Halo REST API Developer Guide

How to use the Halo REST API	Overview

Topic	REST API Endpoints
Halo users	Users
Halo server groups	Server Groups
Halo-protected servers	Servers Server Accounts Server Commands Server Scans
Historical Halo scans	Scan History
Configuration Security Monitoring	Configuration Policies
File Integrity Monitoring	File Integrity Policies File Integrity Baselines
Software Vulnerability Assessment	CVE Exceptions
Workload Firewall Management	Firewall Policies Firewall Rules Firewall Interfaces Firewall Services Firewall Zones

Log-Based Intrusion Detection	▸ Log-Based Intrusion Detection Policies
Halo event logging and alerting	▸ Special Events Policies ▸ Events ▸ Alert Profiles
Halo reporting	▸ Saved Searches
System information	▸ System Announcements

Next Topic ▸

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. The API version number is independent of the CloudPassage Halo daemon 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 over 20 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 (client ID and client secret) in the request. To retrieve your client credentials, access the Halo Portal web interface and navigate to [Settings menu] **> Site Administration > API Keys**.

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 API Keys in the *Halo Operations Guide*.

Send the client id and client secret in an Authorization header of the POST request. Construct the Authorization header as follows:

1. Combine the client id and client secret into a string "client_id:client_secret" (with a colon seprating 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
```

Authentication with x-cpauth-access no longer supported

Support for use of the `x-cpauth-access` request header has been removed from Halo. You must authenticate with the authorization endpoint and with the API as described above.

Call Formats

Note: In the API calls in this document, metaparameters that you must replace with values are shown with curly brackets (for example, `...groups/{id}`). In your call, you replace the metaparameter with the actual value (for example, `...groups/1e9d5320a9b9012e0e53442c030d794d`).

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/users
```

Note the use of HTTPS, and note the API version number in the URL. This call returns a list of your Halo users 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 server 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 server 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 server group whose group ID is `{id}`. Note that the server 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

Code	Status	Explanation
200	OK	The request was successful and the response body contains the representation requested.
401	Unauthorized	The supplied credentials, if any, are not sufficient to access the resource.
403	Forbidden	The authorization level is not sufficient to access the resource.
404	Not Found	Resource not found.
500	Server Error	We could not return the representation due to an internal server error.

Possible POST or PUT Response Status Codes

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

Possible DELETE Response Status Codes

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

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:

```
 Status: 500

{
  "code" : 500,
  "message" : "Internal Server Error",
}
```

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.

```
{
 "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"
```

```
    }
}
```

Previous Topic Next Topic

Users

The Users endpoint includes all Halo user profiles in your CloudPassage customer account. You can use the API to retrieve the information for a single user or for all users in your account. To create or modify users, use the Halo Portal UI.

- Object Representation
- List users
- Get a single user

Object Representation

User object location

api.cloudpassage.com/v1
└users
└*id*

User object fields

Two levels of user information are available: core user fields (accessed through, for example, the **List users** call), and user details fields (accessed through the **Get a single user** call).

Core user fields

Field	Description
id	A unique string identifier for this user.
username	A unique username for this user.
email	User's email.
firstname	User's first name.
lastname	User's last name.
active	true if user is active.
portal_access	true if user has access to the Halo Portal.
ghostport_access	true if user has GhostPorts access.

Fields present only in user details

Field	Description
last_login_at	Timestamp of the last user login.
last_login_ip	Ip Address of the last user login.
created_at	Timestamp of the user creation.

List users

Lists all available profile information, including user ID and URL to the user resource, for all users in your Halo account.

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/users
```

Response

```
 Status: 200

{
  "users": [{
    "url": "https://api.cloudpassage.com/v1/users/ebc4b7e0e139012e1a1e442c030d794d",
    "active": true,
    "portal_access": true,
    "firstname": "Barney",
    "ghostport_access": false,
    "lastname": "Jones",
    "username": "barney",
    "id": "ebc4b7e0e139012e1a1e442c030d794d",
    "email": "barney@cloudpassage.com"
  }, {
    "url": "https://api.cloudpassage.com/v1/users/ebc4c700e139012e1a1e442c030d794d",
    "active": true,
    "portal_access": true,
    "firstname": "Carolyne",
    "ghostport_access": false,
    "lastname": "Johnson",
    "username": "carolyne",
    "id": "ebc4c700e139012e1a1e442c030d794d",
    "email": "carolyne@cloudpassage.com"
  }, {
    "url": "https://api.cloudpassage.com/v1/users/ebc4a450e139012e1a1e442c030d794d",
    "active": true,
    "portal_access": true,
    "firstname": "Abigail",
    "ghostport_access": false,
    "lastname": "Smith",
    "username": "abigail",
    "id": "ebc4a450e139012e1a1e442c030d794d",
    "email": "abigail@cloudpassage.com"
  }]
}
```

Get a single user

Lists the profile information for a single user, specified by user ID.

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

Response

```
 Status: 200

{
  "user": {
    "url": "https://api.cloudpassage.com/v1/users/ebc4a450e139012e1a1e442c030d794d",
    "active": true,
    "last_login_at": "2011-10-26T21:18:11Z",
    "last_login_ip": "10.10.10.10",
    "portal_access": true,
    "firstname": "Abigail",
    "ghostport_access": false,
    "lastname": "Smith",
    "username": "abigail",
    "id": "ebc4a450e139012e1a1e442c030d794d",
    "created_at": "2011-10-02T10:14:21Z",
    "email": "abigail@cloudpassage.com"
  }
}
```

Previous Topic *Next Topic*

Server 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 server groups
- Search for server groups that use a specific configuration policy
- Get a single server group
- Create a new server group
- Update server group attributes
- Assign a firewall policy to a server group
- Remove Windows and Linux firewall policies from a server group
- Assign one or more configuration policies to a server group
- Assign one or more file integrity policies to a server group
- Assign one or more log-based intrusion detection policies to a server group
- Remove log-based intrusion detection policies from a server group
- Assign a special events policy to a server group
- Assign one or more alert profiles to a server group
- Delete a server group without any servers
- Delete a server group and move the group's servers into the root group
- List common vulnerability and exposure exception identifiers applied to a server group
- List details of a common vulnerability and exposure exception identifier

Object Representation

Server group object location

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

Server group object fields

Two levels of server-group information are available: core server-group fields (accessed through, for example, the **List**

Server Groups and **Create a new server group** calls), and user details fields (accessed through, for example, the **Get a Single Server Group** and **Update server group attributes** calls).

Core server group fields

Field	Description
id	The Halo ID (a unique string identifier) for this server group.
name	A unique name for this server group.
tag	*Optional*. A unique tag assigned to this server group. Tag is used to assign servers to the group. Server started with the specific tag will be assigned to the group with that tag. Tag should start with a letter and contain only letters, numbers, . (dot), - (dash), and _ (underscore).
policy_ids	*Optional.* An array of one or more Halo IDs of Linux configuration policies assigned to this server group.
windows_policy_ids	*Optional.* An array of one or more Halo IDs of Windows configuration policies assigned to this server group.
fim_policy_ids *or* linux_fim_policy_ids	*Optional.* An array of one or more Halo IDs of Linux file integrity policies assigned to this server group.
windows_fim_policy_ids	*Optional.* An array of one or more Halo IDs of Windows file integrity policies assigned to this server group.
lids_policy_ids	*Optional.* An array of one or more Halo IDs of log-based intrusion detection policies assigned to this server group.
linux_firewall_policy_id	*Optional.* Halo ID of the Linux firewall policy assigned to this server group.
windows_firewall_policy_id	*Optional.* Halo ID of the Windows firewall policy assigned to this server group.
firewall_policy_id	**DEPRECATED** *Optional.* Halo ID of the Linux firewall policy assigned to this server group.
special_events_policy_id	*Optional.* Halo ID of the special events policy assigned to this server group.
alert_profile_ids	*Optional.* An array of one or more Halo IDs of alert profiles assigned to this server group.

Fields present only in server group details

Field	Description
cve_exception_ids	*Optional.* An array of common vulnerabilities and exposures exception identifiers.

Note: The field `firewall_policy_id` is shown in several example response bodies below. It is a deprecated field; you should use `linux_firewall_policy_id` instead.

List server groups

Returns the names and details, including group ID, of all of your currently defined server 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
```

```
{
  "groups": [{
    "id": "dfd487604d302a4318ft945jdhfgsdf446aaba",
    "url":
"https://api.cloudpassage.com/v1/groups/dfd487604d302a4318ft945jdhfgsdf446aaba",
    "name": "Unretired",
    "tag": null,
    "firewall_policy_id": null,
    "linux_firewall_policy_id": null,
    "windows_firewall_policy_id": null,
    "policy_ids": ["96cb9470a9b9012e0e56442c030d794d"],
    "windows_policy_ids:["864bae2074de013036c7404032d4ed47"]
  },
  {
    "id": "f8c0499b0130e9efsf3r45555446aaba",
    "url": "https://api.cloudpassage.com/v1/groups/f8c0499b0130e9efsf3r45555446aaba",
    "name": "Retired",
    "tag": null,
    "firewall_policy_id": null,
    "linux_firewall_policy_id": null,
    "windows_firewall_policy_id": null,
    "policy_ids": ["96cb9470a9b9012e0e56442c030d794d"]
  },
  {
    "id": "0499b01302e9445523235t6aaba",
    "url": "https://api.cloudpassage.com/v1/groups/0499b01302e9445523235t6aaba",
    "name": "Unassigned",
    "tag": null,
    "firewall_policy_id": null,
    "linux_firewall_policy_id": null,
    "windows_firewall_policy_id": null,
    "windows_policy_ids:["864bae2074de013036c7404032d4ed47"]
  }]
}
```


Search for server groups that use a specific configuration policy

Returns a list of server 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

{
  "groups": [{
    "url": "https://api.cloudpassage.com/v1/groups/1e9d5320a9b9012e0e53442c030d794d",
    "firewall_policy_id": null,
    "linux_firewall_policy_id": null,
    "windows_firewall_policy_id": null,
    "exception_ids": [],
    "name": "Unassigned",
    "policy_ids": ["96cb9470a9b9012e0e56442c030d794d"],
    "id": "1e9d5320a9b9012e0e53442c030d794d",
    "tag": null
```

```
  }, {
    "url": "https://api.cloudpassage.com/v1/groups/1ea83e60a9b9012e0e53442c030d794d",
    "firewall_policy_id": null,
    "linux_firewall_policy_id": null,
    "windows_firewall_policy_id": null,
    "exception_ids": [],
    "name": "Retired",
    "policy_ids": ["96cb9470a9b9012e0e56442c030d794d"],
    "id": "1ea83e60a9b9012e0e53442c030d794d",
    "tag": null
  }, {
    "url": "https://api.cloudpassage.com/v1/groups/1ea85fd0a9b9012e0e53442c030d794d",
    "firewall_policy_id": null,
    "linux_firewall_policy_id": null,
    "windows_firewall_policy_id": null,
    "exception_ids": [],
    "name": "Unretired",
    "policy_ids": ["96cb9470a9b9012e0e56442c030d794d"],
    "id": "1ea85fd0a9b9012e0e53442c030d794d",
    "tag": null
  }]
}
```

Get a single server group

Returns information describing a single server group specified by group ID.

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

Response

```
 Status: 200

{
  "group": {
    "url": "https://api.cloudpassage.com/v1/groups/1e9d5320a9b9012e0e53442c030d794d",
    "firewall_policy_id": null,
    "linux_firewall_policy_id": null,
    "windows_firewall_policy_id": null,
    "exception_ids": [],
    "name": "Unassigned",
    "policy_ids": ["96cb9470a9b9012e0e56442c030d794d"],
    "id": "1e9d5320a9b9012e0e53442c030d794d",
    "tag": null
  }
}
```

Create a new server group

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

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

Request Body

```
{
  "group": {
    "linux_firewall_policy_id": null,
    "windows_firewall_policy_id": null,
    "name": "Load Balancers",
    "policy_ids": ["96cb9470a9b9012e0e56442c030d794d"],
    "tag": "load_balancers"
  }
}
```

Response

```
Status: 201
Location: https://api.cloudpassage.com/v1/groups/e04b92e0b61e012ec6e8404096c01709


{
  "group": {
    "firewall_policy_id": null,
    "linux_firewall_policy_id": null,
    "windows_firewall_policy_id": null,
    "cve_exception_ids": [],
    "tag": "load_balancers",
    "policy_ids": ["96cb9470a9b9012e0e56442c030d794d"],
    "fim_policy_ids": [],
    "name": "Load Balancers",
    "url": "https://api.cloudpassage.com/v1/groups/e04b92e0b61e012ec6e8404096c01709",
    "id": "e04b92e0b61e012ec6e8404096c01709"
  }
}
```

Update server group attributes

Use this call to update individual attributes of the server 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.

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

Request Body

```
{

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

Response

```
Status: 204
```

Assign a firewall policy to a server group

To the group that you specify by group ID in the call URL, Halo assigns the Linux or Windows firewall policy that you specify by policy ID in the request body. Any existing firewall policy of the same platform type (Windows or Linux) that is assigned to the group will be replaced by this policy.

