



Cisco Network Assurance Engine REST API User Guide

Table of Contents

| | |
|--|----|
| The Cisco Network Assurance Engine REST API | 3 |
| Overview | 4 |
| Authentication and Web Security | 5 |
| User Accounts and Roles | 5 |
| Logging in to the Cisco NAE | 5 |
| API login example | 6 |
| Additional web security measures | 12 |
| Concurrent Session protection | 12 |
| Session Fixation protection | 12 |
| XSS protection | 12 |
| Query and Response | 13 |
| Standardized Query Responses | 13 |
| Common Response Structure | 13 |
| Query Response Pagination | 14 |
| Pagination Links | 14 |
| Request Query Parameters | 15 |
| Query Parameter Examples | 15 |
| Common Response Structure Example | 15 |
| About The Cisco NAE REST API Reference (Swagger) | 18 |
| Common API Examples | 19 |
| Assurance Group Management Operations | 19 |
| Create ACI Fabric | 19 |
| Get ACI Fabric | 23 |
| Get All ACI Fabrics | 26 |
| Edit ACI Fabric | 27 |
| Start Online Analysis | 30 |
| Stop Analysis | 31 |
| Delete ACI Fabric | 32 |
| Epoch Operations | 34 |
| Get An Epoch | 34 |
| Get Epochs of an ACI Fabric | 38 |
| Get Epochs by Collection Timestamp | 40 |
| Get Latest Epoch | 42 |
| Smart Events Operations | 45 |
| Get Smart Event Summary | 45 |
| Get Smart Event Detail | 50 |
| User Management Operations | 54 |
| Create a User | 55 |

| | |
|----------------------------------|----|
| Change User Password | 57 |
| Get User | 60 |
| Get All Users | 63 |
| Edit User | 68 |
| Delete User | 71 |
| Update password expiration time | 72 |
| Forgot Password | 75 |
| Reset Password | 76 |
| Session Management Operations | 78 |
| View All Sessions | 78 |
| View a Single Session | 81 |
| Delete a Session | 83 |
| Common Workflows | 85 |
| Smart Events Workflow | 85 |
| Pagination Workflow | 86 |
| Password Reset Workflow | 87 |
| Status and Error Codes | 89 |
| HTTP Status Codes | 89 |
| Cisco NAE Status and Error Codes | 90 |
| System Codes | 91 |
| Authentication Codes | 92 |
| User Management Codes | 92 |
| Epoch Codes | 93 |
| Session Codes | 93 |
| Related Documentation | 94 |
| Documentation Feedback | 94 |

First Published: 2019-07-19

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

<http://www.cisco.com>

Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017-2019 Cisco Systems, Inc. All rights reserved.

The Cisco Network Assurance Engine REST API



This document describes the features, operation, and syntax of the Cisco Network Assurance Engine (NAE) REST API as of the current release when written. The features, operation, and syntax of the API are subject to change in future releases, and Cisco cannot guarantee backwards compatibility with prior releases.

Overview

The Cisco Network Assurance Engine (NAE) REST API provides an alternative operation method to the Cisco NAE GUI. The REST API gives programmatic access to all assurance models in addition to providing fully automatable management of the Cisco NAE.

The REST API is a set of programming interfaces that uses Representational State Transfer (REST) architecture. The API contains resources represented by Uniform Resource Identifiers (URIs), which allow you to unambiguously identify each resource. Each URI contains a protocol used to exchange the messages and the resource location string. A URI can refer to a single object or a collection of objects.

A REST API operation is executed by sending an HTTP GET, POST, PUT, or DELETE request in the format of `/api/v1/{resource}` to a URI within the Cisco NAE. The HTTP request typically includes a payload message in JavaScript Object Notation (JSON) format, and the HTTP response typically includes a JSON format message body. In some cases, the HTTP request may also contain URL parameters.

- A GET request may submit URL parameters and returns a JSON data structure containing the requested data or status. The GET method is nullipotent, meaning that it can be called zero or more times without making any changes; in other words, it is a read-only operation.
- A POST request typically creates a new object, such as a user or fabric. It should be sent only once for each object created. A POST request submits a JSON data structure to the specified resource and returns a JSON data structure containing confirmation or failure information.
- A PUT request is used to modify an attribute of an existing object. A PUT request submits a JSON data structure to the specified resource and returns a JSON data structure containing confirmation or failure information. It is not necessary for the payload structure of a PUT request to contain the attributes that are not being modified. The PUT method is idempotent, meaning that there is no additional effect when a request is sent more than once with the same input parameters.
- A DELETE request may submit URL parameters and returns a JSON data structure containing confirmation or failure information. The DELETE method is idempotent, meaning that there is no additional effect when a request is sent more than once with the same input parameters.

You can use common developer tools such as cURL, Postman, or a programming language to compose and send the HTTP request and the JSON payload.

For information about the complete reference documentation for all available REST API commands, see [About The Cisco NAE REST API Reference \(Swagger\)](#).

Authentication and Web Security

The Cisco NAE REST API server protects API sessions against common web threats as described in the following sections.

User Accounts and Roles

Most functions of the Cisco NAE REST API require that the user be authenticated and logged in with an active session. The REST API supports both local authentication and LDAP authentication.

Two roles are supported for user accounts:

- **User:** Normal user accounts can be created locally or on a remote authentication server. Some APIs cannot be executed by a normal user.
- **Super Administrator:** The local account named **admin** is considered a super administrator, with higher privileges than a normal user. When logged in as **admin**, you can execute several APIs that are not allowed for normal users. The **admin** account is permanent and cannot be deleted.

Logging in to the Cisco NAE

To prevent a Cross Site Request Forgery (CSRF) attack and other common web threats, the REST API server implements a multi-step login sequence in order to issue a unique session token.



For more information about CSRF, visit [https://www.owasp.org/index.php/Cross-Site_Request_Forgery_\(CSRF\)](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF))

The following steps describe the login sequence:

1. The client sends an HTTP GET request to `/api/v1/whoami`.
2. The server returns an HTTP response that includes an `X-NAE-LOGIN_OTP` header containing a one-time password (OTP) with a five-minute expiration.
3. The client sends an HTTP POST request to `/api/v1/login` with local or LDAP authentication credentials and with an HTTP request header field of `X-NAE-LOGIN_OTP` containing the OTP value.
4. If the credentials are valid, the server returns an HTTP response that includes an `X-NAE-CSRF-TOKEN` header containing a session password.
5. For all subsequent POST/PUT/DELETE messages for the duration of the session, the client must include the `X-NAE-CSRF-TOKEN` header in the HTTP request.

The following table summarizes the use of the request and response headers:

| Request URI | Request Header Name | Response Header Name | Notes |
|----------------|---------------------|----------------------|---|
| /api/v1/whoami | None | X-NAE-LOGIN-OTP | The OTP is returned in the header only if the user is not already authenticated. |
| /api/v1/login | X-NAE-LOGIN-OTP | X-NAE-CSRF-TOKEN | The OTP header is sent with the login request. The response header must be included in all subsequent API requests for the duration of the session. |
| /api/v1/* | X-NAE-CSRF-TOKEN | N/A | The request header is required for all API(GET/POST/PUT/DELETE) operations. |

API login example

The following example session shows the login sequence:

Whoami request sent by unauthenticated client

Request

```
GET /api/v1/whoami HTTP/1.1
Content-Type: application/json
Accept: application/json
Host: localhost:8080
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
X-NAE-LOGIN-OTP: 8981df87-d763-4f89-b9de-65895d002836
Set-Cookie: SESSION=c52a8f7a-7a48-433b-9556-816f1eb154e1; Path=/; HttpOnly
Content-Length: 684
```

```
{
  "success" : true,
  "messages" : [ {
    "code" : 7005,
    "severity" : "INFO",
    "message" : "User is not authenticated. Use One Time Password found in the
response header X-NAE-LOGIN-OTP within the next 5 minutes to login"
  } ],
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "authenticated" : false
    },
    "data_summary" : {
      "links" : [ {
        "rel" : "self",
        "href" : "http://localhost:8080/api/v1/whoami"
      }, {
        "rel" : "login",
        "href" : "https://localhost:8080/api/v1/api/v1/login"
      } ],
      "total_count" : 1,
      "has_more_data" : false
    }
  }
}
```

Response headers

| Name | Description |
|-----------------|---|
| X-NAE-LOGIN-OTP | A one-time password to be sent in the HTML header of the /whoami API. The password expires five minutes after it is issued. |

Login request sent by unauthenticated client

Request headers

| Name | Description |
|-----------------|--|
| X-NAE-LOGIN-OTP | One-time password that was sent in the HTML header of the /whoami API must be provided here. |

Request

```
POST /api/v1/login HTTP/1.1
Content-Type: application/json
Accept: application/json
Accept: application/json
X-NAE-LOGIN-OTP: 879e4f8f-78dd-4bdf-adca-c4f7575bf4c4
Host: localhost:8080
Content-Length: 122
Cookie: SESSION=659a7415-f3af-4f18-b5ae-f15463cb05ea

{
  "username" : "NbUserRepositoryTestVXvBcncodo",
  "password" : "NbUserRepositoryTestVXvBcncodo",
  "domain" : "Local"
}
```

Response

```
HTTP/1.1 200 OK
X-NAE-CSRF-TOKEN: ed63752e-eb98-4854-bc1e-2675c3b58107
Content-Type: application/json;charset=UTF-8
Set-Cookie: SESSION=374f073a-4c57-4f66-be7c-c3b97a5a47bf; Path=/; HttpOnly
Content-Length: 535
```

```
{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "username" : "NbUserRepositoryTestVXvBcncodo",
      "uuid" : "59f9b79a-d11f-4e24-97ea-e6710a09a627",
      "domain" : "Local",
      "password_status" : "ACTIVE",
      "remaining_days" : 0
    },
    "data_summary" : {
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost:8080/api/v1/login"
      } ],
      "total_count" : 1,
      "has_more_data" : false
    }
  }
}
```

Response headers

| Name | Description |
|------------------|--|
| X-NAE-CSRF-TOKEN | A random token that is valid for the entire session and must be submitted in the X-NAE-CSRF-TOKEN request header of every GET/POST/PUT/DELETE request. |

Logout request sent by authenticated client

Request headers

| Name | Description |
|------------------|--|
| X-NAE-CSRF-TOKEN | The token that is generated as part of login request must be submitted here. |

Request

```
POST /api/v1/logout HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: 2d3ab2a0-3ee5-4605-a61f-f689ac8c226b
Cookie: SESSION=0a59c1e6-de2d-4237-9ff0-68c0953f5925
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 318

{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data_summary" : {
      "links" : [ {
        "rel" : "whoami",
        "href" : "http://localhost:8080/api/v1/whoami"
      } ],
      "total_count" : 0,
      "has_more_data" : false
    }
  }
}
```

Whoami request sent by authenticated client (optional)

Request

```
GET /api/v1/whoami HTTP/1.1
Content-Type: application/json
Accept: application/json
Host: localhost:8080
Cookie: SESSION=edc3558b-504d-4d77-91cd-3e8196539205
```

Response

HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 675

```
{
  "success" : true,
  "messages" : [ {
    "code" : 7003,
    "severity" : "INFO",
    "message" : "The user is already authenticated to this session"
  } ],
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "authenticated" : true,
      "password_status" : "ACTIVE",
      "domain" : "Local",
      "uuid" : "610b23cd-9aa9-4e48-90ae-c75d090507e8",
      "username" : "NbUserRepositoryTestIStFtrATXC"
    },
    "data_summary" : {
      "links" : [ {
        "rel" : "self",
        "href" : "http://localhost:8080/api/v1/whoami"
      } ],
      "total_count" : 1,
      "has_more_data" : false
    }
  }
}
```

Response headers

| Path | Type | Description |
|----------------------------------|--------|--|
| <code>messages</code> | Array | Descriptive messages provided for this request |
| <code>messages[].code</code> | Number | An error code indicating that the user is already authenticated |
| <code>messages[].severity</code> | String | The severity level of this message, which is informational |
| <code>messages[].message</code> | String | An informational message indicating that the user is already authenticated |

| Path | Type | Description |
|--|---------|--|
| <code>value.data.domain</code> | String | User authentication domain name |
| <code>value.data.authenticated</code> | Boolean | If true, the user is already authenticated |
| <code>value.data.username</code> | String | The user name of the user who is currently logged in |
| <code>value.data.password_status</code> | String | Password status. Possible values: ACTIVE, EXPIRED, EXPIRY_WARNING, LOCKED |
| <code>value.data.uuid</code> | String | The UUID of the user who is currently logged in |
| <code>value.data_summary.links</code> | Array | An array of links relevant to this request |
| <code>value.data_summary.links[].rel</code> | String | A keyword indicating the type of link in the "href" field. In this case, the provided link is a self link. |
| <code>value.data_summary.links[].href</code> | String | A link to the resource identified by the "rel" keyword. In this case, the URL is a self link for this request. |

Additional web security measures

Concurrent Session protection

The Cisco NAE REST API server limits the number of concurrent active sessions for a single user account.

Session Fixation protection

The Cisco NAE REST API server provides a mechanism for preventing session fixation attacks.



For more information about Session Fixation protection, visit https://www.owasp.org/index.php/Session_Fixation_Protection

XSS protection

The Cisco NAE REST API server provides XSS (Cross Site Scripting) prevention.



For more information about XSS protection, visit <https://www.owasp.org/index.php/XSS>

Query and Response

Standardized Query Responses

In response to any API command or query, the Cisco NAE REST API server returns an HTTP status code that indicates whether the request was successful, along with other information related to the request. The HTTP status codes are listed in [HTTP Status Codes](#).

