-1540-4f6c-8008-43bf33844bec",
"repository": {
"name": "kishore-vuln"
},
"repository_id": "f11045c5-3342-4163-9865-28d10974f2fc",
"tag": "vuln-1"
},
"image_id": "43c8934a-3db7-471b-aeb5-30334c52971",
"issue_type": "image_sva",
"last_seen_at": "2017-12-20T21:04:59.01Z",
"max_cvss": 7.2,
"name": "bash",
"name_dc": "bash",
"os_type": "Linux",
"policy_id": "null_value",
"policy_name": "",
Get a single image issue

**Note:** The v1/image_issues endpoint has been deprecated. Please use the v3/Issues endpoint. The following section is for reference purposes only and will remain available for a limited time.

Returns the fields of the Halo security issue specified by ID in the call URL.

**GET** https://api.cloudpassage.com/v1/image_issues/{id}

**Response**

**Status:** 200

```
{
  "image_issue": {
    "comment": null,
    "created_at": "2017-12-20T21:34:27.540Z",
    "critical": true,
    "customer_id": "f4fa0b56e5c611e7b6655529d25d6abf",
    "cves": [
      {
        "score": 6.8,
        "name": "cve-2016-9840"
      },
      {
        "score": 7.5,
        "name": "cve-2016-9841"
      },
      {
        "score": 6.8,
        "name": "cve-2016-9842"
      },
      {
        "score": 7.5,
        "name": "cve-2016-9843"
      }
    ],
    "group_id": "f51e674e-e5c6-11e7-81ec-23c27568c85c",
    "image": {
      "current": true,
      "id": "f4653bf2-9592-4064-9402-0702aabb262",
      "image_sha": "sha256:3b97d11fb15083b436339185cf0ea73c5f35ae9dbc3cd8c2fa3e3546b343e6",
      "in_use": 1,
      "registry": {
        "name": "ECR-kishore",
        "registry_id": "2d76fa60-1540-4f6c-8008-43bf33844bec",
        "repository": {
          "name": "kishore-vuln",
          "repository_id": "f11045c5-3342-4163-9865-28d10974f2fc",
          "tag": "vuln-2"
        }
      },
      "image_id": "f4653bf2-9592-4064-9402-e0702aabb262",
      "issue_type": "image_sva",
      "last_seen_at": "2017-12-20T21:34:27.542Z",
      "max_cvss": 7.5,
      "name": "zlib1g:amd64"
    }
  },
  "count": 12
}
```
"os_type": "Linux",
"policy_id": "null_value",
"policy_name": null,
"remotely_exploitable": true,
"resolved_at": null,
"resolved_by": null,
"rule_key": "image_sva:::zlib1g:amd64",
"status": "active",
"updated_at": null,
"version": "1:1.2.8.dfsg-2ubuntu4",
"id": "8e3b7d94e5cd11e7b6655529d25d6abf",
"findings": [
  "8d323bea-e5cd-11e7-b665-5529d25d6abf::8d54401e-e5cd-11e7-b665-5529d25d6abf::active:
],
"image_sha": null}