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

Request Body

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

Response

```
Status: 204
```

Remove Windows and Linux firewall policies from a server group

From the group that you specify by group ID in the call URL, Halo removes the firewall policy or policies for which you pass a policy ID value of `null` in the request body . You can remove the Windows policy, the Linux policy, or both.

Note: When a firewall policy is removed from a server 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).

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

Request Body

```
{
  "group": {
    "linux_firewall_policy_id": null,
    "windows_firewall_policy_id": null
  }
}
```

Response

```
 Status: 204
```

Assign one or more configuration policies to a server group

To the server group that you specify by group ID in the call URL, Halo assigns one or more configuration policies that you specify by policy ID in the request body. All existing configuration policies assigned to the group will be replaced by these policies.

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

Request Body

```
{

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

Response

```
 Status: 204
```

Assign one or more file integrity policies to a server group

To the server group that you specify by group ID in the call URL, Halo assigns one or more file integrity policies that you specify by policy ID in the request body. All existing file integrity policies assigned to the group will be replaced by these policies.

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

Request Body

```
{

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

Response

```
 Status: 204
```

Assign one or more log-based intrusion detection policies to a server group

To the server group that you specify by group ID in the call URL, Halo assigns one or more log-based intrusion detection policies that you specify by policy ID in the request body. All existing log-based intrusion detection policies assigned to the group will be replaced by these policies.

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

Request Body

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

Response

```
 Status: 204
```

Remove log-based intrusion detection policies from a server group

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 a policy ID value of `null` in the request body.

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

Request Body

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

Response

```
 Status: 204
```

Assign a special events policy to a server group

To the server group that you specify by group ID in the call URL, Halo assigns the special events policy that you specify by ID in the request body. Any existing special events policy assigned to the group will be replaced by this one.

Note: A server group cannot have more than one special events policy assigned to it.

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

Request Body

```
{

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

Response

```
 Status: 204
```

Assign one or more alert profiles to a server group

To the server group that you specify by group ID in the call URL, Halo assigns one or more alert profiles that you specify by ID in the request body. All existing alert profiles assigned to the group will be replaced by these profiles.

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

Request Body

```
{

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

Response

```
 Status: 204
```

Delete a server group without any servers

Deletes the server group that you specify by group ID. The server 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: 204
```

Delete a server group and move the group's servers into the root group

Deletes the server group that you specify by group ID, regardless of whether or not it is empty. Any servers assigned to the group are moved into the root group (equivalent to the "Unassigned" group in earlier versions of Halo). 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_unassigned=true
```

Response

```
 Status: 204
```

List common vulnerability and exposure exception identifiers applied to a server group

For the server group that you specify by group ID in the call URL, Halo returns the IDs of any CVE exceptions that have been defined for the group. The response body contains a list of those IDs plus other attributes of the group.

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

Response

```
 Status: 200

{
  "group": {
    "firewall_policy_id": null,
    "linux_firewall_policy_id": null,
    "windows_firewall_policy_id": null,
    "cve_exception_ids": ["302ed800b61a012ec6e8404096c01709"],
    "tag": "",
    "policy_ids": ["7bef46c072b1012ec681404096c01709",
"8883c860b0ce012ec6a4404096c01709"],
    "name": "Unassigned",
```

```
    "url": "https://api.cloudpassage.com/v1/groups/8cdc2200b576012ec6d7404096c01709",
    "id": "8cdc2200b576012ec6d7404096c01709"
  }
}
```

List details of a common vulnerability and exposure exception identifier

Returns details of the CVE exception specified by ID in the call URL. If you used the previous call to obtain a list of the vulnerability exceptions in a server group, you can now examine the details of the exceptions by making this call for each of them. The response body contains a CVE exception object that includes the name and version number of the package, the expiration date of the exception, and a list of the CVEs in the package.

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

Response

```
 Status: 200

{
  "cve_exception": {
    "package_name": "bzip2.x86_64",
    "server_id": null,
    "expires_at": "2011-09-01T23:59:59Z",
    "package_version": "1.0.3",
    "created_at": "2011-08-31T16:14:12Z",
    "id": "302ed800b61a012ec6e8404096c01709",
    "group_id": "8cdc2200b576012ec6d7404096c01709"
    "cve_entries": ["CVE-2010-0542", "CVE-2010-1748", "CVE-2010-2431"]
  }
}
```

Previous Topic Next Topic

Servers

Use the Servers endpoint to manage individual server resources. Any physical or virtual server on which you have installed a Halo Daemon is represented in the API by a server object. You can use the API to list your servers, move servers among server 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 server group
- Remove a server from a server group
- Retire a server
- Delete a server
- List server issues

Object Representation

Server object location

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

Server object fields

Field	Description
id	A unique identifier of the server.
url	The API URL to the server object.
hostname*	A calculated hostname of the server.
server_label*	A user-assigned label or description for the server.
reported_fqdn*	The internal fully qualified domain name of the server.
connecting_ip_address	The last reported IP address of the server.

state	The current state of the server Daemon: `active`, `deactivated`, or `missing`.
daemon_version	The version number of the currently installed Halo Daemon.
read_only	`true` if the Halo Daemon is running in read-only mode; otherwise `false`.
platform	Family of the currently installed operating system: `windows`, `linux`, or a Linux distribution name.
platform_version*	*Linux:* The version number of the O.S. distribution. *Windows:* same as `os_version`.
os_version*	The full version number of the operating system.
kernel_name	*Windows:* The full name of the operating system, such as `Microsoft Windows Server 2008 Datacenter`. *Linux:* Same as `platform`.
kernel_machine	The general chip architecture, such as `32-bit`, `64-bit`, or `x86_64`.
self-verification_failed	`true` if the most recent Daemon self-verification test failed; otherwise `false`.
connecting_ip_fqdn*	The fully qualified domain name of the server, using the connecting IP address as the hostname.
group_id	The Halo ID of the server group to which the server belongs.
group_name*	The name of the server group to which the server belongs.
proxy	The IP address or FQDN, port number, and name of the proxy server, if this server is configured to use a proxy.
interfaces	A list of reported network interfaces that are present on the server.
firewall_policy	The current firewall policy installed on the server (if any). *Only shown in single server listing details.*

*When using values of these fields as search filters, you can supply a substring of the full value (for example, `west.acme`), and the search will match any field value (for example, `c-127-63-31-15.west.acme.com`) that contains the specified substring (non-case-sensitive).

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:

Server state:

Add 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:

```
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`
(returns all servers that are not active)

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`")

`GET https://api.cloudpassage.com/v1/servers?connecting_ip_fqdn=c-127-63-31-15.west.acme.com`
(returns servers whose connecting-IP-address-based fully qualified domain name matches or contains "`c-127-63-31-15.west.acme.com`")

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

`GET https://api.cloudpassage.com/v1/servers?group_name=US-HQ-balancers`
(returns servers whose server-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`")

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)

`GET https://api.cloudpassage.com/v1/servers?package_version=11.0.9600.17041`
(returns only servers that have a package with that version number)

`GET https://api.cloudpassage.com/v1/servers?cve=CVE-2014-1778`
(returns only servers that have a package containing the specified CVE)

`GET https://api.cloudpassage.com/v1/servers?cve=CVE-2014-1778,CVE-2014-1779`
(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)

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`
- `server_label`

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. (See the second server in the example response below.)

Response

```
 Status: 200

{
  "servers": [
    {
      "id": "93579dd8f8a8df7c850ef8ccd93884ad",
      "url": "https://api.cloudpassage.com/v1/servers/93579dd8f8a8df7c850ef8ccd93884ad",
      "hostname": "ts-pg-build18",
```

```
      "server_label": "Build Server 18",
      "reported_fqdn": "ts-pg-build18.localdomain",
      "connecting_ip_address": "50.56.112.117",
      "state": "active",
      "daemon_version": "2.5.6",
      "platform": "centos",
      "platform_version": "5.6",
      "os_version": "2.6.18-238.19.1.el5.centos.plusxen",
      "kernel_name": "Linux",
      "kernel_machine": "x86_64",
      "self_verification_failed": false,
      "connecting_ip_fqdn": "c-50-56-112-117.ca.megacable.com",
      "group_id": "5ae33a606ac7012ea3c240403472c9f3",
      "group_name": "cruz-westdb",
      "interfaces": [
        {
          "name": "eth0",
          "ip_address": "50.56.112.117"
        },
        {
          "name": "eth1",
          "ip_address": "10.181.57.207"
        }
      ]
    },
    . . .
    {
      "id": "46b023b1e33f0b35d44beb4c82b07c64",
      "url": "https://api.cloudpassage.com/v1/servers/46b023b1e33f0b35d44beb4c82b07c64",
      "hostname": "EC2AMAZ-6BBFCR6",
      "server_label": null,
      "reported_fqdn": "EC2AMAZ-6BBFCR6",
      "connecting_ip_address": "54.241.75.168",
      "state": "deactivated",
      "daemon_version": "2.5.6",
      "platform": "windows",
      "platform_version": "6.0.6002",
      "os_version": "6.0.6002",
      "kernel_name": "Microsoft Windows Server 2008 Datacenter ",
      "kernel_machine": "64-bit",
      "self_verification_failed": true,
      "connecting_ip_fqdn": "c-54-241-75-168.ca.megacable.com",
      "group_id": "a3c242c905ae33a606ac7012e40347f3",
      "group_name": "cruz-westweb",
      "proxy": {
          "address": "x3-proxy-host.com",
          "port": "3129",
          "username": "proxy_user"}
      "interfaces": [
        {
          "name": "{8AAF166D-F7AE-477F-9416-DC2E669D745A}",
          "ip_address": "10.170.219.116"
        }
      ]
    }
  ]
}
```


List servers in a specific group

Returns a list of all active servers in the server 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/groups/{group_id}/servers
```

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

Response

```
 Status: 200

{
  "servers": [
    {
      "id": "bcd55105bbe49fff6d3b2e5717d997a3",
      "url": "https://api.cloudpassage.com/v1/servers/bcd55105bbe49fff6d3b2e5717d997a3",
      "hostname": "ip-10-122-50-65",
      "reported_fqdn": "ip-10-122-50-65.ec2.internal",
      "connecting_ip_address": "184.72.64.178",
      "state": "active",
      "daemon_version": "2.7.8",
      "platform": "amazon",
      "platform_version": "2012.09",
      "os_version": "3.2.30-49.59.amzn1.x86_64",
      "kernel_name": "Linux",
      "kernel_machine": "x86_64",
      "self_verification_failed": true,
      "connecting_ip_fqdn": "c-10-122-50-65.acme.com",
      "group_id": "47a3c242c90305ae33a606ac70403f312e",
      "group_name": "cruz-eastweb",
      "interfaces": [
        {
          "name": "eth0",
          "ip_address": "10.122.50.65"
        }
      ]
    },
    {
      "id": "bb4423c37b0790aa08b3968fb99c02e9",
      "url": "https://api.cloudpassage.com/v1/servers/bb4423c37b0790aa08b3968fb99c02e9",
      "hostname": "ip-10-122-50-66",
      "reported_fqdn": "ip-10-122-50-66.ec2.internal",
      "connecting_ip_address": "184.72.64.179",
      "state": "missing",
      "daemon_version": "2.6.1",
      "platform": "amazon",
      "platform_version": "2012.09",
      "os_version": "3.2.30-49.59.amzn1.x86_64",
      "kernel_name": "Linux",
      "kernel_machine": "x86_64",
      "self_verification_failed": false,
      "connecting_ip_fqdn": "c-10-122-50-66.acme.com",
      "group_id": "43a607a42c90303f05ae36ac704312e3c2",
      "group_name": "cruz-eastlb",
      "interfaces": [
        {
          "name": "eth0",
          "ip_address": "10.122.50.66"
        }
      ]
    },

  . . .
```

```
  ]
}
```