Any Cisco NAE REST API call that returns a response payload will return a JSON structure in the common response format. To aid with programmability and understanding, all responses follow a standard response structure, as described in [Common Response Structure](#).

Common Response Structure

The Cisco NAE REST API common response JSON structure includes the fields described in the *Common Response Field Definitions* table. For an example of the JSON structure, see the [Common Response Structure Example](#).

Table 1. Common Response Field Definitions

| Name | Purpose |
|----------|--|
| success | Indicates whether the request was successful. |
| messages | Displays messages, if any, associated with a request. A single request can return multiple messages, such as when multiple validation errors exist in a submitted form. Each message is composed of three attributes: a severity level (INFO, WARNING, or ERROR), a Cisco NAE-specific error code to assist technical support, and a user-friendly message string. Note that a message may be generated even when a request is successful. For example, a WARNING message is generated if the requested page size exceeds the allowed value. Some common error codes are listed in NAE Error Codes . |
| value | This object holds the actual results of the request as shown in the <i>Response Payload Structure</i> table. |

Table 2. Response Payload Structure (identified by the **value** attribute in the response)

| Name | Purpose |
|------------|---|
| namespaces | Namespace declarations to prevent collisions between property names returned in the API response. |

| Name | Purpose |
|--------------|---|
| data_summary | <p>Summary information about the data returned in the response. The data summary object is composed of the following attributes:</p> <ul style="list-style-type: none"> * total_count: Total number of records matched by this request. If the total count exceeds the page_size, multiple pages of data are returned. The links attribute contains the paging links for navigating between pages. * has_more_data: Boolean indicating whether there are additional data rows available in the response. * page_size: Maximum number of records returned by a single request. This attribute is user configurable using the \$page query parameter (see Request Query Parameters) up to the maximum limit imposed by the system (currently 200 records). * current_page_number: Page number of this response data. Page numbers start at 0 and can be specified using the \$page query parameter. * total_page_count: Total number of pages contained in the response. This value equals the $(total_count/page_size) + 1$ * sort_fields: Array of one or more fields that specify the sorting criteria used in the response. * links: HATEOAS paging links for navigating between response pages. |
| data | <p>The actual data object containing the returned records. This object is documented separately for each API. The data attribute is a mixed object returning a JSON object when only a single row is returned and an array of objects when multiple rows are returned. The self link for this request is contained in the data_summary.links section.</p> |

Query Response Pagination

Because the results of a query may consist of a large number of data records, the query response is typically paginated. A single page of data, page 0, is returned in the response structure of an initial query. When the results of the query exceed the size of a single page, additional pages can be requested either by specifying an explicit page number (**\$page** in the [query parameters](#)) or by using [pagination links](#) in the response structure of the initial query and subsequent queries.

The number of records per page (**\$size**) can be specified as a query parameter.

Pagination Links

The response structure of any multi-page query contains full query URLs that can be sent in subsequent GET operations to fetch the first, last, next, and previous pages of data results.

The Cisco NAE REST API uses the Hypermedia As The Engine Of Application State (HATEOAS) principle to present links to paginated resources in the ATOM format. Including these links in the response relieves the user from the task of composing them.

The following table lists the links that are present for each resource. These pagination links are found in the `value.data_summary.links` section of the response.

| Relation | Description |
|----------|--|
| first | Link to the first page of the result set |
| prev | Previous page from the current page (not supplied for page 0) |
| next | Next page from the current page (not supplied for the last page) |
| last | Link to the last page of the result set |
| self | URL pointing to the resource itself |

Request Query Parameters

Request query parameters are appended to the API request URL with the `?` operator and are of the form `parameter=value`. Multiple query parameters can be combined using the `&` operator. Some query parameters allow more than one value, separated by a comma with no space after.

To support pagination and other query functions, the Cisco NAE REST API reserves all parameters starting with `$` as Cisco NAE REST API keywords. Any keyword not starting with `$` is assumed to be specific to the assurance group and is handled uniquely by the API.

Query Parameter Examples

The following query requests detailed epoch records, delivered two to a page, beginning with the first page, which is page 0.

```
GET /api/v1/epochs?$page=0&$size=2
```

The following query requests critical and major system events for an epoch. Two severity level values are specified, separated by a comma.

```
GET /api/v1/event-services/smart-events?$epoch_id={EPOCHID}&category=SYSTEM&severity=EVENT_SEVERITY_CRITICAL,EVENT_SEVERITY_MAJOR
```

Common Response Structure Example

The following example shows the JSON structure received in response to a request for the third page ("current_page_number") of fifteen ("total_page_count") in a multi-page response. The original query matched 30 epoch records ("total_count"), and the query specified that the response page should contain up to two records ("page_size").

The `value.dataSummary.links` section contains query URLs for requesting additional pages, such as page 0 (the first page), page 2 (the previous page), page 3 (this page), page 4 (the next page), and page 14 (the last page).

The `value.data` section contains the two data records included in this page.

```
{
  "success" : true,
  "messages" : [
    {
      "code" : 1001,
      "severity" : WARNING,
      "message" : "A warning message"
    }
  ],
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "dataSummary" : {
      "total_count" : 30,
      "has_more_data" : false,
      "page_size" : 2,
      "current_page_number" : 3,
      "total_page_count" : 15,
      "sort_fields" : "epoch",
      "links" : [
        {
          "rel": "first",
          "href": "http://localhost:8443/api/v1/epochs?$page=0&size=2"
        },
        {
          "rel": "prev",
          "href": "http://localhost:8443/api/v1/epochs?$page=2&size=2"
        },
        {
          "rel": "next",
          "href": "http://localhost:8443/api/v1/epochs?$page=4&size=2"
        },
        {
          "rel": "last",
          "href": "http://localhost:8443/api/v1/epochs?$page=14&size=2"
        },
        {
          "rel": "self",
          "href":
"http://localhost:8443/api/v1/epochs?$page=3&size=2&view=summary"
        }
      ]
    },
    "data" : [
      {
        "epoch": 6317663284849816765,
        "links": [
```

```
{
  {
    "rel": "self",
    "href": "http://localhost:8443/api/v1/epochs/6317663284849816765"
  }
],
"updated_at": 1470959143974
},
{
  "epoch": 6317663284849816465,
  "links": [
    {
      "rel": "self",
      "href": "http://localhost:8443/api/v1/epochs/6317663284849816465"
    }
  ],
  "updated_at": 1470958842975
}
]
}
}
```

About The Cisco NAE REST API Reference (Swagger)

The Cisco NAE REST API uses OpenAPI, also known as Swagger, to provide a complete and interactive API reference for developers, linked directly from the Cisco NAE GUI. The Swagger reference allows you to visualize and demonstrate the resources of the API. The direct connection from the reference document to the live REST API provides an easy way to write and test simple requests directly from the Swagger reference UI.

You can find the Cisco NAE REST API Swagger Interface document in the Appliance Documentation menu of the Cisco NAE GUI or at this URL: https://<Your_NAE_Appliance>/api/v1/swagger-ui.html



When you use the "Try it out" interactive feature of the Cisco NAE Swagger UI, you are required to enter a value for the session token X-NAE-CSRF-TOKEN, which is obtained in the login process. If you are already logged in to the Cisco NAE GUI, you can either log out of the GUI and then log in using the API, noting the new session token value, or you can use your browser's developer console to inspect the value of `localStorage.CSRF_TOKEN`. This element contains the current session token.

Common API Examples



This document describes the features, operation, and syntax of the Cisco Network Assurance Engine (NAE) REST API as of the current release when written. The features, operation, and syntax of the API are subject to change in future releases, and Cisco cannot guarantee backwards compatibility with prior releases.

Assurance Group Management Operations

Use the APIs in this section to create, read, update, or delete assured entities within Cisco NAE. The listed APIs are supported for ACI fabric management within Cisco NAE.

An assurance group contains all the network nodes that should be analyzed together, which typically consists of an entire network fabric. Cisco NAE enables you to analyze the assurance group in two modes: online analysis and offline analysis. For more information about assured entities, see the *Cisco Network Assurance Engine Fundamentals Guide*.

These APIs require an active authenticated API session. The following table shows the role requirements for executing these APIs.

| Operation | Minimum Role |
|---------------------------------------|--------------|
| Create ACI Fabric | User |
| Get ACI Fabric | User |
| Get All ACI Fabrics | User |
| Edit ACI Fabric | User |
| Start Online Analysis | User |
| Stop Analysis | User |
| Delete ACI Fabric | User |

Create ACI Fabric

A **POST** request creates a new ACI fabric record and returns an HTTP status code of **201 CREATED** upon success. An ACI fabric can be created for continuous live analysis.

Example Request

```
POST /api/v1/config-services/assured-networks/aci-fabric HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
Content-Length: 558
```

```
{
  "tags" : [ "AljASDmwlUyBktyyqlrIrgvSVRtdZA" ],
  "display_name" : "TSkpiNFojU",
  "interval" : 423,
  "analysis_timeout_in_secs" : 1476,
  "password" : "zLzrTibrjY",
  "iterations" : 5,
  "unique_name" : "hjpGKUEywL",
  "assured_network_type" : "ACI_FABRIC",
  "apic_hostnames" : [ "fhJQBFNKVSlOBNTHjEbramRiwaUAjC.cisco.com",
"AyGHjnfprLLtDQqfDRYpHZGnknHPnN.cisco.com",
"UVssCkngHAmXQOTIbcgZCAkZzWTfNK.cisco.com", "rBMgvobbnMptpUFwusNsegFQbGJoPH.cisco.com"
],
  "username" : "zOWXRgMUKj",
  "operational_mode" : "ONLINE",
  "description" : "BJvjKhrmun"
}
```

Example Response

HTTP/1.1 201 Created

Location: http://localhost:8080/api/v1/config-services/assured-networks/aci-fabric/23fb9488-074796a5-d324-4b2f-a547-c73cd43b32b6

Content-Type: application/json;charset=UTF-8

Content-Length: 935

```
{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "uuid" : "23fb9488-074796a5-d324-4b2f-a547-c73cd43b32b6",
      "tags" : [ "AljASDmwLUyBktyyqlrIrgvSVRtdZA" ],
      "display_name" : "TSkpiNFojU",
      "interval" : 423,
      "analysis_timeout_in_secs" : 1476,
      "status" : "STOPPED",
      "iterations" : 5,
      "unique_name" : "hjpGKUEyWL",
      "assured_network_type" : "ACI_FABRIC",
      "apic_hostnames" : [ "fhJQBFNKVSlOBNTHjEbramRiwaUAjC.cisco.com",
"AyGHjnfprLLtDQqfDRYpHZGknHPnN.cisco.com",
"UVssCkngHAmXQOTIbcgZCAkZzWTfNK.cisco.com", "rBMgvobbnMptpUFwusNsegFQbGJoPH.cisco.com"
],
      "username" : "zOWXRgMUKj",
      "active" : false,
      "operational_mode" : "ONLINE",
      "description" : "BJvjKhrmun"
    },
    "data_summary" : {
      "links" : [ ],
      "total_count" : 1,
      "has_more_data" : false
    }
  }
}
```

Request Fields

| Path | Type | Description |
|----------------|--------|--|
| apic_hostnames | Array | An array of strings that are the ACI Controller hostnames. |
| username | String | The login id of the admin user for the APIC host. |
| password | String | The password of the admin user for the APIC host. |

| Path | Type | Description |
|--------------------------|-------------|---|
| tags | Array | (Optional) A collection of user-defined tags associated with this object. The tags are exclusively for use by the user and are not used internally by the application. |
| unique_name | String | An immutable unique name for this object. The uniqueness is enforced with other object instances of the same type. Once created, this attribute cannot be changed. |
| display_name | String | (Optional) A user-defined unique display name for this object. The uniqueness is enforced with other object instances of the same type. Unlike the unique name, this attribute can be modified by the user at any time provided that it remains unique. |
| description | String | (Optional) A description for this object. |
| interval | Number | The polling interval at which the data is collected from this fabric. |
| analysis_timeout_in_secs | Number | The time in seconds after which the analysis is stopped if not completed. |
| iterations | Number | (Optional) The number of times collection and analysis should be run on this fabric, meaning the number of epochs to be generated. If this field is not specified, analysis will be run continuously at the specified interval. |
| assured_network_type | String | An enumerated type indicating the type of Assurance Group. Currently, the only valid type is ACI_FABRIC, and this attribute does not need to be set. |
| operational_mode | String | Valid values are ONLINE and OFFLINE. Indicates whether the ACI fabric is in offline analysis or is in a regularly managed mode. |

Response Fields

See Response Fields for [Get ACI Fabric](#).

Get ACI Fabric

A **GET** request returns a record of the ACI fabric if an ACI fabric with the specified ID is present.

