Alert Logic API documentation

User v1

Contents

Alert Logic User API overview

This document communicates the requirements and unique usage for the API. The primary objective of this document is to provide information about:

- The API and resource endpoint descriptions
- Use case scenarios
- HTTP method and URL endpoints for resource(s)

Document organization

This document is divided into the following major sections:

- About the Alert Logic User API
- Use case scenarios
- POST /api/user/v1
- GET /api/user/v1
- GET /api/user/v1/[userId]
- DELETE /api/user/v1/[userId]

About the Alert Logic User API

The Alert Logic User API provides a simple platform to create and delete users in the Alert Logic user interface. The API also allows for retrieval of user information, either on a broad scale for all users or by narrowing down to a single user.

The API is resource-based web service. The resource in the API is comprised of URL fragments that identify a set of objects. An API endpoint is comprised of the HTTP method and URL associated with a resource. The API endpoints produce JSON Schema formatted responses.

The User API has one resource, user, with multiple endpoints. Details about the resource and the associated endpoints are as follows:

Resource	Method	URL	Description
User	POST	/api/user/v1	creates a new user
User	GET	/api/user/v1	retrieves a list of existing users
User	GET	/api/user/v1/[userId]	retrieves a specified user object
User	DELETE	/api/user/v1/[userId]	deletes an existing user object

Use case scenarios

User provisioning

Access to the Alert Logic user interface requires credentials for authentication. When you create multiple users, utilize the User API to securely acquire those credentials.

To POST a new user to the user interface, make a request call to the API. To GET a list of existing users, make a query to the API. Input a specific user ID to GET the information returned for that user.

User termination

To maintain optimal security of the data accessible via the user interface, delete a user when the user is no longer authorized to access the user interface.

To DELETE an existing user, make a request call to the API. Input the required existing user account ID for the user that you want deleted. If the user was deleted successfully, a status code of 200 OK is returned.

POST /api/user/v1

This endpoint allows you to POST a new user to the Alert Logic user interface.

POST parameters

POST parameters describe the resource being created. The POST parameters for this endpoint are as follows:

Parameter	Required	Default Value	Possible Value	Description
customer_id	true		positive integer ID	The customer_id parameter identifies an integer identifier of the customer.
first_name	true		string	The first_name parameter identifies the first name of the user.
last_name	true		string	The last_name parameter identifies the last name of the user.
email	true		e-mail address	The email parameter identifies the e-mail address of the user.
password	true		series of letters, numbers, and possible special characters	The password parameter identifies the password set for the user's account.

The email address you set when creating the user account will also be set as the username for the user account.

Response fields

Data that is returned from an API call is comprised of response fields. In this endpoint, the same data that is described in the POST parameters is also returned in the response fields. The response fields specific to this endpoint are as follows:

Field	Possible Values	Description
user_id	positive integer ID	The user_id field is a unique integer identifier of a user.

Request examples

POST	/api/user/v1

| cURL | `curl -kv -H "Accept: application/json" --cert alertlogic-api-2-14788.pem -X POST -d @new-user.json "https://api.alertlogic.net/api/user/v1"` |

> If you choose to copy/paste the examples instead of typing them, make sure to paste the examples into a plain text editor first. Copy/pasting directly from the PDF may introduce syntax errors.

Example code

```
Create a user.
  # Request
  POST /api/user/v1 HTTP/1.1
  Accept: application/json
  Content-Type: application/json

  {
   "customer_id": 2,
   "first_name": "Tony",
   "last_name": "Stark",
   "email": "tstark@marvel.net",
   "password": "Ironm@nR0cks"
  }

  # Response
  HTTP/1.1 201 Created
  Content-Type: application/json
  Location: http://localhost:8080/api/user/v1/3
  Content-Location: http://localhost:8080/api/user/v1/3

  {
   "user_id" : 3,
   "customer_id": 2,
   "first_name": "Tony",
   "last_name": "Stark",
   "email": "tstark@marvel.net"
  }
```

GET /api/user/v1

This endpoint allows you to GET a list of user objects for a customer. If you set a customer ID, it must be a child customer of your account. The response fields for this endpoint are generated together in a single object. Multiple objects are returned based on the number of existing users in the system at the time of the call to the API.

Query parameters

Query parameters act as search filters and change to modify the behavior of the search. The query parameter for this endpoint is as follows:

Parameter	Required	Default Value	Possible Value	Description
customer_id	false	the customer ID of the API caller	positive integer ID	The customer_id parameter identifies the integer customer identifier.

Response fields

Data returned from an API call is comprised of response fields. The response fields specific to this endpoint are as follows:

Field	Possible Values	Description
user_id	positive integer ID	The user_id field is an integer identifier of the user.
customer_id	positive integer ID	The customer_id field is an integer identifier of the customer.
first_name	string	The first_name field identifies the first name of the user.
last_name	string	The last_name field identifies the last name of the user.
email	e-mail address	The email field identifies the e-mail address of the user.