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 server 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}
```

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

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

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

Response

```
 Status: 200

{
  "servers": [
    {
      "id": "bcd55105bbe49fff6d3b2e5717d997a3",
      "url": "https://api.cloudpassage.com/v1/servers/bcd55105bbe49fff6d3b2e5717d997a3",
      "hostname": "ip-10-122-50-65",
      "reported_fqdn": "ip-10-122-50-65.ec2.internal",
      "connecting_ip_address": "184.72.64.178",
      "state": "deactivated",
      "daemon_version": "2.7.8",
      "platform": "amazon",
      "platform_version": "2012.09",
      "os_version": "3.2.30-49.59.amzn1.x86_64",
      "kernel_name": "Linux",
      "kernel_machine": "x86_64",
      "self_verification_failed": false,
      "connecting_ip_fqdn": "c-10-122-50-66.acme.com",
      "group_id": "43a607a42c90303f05ae36ac704312e3c2",
      "group_name": "cruz-northlb",
      "interfaces": [
        {
          "name": "eth0",
          "ip_address": "10.122.50.65"
        }
      ],
      "accounts": [
        {
          "username": "dbtestuser",
          "url":
"https://api.cloudpassage.com/v1/servers/bcd55105bbe49fff6d3b2e5717d997a3/accounts/dbtestu
```

```
          "uid": "333",
          "gid": "501",
          "comment": "",
          "home": "/home/dbtestuser",
          "shell": "/bin/bash",
          "last_login_at": null,
          "last_login_from": null
        }
      ]
    }
  ]
}
```

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

{
  "server": {
    "id": "c827779463036a0b90faf16283927dc2",
    "url": "https://api.cloudpassage.com/v1/servers/c827779463036a0b90faf16283927dc2",
    "hostname": "AMAZONA-CN1DVU6",
    "server_label": "BU15 NW-7",
    "reported_fqdn": "AMAZONA-CN1DVU6",
    "connecting_ip_address": "107.21.199.187",
    "state": "active",
    "daemon_version": "2.8.2",
    "platform": "windows",
    "platform_version": "6.1.7601",
    "os_version": "6.1.7601",
    "kernel_name": "Microsoft Windows Server 2008 R2 Datacenter ",
    "kernel_machine": "64-bit",
    "self_verification_failed": false,
    "connecting_ip_fqdn": "c-107-21-199-187.acme.com",
    "group_id": "3a46a42c90303f05a6ac07704312e3c2e3",
    "group_name": "cruz-eurlb",
    "firewall_policy": {
      "id": "af01a7308818013066b6404096c01709",
      "name": "GhostPorts RDP Inbound",
      "status": "active",
      "installed": "2013-07-12T20:57:28Z",
      "last_checked": "2013-07-26T16:43:34Z",
      "url":
"https://api.cloudpassage.com/v1/firewall_policies/af01a7308818013066b6404096c01709"
    },
    "interfaces": [
      {
        "name": "{06B43C11-860E-4712-A69F-A721B7C39664}",
        "ip_address": "10.41.1.158"
      }
    ]
  }
}
```

Move a server into a server group

Moves the server specified by server ID in the call URL into the server 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: Moving a server into the "Retired" group is a special case. See **Retire a server**.

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

Request Body

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

Response

```
 Status: 204
```

Remove a server from a server group

Removing an active server from a server group means moving it to the Unassigned server group. First obtain the group ID for the Unassigned group by submitting a **List server groups** request:

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

Then move the server to the Unassigned group by submitting a **Move server into a server group** request and supplying the Unassigned group's ID:

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

Request Body

```
 {
  "server": {
    "group_id": "{unassigned_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 is removed from whatever other server group it previously belonged to and added to the "Retired" server group.

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

Request Body

```
{
  "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.

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

```
 Status: 200

{
  "id": "272c13d4a503fa7a851e5373ddcbb8c1",
  "hostname": "ip-10-171-139-167",
  "connecting_ip_address": "184.72.3.57",
  "state": "active",
  "sca": {
    "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": ""
          }
        ],
        "rule_name": "Configuration File Setting"
      },
      {
        "critical": true,
        "status": "bad",
        "details": [
          {
            "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"
        }
      ],
      "rule_name": "dev-4365"
    },

              ...

    {
      "critical": false,
      "status": "bad",
      "details": [
        {
          "type": "dir_acl",
          "status": "bad",
          "target": "/root",
          "expected": "777",
          "actual": "550",
          "scan_status": "ok"
        }
      ],
      "rule_name": "Directory ACL"
    },
    {
      "critical": false,
      "status": "bad",
      "details": [
        {
          "type": "dir_owner_gid",
          "status": "bad",
          "target": "/root",
          "expected": "floppy",
          "actual": "root",
          "scan_status": "ok"
        }
      ],
      "rule_name": "Directory Group Ownership"
    },

              ...

  ]
},
"svm": {
  "status": "completed_clean",
  "critical_findings_count": 34,
  "non_critical_findings_count": 12,
  "findings": [
    {
      "package_name": "busybox.x86_64",
      "package_version": "1.15.1",
      "critical": true,
      "status": "bad",
```

```
        "cve_entries": [
          {
            "cve_entry": "CVE-2011-2716",
            "suppressed": false
          }
        ]
      },
      {
        "package_name": "cpio.x86_64",
        "package_version": "2.10",
        "critical": true,
        "status": "bad",
        "cve_entries": [
          {
            "cve_entry": "CVE-2010-0624",
            "suppressed": false
          }
        ]
      },

                ...

      {
        "package_name": "rsync.x86_64",
        "package_version": "3.0.6",
        "critical": false,
        "status": "bad",
        "cve_entries": [
          {
            "cve_entry": "CVE-2011-1097",
            "suppressed": false
          }
        ]
      },
      {
        "package_name": "ssmtp.x86_64",
        "package_version": "2.61",
        "critical": false,
        "status": "bad",
        "cve_entries": [
          {
            "cve_entry": "CVE-2008-3962",
            "suppressed": false
          },
          {
            "cve_entry": "CVE-2008-7258",
            "suppressed": false
          }
        ]
      }
    ]
  }
}
```


Previous Topic

Next Topic

Server Accounts

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

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

- Object Representation
- List server accounts
- Search for server accounts by username or uid
- 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

```
api.cloudpassage.com/v1
                      └servers
                            └server_id
                                  └accounts
                                        └username
```

Server account object fields

Two levels of server-account information are available: core account fields (accessed through, for example, the **List server accounts** call), and account details fields (accessed through the **Get server account details** call).

Core server account fields

Field	Description

username	A username of the server account.
uid	A user id of the server account.
gid	A group id of the server account.
home	A home directory of the server account.
shell	A server's account shell.
comment	A comment for the server account.
last_login_at	The last time the server account logged on in UTC time (if available)
last_login_from	The last domain and port the account logged on from (if available)

Fields present only in server account details

Field	Description
home_exists	Whether or not the server account's home directory exists or not
groups	Any groups the account belongs to (if any)
last_password_change	When the account's password was last changed (if available)
days_warn_before_password_expiration	How soon the account is warned about password expiration (if available)
minimum_days_between_password_changes	The date before which the account's password *may* be changed (if available)
maximum_days_between_password_changes	The date before which the account's password *must* be changed (if available)
disabled_after_days_inactive	How many days of inactivity before the account is disabled (if available)
days_since_disabled	How many days since the account was disabled (if available)
ssh_authorized_keys	An array of any authorized SSH keys belonging to the account (if available)
sudo_access	A list of sudo access rules for the account, both as a member of a group and as a user (if available)

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

{
  "accounts": [{
    "last_login_at": null,
    "uid": "3",
    "comment": "adm",
    "gid": "4",
    "home": "/var/adm",
    "username": "adm",
    "shell": "/sbin/nologin",
```

```
    "url":
"https://api.cloudpassage.com/v1/servers/1206942686a8a6da1586c8aaeac10452/accounts/adm",
    "last_login_from": null
  }, {
    "last_login_at": null,
    "uid": "70",
    "comment": "Avahi daemon",
    "gid": "70",
    "home": "/",
    "username": "avahi",
    "shell": "/sbin/nologin",
    "url":
"https://api.cloudpassage.com/v1/servers/1206942686a8a6da1586c8aaeac10452/accounts/avahi",

    "last_login_from": null
  }, {
    "last_login_at": null,
    "uid": "100",
    "comment": "avahi-autoipd",
    "gid": "101",
    "home": "/var/lib/avahi-autoipd",
    "username": "avahi-autoipd",
    "shell": "/sbin/nologin",
    "url":
"https://api.cloudpassage.com/v1/servers/1206942686a8a6da1586c8aaeac10452/accounts/avahi-
autoipd",
    "last_login_from": null
  }, {
    "last_login_at": null,
    "uid": "1",
    "comment": "bin",
    "gid": "1",
    "home": "/bin",
    "username": "bin",
    "shell": "/sbin/nologin",
    "url":
"https://api.cloudpassage.com/v1/servers/1206942686a8a6da1586c8aaeac10452/accounts/bin",
    "last_login_from": null
  }
...
]}
```

Search for server accounts by username or uid

Returns all instances of a given server account (specified by either account name or uid) on the server specified by server ID. (To search for an account across all servers, use the **List active servers that have a specific user account** call.)

```
GET https://api.cloudpassage.com/v1/servers/{server_id}/accounts?
search[username]={username}
```

```
GET https://api.cloudpassage.com/v1/servers/{server_id}/accounts?search[uid]={uid}
```

Response

```
 Status: 200

{
  "accounts": [
    {
```

```
      "username": "root",
      "url":
"https://api.cloudpassage.com/v1/servers/1a85bf9f58d619f58d6c33a7dda959fd/accounts/root",

      "uid": "1",
      "gid": "0",
      "comment": "This is root",
      "home": "/root",
      "shell": "/bin/sh",
      "last_login_at": null,
      "last_login_from": null
    }
  ]
}
```

Get server account details

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": {
    "maximum_days_between_password_changes": 99999,
    "days_warn_before_password_expiration": 7,
    "last_login_at": "2011-08-16T14:47:47Z",
    "uid": "500",
    "disabled_after_days_inactive": null,
    "comment": "",
    "gid": "500",
    "home": "/home/bob",
    "groups": "users, bob",
    "home_exists": true,
    "days_since_disabled": null,
    "last_password_change": "2011-08-02",
    "sudo_access": [{
      "as_group": [
        ["%bob ALL = (ALL) ALL"]
      ]
    }],
    "username": "bob",
    "ssh_authorized_keys": [{
      "type": "rsa",
      "comment": "bob@bobs-macbook-pro.local"
    }],
    "shell": "/bin/bash",
    "minimum_days_between_password_changes": 0,
    "url":
"https://api.cloudpassage.com/v1/servers/1206942686a8a6da1586c8aaeac10452/accounts/bob",
    "ssh_acl": "rwx------",
    "last_login_from": "c-22-156-23-228.hsd1.md.comcast.net pts/0"
  }
}
```

Create a new server account

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
    }
  }
}
```

Response

```
 Status: 202
Location:
https://api.cloudpassage.com/v1/servers/bd49ce6e06448012e21a713ce62c039c/commands/ac49ce6e


{
  "command": {
    "id": "ac49ce6e06448012e21a713ce62c039c",
    "url":
"https://api.cloudpassage.com/v1/servers/bd49ce6e06448012e21a713ce62c039c/commands/ac49ce6

    "name": "Create Account",
    "status": "queued",
    "created_at": "2011-10-10T10:10:10Z",
    "updated_at": "2011-10-10T10:10:10Z"
  }
}
```

Reset password for a server account

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

```
 Status: 202
Location:
https://api.cloudpassage.com/v1/servers/bd49ce6e06448012e21a713ce62c039c/commands/ac49ce6e