Example Request

```
GET /api/v1/config-services/assured-networks/aci-fabric/a2839a18-7476-49db-88a5-9360e32277fc HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

HTTP/1.1 200 OK

Content-Type: application/json;charset=UTF-8

Content-Length: 1076

```
{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "uuid" : "a2839a18-7476-49db-88a5-9360e32277fc",
      "tags" : [ "ofhdhKbReG", "oQLYwryaqZ", "aUDgKURSQA", "nLAjAjMcPm", "rDXNKxCLde"
    ],
    "display_name" : "rGkLKOnLHr",
    "application_id" : "odzKWYbHae",
    "interval" : 416,
    "analysis_timeout_in_secs" : 600,
    "status" : "STOPPED",
    "links" : [ {
      "rel" : "self",
      "href" : "https://localhost/api/v1/config-services/assured-networks/aci-fabric/a2839a18-7476-49db-88a5-9360e32277fc"
    } ],
    "unique_name" : "dYllmFbRlc",
    "assured_network_type" : "ACI_FABRIC",
    "apic_hostnames" : [ "hRqaeIFpIR.cisco.com", "MNosfVVUWs.cisco.com", "HwPlLzpyxV.cisco.com", "VazaMKlams.cisco.com" ],
    "username" : "tdHtvJRCsh",
    "active" : false,
    "operational_mode" : "ONLINE",
    "description" : "NALyrngBrv"
  },
  "data_summary" : {
    "links" : [ ],
    "total_count" : 1,
    "has_more_data" : false
  }
}
```

Path Parameters

Table 3. `/api/v1/config-services/assured-networks/aci-fabric/{id}`

| Parameter | Description |
|-----------------|--|
| <code>id</code> | The id path parameter represents the id of the ACI fabric that needs to be returned. |

Response Fields

| Path | Type | Description |
|--|---------|--|
| <code>value.data.tags</code> | Array | A collection of user-defined tags associated with this object. The tags are exclusively for use by the user and are not used internally by the application. |
| <code>value.data.active</code> | Boolean | A flag that identifies whether the fabric is the currently-active fabric. Only one fabric can be active at any given time. An active fabric is one in which periodic data collection and analysis takes place based on the data collection settings. |
| <code>value.data.unique_name</code> | String | An immutable unique name for this object. The uniqueness is enforced with other object instances of the same type. Once created, this attribute cannot be changed. |
| <code>value.data.display_name</code> | String | A user-defined unique display name for this object. The uniqueness is enforced with other object instances of the same type. Unlike the unique name, this attribute can be modified by the user at any time provided that it remains unique. |
| <code>value.data.description</code> | String | A description for this object. |
| <code>value.data.uuid</code> | String | The unique identifier for this fabric. |
| <code>value.data.interval</code> | Number | The polling interval at which the data is collected from this fabric. |
| <code>value.data.assured_network_type</code> | String | An enumerated type indicating the type of Assurance Group. Currently, the only valid type is ACI_FABRIC. |
| <code>value.data.apic_hostnames</code> | Array | A array of strings that are the ACI Controller hostnames. |
| <code>value.data.username</code> | String | The login id of the admin user for the APIC host. |
| <code>value.data.operational_mode</code> | String | Indicates whether the ACI fabric is in offline analysis or is in a regularly managed mode. |

| Path | Type | Description |
|--|--------|--|
| <code>value.data.status</code> | String | The current status of the analysis run. |
| <code>value.data.analysis_timeout_in_secs</code> | Number | The maximum time to wait before an unfinished epoch will be aborted. |

Get All ACI Fabrics

A **GET** request returns the records of all ACI fabrics.

Example Request

```
GET /api/v1/config-services/assured-networks/aci-fabric HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 2152

{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : [ {
      "uuid" : "4f3aa211-beb4-4b9a-ae10-5c68a630c87a",
      "tags" : [ "LYPHIRoznW", "wRmKgOadRg", "qHYEGYsQSg", "MDcgDuZhHP" ],
      "display_name" : "uPwHGGLPJX",
      "application_id" : "GDTVkFoCJF",
      "interval" : 478,
      "analysis_timeout_in_secs" : 600,
      "status" : "STOPPED",
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/config-services/assured-networks/aci-fabric/4f3aa211-beb4-4b9a-ae10-5c68a630c87a"
      } ],
      "unique_name" : "ZhBqRidJCw",
      "assured_network_type" : "ACI_FABRIC",
      "apic_hostnames" : [ "PZlMrlvwVe.cisco.com", "jUCAncChoD.cisco.com", "SgqXFXeTyP.cisco.com", "KoqgyNYCIn.cisco.com" ],
```

```

    "username" : "RuPcTLVcTg",
    "active" : false,
    "operational_mode" : "ONLINE",
    "description" : "cRtVkoRfLL"
  }, {
    "uuid" : "42701ff6-d764-4da6-9cca-df7ecdad01e1",
    "tags" : [ "OcWNZcnMZp", "iadorjxVbu", "FYKhZuNNrY", "kjHtbeoIMp", "tkxbzOiRLi"
  ],
    "display_name" : "ELGFnvGRGE",
    "application_id" : "SGXWGjumjM",
    "interval" : 471,
    "analysis_timeout_in_secs" : 600,
    "status" : "STOPPED",
    "links" : [ {
      "rel" : "self",
      "href" : "https://localhost/api/v1/config-services/assured-networks/aci-fabric/42701ff6-d764-4da6-9cca-df7ecdad01e1"
    } ],
    "unique_name" : "zmlLlamQGU",
    "assured_network_type" : "ACI_FABRIC",
    "apic_hostnames" : [ "AljgSwKLVm.cisco.com", "fRRYmgabMI.cisco.com", "bVxPHnTvBr.cisco.com", "CEiPBPTKXC.cisco.com", "PSbhQqXvkB.cisco.com" ],
    "username" : "yMQSlFFZDy",
    "active" : false,
    "operational_mode" : "ONLINE",
    "description" : "hbqHEXlqan"
  } ],
  "data_summary" : {
    "links" : [ {
      "rel" : "self",
      "href" : "https://localhost/api/v1/config-services/assured-networks/aci-fabric?&page=0&size=50"
    } ],
    "total_count" : 2,
    "has_more_data" : false,
    "page_size" : 50,
    "current_page_number" : 0,
    "total_page_count" : 1
  }
}
}

```

Response Fields

See Response Fields for [Get ACI Fabric](#).

Edit ACI Fabric

A **PUT** request updates the attributes of an ACI fabric if a fabric with the specified ID is present.

Example Request

```
PUT /api/v1/config-services/assured-networks/aci-fabric/fc5b9eca-ad27-47ee-b0f9-  
cd6bbe201a4a HTTP/1.1
```

```
Content-Type: application/json
```

```
Accept: application/json
```

```
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
```

```
Host: localhost:8080
```

```
Content-Length: 280
```

```
{  
  "interval" : 1200,  
  "analysis_timeout_in_secs" : 1500,  
  "password" : "f1I1HhkMDi",  
  "assured_network_type" : "ACI_FABRIC",  
  "apic_hostnames" : [ "apic1@cisco.com", "apic2@cisco.com", "apic3@cisco.com" ],  
  "username" : "apicAdmin",  
  "description" : "fabric description"  
}
```

Example Response

HTTP/1.1 200 OK

Content-Type: application/json;charset=UTF-8

Content-Length: 1046

```
{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "uuid" : "fc5b9eca-ad27-47ee-b0f9-cd6bbe201a4a",
      "tags" : [ "ENfxmzHwqU", "aqgVrgpnQx", "SVYvGAimzy", "LTPyIgovJK", "TnyEtrFPSZ"
    ],
    "display_name" : "bzSDisbyZb",
    "application_id" : "EnzGvUsPmk",
    "interval" : 1200,
    "analysis_timeout_in_secs" : 1500,
    "status" : "STOPPED",
    "links" : [ {
      "rel" : "self",
      "href" : "https://localhost/api/v1/config-services/assured-networks/aci-fabric/fc5b9eca-ad27-47ee-b0f9-cd6bbe201a4a"
    } ],
    "unique_name" : "GkCYIVFygm",
    "assured_network_type" : "ACI_FABRIC",
    "apic_hostnames" : [ "apic1@cisco.com", "apic2@cisco.com", "apic3@cisco.com" ],
    "username" : "apicAdmin",
    "active" : false,
    "operational_mode" : "ONLINE",
    "description" : "fabric description"
  },
  "data_summary" : {
    "links" : [ ],
    "total_count" : 1,
    "has_more_data" : false
  }
}
```

Path Parameters

Table 4. `/api/v1/config-services/assured-networks/aci-fabric/{id}`

| Parameter | Description |
|-----------------|---|
| <code>id</code> | The id path parameter represents the id of the ACI fabric that needs to be updated. |

Response Fields

See Response Fields for [Get ACI Fabric](#).

Start Online Analysis

A **POST** request on a fabric triggers an online analysis run and returns an HTTP status code of **200 OK** upon successful trigger. Valid APIC hostnames, username, and password must be specified for the fabric for a successful analysis. Data is collected for the fabric and analyzed at regular intervals specified by the user. Epochs are generated for each analysis in point of time.

Example Request

```
POST /api/v1/config-services/assured-networks/aci-fabric/8f962f85-6858-4125-8884-8e891729ce83/start-analysis HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
Content-Length: 22

{
  "iterations" : 1
}
```

Example Response

```
HTTP/1.1 410 Gone
Content-Type: application/json;charset=UTF-8
Content-Length: 341
```

```
{
  "success" : false,
  "messages" : [ {
    "code" : 5109,
    "severity" : "ERROR",
    "message" : "This API is deprecated."
  } ],
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data_summary" : {
      "links" : [ ],
      "total_count" : 0,
      "has_more_data" : false
    }
  }
}
```

Request Fields

Unresolved directive in sections/fabricCrud.adoc - include::/home/candid/jenkins-private/workspace/Multibranch-Pipeline-candid_dp-28/nb/candid-docs/target/generated-snippets/start-analysis/request-fields.adoc[]

Stop Analysis

A **POST** request on a fabric stops an ongoing analysis run and returns a HTTP status code of **200 OK** upon successful trigger.

Example Request

```
POST /api/v1/config-services/assured-networks/aci-fabric/a945ceb0-d3aa-405d-82d4-38e7eb17bfea/stop-analysis HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

HTTP/1.1 200 OK

Content-Type: application/json;charset=UTF-8

Content-Length: 1100

```
{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : [
      {
        "uuid" : "a945ceb0-d3aa-405d-82d4-38e7eb17bfea",
        "tags" : [ "nSQqmbRtIy", "RjykFRRtXe", "KjHISrAEhZ", "tfYhQCQIGn", "AVCgEECYlk"
      ],
      "display_name" : "wZKsVvabGZ",
      "application_id" : "qTKBZuOLYy",
      "interval" : 460,
      "analysis_timeout_in_secs" : 600,
      "status" : "STOPPED",
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/config-services/assured-networks/aci-fabric/a945ceb0-d3aa-405d-82d4-38e7eb17bfea"
      } ],
      "unique_name" : "UVsAzPaUGE",
      "assured_network_type" : "ACI_FABRIC",
      "apic_hostnames" : [ "Wn1AEoyopV.cisco.com", "fHOSsQDrHN.cisco.com", "AdQtQTONsy.cisco.com", "VyvEuWDhJz.cisco.com", "OehoPAXkTf.cisco.com" ],
      "username" : "gepeQzneMv",
      "active" : false,
      "operational_mode" : "ONLINE",
      "description" : "RzHZYfVbAB"
    },
    "data_summary" : {
      "links" : [ ],
      "total_count" : 1,
      "has_more_data" : false
    }
  }
}
```

Delete ACI Fabric

A **DELETE** request deletes a fabric if a fabric with the specified ID is present. All epochs of the fabric are eventually deleted.

Example Request

```
DELETE /api/v1/config-services/assured-networks/aci-fabric/f6e30665-2038-44e0-8a47-
c6c9f21b382d HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 1062

{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "uuid" : "f6e30665-2038-44e0-8a47-c6c9f21b382d",
      "tags" : [ "oNVyCyamhC", "VCBQwHPXgL", "nXIwCqCJwb", "m0oayozQMK" ],
      "display_name" : "gyJHPEfIKV",
      "application_id" : "qhWiIKrzsv",
      "interval" : 400,
      "analysis_timeout_in_secs" : 600,
      "status" : "STOPPED",
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/config-services/assured-networks/aci-
fabric/f6e30665-2038-44e0-8a47-c6c9f21b382d"
      } ],
      "unique_name" : "q1Q1ZL1CRt",
      "assured_network_type" : "ACI_FABRIC",
      "apic_hostnames" : [ "nnRYRBXaNr.cisco.com", "aonoxxgmYj.cisco.com",
"FdbHDSn1OI.cisco.com", "fSGLgdLoTK.cisco.com" ],
      "username" : "IDoSoQlsxb",
      "active" : false,
      "operational_mode" : "ONLINE",
      "description" : "PvLmALvSGh"
    },
    "data_summary" : {
      "links" : [ ],
      "total_count" : 1,
      "has_more_data" : false
    }
  }
}
```

Path Parameters

Table 5. `/api/v1/config-services/assured-networks/aci-fabric/{id}`

| Parameter | Description |
|-----------------|---|
| <code>id</code> | The id path parameter represents the id of the ACI fabric that needs to be updated. |

Response Fields

See Response Fields for [Get ACI Fabric](#).

Epoch Operations

Use the APIs in this section to read the epochs of an ACI fabric within Cisco NAE. You must create an ACI fabric before using these APIs.

Cisco NAE performs analysis of a Cisco ACI fabric at regular intervals called epochs. In 15 minute intervals, `product-name-short` captures a snapshot of the controller policies and the fabric run time state, performs analysis, and generates smart events. For more information about epoch analysis, see the *Cisco Network Assurance Engine Getting Started Guide*.

These APIs require an active authenticated API session. The following table shows the role requirements for executing these APIs.

| Operation | Minimum Role |
|--|--------------|
| Get An Epoch | User |
| Get Epochs of an ACI Fabric | User |
| Get Epochs by Collection Timestamp | User |
| Get Latest Epoch | User |

Get An Epoch

A **GET** request with `$epoch_id` query parameter returns a record of the epoch if an epoch with the specified ID is present.