Request examples

GET	/api/user/v1

cURL	curl -kv -H "Accept: application/json" --cert alertlogic-api-2-14788.pem "https://api.alertlogic.net/api/user/v1"

> If you choose to copy/paste the examples instead of typing them, make sure to paste the examples into a plain text editor first. Copy/pasting directly from the PDF may introduce syntax errors.

Example code

```
# Request
GET /api/user/v1 HTTP/1.1
Accept: application/json

# Response
HTTP/1.1 200 OK
Content-Type: application/json

[
 {
  "user_id" : 3,
  "customer_id": 2,
  "first_name": "Tony",
  "last_name": "Stark",
  "email": "tstark@marvel.net"
 },
 {
  "user_id" : 4,
  "customer_id": 2,
  "first_name": "Pepper",
  "last_name": "Potts",
  "email": "ppotts@marvel.net"
 }
]
```

GET /api/user/v1/[userId]

This endpoint allows you to GET information for a specified user object by querying with their user ID.

URL variables

Use the following variable(s) to specify the object(s) to GET in the API call.

Variable	Required	Default value	Possible value	Description
userId	true		positive integer ID	The userId variable is a unique integer identifier of a user.

Response fields

Data returned from an API call is comprised of response fields. The response fields specific to this endpoint are as follows:

Field	Possible Values	Description
user_id	positive integer ID	The user_id field is an integer identifier of the user.
customer_id	positive integer ID	The customer_id field is an integer identifier of the customer.
first_name	string	The first_name field identifies the first name of the user.
last_name	string	The last_name field identifies the last name of the user.
email	e-mail address	The email field identifies the e-mail address of the user.

Request examples

GET	/api/user/v1/[userId]

cURL	curl -kv -H "Accept: application/json" --cert alertlogic-api-2-14788.pem "https://api.alertlogic.net/api/user/v1/2"

> 💡 If you choose to copy/paste the examples instead of typing them, make sure to paste the examples into a plain text editor first. Copy/pasting directly from the PDF may introduce syntax errors.

Example code

Retrieve an existing user.

```
# Request
GET /api/user/v1/2 HTTP/1.1
Accept: application/json

# Response
HTTP/1.1 200 OK
Content-Type: application/json

{
 "user_id" : 3,
 "customer_id": 2,
 "first_name": "Tony",
 "last_name": "Stark",
 "email": "tstark@marvel.net"
}
```

DELETE /api/user/v1/[userId]

This endpoint allows you to DELETE an existing user object.

URL variables

Use the following the variable(s) to specify the object(s) to DELETE in the API call.

Variable	Required	Default value	Possible value	Description
userId	true		positive integer ID	The userId variable is a unique integer identifier of a user.

Request examples

DELETE	/api/user/v1/10464

cURL	curl -kv -H "Accept: application/json" --cert alertlogic-api-2-14788.pem "https://api.alertlogic.net/api/user/v1/10464"

> If you choose to copy/paste the examples instead of typing them, make sure to paste the examples into a plain text editor first. Copy/pasting directly from the PDF may introduce syntax errors.

Example code

Delete an existing user

```
# Request
DELETE /api/user/v1/10464 HTTP/1.1
Accept: application/json

# Response
HTTP/1.1 200 OK
Content-Type: application/json

""
```

Available Alert Logic APIs

Alert Logic APIs, developed as partner-facing web services in an organized, REST-ful environment, provide user-friendly operations. Alert Logic APIs are designed with intuitive, resource-based URLs, allowing for optimal integration with Alert Logic systems.

API	Description
Customer v1	provides an interface to read and create customer accounts
Incident v3	provides an interface to retrieve incident information
Monitoring v1	provides an interface to retrieve appliances and agents status
Ordering v2	provides an interface to submit and track progress of orders
User v1	provides an interface to manage user accounts

ABOUT ALERT LOGIC

Alert Logic, the leader in security and compliance solutions for the cloud, provides Security-as-a-Service for on-premises, cloud, and hybrid infrastructures, delivering deep security insight and continuous protection for customers at a lower cost than traditional security solutions. Fully managed by a team of experts, the Alert Logic Security-as-a-Service solution provides network, system and web application protection immediately, wherever your IT infrastructure resides. Alert Logic partners with the leading cloud platforms and hosting providers to protect over 2,700 organizations worldwide. Built for cloud scale, our patented platform stores petabytes of data, analyzes over 400 million events and identifies over 50,000 security incidents each month, which are managed by our 24x7 Security Operations Center. Alert Logic, founded in 2002, is headquartered in Houston, Texas, with offices in Seattle and London. For more information, please visit www.alertlogic.com.