{
  "command": {
    id: "ac49ce6e06448012e21a713ce62c039c",
    url:
"https://api.cloudpassage.com/v1/servers/bd49ce6e06448012e21a713ce62c039c/commands/ac49ce6

    name: "Reset Password",
    status: "queued",
    created_at: "2011-10-10T10:10:10Z",
    updated_at: "2011-10-10T10:10:10Z"
  }
}
```

Disable a server account

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
Location:
https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c039


{
  "command": {
    id: "ac49ce6e06448012e21a713ce62c039c",
    url:
"https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c03

    name: "Disable Account",
    status: "queued",
    created_at: "2011-10-10T10:10:10Z",
    updated_at: "2011-10-10T10:10:10Z"
  }
}
```

Enable a server account

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}`

Request Body

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

Response

```
 Status: 202
Location:
https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c039


{
  "command": {
    id: "ac49ce6e06448012e21a713ce62c039c",
    url:
"https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c03

    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

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": {
    "ssh_authorized_keys": [{
      "key": "ssh-dsa
AAAAe06448012e21a713e06448012e21a713e06448012e21a713e06448012e21a713==="
    },{
      "key": "ssh-dsa
AAAAe06448012egfjhdgyw3433333rfsfsfs48012e21a713e06448012e21a713==="
    }]
  }
}
```

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:

```
 {
  "account": {
    "ssh_authorized_keys": []
  }
}
```

Response

```
 Status: 202
Location:
https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c039


{
  "command": {
    id: "ac49ce6e06448012e21a713ce62c039c",
    url:
"https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c03

    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/ac49ce6e06448012e21a713ce62c039


{
  "command": {
    id: "ac49ce6e06448012e21a713ce62c039c",
    url:
"https://api.cloudpassage.com/v1/servers/HKJHLKHLK/commands/ac49ce6e06448012e21a713ce62c03

    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

Field	Description
id	A unique identifier of the server command.
name	A name of the command.

status	A status of the command. Possible values *queued*, *pending*, *completed*, *failed*.
created_at	A timestamp when command was created.
updated_at	A timestamp when command was last updated.
result	A result of the command execution once command is finished.

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/ac49ce6e06448012e21a713ce62c03

    "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/3f11b34710360a2e354662cdb6998428/commands/df0715804bce01302a5

    "name": "Reset Password",
    "status": "completed",
    "created_at": "2013-01-28T23:17:55Z",
    "updated_at": "2013-01-28T23:17:55Z",
    "result": {
      "password": "uhgdfd7sdfd$$"
    }
  }
}
```

Server Scans

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

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

Field	Description
id	A unique identifier for the server.
module	The type of scan to execute: `sca`, `svm`, `sam`, or `fim`.

Scan results fields

Field	Description
id	A unique identifier for the server.
hostname	Server host name.
server_label	*Optional*. A label that identifies the server.
connecting_ip_address	Server IP address.
state	Daemon state: `active`, `deactivated`, or `missing`.
scan	Information for the scan. Includes the following sub-fields:
id	A unique identifier for the scan.
url	The URL to the scan object.
module	The type of scan: `sca`, `svm`, `sam`, or `fim`
status	Overall scan status: • `completed_clean`: The scan was successful, and (for a configuration scan) no rule checks failed. • `completed_with_errors`: The scan was successful, some rule checks failed. (Applies to configuration scans only.) • `failed`: The scan was not successful.
created_at	When the scan started.
completed_at	When the scan ended.
server_id	Halo server ID for the server.
server_hostname	Server host name.
server_url	API URL to the server object.
critical_findings_count	The number of scan results considered to be critical issues.
non_critical_findings_count	The number of scan results considered to be non-critical issues.
requested_by	For a manual scan, the Halo user who requested it.
findings	A list of results for each item examined. See tables below.

Configuration scan findings fields

Field	Description
critical	`true` if failure of this rule is a critical issue; otherwise `false`.
status	the result for this rule: `good` (= passed), `indeterminate`, or `bad` (= failed).
details	A list of results for each configuration check in this rule. Includes the following sub-fields:
type	The rule check that was applied.
status	the result for this check: `good` (= passed), `indeterminate`, or `bad` (= failed).
target	The item examined by this check.
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 fields

Field	Description
id	A unique identifier for the finding.
url	The URL to the finding 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 missing.
added	This many new objects were added.
changed	This many objects had changes to their content or metadata.
reference_ids	A comma-separated list of IDs used to mark this rule for compliance purposes.

Vulnerability scan findings fields

Field	Description
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.
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).

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`:

- **`sca`**. A configuration scan. (Requires Halo Professional subscription.)
- **`svm`**. A vulnerability scan. (Requires Halo Professional subscription.)
- **`sam`**. A server access scan. (Requires Halo Professional or NetSec subscription.)
- **`fim`**. A file integrity scan. (Requires Halo Professional subscription.)

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/154e9890


    {
      "command" => {
                "id" => "154e98905860013022d83c0754715774",
               "url" =>
"https://api.cloudpassage.com/v1/servers/5ad1f4534b49ee59335d150cebec4099/commands/154e989

              "name" => "Commands::SamScanCommand",
            "status" => "queued",
        "created_at" => "2013-02-13T23:07:37Z",
        "updated_at" => "2013-02-13T23:07:37Z"
    }
```

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

{
  "id": "c827779463036a0b90faf16283927dc2",
  "hostname": "AMAZONA-CN1DVU6",
  "connecting_ip_address": "107.21.199.187",
  "state": "active",
  "scan": {
    "module": "sca",
    "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,
    "findings": [
      {
        "critical": true,
        "status": "indeterminate",
        "details": [
          {
            "type": "windows_service_started",
            "status": "indeterminate",
            "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": "cphalod",
            "expected": true,
            "actual": false,
            "scan_status": "not_found"
          }
        ],
        "rule_name": "Service Started"
      },

      . . .

    ]
```

```
  }
}
```

List server file integrity scan results

For the server specified in the call URL, returns 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.

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

Response

```
Status: 200

{
  "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,
    "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": true,
          "recurse": true,
          "target": "/home/ec2",
          "alert": false,
          "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

{
  "id": "63a61dda4d1369b3da0761638652ac29",
  "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": "63a61dda4d1369b3da0761638652ac29",
    "server_hostname": "ip-10-197-5-10",
    "server_url":
"https://api.cloudpassage.com/v1/servers/63a61dda4d1369b3da0761638652ac29",
    "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",
            "suppressed": false
          },
          {
            "cve_entry": "CVE-2013-1944",
            "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",
            "suppressed": false
```

```
        }
      ]
    },

    . . .

    {
      "package_name": "zlib.x86_64",
      "package_version": "1.2.7-9.fc18",
      "critical": false,
      "status": "good",
      "cve_entries": []
    }
  ]
 }
}
```

Note: For Windows servers, any of the following three fields may appear at the end of a package description, after the CVE entries:

```
    }],
      "vendor": "Microsoft Corporation",
      "install_date": "2013-11-19T00:00:00.000000Z",
      "cpe": "cpe:/o:microsoft:windows_server_2008:r2:sp1:x64"
    },
    {
```

Previous Topic Next Topic

Scan History

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

- Object Representation
- List historical scans
- Get scan details

Object Representation

Scan object location

api.cloudpassage.com/v1
└scans
└*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 similar to the fields returned as findings from the **List server issues** call of the Servers API endpoint.

Field	Description
id	The ID of this scant.
url	The API URL to the scan object.
module	The type of scan performed: `sca`, `fim`, `svm`, or `sam`.
status	The status of the scan: `queued`, `pending`, `running`, `completed_clean`, `completed_with_errors`, or `failed`.
created_at	Scan start timestamp. Formatted in ISO 8601.
completed_at	Scan completion timestamp. Formatted in ISO 8601.
server_id	Server's unique ID.
server_hostname	Server's hostname.
server_url	Server's URL in Halo.
critical_findings_count	Number of critical issues reported. (Not reported for server access scans.)

non_critical_findings_count	Number of non-critical issues reported. (Not reported for server access scans.)
requested_by	The username of the Halo user who executed the scan (not returned for automatic scans).

List historical scans

Returns JSON-fomatted 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*-*DD***T***hh*:*mm***Z** for Zulu time zone). For example:

  ```
  GET https://api.cloudpassage.com/v1/scans?since=2013-06-22&until=2013-08-21
  ```

- 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,sca

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

  GET https://api.cloudpassage.com/v1/scans?server_hostname=acme-west-22

  GET https://api.cloudpassage.com/v1/scans?status=completed_clean&module=sam
  ```

- 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.

  ```
  GET https://api.cloudpassage.com/v1/scans?page={pagenum}&per_page={pagesize}
  ```

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

Response

```
 Status: 200

{
  "scans": [{
    "id": "42076ff0927d01318e6b3c764e101158",
    "url": "https://portal.cloudpassage.com/v1/scans/42076ff0927d01318e6b3c764e101158",
    "module": "fim",
    "status": "completed_clean",
    "created_at": "2013-06-07T21:30:20Z",
    "completed_at": "2013-06-07T21:30:25Z",
    "server_id": "abc123xyz456abc123xyz456abc123x",
    "server_hostname": "ip-10-244-37-178",
    "server_url":
"https://api.cloudpassage.com/v1/servers/abc123xyz456abc123xyz456abc123x",
    "critical_findings_count": 60,
    "non_critical_findings_count": 0
    "requested_by": "example-user"
  }, {
    "id": "41994780927d01318e653c764e101158",
```

```
    "url": "https://portal.cloudpassage.com/v1/scans/41994780927d01318e653c764e101158",
    "module": "sca",
    "status": "completed_with_errors",
    "created_at": "2013-06-07T19:40:56Z",
    "completed_at": "2013-06-07T19:41:13Z",
    "server_id": "abc123xyz456abc123xyz456abc123x",
    "server_hostname": "ip-10-244-37-178",
    "server_url":
"https://api.cloudpassage.com/v1/servers/abc123xyz456abc123xyz456abc123x",
    "critical_findings_count": 3,
    "non_critical_findings_count": 21
  }, {
    "id": "40426d80927d01318e663c764e101158",
    "url": "https://portal.cloudpassage.com/v1/scans/40426d80927d01318e663c764e101158",
    "module": "sam",
    "status": "completed_clean",
    "created_at": "2013-06-06T21:34:12Z",
    "completed_at": "2013-06-06T21:34:18Z",
    "server_id": "abc123xyz456abc123xyz456abc123x",
    "server_hostname": "ip-10-244-37-178",
    "server_url":
"https://api.cloudpassage.com/v1/servers/abc123xyz456abc123xyz456abc123x"
  }, {
    "id": "40318d80927d01318e663c764e101158",
    "url": "https://portal.cloudpassage.com/v1/scans/40318d80927d01318e663c764e101158",
    "module": "svm",
    "status": "completed_clean",
    "created_at": "2013-06-06T21:34:11Z",
    "completed_at": "2013-06-06T21:34:23Z",
    "server_id": "abc123xyz456abc123xyz456abc123x",
    "server_hostname": "ip-10-244-37-178",
    "server_url":
"https://api.cloudpassage.com/v1/servers/abc123xyz456abc123xyz456abc123x",
    "critical_findings_count": 41,
    "non_critical_findings_count": 6
    ...
  }],
 "count": 35,
 "pagination": {
   "next": "https://api.cloudpassage.com/v1/scans?page=2&per_page=10&since=2013-06-
05T18%3A46%3A44Z&until=2013-06-07T22%3A33%3A24Z"
  }
}
```


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.

```
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"
         },

        . . .

         {
            "package_name": "setup.noarch",
            "package_version": "2.8.14-20.el6_4.1",
            "critical": false,
            "status": "good",
            "cve_entries": [],
            "cpe": "not_found"
         }
      ]
   }
}
```


Previous Topic

Next Topic

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 server group, call **Assign one or more configuration policies to a server 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
- Defined Configuration Checks

Object Representation

Configuration policy object location

```
api.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

Field	Description
id	The Halo ID (unique identifier) of the configuration policy.
name	A name given to the configuration policy.
description	*Optional.* A description of the configuration policy.

platform	*Optional.* The OS platform of the configuration policy. Either `windows` or `linux`. Default = `linux`.
used_by	*Read-only.* A list of the Halo ID's of server groups that use the configuration policy.