Example Request

```
GET /api/v1/event-services/epochs?$epoch_id=13822824-4230143e-c413-41b8-a484-0ea93e7f361d HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 1724

{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : [ {
      "assurance_info" : [ {
        "severity" : "info",
        "count" : 0
      }, {
        "severity" : "warning",
        "count" : 0
      }, {
        "severity" : "minor",
        "count" : 197
      }, {
        "severity" : "major",
        "count" : 166
      }, {
        "severity" : "critical",
        "count" : 0
      } ],
      "status" : "FINISHED",
      "collection_time_rfc3339" : "2019-08-18T03:54:50Z",
      "analysis_start_time_rfc3339" : "2019-08-18T03:54:50Z",
      "appliance_version" : "yhAEqsabfv",
      "is_offline" : false,
      "event_info" : [ {
        "severity" : "major",
        "count" : 166
      }, {
        "severity" : "minor",
        "count" : 197
      } ],
      "links" : [ {
        "rel" : "self",
        "href" : "http://localhost:8080/api/v1/event-
services/epochs?$epoch_id=13822824-4230143e-c413-41b8-a484-0ea93e7f361d"
      } ],
      "collection_time_msecs" : 1566100490000,
      "analysis_completion_time_msecs" : 1566110490000,
      "analysis_completion_time_rfc3339" : "2019-08-18T06:41:30Z",
      "fabric_id" : "d0d15637-fc5a-48c6-bc03-93c6a4f36135",
      "epoch_id" : "13822824-4230143e-c413-41b8-a484-0ea93e7f361d",
```

```

    "processed" : true,
    "analysis_start_time_msecs" : 1566100490000
  } ],
  "data_summary" : {
    "links" : [ {
      "rel" : "self",
      "href" : "https://localhost/api/v1/event-services/epochs?$page=0&size=50"
    } ],
    "total_count" : 1,
    "has_more_data" : false,
    "page_size" : 50,
    "current_page_number" : 0,
    "total_page_count" : 1
  }
}
}
}

```

Request Parameters

| Parameter | Description |
|-------------------------|--|
| <code>\$epoch_id</code> | (Optional) The id of the epoch to be returned. |

Response Fields

| Path | Type | Description |
|---|---------|---|
| <code>value.data[].collection_time_msecs</code> | Number | The UTC time in milliseconds since Jan 1, 1970 when this epoch collection started. |
| <code>value.data[].collection_time_rfc3339</code> | String | The UTC time in RFC3339 format when this epoch collection started. |
| <code>value.data[].epoch_id</code> | String | Unique epoch ID for this resource. |
| <code>value.data[].fabric_id</code> | String | Unique fabric ID for this resource. |
| <code>value.data[].links</code> | Array | An array of links for this request. |
| <code>value.data[].processed</code> | Boolean | This boolean indicates whether the epoch was completely processed. The processed flag is false for an epoch for which analysis has started but is not yet completed for any reason. |
| <code>value.data[].analysis_start_time_msecs</code> | Number | The UTC time in milliseconds since Jan 1, 1970 when this epoch's analysis started. |

| Path | Type | Description |
|---|---------|--|
| value.data[].analysis_start_time_rfc3339 | String | The UTC time in RFC3339 format when the analysis for the epoch was started. |
| value.data[].analysis_completion_time_msecs | Number | The UTC time in milliseconds since Jan 1, 1970 when this epoch's analysis completed. |
| value.data[].analysis_completion_time_rfc3339 | String | The UTC time in RFC3339 format when the data for this epoch was completely analysed. |
| value.data[].status | String | The current state of the analysis run for the epoch. Possible values are: FINISHED, IN_PROGRESS, and FAILED. |
| value.data[].is_offline | Boolean | Indicates whether the epoch is generated due to an offline analysis. |
| value.data[].assurance_info | Array | Provides information about assurance system events for this epoch. |
| value.data[].assurance_info[].severity | String | Indicates the severity of the events for which count is provided. |
| value.data[].assurance_info[].count | Number | Indicates the number of assurance events in the system for this epoch by severity. |
| value.data[].assurance_info[].links | Array | Provides links to access further information about the events of a severity for this epoch. |
| value.data[].event_info | Array | Provides information about the number of all kinds of events categorized by severity for this epoch. |
| value.data[].event_info[].severity | String | Indicates the severity of the events for which count is provided. |
| value.data[].event_info[].count | Number | Indicates the number of events in the system for this epoch by severity. |
| value.data[].event_info[].links | Array | Provides links to access further information about the events of a severity for this epoch. |
| value.data[].appliance_version | String | The version of the NAE when this epoch was generated. |

| Path | Type | Description |
|---------------------------------------|-------|---|
| <code>value.data.[].links</code> | Array | Provides links to access further relevant information for this epoch. |
| <code>value.data_summary.links</code> | Array | Provides links to access further relevant information for this epoch. |

Get Epochs of an ACI Fabric

A **GET** request with `$fabric_id` query parameter returns all epochs for a specified fabric. Additional query parameters documented below can also be specified to apply more filters.

Example Request

```
GET /api/v1/event-services/epochs?$fabric_id=f8dd3f76-d2b1-4891-9cf7-
0df00bc8de75&$size=1 HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 1924

{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : [ {
      "assurance_info" : [ {
        "severity" : "info",
        "count" : 0
      }, {
        "severity" : "warning",
        "count" : 0
      }, {
        "severity" : "minor",
        "count" : 0
      }, {
        "severity" : "major",
        "count" : 0
      }, {
```

```

    "severity" : "critical",
    "count" : 0
  } ],
  "status" : "FINISHED",
  "collection_time_rfc3339" : "2961-11-30T15:36:08Z",
  "analysis_start_time_rfc3339" : "2961-11-30T15:36:08Z",
  "appliance_version" : "vRuWAsMqMZ",
  "is_offline" : false,
  "links" : [ {
    "rel" : "self",
    "href" : "http://localhost:8080/api/v1/event-
services/epochs?$epoch_id=40422233-06a2d009-89f7-457f-85ff-eee06b2a7e65"
  } ],
  "collection_time_msecs" : 31301825768000,
  "analysis_completion_time_msecs" : 31301835768000,
  "analysis_completion_time_rfc3339" : "2961-11-30T18:22:48Z",
  "fabric_id" : "f8dd3f76-d2b1-4891-9cf7-0df00bc8de75",
  "epoch_id" : "40422233-06a2d009-89f7-457f-85ff-eee06b2a7e65",
  "processed" : true,
  "analysis_start_time_msecs" : 31301825768000
} ],
"data_summary" : {
  "links" : [ {
    "rel" : "first",
    "href" : "https://localhost/api/v1/event-services/epochs?$page=0&size=1"
  }, {
    "rel" : "self",
    "href" : "https://localhost/api/v1/event-services/epochs?$page=0&size=1"
  }, {
    "rel" : "next",
    "href" : "https://localhost/api/v1/event-services/epochs?$page=1&size=1"
  }, {
    "rel" : "last",
    "href" : "https://localhost/api/v1/event-services/epochs?$page=19&size=1"
  } ],
  "total_count" : 20,
  "has_more_data" : true,
  "page_size" : 1,
  "current_page_number" : 0,
  "total_page_count" : 20
}
}
}

```

Request Parameters

| Parameter | Description |
|--------------------------|--|
| <code>\$fabric_id</code> | (Optional) The ID of the ACI fabric for which the epochs should be returned. |

| Parameter | Description |
|---|--|
| <code>\$page</code> | (Optional) The page number of the paginated results to return. Defaults to 0 if not specified. The 'data_summary' element in the response provides links to fetch data for remaining pages. |
| <code>\$size</code> | (Optional) Specifies the number of epochs to return in a single page. Defaults to 50 if not specified. |
| <code>\$processed</code> | (Optional) A boolean parameter to allow the user to query for epochs which are processed completely. The processed flag is false for an epoch for which analysis has started but is not yet completed. |
| <code>\$status</code> | (Optional) Specifies the status of epochs that need to be returned. Multiple values separated by comma can be specified. Valid values are [IN_PROGRESS, FINISHED, FAILED, DELETING, PARTIALLY_FAILED] |
| <code>\$from_collection_time_msecs</code> | (Optional) A unix timestamp in milliseconds. All epochs with a collection time later than or equal to the specified value will be returned. |
| <code>\$to_collection_time_msecs</code> | (Optional) A unix timestamp in milliseconds. All epochs with a collection time earlier than the specified value will be returned. |
| <code>\$sort</code> | (Optional) Specifies the sort order for the returned results. Valid values are collection_time, analysis_start_time, analysis_completion_time. More than one sort order can be specified using comma separated values. Prepend the value with '-' to specify descending order. For example: \$sort=collection_time,-analysis_completion_time will sort the results first by collection time in ascending order and then by analysis completion time in descending order. If \$sort is not specified, returned epochs will be sorted by their collection time in descending order. |

Get Epochs by Collection Timestamp

A **GET** request with `$from_collection_time_msec`, `$to_collection_time_msecs` returns all epochs within the specified collection time range. Additional query parameters documented above can also be specified to apply more filters.

Example Request

```
GET /api/v1/event-
services/epochs?$from_collection_time_msecs=1568638592000&$to_collection_time_msecs=15
68638594000&$sort=-collection_time HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 1592

{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : [ {
      "assurance_info" : [ {
        "severity" : "info",
        "count" : 0
      }, {
        "severity" : "warning",
        "count" : 0
      }, {
        "severity" : "minor",
        "count" : 0
      }, {
        "severity" : "major",
        "count" : 0
      }, {
        "severity" : "critical",
        "count" : 0
      } ],
      "status" : "FINISHED",
      "collection_time_rfc3339" : "2019-09-16T12:56:32Z",
      "analysis_start_time_rfc3339" : "2019-09-16T12:56:32Z",
      "appliance_version" : "vdiJuureMI",
      "is_offline" : false,
      "links" : [ {
        "rel" : "self",
        "href" : "http://localhost:8080/api/v1/event-
services/epochs?$epoch_id=65723801-070d1614-d353-40ec-858e-c379e8d9d5f4"
      } ],
      "collection_time_msecs" : 1568638592000,
      "analysis_completion_time_msecs" : 1568648592000,
```

```

    "analysis_completion_time_rfc3339" : "2019-09-16T15:43:12Z",
    "fabric_id" : "13a8d19c-88bf-407d-bea8-f6b5592f9fbb",
    "epoch_id" : "65723801-070d1614-d353-40ec-858e-c379e8d9d5f4",
    "processed" : true,
    "analysis_start_time_msecs" : 1568638592000
  } ],
  "data_summary" : {
    "links" : [ {
      "rel" : "self",
      "href" : "https://localhost/api/v1/event-
services/epochs?$page=0&$size=50&$sort=-collection_time"
    } ],
    "total_count" : 1,
    "has_more_data" : false,
    "page_size" : 50,
    "current_page_number" : 0,
    "total_page_count" : 1
  }
}
}
}

```

Request Parameters

| Parameter | Description |
|---|---|
| <code>\$from_collection_time_msecs</code> | (Optional) A unix timestamp in milliseconds. All epochs with a collection time later than or equal to the specified value will be returned. |
| <code>\$to_collection_time_msecs</code> | (Optional) A unix timestamp in milliseconds. All epochs with a collection time earlier than the specified value will be returned. |
| <code>\$sort</code> | (Optional) Specifies the sort order for the returned results. Valid values are <code>collection_time</code> , <code>analysis_start_time</code> , <code>analysis_completion_time</code> . More than one sort order can be specified using comma separated values. For example: <code>\$sort=collection_time,-analysis_completion_time</code> . If <code>\$sort</code> is not specified, returned epochs will be sorted by their collection time in descending order. |

Get Latest Epoch

A **GET** request with values specified for `$page`, `$size`, and `$sort` query parameters can return the latest epoch in the system. Specifying a sort criteria to sort the epochs by analysis start time in descending order, and then picking the first record in the list through `$page=0` and `$size=1` returns the latest epoch. Additional query parameters documented above can also be specified to apply more filters.

Example Request

```
GET /api/v1/event-services/epochs?$page=0&$size=1&$sort=-analysis_start_time HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 2038

{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : [ {
      "assurance_info" : [ {
        "severity" : "info",
        "count" : 0
      }, {
        "severity" : "warning",
        "count" : 0
      }, {
        "severity" : "minor",
        "count" : 0
      }, {
        "severity" : "major",
        "count" : 0
      }, {
        "severity" : "critical",
        "count" : 0
      } ],
      "status" : "FINISHED",
      "collection_time_rfc3339" : "6582-01-06T02:30:03Z",
      "analysis_start_time_rfc3339" : "6582-01-06T02:30:03Z",
      "appliance_version" : "ZcdvPYsBDM",
      "is_offline" : false,
      "links" : [ {
        "rel" : "self",
        "href" : "http://localhost:8080/api/v1/event-
services/epochs?$epoch_id=50741168-ab4238a2-93f2-4122-a9f2-55bc0fce309c"
      } ],
      "collection_time_msecs" : 145541154603000,
      "analysis_completion_time_msecs" : 145541164603000,
```

```

"analysis_completion_time_rfc3339" : "6582-01-06T05:16:43Z",
"fabric_id" : "13a8d19c-88bf-407d-bea8-f6b5592f9fbb",
"epoch_id" : "50741168-ab4238a2-93f2-4122-a9f2-55bc0fce309c",
"processed" : true,
"analysis_start_time_msecs" : 145541154603000
} ],
"data_summary" : {
  "links" : [ {
    "rel" : "first",
    "href" : "https://localhost/api/v1/event-
services/epochs?$page=0&size=1&sort=-analysis_start_time"
  }, {
    "rel" : "self",
    "href" : "https://localhost/api/v1/event-
services/epochs?$page=0&size=1&sort=-analysis_start_time"
  }, {
    "rel" : "next",
    "href" : "https://localhost/api/v1/event-
services/epochs?$page=1&size=1&sort=-analysis_start_time"
  }, {
    "rel" : "last",
    "href" : "https://localhost/api/v1/event-
services/epochs?$page=210&size=1&sort=-analysis_start_time"
  } ],
  "total_count" : 211,
  "has_more_data" : true,
  "page_size" : 1,
  "current_page_number" : 0,
  "total_page_count" : 211
}
}
}

```

Request Parameters

| Parameter | Description |
|---------------------|--|
| <code>\$page</code> | (Optional) The page number of the paginated results to return. Defaults to 0 if not specified. The 'data_summary' element in the response provides links to fetch data for remaining pages. |
| <code>\$size</code> | (Optional) The number of epochs to return in a single page. Defaults to 50 if not specified. |
| <code>\$sort</code> | (Optional) Specifies the sort order. Valid values are <code>collection_time</code> , <code>analysis_start_time</code> , <code>analysis_completion_time</code> . More than one sort order can be specified using comma separated values. If <code>\$sort</code> is not specified, returned epochs will be sorted by default by their collection time in descending order. |

Smart Events Operations

Use the APIs in this section to view smart events triggered in Cisco NAE.

A smart event provides information about the state of your network at the time represented by an epoch. For more information about smart events, see the *Cisco Network Assurance Engine Fundamentals Guide* and *Cisco Network Assurance Engine Smart Events Reference Guide*.

These APIs require an active authenticated API session. The following table shows the role requirements for executing these APIs.

| Operation | Minimum Role |
|---|--------------|
| Get Smart Event Summary | User |
| Get Smart Event Detail | User |

Get Smart Event Summary

A **GET** request returns a summary of all requested smart events. Using request parameters, you can restrict the summary by category, subcategory, mnemonics, or severity. For allowed values of these parameters, see the *Cisco Network Assurance Engine Smart Events Reference Guide*. You can also specify a page number and page size.

Example Request

```
GET /api/v1/event-services/smart-events?$epoch_id=80856453-9db875e5-3088-4fac-89a0-54fbe41c0a96 HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 3545

{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : [ {
      "identifier" : "80856453-9db875e5-3088-4fac-89a0-54fbe41c0a96-4ee045ac03b5eb0a191ef52d182c53f5",
      "generating_appliance_version" : "4.0.1",
```



```

"reserved_fields" : {
  "database_schema_version" : 1,
  "json_schema_version" : 1,
  "object_type" : "CNAE:reservedFields"
},
"smart_event_info" : {
  "code" : 7005,
  "name" : "ACCESS_ENTITY_PROFILE_NOT_ASSOCIATED_WITH_ANY_DOMAINS",
  "object_type" : "CNAE:smartEvent",
  "event_code_major_version" : "1.0",
  "event_code_minor_version" : "1.0"
},
"category" : {
  "code" : 6,
  "name" : "CHANGE_ANALYSIS",
  "object_type" : "CNAE:eventCategory"
},
"sub_category" : {
  "code" : 30,
  "name" : "FORWARDING_POLICY",
  "object_type" : "CNAE:eventSubcategory"
},
"severity" : {
  "code" : 400,
  "name" : "EVENT_SEVERITY_MAJOR",
  "object_type" : "CNAE:eventSeverity"
},
"description" : "The access entity profile is not associated to any domain.",
"epoch_uuid" : "80856453-9db875e5-3088-4fac-89a0-54fbe41c0a96",
"aci_fabric_settings_dto" : {
  "uuid" : "597be591-f0fe-42e3-8e52-5261c0dcadd1",
  "application_id" : "IHYofrLHuQ",
  "interval" : 456,
  "analysis_timeout_in_secs" : 0,
  "status" : "STOPPED",
  "unique_name" : "mfrNGlzyhq",
  "assured_network_type" : "ACI_FABRIC",
  "apic_hostnames" : [ "CwfGcRboCf.cisco.com", "rPteMdl0nd.cisco.com",
"lZgFhxoGLi.cisco.com" ],
  "username" : "YaBXlGCsuG",
  "active" : false,
  "operational_mode" : "ONLINE"
},
"additional_details" : [ {
  "identifier" : "uni/infra/attentp-kilo_AEP_08",
  "object_types" : [ {
    "code" : 237,
    "name" : "CANDID_OBJECT_TYPE_ACCESS_ENTITY_PROFILE",
    "object_type" : "CNAE:candidObjectType"
  } ],
  "name" : "kilo_AEP_08"
}

```

```

}, {
  "identifiant" : "uni/tn-kilo",
  "object_types" : [ {
    "code" : 2,
    "name" : "CANDID_OBJECT_TYPE_TENANT",
    "object_type" : "CNAE:candidObjectType"
  } ],
  "name" : "kilo"
}, {
  "identifiant" : "uni/tn-kilo/ap-kilo-app3",
  "object_types" : [ {
    "code" : 8,
    "name" : "CANDID_OBJECT_TYPE_APP_PROFILE",
    "object_type" : "CNAE:candidObjectType"
  } ],
  "name" : "kilo-app3"
}, {
  "identifiant" : "uni/tn-kilo/ap-kilo-app3/epg-kilo_ctx1_bd1_epg08",
  "object_types" : [ {
    "code" : 7,
    "name" : "CANDID_OBJECT_TYPE_EPG",
    "object_type" : "CNAE:candidObjectType"
  } ],
  "name" : "kilo_ctx1_bd1_epg08"
}, {
  "identifiant" : 948,
  "object_types" : [ {
    "code" : 3001,
    "name" : "CANDID_OBJECT_TYPE_ENCAP_VLAN",
    "object_type" : "CNAE:candidObjectType"
  } ]
} ],
"object_type" : "CNAE:smartEventsSummary",
"links" : [ ]
} ],
"data_summary" : {
  "links" : [ {
    "rel" : "self",
    "href" : "https://localhost/api/v1/event-services/smart-
events?$epoch_id=80856453-9db875e5-3088-4fac-89a0-54fbe41c0a96&$page=0&$size=50"
  } ],
  "total_count" : 1,
  "has_more_data" : false,
  "page_size" : 50,
  "current_page_number" : 0,
  "total_page_count" : 1
}
}
}

```

Request parameters

| Parameter | Description |
|---------------------------|---|
| <code>\$epoch_id</code> | Epoch UUID to fetch. This is a mandatory parameter. |
| <code>\$page</code> | Page number to fetch. Starts from 0. |
| <code>\$size</code> | Page size to fetch. Valid value is 1-200 (inclusive). |
| <code>category</code> | Smart Event category to fetch. Valid categories are one of: COMPLIANCE,TENANT_ENDPOINT,TENANT_FORWARDING,TENANT_SECURITY,CHANGE_ANALYSIS,RESOURCE_UTILIZATION,SYSTEM. A comma separated list of two or more categories is allowed. |
| <code>sub_category</code> | Smart Event sub_category to fetch. Example sub_categories: CONTRACT_SECURITY,ENDPOINT_LEARNING, etc. A comma separated list of two or more sub_categories is allowed. To get a list of all sub_categories, refer to the 'Cisco NAE Smart Events Reference Guide'. You may use this parameter without the category parameter. But note if you give an invalid combination of category, sub_category - API will not return results. |
| <code>mnemonic</code> | Smart Event mnemonic (name) to fetch. Example mnemonics: ENFORCED_VRF_POLICY_VIOLATION,CONNECTED_EP_LEARNING_ERROR, etc. A comma separated list of two or more mnemonics is allowed. To get a list of all mnemonics, refer to the 'Cisco NAE Smart Events Reference Guide'. You may use this parameter without the category / sub_category parameter. But note if you give an invalid combination of category, sub_category, mnemonic - API will not return results. |
| <code>severity</code> | Smart Event severity to fetch. Valid severities are one of: EVENT_SEVERITY_CRITICAL,EVENT_SEVERITY_MAJOR,EVENT_SEVERITY_MINOR,EVENT_SEVERITY_WARNING,EVENT_SEVERITY_INFO. A comma separated list of two or more severities is allowed. |

Response fields

| Path | Type | Description |
|-------------------------|-------|----------------------|
| <code>value.data</code> | Array | List of Smart Events |

| Path | Type | Description |
|--|--------|---|
| value.data[].identifier | String | Smart Event UUID |
| value.data[].generating_appliance_version | String | NAE appliance version that generated this Smart Event |
| value.data[].smart_event_info | Object | Smart Event type information |
| value.data[].smart_event_info.code | Number | Smart Event numeric code |
| value.data[].smart_event_info.name | String | Smart Event mnemonic |
| value.data[].smart_event_info.event_code_major_version | String | Smart Event major version |
| value.data[].smart_event_info.event_code_minor_version | String | Smart Event minor version |
| value.data[].category | Object | Smart Event category information |
| value.data[].sub_category | Object | Smart Event subcategory information |
| value.data[].severity | Object | Smart Event severity level |
| value.data[].description | String | Smart Event description |
| value.data[].epoch_uuid | String | Smart Event Epoch UUID |
| value.data[].aci_fabric_settings_dto | Object | Smart Event Assurance Group info |
| value.data[].additional_details | Array | Array of objects summarizing the Smart Event instance |
| value.data[].additional_details[].identifier | Varies | Identifier of the object |
| value.data[].additional_details[].name | String | Name of the object |
| value.data[].additional_details[].object_types | Array | Type describing the object |
| value.data_summary | Object | Summary of the Smart Events returned |
| value.data_summary.links | Array | An array of links relevant to this request |
| value.data_summary.links[].rel | String | A keyword indicating the type of link in the "href" field |
| value.data_summary.links[].href | String | A link to the resource identified by the "rel" keyword |
| value.data_summary.page_size | Number | Page size requested |
| value.data_summary.current_page_number | Number | Response page number |
| value.data_summary.total_page_count | Number | Total number of pages in response |

Get Smart Event Detail

A **GET** request returns the details of a single smart event.

Example Request

```
GET /api/v1/event-services/smart-events/detail?$event_id=80856453-9db875e5-3088-4fac-89a0-54fbe41c0a96-4ee045ac03b5eb0a191ef52d182c53f5 HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 4784

{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : [ {
      "identifier" : "80856453-9db875e5-3088-4fac-89a0-54fbe41c0a96-4ee045ac03b5eb0a191ef52d182c53f5",
      "generating_appliance_version" : "4.0.1",
      "reserved_fields" : {
        "database_schema_version" : 1,
        "json_schema_version" : 1,
        "object_type" : "CNAE:reservedFields"
      },
      "smart_event_info" : {
        "code" : 7005,
        "name" : "ACCESS_ENTITY_PROFILE_NOT_ASSOCIATED_WITH_ANY_DOMAINS",
        "object_type" : "CNAE:smartEvent",
        "event_code_major_version" : "1.0",
        "event_code_minor_version" : "1.0"
      },
      "category" : {
        "code" : 6,
        "name" : "CHANGE_ANALYSIS",
        "object_type" : "CNAE:eventCategory"
      },
      "sub_category" : {
        "code" : 30,
        "name" : "FORWARDING_POLICY",
```

```

    "object_type" : "CNAE:eventSubcategory"
  },
  "severity" : {
    "code" : 400,
    "name" : "EVENT_SEVERITY_MAJOR",
    "object_type" : "CNAE:eventSeverity"
  },
  "description" : "The access entity profile is not associated to any domain.",
  "epoch_uuid" : "80856453-9db875e5-3088-4fac-89a0-54fbe41c0a96",
  "aci_fabric_settings_dto" : {
    "uuid" : "597be591-f0fe-42e3-8e52-5261c0dcadd1",
    "application_id" : "IHYofrLHuQ",
    "interval" : 456,
    "analysis_timeout_in_secs" : 0,
    "status" : "STOPPED",
    "unique_name" : "mfrNGlzyhq",
    "assured_network_type" : "ACI_FABRIC",
    "apic_hostnames" : [ "CwfGcRboCf.cisco.com", "rPteMdlOnd.cisco.com",
"lZgFhxoGLi.cisco.com" ],
    "username" : "YaBXlGCsuG",
    "active" : false,
    "operational_mode" : "ONLINE"
  },
  "primary_affected_object" : {
    "identifier" : "434980d919ba02d5",
    "type" : "CANDID_OBJECT_TYPE_PRIMARY_KEY",
    "name" : "434980d919ba02d5",
    "composite_key" : [ {
      "identifier" : "uni/infra/attentp-kilo_AEP_08",
      "type" : "CANDID_OBJECT_TYPE_ACCESS_ENTITY_PROFILE",
      "name" : "kilo_AEP_08",
      "attributes" : [ {
        "name" : "healthy",
        "value" : false
      } ]
    } ]
  } ]
},
"checks" : [ {
  "code" : 3015,
  "name" : "CC_EPG_ACCESS_ENTITY_PROFILE_NOT_ASSOCIATED_WITH_ANY_DOMAINS",
  "additional_info" : {
    "type" : "CANDID_OBJECT_TYPE_TABLE",
    "name" : "EpgPathTable",
    "associated_objects" : [ {
      "type" : "CANDID_OBJECT_TYPE_ROW",
      "associated_objects" : [ {
        "identifier" : "uni/tn-kilo",
        "type" : "CANDID_OBJECT_TYPE_TENANT",
        "name" : "kilo",
        "attributes" : [ {
          "name" : "healthy",