Configuration policy detail fields

Field	Description
url	The full URL (including policy ID) to the configuration policy object.
rules	A list of the rules in the policy.Each rule includes the following sub-fields:
active	`true` if the rule is active; `false` if it is inactive (not used by the policy).
alert	`true` if failure of the rule generates an email alert; `false` if not.
comment	An optional comment or description for the rule.
critical	`true` if an event logged by the failure of the rule should be classified as critical; `false` if not.
log	`true` if failure of the rule is logged as an event; `false` if not.
name	A name for the rule.
taxonomy	The general category of the rule (from the Edit Configuration Policy page of the Halo Portal), such as `system_configuration` or `other`.
checks	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 *Monitoring Server Configuration Security* for descriptions of each check's specific fields. Also, the following fields are returned for all checks:
object_type	The name of the check, as documented in the Configuration Rule Checks appendix.
active	`true` if the check is active; `false` if it is inactive (not used by the rule).
exportable	`true` if the check is API-exportable (its failures are to be included in the results returned by the **List server issues** method of the API); `false` if not.
suggestion	An optional remediation suggestion for failures of this check.
reference_identifiers	An optional comma-separated list of IDs applied to this rule for compliance purposes.

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
```

Response

```
 Status: 200

{
  "policies": [{
    "used_by": [{
      "name": "AcmeCorp - AMI (Amazon)",
      "id": "7bbea00072b1012ec681404096c01709"
    }],
    "description": "This configuration security policy has been configured for a default
Amazon Linux distribution.",
    "name": "AMI - Core OS Policy",
    "platform": "linux",
    "id": "7bcb0a0072b1012ec681404096c01709"
  }, {
    "used_by": [],
    "description": null,
    "name": "Basic Windows Copy",
    "platform": "windows",
    "id": "a44c24a07da6012ec688404096c01709"
  }]
}
```

Get configuration policy details

Returns detailed information—including all policy rules and all configuration chcecks—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 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": false,
        "comment": null,
        "critical": false,
        "log": false,
        "name": "system-level checks",
        "taxonomy": "system_configuration",
        "checks": [
          {
            "object_type": "file_presence",
            "active": true,
            "exportable": true,
```

```
            "suggestion": "Replace fle if missing",
            "files": "C:\Windows\System32\wininit.exe",
            "present": true
          },
          {
            "object_type": "local_security_policy_settings",
            "active": true,
            "exportable": true,
            "suggestion": "Restore setting to desired value",
            "setting": "AuditDSAccess",
            "desired_value": "1"
          },
          {
            "object_type": "registry_key_value_setting",
            "active": true,
            "exportable": true,
            "suggestion": "",
            "registry_key":
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer",
            "value_name": "MsiExecCA64",
            "expected_data": "C:\Windows\system32\msiexec.exe"
          },

          . . .

        ]
      }
    ]
  }
}
```

Create a new configuration policy

Creates a new configuration policy with the initial values and rules specified in the request body. The minimum required field to supply is `name`.

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
```

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

Object type (= check name)	Attribute values (= defined fields)
configuration_file_setting	active, comment_character, config_file_path, config_file_section, config_item, delimiter, desired_value, exportable, suggestion
directory_acl	acls, active, exportable, files, suggestion
directory_group_ownership	active, exportable, files, owned_by, suggestion
directory_presence	active, exportable, folders, present, suggestion
directory_user_ownership	active, exportable, folders, owned_by, suggestion
file_acl	acls, active, exportable, files, suggestion
file_group_ownership	active, exportable, files, owned_by, suggestion
file_presence	active, exportable, files, present, suggestion
file_setgid	active, exportable, files, setgid, suggestion
file_setuid	active, exportable, files, setuid, suggestion
file_string_presence	active, exportable, files, patterns, present, suggestion
file_user_ownership	active, exportable, files, owned_by, suggestion
geolocation_by_country	active, allowed, countries, exportable, suggestion
group_gid	active, exportable, gid, group, suggestion
group_has_password	active, exportable, groups, suggestion
group_members	active, exportable, group, suggestion, users
home_directory_exists	active, exportable, suggestion, users
home_directory_file_presence	active, exportable, files, present, suggestion, users

home_directory_files_have_no_invalid_umask_commands	active, exportable, files, suggestion, umask, users
home_directory_files_have_no_unsafe_path_statements	active, exportable, files, suggestion, users
home_directory_files_owned_by_correct_group	active, exportable, suggestion, users
home_directory_files_owned_by_correct_user	active, exportable, suggestion, users
home_directory_has_no_device_files	active, exportable, suggestion, users
home_directory_has_no_setgid_files	active, exportable, suggestion, users
home_directory_has_no_setuid_files	active, exportable, suggestion, users
home_directory_owned_by_correct_group	active, exportable, suggestion, users
home_directory_owned_by_correct_user	active, exportable, suggestion, users
mount_point	active, exportable, mount_point, mounted, target, suggestion
network_service_accessibility	active, exportable, interfaces, ports, suggestion
network_service_processes	active, exportable, interface_port, process, suggestion
no_recent_account_login	active, days, exportable, suggestion, users
password_does_not_match_username	active, exportable, suggestion, users
password_is_not_expired	active, exportable, suggestion, users
process_group_ownership	active, exportable, owned_by, processes, suggestion
process_presence	active, exportable, present, processes, suggestion
process_user_ownership	active, exportable, owned_by, processes, suggestion
recent_account_login	active, days, exportable, suggestion, users
user_account_uid	active, exportable, suggestion, uid, user
user_group_membership	active, exportable, groups, suggestion, user
user_has_password	active, exportable, suggestion, users
world_writable_directories_have_sticky_bit_set	active, exclude_directories, exportable, suggestion

Windows checks

Object type (= check name)	Attribute values (= defined fields)
advanced_audit_policy_setting	active, audit_subcategory, desired_value,exportable, suggestion
directory_presence	active, exportable, folders, present, suggestion
file_presence	active, exportable, files, present, suggestion
geolocation_by_country	active, allowed, countries, exportable, suggestion
local_security_policy_settings	active, desired_value, exportable, setting, suggestion
local_user_rights_assignment	active, desired_value, exportable, setting, suggestion

registry_key_value_setting	active, expected_data, exportable,registry_key, suggestion, value_name
service_started	active, exportable, services, started, suggestion

Previous Topic Next Topic

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

Field	Description
id	A unique identifier for the policy

name	The name of the policy
description	The description given to the policy
platform	The OS platform of the policy (`linux` or `windows`)
template	`true` if this policy is a policy template, `false` if not
url	The URL of the policy object
active	`true` if this policy has at least one active baseline, `false` if not
rules	An array of rules that make up the policy

Rule fields

Field	Description
target	The path or wildcard for monitoring
description	The description of this rule
active	`true` if this rule is active, `false` if it is inactive (deactivated)
recurse	`true` if Halo should recursively scan all subdirectories of this target
critical	`true` if this rule should be marked as critical
alert	`true` if this rule should generate an alert when matched
patterns	An array of files or wildcards to include or exclude from monitoring (see below)
reference_identifiers	A comma-separated list of IDs used to mark this rule for compliance purposes

Pattern fields

Field	Description
pattern	The file or wildcard for including or excluding from the rule's target
description	The description for this pattern
inclusion	`true` if the pattern is an inclusion, `false` if it is an exclusion

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

{
  "fim_policies": [{
    "id": "78eb8ea0053442c031a719c501307981",
    "url":
"https://api.cloudpassage.com/v1/fim_policies/78eb8ea0053442c031a719c501307981",
    "name": "My 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
      }]
    }]
  }, {
    "id": "454gs578we334546uui343pppu343ui1",
    "url":
"https://api.cloudpassage.com/v1/fim_policies/454gs578we334546uui343pppu343ui1",
    "name": "Another policy",
    "description": "Just watches system32 dir",
    "platform": "windows",
    "rules": [{
      "target": "C:\Windows\system32",
      "recurse": true,
      "critical": true,
      "alert": true
    }]
  }]
}
```

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

{
  "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
      }]
      "reference_identifiers": []
    }]
  }
}
```

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

```
 Status: 201
Location: https://api.cloudpassage.com/v1/fim_policies/2343sh34h23254543543hgf5

{
  "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

```
{
  "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
```

Previous Topic Next Topic

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

Field	Description
id	A unique identifier for the baseline.
url	The API URL to the baseline object.
server_id	The id of the server used for the baseline.
comment	Any comments associated with the baseline.
status	The current status of the baseline, for example `Pending`, `Active`, `Expired`, or `Invalid`.
effective_at	When the baseline takes effect.
expires_at	When the baseline will expire (or null if there is no expiration).
policy_name	The name of the file integrity policy that this baseline is assigned to.
server_name	The host name of the baseline server.
platform	The platform family (`windows` or `linux`) of the baseline server.
details	Appears only in *Show baseline details* call. See table below.

File integrity baseline details fields

Field	Description
total_objects	The total number of target objects scanned in the baseline scan.
targets	A list of the scanned target objects. Includes the following subfields:
target	Full path to the target, as specified in the file integrity policy.
inclusions	A pattern specifying which objects within the target directory *should* be scanned.
exclusions	A pattern specifying which objects within the target directory *should not* be scanned.
number_of_objects	the number of individual objects within this target specification that were scanned.
objects	Details about each of the scanned objects. Includes the following sub-fields:
name	Full path to the scanned object.
type	The kind of object scanned, such as `file`, `directory`, or `registry` (key).
owner	The username of the owner of the object.
permissions	The set of permissions on the object.
contents	The signature (SHA-256 hash) of the object's contents.

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
{
```

```
  "baselines": [
    {
      "id": "42b43bb07f90013062c2404096c01709",
      "url":
"https://api.cloudpassage.com/v1/fim_policies/3310d1707f90013062be404096c01709/baselines/4

      "server_id": "04a50e1aec4bdc5fe2cf7d23f020f47a",
      "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/78eb8ea00

      "server_id": "hsjfs323212342jh343",
      "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"
    }
  ]
}
```


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/c

    "server_id": "a6417fd571979758f0dd685f94ce52f8",
    "comment": "",
    "status": "Expired",
    "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"
  }
}
```

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": "42b43bb07f90013062c2404096c01709",
    "url":
"https://api.cloudpassage.com/v1/fim_policies/3310d1707f90013062be404096c01709/baselines/4

    "server_id": "04a50e1aec4bdc5fe2cf7d23f020f47a",
    "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",
    "server_name": "ATOM7D80",
    "platform": "windows",
    "details": {
      "total_objects": 122,
      "targets": [
        {
          "target": "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":
"33bfbf90ce5f4f88169a8dba94ac2d1d01816f6a5bf99d532cbdd4f41641b6dc"
            }
          ]
        },

        . . .

        {
          "target": "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":
"3dcd88d48c0039de469d390cdb84a8a490490f939378eb7dc8f090b1428d1966"
            }
          ]
        }
      ]
    }
  }
}
```

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

```
 {
  "baseline": {
    "server_id": "83734bh3bv347iy343bh3423",
    "expires": null,
    "comment": "This one will not expire"
  }
}
```

Response

```
 Status: 201
Location:
https://api.cloudpassage.com/v1/fim_policies/2343sh34h23254543543hgf5/baselines/78eb8ea005


{
  "baseline": {
```

```
    "id": "78eb8ea0053442c031a719c501307981",
    "url":
"https://api.cloudpassage.com/v1/fim_policies/2343sh34h23254543543hgf5/baselines/78eb8ea00

    "server_id": "83734bh3bv347iy343bh3423",
    "effective_at": null,
    "expires_at": null,
    "comment": "This one will not expire",
    "status": "Pending"
  }
}
```

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/78eb8ea005


{
  "baseline": {
    "id": "78eb8ea0053442c031a719c501307981",
    "url":
"https://api.cloudpassage.com/v1/fim_policies/2343sh34h23254543543hgf5/baselines/78eb8ea00

    "server_id": "8343jb3hbv233834g32hgh34",
    "effective_at": "2012-10-22T05:28:19.148087Z",
    "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
```

Previous Topic Next Topic

CVE Exceptions

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. For further discussion of software exceptions, see Define Exceptions in *Assessing Software Vulnerabilities with CloudPassage Halo*.

- Object Representation
- List CVE exceptions
- Get a single CVE exception

Object Representation

CVE exception object location

api.cloudpassage.com/v1
└cve_exceptions
└*id*

CVE exception object fields

Field	Description
url	The API URL to the CVE exception object.
id	Unique Identifier for this CVE exception.
username	The name of the Halo user who created this CVE exception.
package_name	The name of the vulnerable package to be excepted.
package_version	The version number of the vulnerable package.
comment	A text description or comment entered when the exception was created.
created_at	Date/time at which the exception was created. Formatted in ISO 8601.
expires_at	Date/time at which the exception expires. Formatted in ISO 8601.
server_id	Unique ID of the server to which this exception applies. If this field is empty, 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).
group_id	The ID of the server group to which this exception applies. If this field is empty, 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).
cve_entries	An array of CVE reference numbers, listing all of the package's known vulnerabilities.

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

{
  "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": "2152f490be98013199b83c764e101158",
      "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",
        "CVE-2010-2519",
```

```
        "CVE-2010-2520",
        "CVE-2010-2527",
        "CVE-2010-2541"
      ]
    },
    {
      "url":
"https://api.cloudpassage.com/v1/cve_exceptions/98b79dd046320130107b404096c01709",
      "id": "98b79dd046320130107b404096c01709",
      "username": "ericaj",
      "package_name": "busybox.x86_64",
      "package_version": "1.15.1",
      "comment": "except 44",
      "created_at": "2013-01-21T19:56:40.659Z",
      "expires_at": null,
      "server_id": null,
      "group_id": "eb26b3a0add1012fc92f404096c01709",
      "cve_entries": [
        "CVE-2011-2716"
      ]
    }
  ]
}}
```

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

{
  "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",
    "comment": "",
    "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"
    ]
  }
}
```

Previous Topic Next Topic

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.

Field	Description	Default
id	A unique identifier of the firewall policy.	
name	A unique name given to the firewall policy.	
description	*Optional*. A description of the firewall policy.	
platform	*Optional*. The OS platform of the firewall policy. Either "windows" or "linux".	linux
used_by	*Read-only*. The identifiers and names of server groups that use the firewall policy.	
log_allowed	*Windows-only*. Whether to log allowed connections or not by default.	false

log_dropped	*Windows-only*. Whether to log dropped connections or not by default.	false
block_inbound	*Windows-only*. Whether to block all inbound connections by default.	true
block_outbound	*Windows-only*. Whether to block all outbound connections by default.	false

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

{
  "firewall_policies": [{
    "used_by": [{
      "name": "Group One",
      "id": "f5e1ada0a4c0012ec693404096c01709"
    }],
    "description": "",
    "name": "SSH-Only",
    "url":
"https://api.cloudpassage.com/v1/firewall_policies/7ba8ebc072b1012ec681404096c01709",
    "id": "7ba8ebc072b1012ec681404096c01709",
    "platform" : "linux"
  }, {
    "used_by": [],
    "description": "Firewall policy for the Load Balancer server group with connections
to the Internet and to the Web-Apps server group. Includes ssl on eth1.",
    "name": "Load Balancer",
    "url":
"https://api.cloudpassage.com/v1/firewall_policies/7ba8a00072b1012ec681404096c01709",
    "id": "7ba8a00072b1012ec681404096c01709",
    "platform" : "linux"
  }, {
    "used_by": [],
    "description": "Firewall policy for the Web-Apps server group with connections to
the Load Balancers server group and to the Database server group. Includes ssl on
eth1.",
    "name": "Web-Apps",
    "url":
"https://api.cloudpassage.com/v1/firewall_policies/7ba8c5d072b1012ec681404096c01709",
    "id": "7ba8c5d072b1012ec681404096c01709",
    "platform" : "linux"
  }]
}
```

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" : "b1553ab07287012e23f3442c031a719c",
    "url":
"https://api.cloudpassage.com/v1/firewall_policies/b1553ab07287012e23f3442c031a719c"
    "name" : "policy one",
    "description" : "",
    "platform" : "linux",
    "used_by" : [
      {
        "id" : "b6dd45907287012e23f3442c031a719c",
        "name" : "group one"
      }
    ],
    "firewall_rules" : [
      {
        "id" : "d09ac7d07287012e23f3442c031a719c",
        "url":
"https://api.cloudpassage.com/v1/firewall_policies/b1553ab07287012e23f3442c031a719c/firewa

        "chain" : "INPUT",
        "active" : true,
        "firewall_interface" : null,
        "firewall_source": {
          "name": "any",
          "system": true,
          "id": "649acdf06ac8012e23ce442c031a719c",
          "url":
"https://api.cloudpassage.com/v1/firewall_zones/649acdf06ac8012e23ce442c031a719c"
          "type": "FirewallZone",
          "ip_address": "0.0.0.0/0"
        },
        "firewall_service": {
          "name": "smtp",
          "port": "25",
          "protocol": "tcp",
          "system": true,
          "id": "649871106ac8012e23ce442c031a719c",
          "url":
"https://api.cloudpassage.com/v1/firewall_services/649871106ac8012e23ce442c031a719c"
        },
        "connection_states" : "NEW, ESTABLISHED",
        "action" : "ACCEPT",
        "log" : false,
        "comment": "Accept SMTP connections over port 25 only from the specified IP
addresses"
      },
      {
        "id" : "d63c5b707287012e23f3442c031a719c",
        "url":
"https://api.cloudpassage.com/v1/firewall_policies/b1553ab07287012e23f3442c031a719c/firewa

        "chain" : "INPUT",
        "active" : true,
        "firewall_interface": {
          "name": "eth0",
          "system": true,
          "id": "649ce6e06ac8012e23ce442c031a719c",
          "url":
"https://api.cloudpassage.com/v1/firewall_interaces/649ce6e06ac8012e23ce442c031a719c"
        },
        "firewall source" : null,
```

```
        "firewall_service" : null,
        "connection_states" : null,
        "action" : "REJECT",
        "log" : true,
        "comment": ""
      },
      {
        "id" : "da80ec907287012e23f3442c031a719c",
        "url":
"https://api.cloudpassage.com/v1/firewall_policies/b1553ab07287012e23f3442c031a719c/firewa

        "chain" : "OUTPUT",
        "active" : true,
        "firewall_interface" : null,
        "firewall_target" : null,
        "firewall_service" : null,
        "connection_states" : null,
        "action" : "ACCEPT",
        "log" : false,
        "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

```
{
 "firewall_policy" : {
   "name" : "policy one",
   "description" : "my new policy",
   "platform" : "linux",
   "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",
    "used_by": [],
    "description": "my new policy",
    "platform": "linux",
    "firewall_rules": [{
      "firewall_service": {
        "port": "53",
        "protocol": "TCP",
        "name": "dns AXFR",
        "system": true,
        "url":
"https://api.cloudpassage.com/v1/firewall_services/7b6409a072b1012ec681404096c01709",
        "id": "7b6409a072b1012ec681404096c01709"
      },
      "firewall_source" : {
        "id" : "c26c6a50b190012ec6b4404096c01709",
        "type" : "FirewallZone"
      },
      "log": false,
      "comment": "",
      "active": true,
      "action": "ACCEPT",
      "chain": "INPUT",
      "url":
"https://api.cloudpassage.com/v1/firewall_policies/812b7500b27b012ec6c4404096c01709/firewa

      "id": "812d3bf0b27b012ec6c4404096c01709",
      "connection_states": "NEW, ESTABLISHED"
    }, {
      "log": true,
      "comment": "Default reject-all",
      "active": true,
      "firewall_interface": {
        "name": "eth0",
```

```
        "system": true,
        "url": "https://api.cloudpassage.com/v1/firewall_interfaces?
id=7b881ca072b1012ec681404096c01709",
        "id": "7b881ca072b1012ec681404096c01709"
      },
      "action": "REJECT",
      "chain": "INPUT",
      "url":
"https://api.cloudpassage.com/v1/firewall_policies/812b7500b27b012ec6c4404096c01709/firewa

      "id": "812f26a0b27b012ec6c4404096c01709",
      "connection_states": null
    }, {
      "log": false,
      "comment": "",
      "active": true,
      "firewall_interface": {
        "name": "eth0",
        "system": true,
        "url": "https://api.cloudpassage.com/v1/firewall_interfaces?
id=7b881ca072b1012ec681404096c01709",
        "id": "7b881ca072b1012ec681404096c01709"
      },
      "action": "ACCEPT",
      "chain": "OUTPUT",
      "url":
"https://api.cloudpassage.com/v1/firewall_policies/812b7500b27b012ec6c4404096c01709/firewa

      "id": "81304d50b27b012ec6c4404096c01709",
      "connection_states": 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

```
 {
  "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 server groups, the call fails and a response status 422 is returned. Remove the policy from all server groups before attempting to delete it again.

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

Response

```
Status: 204
```

Previous Topic *Next Topic*

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 filrewall interfaces, zones, and services are described with those API endpoints.

Core firewall rule fields

Field	Description
id	A unique identifier of the firewall rule.
url	The API URL to the firewall rule object.

chain	Whether the firewall rule covers INPUT or OUTPUT connections. Allowed values are `INPUT` and `OUTPUT`.
active	Whether the firewall rule is active or not.
firewall_interface	*Linux-only*. The specified firewall interface for this rule. Specify the ID of the interface you wish to use.
firewall_source	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 "All 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*.
firewall_target	The specified source/zone for an OUTPUT rule. You must specify the ID **and** type of destination you wish to use. Allowed values for `type` are `FirewallZone` or `Group`.
firewall_service	The specified firewall service for this rule. Specify the ID of the service you wish to use.
connection_states	*Linux-only*. The specified firewall connection state(s) for this rule. `NEW`, `RELATED`, and `ESTABLISHED` are allowed.
action	The specified action to take if this rule is matched. Allowed values are `ACCEPT`, `DROP`, and `REJECT` (`REJECT` is *Linux-only*).
log	*Linux-only*. Whether matches to this rule are logged or not.
comment	An optional description of this rule.

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

{
   "firewall_rules": [
      {
         "id": "f99fc8b0c2da012f11ab40403472c9f3",
         "url":
"https://api.cloudpassage.com/v1/firewall_policies/f99222d0c2da012f11ab40403472c9f3/firewa

         "chain": "INPUT",
         "action": "ACCEPT",
         "active": true,
         "connection_states": null,
         "log": false,
         "comment": "Accept HTTP connections on port 80",
```

```
         "firewall_service": {
            "id": "5a8c53106ac7012ea3c240403472c9f3",
            "url":
"https://api.cloudpassage.com/v1/firewall_services/5a8c53106ac7012ea3c240403472c9f3",
            "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/firewa

         "chain": "INPUT",
         "action": "DROP",
         "active": true,
         "connection_states": null,
         "log": false,
         "comment": ""
      },
      {
         "id": "f9d4e740c2da012f11ab40403472c9f3",
         "url":
"https://api.cloudpassage.com/v1/firewall_policies/f99222d0c2da012f11ab40403472c9f3/firewa

         "chain": "OUTPUT",
         "action": "ACCEPT",
         "active": true,
         "connection_states": null,
         "log": false,
         "comment": ""
      }
   ]
}
```


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": {
    "log": false,
    "comment": ""
    "active": true,
    "position": 1,
```

```
    "firewall_interface": {
      "name": "eth0",
      "system": true,
      "url": "https://api.cloudpassage.com/v1/firewall_interfaces?
id=7b881ca072b1012ec681404096c01709",
      "id": "7b881ca072b1012ec681404096c01709"
    },
    "action": "ACCEPT",
    "chain": "OUTPUT",
    "url":
"https://api.cloudpassage.com/v1/firewall_policies/812b7500b27b012ec6c4404096c01709/firewa

    "id": "81304d50b27b012ec6c4404096c01709",
    "connection_states": null
  }
}
```

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.

`POST`
`https://api.cloudpassage.com/v1/firewall_policies/{firewall_policy_id}/firewall_rules`

Request Body

```
 {
  "firewall_rule" : {
    "chain" : "INPUT",
    "active" : true,
    "firewall_interface" : "7b881ca072b1012ec681404096c01709",
    "firewall_service" : "7b6409a072b1012ec681404096c01709",
    "connection_states" : "NEW, ESTABLISHED",
    "action" : "ACCEPT",
    "log" : false,
    "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/firewal