```

```

        "value" : false
      } ]
    }, {
      "identifier" : "uni/tn-kilo/ap-kilo-app3",
      "type" : "CANDID_OBJECT_TYPE_APP_PROFILE",
      "name" : "kilo-app3",
      "attributes" : [ {
        "name" : "healthy",
        "value" : false
      } ]
    }, {
      "identifier" : "uni/tn-kilo/ap-kilo-app3/epg-kilo_ctx1_bd1_epg08",
      "type" : "CANDID_OBJECT_TYPE_EPG",
      "name" : "kilo_ctx1_bd1_epg08",
      "attributes" : [ {
        "name" : "healthy",
        "value" : false
      } ]
    }, {
      "identifier" : "uni/tn-kilo/ap-kilo-app3/epg-
kilo_ctx1_bd1_epg08/rsnodeAtt-[topology/pod-2/node-8008]",
      "type" : "CANDID_OBJECT_TYPE_STATIC_LEAF_PATH_BINDING_INFORMATION",
      "name" : "[topology/pod-2/node-8008]",
      "attributes" : [ {
        "name" : "healthy",
        "value" : false
      } ]
    }, {
      "identifier" : 948,
      "type" : "CANDID_OBJECT_TYPE_ENCAP_VLAN",
      "name" : "948",
      "attributes" : [ {
        "name" : "healthy",
        "value" : false
      } ]
    }, {
      "identifier" : "STATIC",
      "type" : "CANDID_OBJECT_TYPE_EPG_PATH_TYPE",
      "name" : "STATIC"
    } ]
  } ]
},
"check_status" : 3,
"object_type" : "CNAE:conditionCheck"
} ],
"object_type" : "CNAE:smartEventDetails",
"links" : [ ]
} ],
"data_summary" : {
  "links" : [ {
    "rel" : "self",

```

```

    "href" : "https://localhost/api/v1/event-services/smart-
events/detail?$event_id=80856453-9db875e5-3088-4fac-89a0-54fbe41c0a96-
4ee045ac03b5eb0a191ef52d182c53f5"
  } ],
  "total_count" : 1,
  "has_more_data" : false
}
}
}

```

Request parameters

| Parameter | Description |
|-------------------------|---|
| <code>\$event_id</code> | Smart Event UUID to fetch. This is a mandatory parameter. |

Response fields

| Path | Type | Description |
|---|--------|--|
| <code>value.data[].identifier</code> | String | Smart Event UUID |
| <code>value.data[].generating_appliance_version</code> | String | NAE appliance version that generated this Smart Event |
| <code>value.data[].smart_event_info</code> | Object | Smart Event type information |
| <code>value.data[].smart_event_info.code</code> | Number | Smart Event numeric code |
| <code>value.data[].smart_event_info.name</code> | String | Smart Event mnemonic |
| <code>value.data[].smart_event_info.event_code_major_version</code> | String | Smart Event major version |
| <code>value.data[].smart_event_info.event_code_minor_version</code> | String | Smart Event minor version |
| <code>value.data[].category</code> | Object | Smart Event category information |
| <code>value.data[].sub_category</code> | Object | Smart Event sub category information |
| <code>value.data[].severity</code> | Object | Smart Event severity level |
| <code>value.data[].description</code> | String | Smart Event description |
| <code>value.data[].epoch_uuid</code> | String | Smart Event Epoch UUID |
| <code>value.data[].aci_fabric_settings_dto</code> | Object | Smart Event Assurance Group info |
| <code>value.data[].primary_affected_object</code> | Object | Primary affected object on which this Smart Event instance is raised |
| <code>value.data[].primary_affected_object.identifier</code> | String | Identifier of the object |

| Path | Type | Description |
|---|--------|---|
| value.data[].primary_affected_object.type | String | Type of the object |
| value.data[].primary_affected_object.name | String | Name of the object |
| value.data[].primary_affected_object.composite_key | Array | Array of sub-objects that logically compose this object |
| value.data[].primary_affected_object.associated_objects | Array | Array of sub-objects that are logically associated with this object |
| value.data[].checks | Array | List of checks performed |
| value.data[].checks[].code | Number | Numeric check code |
| value.data[].checks[].name | String | Check mnemonic |
| value.data[].checks[].check_status | Number | Status of the check |
| value.data[].checks[].additional_info | Object | Information describing this check. Follows the same structure as that of primary_affected_object. |
| value.data_summary | Object | Summary of the Smart Events returned |
| value.data_summary.links | Array | An array of links relevant to this request |
| value.data_summary.links[].rel | String | A keyword indicating the type of link in the "href" field |
| value.data_summary.links[].href | String | A link to the resource identified by the "rel" keyword |

User Management Operations

Use the APIs in this section to create, read, update, or delete a local user account within Cisco NAE.

In Cisco NAE, you can choose to configure and authenticate users locally on the Cisco NAE appliance itself instead of using an external AAA server. For more information about User Management, see the *Cisco Network Assurance Engine Getting Started Guide*.

These APIs require an active authenticated API session. The following table shows the role requirements for executing these APIs.

| Operation | Minimum Role |
|--------------------------------------|---------------------|
| Create a User | Super Administrator |
| Change User Password | Note 1 |
| Get User | Super Administrator |
| Get All Users | Super Administrator |
| Edit User | Note 1 |

| Operation | Minimum Role |
|---|---------------------|
| Delete User | Super Administrator |
| Update Password Expiration Time | Super Administrator |
| Forgot Password | Note 1 |
| Reset Password | Note 1 |

Note 1: Users can change only their own passwords and email addresses. Only a super administrator can make changes for others.

Create a User

A **POST** request creates a new user account and returns an HTTP status code of **201 CREATED** upon success. Only a super administrator can create a user account.

If `system_generated_password` is `true`, the Create User Password API will generate an email with a GUI link for setting the new password. The link in the email contains the one-time token as a URL parameter. Because an email is generated, SMTP must be configured and enabled in the appliance. For information about configuring SMTP, see *Cisco Network Assurance Engine Getting Started Guide*.

Example Request

```
POST /api/v1/config-services/users HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
Content-Length: 182
```

```
{
  "email" : "DvZCxuBoKk@cisco.com",
  "username" : "kfVTdECAhi",
  "password" : "TFEhpZgdQsqTyoX",
  "confirm_password" : "TFEhpZgdQsqTyoX",
  "system_generated_password" : false
}
```

Example Response

HTTP/1.1 201 Created

Location: <https://localhost/api/v1/config-services/users>

Content-Type: application/json;charset=UTF-8

Content-Length: 1371

```
{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "uuid" : "23fb9488-90c30087-3510-4268-9ac1-6d066537e45d",
      "email" : "DvZCxuBoKk@cisco.com",
      "username" : "kfVTdECAhi",
      "password_expiry_date" : {
        "rfc3339" : "2029-08-01T07:27:10Z",
        "milliseconds" : 1880263630074
      },
      "is_super_admin" : false
    },
    "data_summary" : {
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/config-services/users"
      }, {
        "rel" : "getUser",
        "href" : "https://localhost/api/v1/config-services/users/23fb9488-90c30087-3510-4268-9ac1-6d066537e45d"
      }, {
        "rel" : "getUsers",
        "href" : "https://localhost/api/v1/config-services/users"
      }, {
        "rel" : "editUser",
        "href" : "https://localhost/api/v1/config-services/users/23fb9488-90c30087-3510-4268-9ac1-6d066537e45d"
      }, {
        "rel" : "deleteUser",
        "href" : "https://localhost/api/v1/config-services/users/23fb9488-90c30087-3510-4268-9ac1-6d066537e45d"
      }, {
        "rel" : "changePassword",
        "href" : "https://localhost/api/v1/config-services/users/23fb9488-90c30087-3510-4268-9ac1-6d066537e45d/change-password"
      } ],
      "total_count" : 1,
      "has_more_data" : false
    }
  }
}
```

Request Fields

| Path | Type | Description |
|---------------------------|---------|--|
| email | String | The user's email address. |
| username | String | User's NAE login username. |
| password | String | User's password. |
| system_generated_password | Boolean | Indicates whether the system must generate a random password or use the password provided by the user. |
| confirm_password | String | Confirm user's password. |

Response Fields

| Path | Type | Description |
|---------------------------------|---------|--|
| value.data.is_super_admin | Boolean | Indicates whether this user is a super admin. |
| value.data_summary | Object | The number of users returned. |
| value.data_summary.links | Array | An array of links relevant to this request. |
| value.data_summary.links[].rel | String | A keyword indicating the type of link in the "href" field. |
| value.data_summary.links[].href | String | A link to the resource identified by the "rel" keyword. |
| value.data.uuid | String | UUID associated to this user. |

Change User Password

A **POST** request changes a user password and returns an HTTP status code of **200 OK** upon success. The requester must supply the current password and the new password.

If the `system_generated_password` request field is set to `true`, the Change User Password API will generate an email with a GUI link for resetting the password. The link in the email contains the one-time token as a URL parameter. Because an email is generated, SMTP must be configured and enabled in the appliance. For information about configuring SMTP, see *Cisco Network Assurance Engine Getting Started Guide*.

Only a super administrator can change the password of another user.

Example Request

```
POST /api/v1/config-services/users/35645a39-4294-43f1-b43a-99a9d7c53d9e/change-  
password HTTP/1.1  
Content-Type: application/json  
Accept: application/json  
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER  
Host: localhost:8080  
Content-Length: 217
```

```
{  
  "new_password" : "snpnQRnAJSZjMUH",  
  "logged_in_user_password" : "FkjsxwMixhG",  
  "confirm_password" : "snpnQRnAJSZjMUH",  
  "system_generated_password" : false,  
  "password_expiration_time_milli" : 1564903629625  
}
```

Example Response

HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 703

```
{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "uuid" : "35645a39-4294-43f1-b43a-99a9d7c53d9e",
      "email" : "ZJAOHSNDZk@cisco.com",
      "username" : "NbUserRepositoryTestftNCVQKPEI",
      "password_expiry_date" : {
        "rfc3339" : "2019-08-04T07:27:09Z",
        "milliseconds" : 1564903629625
      },
      "is_super_admin" : false
    },
    "data_summary" : {
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/config-services/users/35645a39-4294-43f1-b43a-99a9d7c53d9e/change-password"
      } ],
      "total_count" : 1,
      "has_more_data" : false
    }
  }
}
```

Path Parameters

Table 6. `/api/v1/config-services/users/{userId}/change-password`

| Parameter | Description |
|---------------------|---------------------------------|
| <code>userId</code> | The UUID of the user to update. |

Request Fields

| Path | Type | Description |
|--------------------------------------|--------|---|
| <code>logged_in_user_password</code> | String | Logged in user password. This field is mandatory for a user who is not a super admin. |
| <code>new_password</code> | String | User's new password. |
| <code>confirm_password</code> | String | Confirm user's password. |

| Path | Type | Description |
|---|---------|--|
| <code>system_generated_password</code> | Boolean | Indicates whether the system must generate a random password or use the password provided by the user. |
| <code>password_expiration_time_milli</code> | Number | (Optional field) The user's password expiration time in milliseconds since epoch. Default value is the sum of current timestamp and the default password lifetime defined by administrator |

Response Fields

| Path | Type | Description |
|--|---------|---|
| <code>value.data.email</code> | String | The user's email address |
| <code>value.data.username</code> | String | The user's NAE login username |
| <code>value.data.password_expiry_date.rfc3339</code> | String | Password expiry date as String |
| <code>value.data.password_expiry_date.millisecs</code> | Number | Password expiry date in milliseconds since epoch |
| <code>value.data.uuid</code> | String | UUID associated to this user |
| <code>value.data.is_super_admin</code> | Boolean | Indicates whether this user is a super admin |
| <code>value.data_summary</code> | Object | The number of users returned |
| <code>value.data_summary.links</code> | Array | An array of links relevant to this request |
| <code>value.data_summary.links[].rel</code> | String | A keyword indicating the type of link in the "href" field |
| <code>value.data_summary.links[].href</code> | String | A link to the resource identified by the "rel" keyword |

Get User

A **GET** request returns a record of the user if a user with the specified ID is present.

Example Request

```
GET /api/v1/config-services/users/37190a5b-509c-468e-8736-2188f3d05421 HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 1400

```
{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "uuid" : "37190a5b-509c-468e-8736-2188f3d05421",
      "email" : "gOyOvfNfaK@cisco.com",
      "username" : "NbUserRepositoryTestQvfVHhkFdI",
      "password_expiry_date" : {
        "rfc3339" : "2029-08-04T07:27:09Z",
        "millisecs" : 1880522829962
      },
      "is_super_admin" : false
    },
    "data_summary" : {
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/config-services/users/37190a5b-509c-468e-8736-2188f3d05421"
      }, {
        "rel" : "getUsers",
        "href" : "https://localhost/api/v1/config-services/users"
      }, {
        "rel" : "editUser",
        "href" : "https://localhost/api/v1/config-services/users/37190a5b-509c-468e-8736-2188f3d05421"
      }, {
        "rel" : "deleteUser",
        "href" : "https://localhost/api/v1/config-services/users/37190a5b-509c-468e-8736-2188f3d05421"
      }, {
        "rel" : "changePassword",
        "href" : "https://localhost/api/v1/config-services/users/37190a5b-509c-468e-8736-2188f3d05421/change-password"
      }, {
        "rel" : "forgotPassword",
        "href" : "https://localhost/api/v1/config-services/users/NbUserRepositoryTestQvfVHhkFdI/forgot-password"
      } ],
      "total_count" : 1,
      "has_more_data" : false
    }
  }
}
```

Path Parameters

Table 7. `/api/v1/config-services/users/{userId}`

| Parameter | Description |
|---------------------|---------------------------------|
| <code>userId</code> | The UUID of the user to update. |

Response Fields

| Path | Type | Description |
|--|---------|--|
| <code>value.data.email</code> | String | The user's email address. |
| <code>value.data.username</code> | String | The user's NAE login username. |
| <code>value.data.password_expiry_date.rfc3339</code> | String | Password expiry date as String. |
| <code>value.data.password_expiry_date.millisecs</code> | Number | Password expiry date in milliseconds since epoch. |
| <code>value.data.uuid</code> | String | UUID associated to this user. |
| <code>value.data.is_super_admin</code> | Boolean | Indicates whether this user is a super admin. |
| <code>value.data_summary</code> | Object | The number of users returned. |
| <code>value.data_summary.links</code> | Array | An array of links relevant to this request. |
| <code>value.data_summary.links[].rel</code> | String | A keyword indicating the type of link in the "href" field. |
| <code>value.data_summary.links[].href</code> | String | A link to the resource identified by the "rel" keyword. |

Get All Users

A **GET** request returns the records of all users.

Example Request

```
GET /api/v1/config-services/users HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 7379

{
```

```

"success" : true,
"value" : {
  "namespaces" : {
    "default" : "https://www.cisco.com/api/schema"
  },
  "data" : [ {
    "uuid" : "d6ce1ee3-f105-4fb4-949b-8124f0de5864",
    "email" : "ELdozYHoVg@cisco.com",
    "username" : "admin",
    "password_expiry_date" : {
      "rfc3339" : "2029-08-04T07:27:09Z",
      "millisecs" : 1880522829554
    },
    "is_super_admin" : true,
    "links" : [ {
      "rel" : "self",
      "href" : "https://localhost/api/v1/config-services/users"
    }, {
      "rel" : "getUser",
      "href" : "https://localhost/api/v1/config-services/users/d6ce1ee3-f105-4fb4-949b-8124f0de5864"
    }, {
      "rel" : "editUser",
      "href" : "https://localhost/api/v1/config-services/users/d6ce1ee3-f105-4fb4-949b-8124f0de5864"
    }, {
      "rel" : "deleteUser",
      "href" : "https://localhost/api/v1/config-services/users/d6ce1ee3-f105-4fb4-949b-8124f0de5864"
    }, {
      "rel" : "changePassword",
      "href" : "https://localhost/api/v1/config-services/users/d6ce1ee3-f105-4fb4-949b-8124f0de5864/change-password"
    }, {
      "rel" : "forgotPassword",
      "href" : "https://localhost/api/v1/config-services/users/admin/forgot-password"
    } ]
  }, {
    "uuid" : "35645a39-4294-43f1-b43a-99a9d7c53d9e",
    "email" : "ZJAOHSNDZk@cisco.com",
    "username" : "NbUserRepositoryTestftNCVQKPEI",
    "password_expiry_date" : {
      "rfc3339" : "2019-08-04T07:27:09Z",
      "millisecs" : 1564903629625
    },
    "is_super_admin" : false,
    "links" : [ {
      "rel" : "self",
      "href" : "https://localhost/api/v1/config-services/users"
    }, {

```

```

    "rel" : "getUser",
    "href" : "https://localhost/api/v1/config-services/users/35645a39-4294-43f1-
b43a-99a9d7c53d9e"
  }, {
    "rel" : "editUser",
    "href" : "https://localhost/api/v1/config-services/users/35645a39-4294-43f1-
b43a-99a9d7c53d9e"
  }, {
    "rel" : "deleteUser",
    "href" : "https://localhost/api/v1/config-services/users/35645a39-4294-43f1-
b43a-99a9d7c53d9e"
  }, {
    "rel" : "changePassword",
    "href" : "https://localhost/api/v1/config-services/users/35645a39-4294-43f1-
b43a-99a9d7c53d9e/change-password"
  }, {
    "rel" : "forgotPassword",
    "href" : "https://localhost/api/v1/config-
services/users/NbUserRepositoryTestftNCVQKPEI/forgot-password"
  } ]
}, {
  "uuid" : "5094e0c3-4235-4689-9f14-351a9268adcc",
  "email" : "yZXIdtPgrJ@cisco.com",
  "username" : "NbUserRepositoryTestLaJKJUpNKR",
  "password_expiry_date" : {
    "rfc3339" : "2029-08-04T07:27:09Z",
    "milliseconds" : 1880522829844
  },
  "is_super_admin" : false,
  "links" : [ {
    "rel" : "self",
    "href" : "https://localhost/api/v1/config-services/users"
  }, {
    "rel" : "getUser",
    "href" : "https://localhost/api/v1/config-services/users/5094e0c3-4235-4689-
9f14-351a9268adcc"
  }, {
    "rel" : "editUser",
    "href" : "https://localhost/api/v1/config-services/users/5094e0c3-4235-4689-
9f14-351a9268adcc"
  }, {
    "rel" : "deleteUser",
    "href" : "https://localhost/api/v1/config-services/users/5094e0c3-4235-4689-
9f14-351a9268adcc"
  }, {
    "rel" : "changePassword",
    "href" : "https://localhost/api/v1/config-services/users/5094e0c3-4235-4689-
9f14-351a9268adcc/change-password"
  }, {
    "rel" : "forgotPassword",
    "href" : "https://localhost/api/v1/config-

```

```

services/users/NbUserRepositoryTestLaJKJUpNKR/forgot-password"
  } ]
}, {
  "uuid" : "1eeb8948-2ff5-48c8-a430-9f6bce4e5d81",
  "email" : "nTjWVmvYGA@cisco.com",
  "username" : "NbUserRepositoryTestfJMFnyDFNI",
  "password_expiry_date" : {
    "rfc3339" : "2029-08-04T07:27:09Z",
    "millisecs" : 1880522829905
  },
  "is_super_admin" : false,
  "links" : [ {
    "rel" : "self",
    "href" : "https://localhost/api/v1/config-services/users"
  }, {
    "rel" : "getUser",
    "href" : "https://localhost/api/v1/config-services/users/1eeb8948-2ff5-48c8-
a430-9f6bce4e5d81"
  }, {
    "rel" : "editUser",
    "href" : "https://localhost/api/v1/config-services/users/1eeb8948-2ff5-48c8-
a430-9f6bce4e5d81"
  }, {
    "rel" : "deleteUser",
    "href" : "https://localhost/api/v1/config-services/users/1eeb8948-2ff5-48c8-
a430-9f6bce4e5d81"
  }, {
    "rel" : "changePassword",
    "href" : "https://localhost/api/v1/config-services/users/1eeb8948-2ff5-48c8-
a430-9f6bce4e5d81/change-password"
  }, {
    "rel" : "forgotPassword",
    "href" : "https://localhost/api/v1/config-
services/users/NbUserRepositoryTestfJMFnyDFNI/forgot-password"
  } ]
}, {
  "uuid" : "37190a5b-509c-468e-8736-2188f3d05421",
  "email" : "gOyOvfnfaK@cisco.com",
  "username" : "NbUserRepositoryTestQvfVHhkFdI",
  "password_expiry_date" : {
    "rfc3339" : "2029-08-04T07:27:09Z",
    "millisecs" : 1880522829962
  },
  "is_super_admin" : false,
  "links" : [ {
    "rel" : "self",
    "href" : "https://localhost/api/v1/config-services/users"
  }, {
    "rel" : "getUser",
    "href" : "https://localhost/api/v1/config-services/users/37190a5b-509c-468e-
8736-2188f3d05421"
  } ]
} ]

```

```

    }, {
      "rel" : "editUser",
      "href" : "https://localhost/api/v1/config-services/users/37190a5b-509c-468e-8736-2188f3d05421"
    }, {
      "rel" : "deleteUser",
      "href" : "https://localhost/api/v1/config-services/users/37190a5b-509c-468e-8736-2188f3d05421"
    }, {
      "rel" : "changePassword",
      "href" : "https://localhost/api/v1/config-services/users/37190a5b-509c-468e-8736-2188f3d05421/change-password"
    }, {
      "rel" : "forgotPassword",
      "href" : "https://localhost/api/v1/config-services/users/NbUserRepositoryTestQvfVHhkFdI/forgot-password"
    } ]
  }, {
    "uuid" : "9efd4cc6-0a2d-4d60-943b-6ff87bd2f405",
    "email" : "HkTNGeYLRE@cisco.com",
    "username" : "NbUserRepositoryTestDXDCvvKcgD",
    "password_expiry_date" : {
      "rfc3339" : "2029-08-04T07:27:10Z",
      "milliseconds" : 1880522830003
    },
    "is_super_admin" : false,
    "links" : [ {
      "rel" : "self",
      "href" : "https://localhost/api/v1/config-services/users"
    }, {
      "rel" : "getUser",
      "href" : "https://localhost/api/v1/config-services/users/9efd4cc6-0a2d-4d60-943b-6ff87bd2f405"
    }, {
      "rel" : "editUser",
      "href" : "https://localhost/api/v1/config-services/users/9efd4cc6-0a2d-4d60-943b-6ff87bd2f405"
    }, {
      "rel" : "deleteUser",
      "href" : "https://localhost/api/v1/config-services/users/9efd4cc6-0a2d-4d60-943b-6ff87bd2f405"
    }, {
      "rel" : "changePassword",
      "href" : "https://localhost/api/v1/config-services/users/9efd4cc6-0a2d-4d60-943b-6ff87bd2f405/change-password"
    }, {
      "rel" : "forgotPassword",
      "href" : "https://localhost/api/v1/config-services/users/NbUserRepositoryTestDXDCvvKcgD/forgot-password"
    } ]
  } ],

```

```

    "data_summary" : {
      "links" : [ {
        "rel" : "createUser",
        "href" : "https://localhost/api/v1/config-services/users"
      } ],
      "total_count" : 6,
      "has_more_data" : false
    }
  }
}

```

Response Fields

| Path | Type | Description |
|--|---------|--|
| <code>value.data[].email</code> | String | The user's email address. |
| <code>value.data[].username</code> | String | The user's NAE login username. |
| <code>value.data[].uuid</code> | String | UUID associated to this user. |
| <code>value.data[].password_expiry_date.rfc3339</code> | String | Password expiry date as String. |
| <code>value.data[].password_expiry_date.millisecs</code> | Number | Password expiry date in milliseconds since epoch. |
| <code>value.data[].is_super_admin</code> | Boolean | Indicates whether this user is a super admin. |
| <code>value.data[].links</code> | Array | An array of links relevant to this request. |
| <code>value.data[].links[].rel</code> | String | Self Link |
| <code>value.data[].links[].href</code> | String | Self Link |
| <code>value.data_summary</code> | Object | The number of users returned. |
| <code>value.data_summary.links</code> | Array | An array of links relevant to this request. |
| <code>value.data_summary.links[].rel</code> | String | A keyword indicating the type of link in the "href" field. |
| <code>value.data_summary.links[].href</code> | String | A link to the resource identified by the "rel" keyword. |

Edit User

A **PUT** request updates the email address of the user if a user with the specified ID is present. Only a super administrator can edit the settings of another user.

Example Request

```
PUT /api/v1/config-services/users/5094e0c3-4235-4689-9f14-351a9268adcc HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
Content-Length: 38
```

```
{
  "email" : "yZXIdtPgrJ@cisco.com"
}
```

Example Response

HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 1153

```
{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "uuid" : "5094e0c3-4235-4689-9f14-351a9268adcc",
      "email" : "yZXIdtPgrJ@cisco.com",
      "username" : "NbUserRepositoryTestLaJKJUpNKR",
      "password_expiry_date" : {
        "rfc3339" : "2029-08-04T07:27:09Z",
        "millisecs" : 1880522829844
      },
      "is_super_admin" : false
    },
    "data_summary" : {
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/config-services/users/5094e0c3-4235-4689-9f14-351a9268adcc"
      }, {
        "rel" : "deleteUser",
        "href" : "https://localhost/api/v1/config-services/users/5094e0c3-4235-4689-9f14-351a9268adcc"
      }, {
        "rel" : "changePassword",
        "href" : "https://localhost/api/v1/config-services/users/5094e0c3-4235-4689-9f14-351a9268adcc/change-password"
      }, {
        "rel" : "forgotPassword",
        "href" : "https://localhost/api/v1/config-services/users/NbUserRepositoryTestLaJKJUpNKR/forgot-password"
      } ],
      "total_count" : 1,
      "has_more_data" : false
    }
  }
}
```

Path Parameters

Table 8. `/api/v1/config-services/users/{userId}`

| Parameter | Description |
|---------------------|---------------------------------|
| <code>userId</code> | The UUID of the user to update. |

Response Fields

| Path | Type | Description |
|---|---------|--|
| <code>value.data.email</code> | String | The user's email address. |
| <code>value.data.username</code> | String | The user's NAE login username. |
| <code>value.data.uuid</code> | String | UUID associated to this user. |
| <code>value.data.password_expiry_date.rfc3339</code> | String | Password expiry date as String. |
| <code>value.data.password_expiry_date.milliseconds</code> | Number | Password expiry date in milliseconds since epoch. |
| <code>value.data.is_super_admin</code> | Boolean | Indicates whether this user is a super admin. |
| <code>value.data_summary</code> | Object | The number of users returned. |
| <code>value.data_summary.links</code> | Array | An array of links relevant to this request. |
| <code>value.data_summary.links[].rel</code> | String | A keyword indicating the type of link in the "href" field. |
| <code>value.data_summary.links[].href</code> | String | A link to the resource identified by the "rel" keyword. |

Delete User

A **DELETE** request deletes a user if a user with the specified ID is present. Only a super administrator can delete a user account.

Example Request

```
DELETE /api/v1/config-services/users/caf4b59e-ef31-44cb-a659-3782c8e27e80 HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Example Response

```

HTTP/1.1 200 OK
sessionsToEvictUserId: caf4b59e-ef31-44cb-a659-3782c8e27e80
Content-Type: application/json;charset=UTF-8
Content-Length: 471

{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data_summary" : {
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/config-services/users/caf4b59e-ef31-44cb-a659-3782c8e27e80"
      }, {
        "rel" : "createUser",
        "href" : "https://localhost/api/v1/config-services/users"
      } ],
      "total_count" : 0,
      "has_more_data" : false
    }
  }
}

```

Path Parameters

Table 9. `/api/v1/config-services/users/{userId}`

| Parameter | Description |
|---------------------|---------------------------------|
| <code>userId</code> | The UUID of the user to update. |

Response Fields

| Path | Type | Description |
|--|--------|--|
| <code>value.data_summary</code> | Object | The number of users returned. |
| <code>value.data_summary.links</code> | Array | An array of links relevant to this request. |
| <code>value.data_summary.links[].rel</code> | String | A keyword indicating the type of link in the "href" field. |
| <code>value.data_summary.links[].href</code> | String | A link to the resource identified by the "rel" keyword. |

Update password expiration time

A **PATCH** request updates the password expiration time of the user if a user with the specified ID is present. User with the specified ID will be logged out if the password expires as a result of this

operation. Only a super administrator can update the password expiration time of another user. Administrators can not update their own password expiration time.