{
  "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": false,
    "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/firewa

    "id": "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 `FirewallZone`, `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, if you have a Professional or NetSec subscription to Halo, you can specify a source or target of type `UserGroup` (such as â€œAll GhostPorts usersâ€), 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" : {
    "firewall_interface" : "649cf9806ac8012e23ce442c031a719c",
```

```
  }
}
```

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

Field	Description
id	A unique identifier of the firewall interface.
name	A unique name given to the firewall interface.
system	Denotes whether the firewall interface is built-in/system or not. System interfaces cannot be deleted.

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"
  }, {
    "name": "eth0:1",
    "system": true,
    "url": "https://api.cloudpassage.com/v1/firewall_interfaces?
id=5a9a65806ac7012ea3c240403472c9f3",
    "id": "5a9a65806ac7012ea3c240403472c9f3"
  }, {
    "name": "eth0:15",
    "system": false,
    "url": "https://api.cloudpassage.com/v1/firewall_interfaces?
id=5a9b5b406ac7012ea3c240403472c9f3",
    "id": "5a9b5b406ac7012ea3c240403472c9f3"
  }]
}
```

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
```

Previous Topic *Next Topic*

Firewall Services

Use the Firewall Services endpoint to manage the descriptions of the software services, protocols, and ports (such as `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

api.cloudpassage.com/v1
└firewall_services
└*id*

Firewall service object fields

Field	Description
id	A unique identifier of the firewall service.
url	The API URL to the firewall service object.
name	A unique name given to the firewall service.
protocol	The specified protocol of the firewall service. `TCP`, `UDP`, and `ICMP` are allowed.
port	The specified port(s) of the firewall service.
system	Denotes whether the firewall service is built-in/system or not. System firewall services cannot be deleted.

List firewall services

Returns a list of all defined firewall services.

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

Response

```
 Status: 200

{
  "firewall_services": [{
    "port": "53",
    "protocol": "TCP",
    "name": "dns AXFR",
    "system": true,
    "url":
"https://api.cloudpassage.com/v1/firewall_services/5a8ce2e06ac7012ea3c240403472c9f3",
    "id": "5a8ce2e06ac7012ea3c240403472c9f3"
  }, {
    "port": "53",
    "protocol": "UDP",
    "name": "dns query",
    "system": true,
    "url":
"https://api.cloudpassage.com/v1/firewall_services/5a8cc0a06ac7012ea3c240403472c9f3",
    "id": "5a8cc0a06ac7012ea3c240403472c9f3"
  }, {
    "port": "5432",
    "protocol": "TCP",
    "name": "postgres",
    "system": false,
    "url":
"https://api.cloudpassage.com/v1/firewall_services/5a8e66606ac7012ea3c240403472c9f3",
    "id": "5a8e66606ac7012ea3c240403472c9f3"
  }]
}
```

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.cloudpassage.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.cloudpassage.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.

- 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
└firewall_zones
└*id*

Firewall zone object fields

Field	Description
id	A unique identifier of the firewall zone.
name	A unique name given to the firewall zone.
ip_address	The specified IP address(es) of the firewall zone.
system	Denotes whether the firewall zone is built-in/system or not. System zones can not be updated or deleted.
used_by	*Read-only*. The list of firewall policies that use this firewall zone.

List firewall zones

Returns a list of all defined firewall zones.

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

Response

```
 Status: 200

{
  "firewall_zones": [{
    "ip_address": "0.0.0.0/0",
    "used_by": [{
      "name": "CentOS firewall policy",
      "id": "5ab5a3106ac7012ea3c240403472c9f3"
    }, {
      "name": "Drop everything in all directions policy",
      "id": "5ab8a7e06ac7012ea3c240403472c9f3"
    }],
    "name": "any",
    "system": true,
    "url":
"https://api.cloudpassage.com/v1/firewall_zones/5a935b306ac7012ea3c240403472c9f3",
    "id": "5a935b306ac7012ea3c240403472c9f3"
  }, {
    "ip_address": "10.1.2.1, 102.19.6.14",
    "used_by": [],
    "name": "DevelopmentCo",
    "system": false,
    "url":
"https://api.cloudpassage.com/v1/firewall_zones/5a9585706ac7012ea3c240403472c9f3",
    "id": "5a9585706ac7012ea3c240403472c9f3"
  }]
}
```

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}
```

Response

```
 Status: 200

{
  "firewall_zone": {
    "ip_address": "10.1.2.1, 102.19.6.14",
    "used_by": [],
    "name": "DevelopmentCo",
    "system": false,
    "url":
"https://api.cloudpassage.com/v1/firewall_zones/5a9585706ac7012ea3c240403472c9f3",
    "id": "5a9585706ac7012ea3c240403472c9f3"
  }
}
```

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

```
 {
  "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
```

Previous Topic Next Topic

Log-Based Intrusion Detection Policies

Use the Log-Based Intrusion Detection Poilcies endpoint to create and manipulate log-based intrusion detection policies.

To assign a log-based intrusion detection policy to a server group, call the **Assign one or more log-based intrusion detection policies to a server 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
└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

Field	Description
id	The Halo ID (unique identifier) of the log-based intrusion detection policy.
url	The full URL (including policy ID) to the log-based intrusion detection policy object.
name	A name given to the log-based intrusion detection policy.
description	*Optional.* A description of the log-based intrusion detection policy.
platform	The OS platform of the log-based intrusion detection policy. Either `windows` or `linux`.

template	`true` if this policy is a policy template; otherwise `false`.
retired	`true` if this policy is retired; otherwise `false`.
used_by	A list of IDs of the server groups that use the log-based intrusion detection policy.
rules	An array of the rules that make up the policy. (Appears only in policy details.)

Log-based intrusion detection policy rule object fields

Field	Description
name	A name or description for the rule.
kind	`windows_channel` (Windows only) or `text` (Windows or Linux) .
search_pattern	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.
critical	`true` if an event logged by a match of this rule should be classified as critical; `false` if not.
active	`true` if this rule is active; `false` if it is inactive (not used by the policy).
alert	`true` if failure of this rule generates an email alert; `false` if not.
windows_event_channel	If the rule `kind` is `windows_channel`, this is the name of the event channel.
windows_event_id	If the rule `kind` is `windows_channel`, this is the ID of the target event.
file_path	If the rule `kind` is `text`, this is the full path to the log file to examine for this rule.

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

{
  "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": "0a622ea01cba01315e6f3c764e101158",
      "url":
"https://api.cloudpassage.com:/v1/lids_policies/0a622ea01cba01315e6f3c764e101158",
      "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",
        "id": "f5e1ada0a4c0012ec693404096c01709"
      }]
    },

      . . .

    {
      "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"
      }]
    }
  ]
}
```

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

{
  "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

Creates 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

```
{
  "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

{
  "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

```
{
  "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 server group.

`DELETE https://api.cloudpassage.com/v1/lids_policies/{policy_id}`

Response

```
Status: 204
```

Previous Topic Next Topic

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 server group** method of the Server Groups endpoint.

- Object Representation
- List special events policies

Object Representation

Special events policy object location

api.cloudpassage.com/v1
└special_events_policies
└*id*

Special events policy object fields

Field	Description
id	The Halo ID (a unique identifier) of the special-events policy.
name	The name of the special events policy.
description	An optional description of the policy.
global	`true` if it is the Global Events Policy; otherwise `false`.
used_by	A list of the server groups that use this special events policy. Includes the following sub-fields:
id	The Halo ID of the server group.
name	The name of the server group.

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 a profile's list of alert recipients.

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

Response

```
 Status: 200

{
  "special_events_policies": [
    {
      "id": "dff5ca00ebe60130662b3c764e101158",
      "name": "Global Events Policy",
      "description": "This is the default Special Events policy. You can edit this
policy if you wish, but it can't be deleted.",
      "global": true,
      "used_by": []
    },
    {
      "id": "dffd09e0ebe60130662b3c764e101158",
      "name": "Security Events",
      "description": "All non-audit special events",
      "global": false,
      "used_by": [
        {
          "id": "994352806c70012f21a8404096c01709",
          "name": "Webservers-East"
        },
        {
          "id": "75a751406240012f1ddf404096c01709",
          "name": "Webservers-Main"
        }
      ]
    },
    {
      "id": "e0032850ebe60130662b3c764e101158",
      "name": "Audit Events",
      "description": "",
      "global": false,
      "used_by": [
        {
          "id": "994352806c70012f21a8404096c01709",
          "name": "DMZ"
        }
      ]
    }
  ]
}
```

Previous Topic Next Topic

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

Field	Description
id	Identifier for this event.
type	The name of the event type, as used by the CloudPassage API. See Supported Event Types, below.
name	The name of the event, as displayed in the Halo Portal.
critical	Criticality of the event.
created_at	Event creation timestamp. Formatted in ISO 8601.
message	Event's message.
policy_name	Name of the policy that triggered the event.
server_hostname	Server's hostname.
server_ip_address	Server's connecting ip address.
server_id	Server's unique ID.
server_platform	Server's platform.
server_group_name	Server's group name.
server_new_ip_address	Server's new IP address when address changes.

server_old_ip_address	Server's old IP address when address changes.
server_interface	Name of the server's interface.
actor_key_id	The ID of the API key used.
actor_key_label	The label of the API key used.
actor_username	Username of the user who requested the change.
actor_ip_address	IP address of the user who requested the change.
actor_country	Location of the user who requested the change.
target_username	Username of the user that is being modified.
daemon_version	Current version of the daemon.
previous_daemon_version	Previous version of the daemon.
rule_name	Configuration policy rule that failed.
rule_reference_identifier	An optional comma-separated list of IDs applied to this policy rule for compliance purposes.
server_account_username	Local server account username.
server_account_id	Local server account id.
object_name	Name of the FIM object. For a file it is a file path.
api_key_id	API Key's ID.
api_key_label	API Key's name.

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*-*DD***T***hh*:*mm***Z** for Zulu time zone). For example:

  `GET https://api.cloudpassage.com/v1/events?since=2013-06-22&until=2013-08-21`

- 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 server 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,sca_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`

- 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.

```
https://api.cloudpassage.com/v1/events?page={pagenum}&per_page={pagesize}
```

You can combine any of the above parameters in your **List events** calls.

Response

```
Status: 200

{
  "events": [{
    "id": "831753ae-0ed9-11e3-9d7f-7ac7009536f5",
    "type": "fim_signature_changed",
    "name": "File Integrity object signature changed",
    "message": "A change in file /etc/test was detected on Linux server qa-test3
(50.57.229.144)",
    "created_at": "2012-10-22T05:28:19.148087Z",
    "critical": true,
    "server_id": "1cc0d4fc9cacasdswwd9232869bdcde",
    "server_platform": "Linux",
    "server_hostname": "qa-test3",
    "server_group_name": "QA hosts",
    "server_ip_address": "50.57.229.144",
    "server_reported_fqdn": null,
    "policy_name": "fim-policy1",
    "object_name": "/etc/test"
    "rule_reference_identifiers": null
  }, {

   ...

  }, {
     "id": "3c00f3d2-2acf-11e3-8e4d-eeed97132a7c",
     "type": "sca_rule_failed",
     "name": "Configuration rule matched",
     "message": "Server configuration rule iptables should always run matched on Linux
server adriatica (162.209.79.104). (source: Scan)",
     "server_id": "0d0dcaf00cfd0131932f3c764e10b50e",
     "created_at": "2013-10-01T19:25:30.453909Z",
     "critical": true,
     "server_platform": "Linux",
     "server_hostname": "adriatica",
     "server_group_name": "Unassigned",
     "server_ip_address": "162.209.79.104",
     "server_reported_fqdn": "adriatica",
     "rule_name": "iptables should always run",
     "rule_reference_identifiers": null
  }, {

   ...

  }],
  "count": 167,
  "pagination": {
    "prev": "https://api.cloudpassage.com/v1/events?page=1&per_page=30&since=2012-10-
22&until=2012-10-23",
    "next": "https://api.cloudpassage.com/v1/events?page=3&per_page=30&since=2012-10-
22&until=2012-10-23"
  }
}
```

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 below (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.

API value	Portal value	Notes
`activation_link_failed`	Halo user activation failed	(Used activation link clicked)
`api_client_created`	Api key created	
`api_client_deleted`	Api key deleted	
`api_client_secret_viewed`	Api secret key viewed	
`api_client_updated`	Api key modified	
`api_login_success`	Halo API authentication success	(Client receives access token)
`authorized_ips_modified`	Authorized ips modified	(Authorized IP addresses)
`cve_exception_created`	Software vulnerability exception created	
`cve_exception_expired`	Software vulnerability exception expired	
`cve_exception_deleted`	Software vulnerability exception deleted	
`daemon_compromised`	Daemon compromised	
`daemon_version_change`	Daemon version changed	
`fim_baseline_created`	File integrity baseline	
`fim_baseline_deleted`	File integrity baseline deleted	
`fim_baseline_expired`	File integrity baseline expired	
`fim_baseline_failed`	File integrity baseline failed	(Baseline scan failed)
`fim_baseline_invalid`	File integrity baseline invalid	(policy changed/too many objects)
`fim_change_detected`	File integrity change detected	(if multiple changes per event)
`fim_exception_created`	File integrity exception created	
`fim_exception_deleted`	File integrity exception deleted	
`fim_exception_expired`	File integrity exception expired	
`fim_object_added`	File integrity object added	(Object not in baseline found)
`fim_object_missing`	File integrity object missing	(Object in baseline not found)
`fim_policy_assigned`	File integrity policy assigned	(Assigned to a server group)
`fim_policy_created`	File integrity policy created	
`fim_policy_deleted`	File integrity policy deleted	
`fim_policy_exported`	File integrity policy exported	
`fim_policy_imported`	File integrity policy	
`fim_policy_modified`	File integrity policy modified	
`fim_policy_unassigned`	File integrity policy unassigned	(Removed from server group)
`fim_re_baseline`	File integrity re-baseline	(New baseline scan was run)
`fim_scan_disabled`	Automatic file integ. scanning disabled	
`fim_scan_enabled`	Automatic file integ. scanning enabled	
`fim_scan_failed`	File integrity scan failed	(Scan did not complete)
`fim_scan_modified`	Auto. file integ. scan schedule modified	
`fim_scan_requested`	File integrity scan requested	
`fim_signature_changed`	File integrity object signature changed	(Content or metadata changed)
`firewall_policy_assigned`	Halo firewall policy assigned	(Assigned to a server group)
`firewall_policy_created`	Halo firewall policy created	
`firewall_policy_deleted`	Halo firewall policy deleted	

firewall_policy_modified	Halo firewall policy modified	
firewall_policy_unassigned	Halo firewall policy unassigned	(Removed from a server group)
firewall_restore_requested	Server firewall restore requested	
firewall_service_added	Network service added	
firewall_service_deleted	Network service deleted	
firewall_service_modified	Network service modified	
ghostport_close	Ghostports session close	
ghostport_failure	Ghostports login failure	
ghostport_provisioning	Ghostports provisioning	(GhostPorts user created/enabled)
ghostport_success	Ghostports login success	
halo_login_failure	Halo login failure	
halo_login_success	Halo login success	
halo_user_logout	Halo logout	
halo_user_deactivated	Halo user deactivated	
halo_user_invited	Halo user invited	
halo_user_locked	Halo user account locked	
halo_user_modified	Halo user modified	
halo_user_reactivated	Halo user reactivated	
halo_user_reinvited	Halo user reinvited	
halo_user_unlocked	Halo user account unlocked	
ip_address_changed	Server IP address changed	
lids_rule_failed	Log-based intrusion detection rule matched	
lids_scan_disabled	Log-based intrusion detection disabled	
lids_scan_enabled	Log-based intrusion detection enabled	
lids_policy_assigned	Log-based intrusion detection policy assigned	
lids_policy_created	Log-based intrusion detection policy created	
lids_policy_deleted	Log-based intrusion detection policy deleted	
lids_policy_exported	Log-based intrusion detection policy exported	
lids_policy_modified	Log-based intrusion detection policy modified	
lids_policy_unassigned	Log-based intrusion detection policy unassigned	
local_account_activate_request	Local account activation requested	
local_account_create_request	Local account creation requested	
local_account_delete_request	Local account deactivation requested	
local_account_update_request	Local account modification requested	
local_account_update_ssh_keys_request	Local account ssh keys update requested	
master_account_linked	Master account linked	(Halo acct. linked to master acct.)
multiple_root_accounts	Multiple root accounts detected (linux)	
new_server	New server	
password_changed	Halo password changed	
password_config_changed	Halo authentication settings modified	
password_recovery_requested	Halo password recovery requested	
password_recovery_request_failed	Halo password recovery request failed	
password_recovery_success	Halo password recovery success	
sca_policy_assigned	Configuration policy assigned	(Assigned to a server group)
sca_policy_created	Configuration polcy created	
sca_policy_deleted	Configuration policy deleted	
sca_policy_exported	Configuration policy exported	
sca_policy_imported	Configuration policy imported	

sca_policy_modified	Configuration policy modified	
sca_policy_unassigned	Configuration policy unassigned	(Removed from a server group)
sca_rule_failed	Configuration rule matched	(One or more rule checks failed)
server_account_created	Local account created (linux only)	
server_account_deleted	Local account deleted (linux only)	
server_deleted	Server deleted	
server_firewall_modified_locally	Server firewall modified	(Modified outside of Halo)
server_missing	Server missing	(No Daemon contact with Grid)
server_moved	Server moved to another group	(Moved to another server group)
server_restarted	Server restarted	
server_retired	Server retired	
server_shutdown	Server shutdown	
server_unretired	Server un-retired	
session_timeout	Halo session timeout	
sms_phone_number_verified	Sms phone number verified	(For two-factor authentication)
vulnerable_software_package_found	Vulnerable software package found	(Software vulnerability scan result)

Previous Topic *Next Topic*

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 server 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

Field	Description
id	The Halo ID (a unique identifier) of the alert profile.
name	The name of the alert profile.
description	Optional description of the alert profile.
frequency	How frequently alert notifications are sent out. Ranges from `instant` to `every_week`.
used_by	A list of the server groups that use this alert profile. Includes the following sub-fields:
id	The Halo ID of the server group.
name	The name of the server group.

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.

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

Response

```
 Status: 200

{
  "alert_profiles": [
    {
      "id": "dfdc1480ebe60130662b3c764e101158",
      "name": "alerts-execs",
      "description": "",
      "frequency": "every_week",
      "used_by": [
        {
          "id": "994352806c70012f21a8404096c01709",
          "name": "Webservers East"
        }
      ]
    },
    {
      "id": "dfdbf2f0ebe60130662b3c764e101158",
      "name": "alerts-secops",
      "description": "",
      "frequency": "instant",
      "used_by": [
        {
          "id": "994352806c70012f21a8404096c01709",
          "name": "Webservers East"
        }
      ]
    },
    {
      "id": "dfeb4d60ebe60130662b3c764e101158",
      "name": "alerts-standard",
      "description": "",
      "frequency": "every_24_hours",
      "used_by": []
    }
  ]
}
```

Previous Topic Next Topic

Saved Searches

Use the Saved Searches endpoint to create and manage the saved search URLs that underlie the Halo reporting service. 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

Field	Description
id	A unique identifier for the search.
name	The name of the search.
endpoint	The API endpoint that the search accesses.
criteria	*(Optional)* An array of one or more search criteria (filters) that, along with the `endpoint` value, compose the search URL.
url	*(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.

search_url	*(In response JSON only)* A URL to use in a GET request to the Halo API to execute this search.

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"
      },
      "search_url": "https://api.cloudpassage.com/v1/servers?
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": "1f8503e07dc6012f112040403472c9f3"
      },
      "search_url": "https://api.cloudpassage.com/v1/events?
type=daemon_compromised,daemon_version_change&server_platform=windows&group_id=1f8503e07dc

      "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",
    "criteria": {
      "state": "missing,deactivated",
      "platform": "linux"
    },
    "search_url": "https://api.cloudpassage.com/v1/servers?
state=missing,deactivated&platform=linux",
    "url": "https://api.cloudpassage.com/v1/searches/118a18a0d7b301319c1e3c764e101158"
  }
}
```

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=1f8503e07dc6012f

    "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

```
{
  "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`

`https://api.cloudpassage.com/v1/servers.pdf?state=missing,deactivated&platform=linux`

Alternatively, you can append a `format` parameter to the search URL, like this:

`https://api.cloudpassage.com/v1/servers?state=missing,deactivated&platform=linux&format=csv`

`https://api.cloudpassage.com/v1/servers?state=missing,deactivated&platform=linux&format=pdf`

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_announcements
└*announcement*

System announcement object fields

Field	Description
announcement	The content of the announcement. May contain HTML source as well as text.
message_begin_at	The date/time (in ISO 8601 format) when the announcement was posted or will be posted.
message_expire_at	The date/time (in ISO 8601 format) when the announcement expired and was removed, or will expire.
announcement_type	The type of announcement. Can be `planned_outage` or `information`.
status	The current status of the announcement. Can be `active` or `expired`.
outage_time_start	For announcements involving an outage, the date/time (in ISO form) at which the outage occurred or will occur.
outage_time_end	For announcements involving an outage, the date/time (in ISO form) at which the outage ended.

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
```

Response


```
Status: 200
{
  "announcements": [
    {
      "announcement": "INFRASTRUCTURE UPGRADE NOTICE: We will be performing an
infrastructure upgrade on Wednesday, November 12, 2014 between the hours of 6:00 PM
until 8:00 PM U.S. Pacific Time. Expected Impact: This change will NOT impact most
customers; however, there may be some customers affected due to the IP address changes
in our DNS records.  More detailed information is here: <a
href=\"https://support.cloudpassage.com/entries/58793830\" target=\"_blank\">
https://support.cloudpassage.com/entries/58793830</a>;.  All of your Halo-protected
servers will continue to be secured. If you have questions, please submit a support
ticket. - CloudPassage Operations Team",
      "message_begin_at": "2014-11-07T00:00:00Z",
      "message_expire_at": "2014-11-13T01:00:00Z",
      "announcement_type": "information",
      "status": "expired",
      "outage_time_start": "2014-11-13T02:00:00Z",
      "outage_time_end": "2014-11-13T04:00:00Z"
    },
    {
      "announcement": "There's a new release of Halo! This release includes general
availability of Windows Configuration Security Monitoring, and improvements to both the
Halo API and to Halo File Integrity Monitoring. For more information, please see the
release notes: 29 July 2013 Release.",
      "message_begin_at": "2013-07-31T00:00:00Z",
      "message_expire_at": "2013-08-01T16:47:21Z",
      "announcement_type": "information",
      "status": "expired",
      "outage_time_start": null,
      "outage_time_end": null
    },
    {
      "announcement": "We’re happy to bring you another release of Halo this month,
which includes our beta release of <b>Windows Configuration Security Monitoring (Windows
CSM)<\/b>. Full release notes here: <a
href=\"https://support.cloudpassage.com/entries/23873408-Halo-May-2013-Release-Notes
\">https://support.cloudpassage.com/entries/23873408-Halo-May-2013-Release-Notes
<\/a>",
      "message_begin_at": "2013-07-16T00:00:00Z",
      "message_expire_at": "2013-07-18T23:59:00Z",
      "announcement_type": "information",
      "status": "expired",
      "outage_time_start": null,
      "outage_time_end": null
    },
     {
      "announcement": “Check out these release notes!<a
href=\"https://support.cloudpassage.com/entries/23443303-Halo-Late-March-2013-Release-
Notes\">Halo Releaase Notes - Late March 2013<\/a>",
      "message_begin_at": "2013-04-04T00:00:00Z",
      "message_expire_at": "2013-04-05T23:59:00Z",
      "announcement_type": "information",
      "status": "expired",
      "outage_time_start": null,
      "outage_time_end": null
```

```
    },

    . . .

    {
      "announcement": "This system is now running Release 7",
      "message_begin_at": "2012-07-11T00:00:00Z",
      "message_expire_at": "2012-07-12T17:52:34Z",
      "announcement_type": "information",
      "status": "expired",
      "outage_time_start": null,
      "outage_time_end": null
    }
  ],
  "count": 29
}
```

Previous Topic