Example Request

```
PATCH /api/v1/config-services/users/34189e57-4dcb-4e7a-ad04-0429a1caf37b/change-  
password HTTP/1.1  
Content-Type: application/json  
Accept: application/json  
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER  
Host: localhost:8080  
Content-Length: 54  
  
{  
  "password_expiration_time_milli" : 1564903630174  
}
```

Example Response

HTTP/1.1 200 OK

sessionsToEvictUserId: 34189e57-4dcb-4e7a-ad04-0429a1caf37b

Content-Type: application/json;charset=UTF-8

Content-Length: 1169

```
{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "uuid" : "34189e57-4dcb-4e7a-ad04-0429a1caf37b",
      "email" : "PqizAbYmjx@cisco.com",
      "username" : "NbUserRepositoryTestRecdNMXujp",
      "password_expiry_date" : {
        "rfc3339" : "2019-08-04T07:27:10Z",
        "milliseconds" : 1564903630174
      },
      "is_super_admin" : false
    },
    "data_summary" : {
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/config-services/users/34189e57-4dcb-4e7a-ad04-0429a1caf37b/change-password"
      }, {
        "rel" : "deleteUser",
        "href" : "https://localhost/api/v1/config-services/users/34189e57-4dcb-4e7a-ad04-0429a1caf37b"
      }, {
        "rel" : "changePassword",
        "href" : "https://localhost/api/v1/config-services/users/34189e57-4dcb-4e7a-ad04-0429a1caf37b/change-password"
      }, {
        "rel" : "forgotPassword",
        "href" : "https://localhost/api/v1/config-services/users/NbUserRepositoryTestRecdNMXujp/forgot-password"
      } ],
      "total_count" : 1,
      "has_more_data" : false
    }
  }
}
```

Path Parameters

Table 10. */api/v1/config-services/users/{userId}/change-password*

| Parameter | Description |
|---------------------|--------------------------------|
| <code>userId</code> | The UUID of the user to update |

Response Fields

| Path | Type | Description |
|--|---------|--|
| <code>value.data.email</code> | String | The user's email address. |
| <code>value.data.username</code> | String | The user's NAE login username. |
| <code>value.data.password_expiry_date.rfc3339</code> | String | Password expiry date as String. |
| <code>value.data.password_expiry_date.millisecs</code> | Number | Password expiry date in milliseconds since epoch. |
| <code>value.data.uuid</code> | String | UUID associated to this user. |
| <code>value.data.is_super_admin</code> | Boolean | Indicates whether this user is a super admin. |
| <code>value.data_summary</code> | Object | The number of users returned. |
| <code>value.data_summary.links</code> | Array | An array of links relevant to this request. |
| <code>value.data_summary.links[].rel</code> | String | A keyword indicating the type of link in the "href" field. |
| <code>value.data_summary.links[].href</code> | String | A link to the resource identified by the "rel" keyword. |

Forgot Password

A **POST** request initiates a two-step user password recovery if a user with the specified username is present. For a normal password change by a user, use the [Change User Password](#) API, but if the current password has been forgotten, use this API followed by [Reset Password](#).

The Forgot Password API provides a URL for the next step ([Reset Password](#)) in the response structure at `value.data_summary.links`, where "rel": "resetPassword". The provided URL contains a one-time token for resetting the password.

The Forgot Password API also generates an email with a GUI link for resetting the password. The link in the email contains the one-time token as a URL parameter. Because an email is generated, SMTP must be configured and enabled in the appliance. For information about configuring SMTP, see *Cisco Network Assurance Engine Getting Started Guide*.

Example Request

```
POST /api/v1/config-services/users/NbUserRepositoryTestfJMFnyDFNI/forgot-password
HTTP/1.1
Content-Type: application/json
Accept: application/json
Host: localhost:8080
```

Example Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 536

{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data_summary" : {
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/config-
services/users/NbUserRepositoryTestfJMFnyDFNI/forgot-password"
      }, {
        "rel" : "resetPassword",
        "href" : "https://localhost/api/v1/config-services/users/c03ca3d5-aa31-4ffc-
b21d-84192cf08052/reset-password"
      } ],
      "total_count" : 0,
      "has_more_data" : false
    }
  }
}
```

Path Parameters

Table 11. `/api/v1/config-services/users/{username}/forgot-password`

| Parameter | Description |
|-----------------------|-----------------|
| <code>username</code> | Forgot-password |

Reset Password

A **POST** request resets a forgotten user password to a new password provided in the request structure. This API is the second step in a two-step user password recovery operation. Send this API after you send a [Forgot Password](#) API. The URL of this API must contain a one-time reset token that was provided in the response structure of the [Forgot Password](#) request. The URL form for the Reset Password API is:

```
POST /api/v1/config-services/users/{token}/reset-password
```

For convenience, the [Forgot Password](#) API returns a valid URL for the Reset Password API in the response structure at `value.data_summary.links` under `"rel":"resetPassword"`. To set the new password, call that URL with a request structure that includes the new password, as shown in the

example below.

As an alternative, you can use the password reset link provided in the email generated by the [Forgot Password](#) API to reset the password using a browser.

Example Request

```
POST /api/v1/config-services/users/UAKkTZHbNbVGMBf/reset-password HTTP/1.1
Content-Type: application/json
Accept: application/json
Host: localhost:8080
Content-Length: 82

{
  "new_password" : "WjyTJlSQLgIXCTY",
  "confirm_password" : "WjyTJlSQLgIXCTY"
}
```

Example Response

```
HTTP/1.1 200 OK
sessionsToEvictUserId: 85ade3d3-c4ec-43bf-bba4-049114d4c8f7
Content-Type: application/json;charset=UTF-8
Content-Length: 398

{
  "success" : true,
  "messages" : [ {
    "code" : 9007,
    "severity" : "INFO",
    "message" : "The password for user NbUserRepositoryTestHgShueWubH has been
successfully changed"
  } ],
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data_summary" : {
      "links" : [ ],
      "total_count" : 0,
      "has_more_data" : false
    }
  }
}
```

Path Parameters

Table 12. `/api/v1/config-services/users/{token}/reset-password`

| Parameter | Description |
|-----------|--|
| token | Token generated when password recovery is initiated. |

Session Management Operations

Use the APIs in this section to view or delete active user sessions in Cisco NAE.

These APIs require an active authenticated API session. The following table shows the role requirements for executing these APIs.

| Operation | Minimum Role |
|---------------------------------------|---------------------|
| View All Sessions | Super Administrator |
| View a Single Session | Super Administrator |
| Delete a Session | Super Administrator |

View All Sessions

Request

```
GET /api/v1/sessions HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Response

HTTP/1.1 200 OK

Content-Type: application/json;charset=UTF-8

Content-Length: 1050

```
{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : [ {
      "session_id" : "c467b7c4-f1a9-4c00-8a15-7dad5cb6fbe7",
      "username" : "admin",
      "domain" : "Local",
      "created_time" : {
        "rfc3339" : "2019-08-04T07:24:39Z",
        "milliseconds" : 1564903479855
      },
      "last_accessed_time" : {
        "rfc3339" : "2019-08-04T07:24:39Z",
        "milliseconds" : 1564903479855
      },
      "expire_time" : {
        "rfc3339" : "2019-08-04T07:54:39Z",
        "milliseconds" : 1564905279855
      },
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/sessions/c467b7c4-f1a9-4c00-8a15-7dad5cb6fbe7"
      } ]
    } ],
    "data_summary" : {
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/sessions?$page=0&$size=50"
      } ],
      "total_count" : 1,
      "has_more_data" : false,
      "page_size" : 50,
      "current_page_number" : 0,
      "total_page_count" : 1
    }
  }
}
```

Request Parameters

| Parameter | Description |
|-------------------------|---|
| <code>\$domain</code> | An optional parameter to specify the domain user belongs to. |
| <code>\$username</code> | An optional parameter to specify the username of the user that session belongs to. Username can be used only in combination with domain query param |
| <code>\$page</code> | The page number of the paginated results to return. It is an optional param, and defaults to 0 if not specified. 'data_summary' element in the response provides links to fetch data for remaining pages. |
| <code>\$size</code> | An optional parameter to specify the number of epochs to return in a single page. Defaults to 50 if not specified. |

Response Fields

| Path | Type | Description |
|---|--------|--|
| <code>value.data[].session_id</code> | String | Sessions ID |
| <code>value.data[].username</code> | String | Username associated with this session |
| <code>value.data[].domain</code> | String | Domain associated with the user |
| <code>value.data[].created_time.rfc3339</code> | String | Time at which the session is created, in RFC format |
| <code>value.data[].created_time.milliseconds</code> | Number | Time at which the session is created, in milliseconds |
| <code>value.data[].last_accessed_time.rfc3339</code> | String | Time at which the session is last accessed, in RFC format |
| <code>value.data[].last_accessed_time.milliseconds</code> | Number | Time at which the session is last accessed, in milliseconds |
| <code>value.data[].expire_time.rfc3339</code> | String | Time at which the session is expired, in RFC format |
| <code>value.data[].expire_time.milliseconds</code> | Number | Time at which the session is expired, in milliseconds |
| <code>value.data[].links</code> | Array | Provides links to access further relevant information for this session |
| <code>value.data[].links[].rel</code> | String | A link to the resource identified by the "rel" keyword |
| <code>value.data[].links[].href</code> | String | A keyword indicating the type of link in the "href" field |
| <code>value.data_summary</code> | Object | Summary of the sessions returned |

| Path | Type | Description |
|--|--------|---|
| value.data_summary.links | Array | An array of links relevant to this request |
| value.data_summary.links.[].rel | String | A link to the resource identified by the "rel" keyword |
| value.data_summary.links.[].href | String | A keyword indicating the type of link in the "href" field |
| value.data_summary.page_size | Number | Page size requested |
| value.data_summary.current_page_number | Number | Response page number |
| value.data_summary.total_page_count | Number | Total number of pages in response |

View a Single Session

Request

```
GET /api/v1/sessions/c467b7c4-f1a9-4c00-8a15-7dad5cb6fbe7 HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Response

HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 989

```
{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data" : {
      "session_id" : "c467b7c4-f1a9-4c00-8a15-7dad5cb6fbe7",
      "username" : "admin",
      "domain" : "Local",
      "created_time" : {
        "rfc3339" : "2019-08-04T07:24:39Z",
        "milliseconds" : 1564903479855
      },
      "last_accessed_time" : {
        "rfc3339" : "2019-08-04T07:24:39Z",
        "milliseconds" : 1564903479855
      },
      "expire_time" : {
        "rfc3339" : "2019-08-04T07:54:39Z",
        "milliseconds" : 1564905279855
      },
      "links" : [ ]
    },
    "data_summary" : {
      "links" : [ {
        "rel" : "self",
        "href" : "https://localhost/api/v1/sessions/c467b7c4-f1a9-4c00-8a15-7dad5cb6fbe7"
      }, {
        "rel" : "deleteSession",
        "href" : "https://localhost/api/v1/sessions/c467b7c4-f1a9-4c00-8a15-7dad5cb6fbe7"
      } ],
      "total_count" : 1,
      "has_more_data" : false
    }
  }
}
```

Response Fields

| Path | Type | Description |
|-----------------------|--------|-------------|
| value.data.session_id | String | Sessions ID |

| Path | Type | Description |
|--|--------|--|
| value.data.username | String | Username associated with this session |
| value.data.domain | String | Domain associated with the user |
| value.data.created_time.rfc3339 | String | Time at which the session is created, in RFC format |
| value.data.created_time.milliseconds | Number | Time at which the session is created, in milliseconds |
| value.data.last_accessed_time.rfc3339 | String | Time at which the session is last accessed, in RFC format |
| value.data.last_accessed_time.milliseconds | Number | Time at which the session is last accessed, in milliseconds |
| value.data.expire_time.rfc3339 | String | Time at which the session is expired, in RFC format |
| value.data.expire_time.milliseconds | Number | Time at which the session is expired, in milliseconds |
| value.data.links | Array | Provides links to access further relevant information for this session |
| value.data_summary | Object | Summary of the session returned |
| value.data_summary.links | Array | An array of links relevant to this request |
| value.data_summary.links[].rel | String | A link to the resource identified by the "rel" keyword |
| value.data_summary.links[].href | String | A keyword indicating the type of link in the "href" field |

Delete a Session

Request

```
DELETE /api/v1/sessions/41b7331d-f4a1-48c2-b054-3f6d4083d44f HTTP/1.1
Content-Type: application/json
Accept: application/json
X-NAE-CSRF-TOKEN: CANDID_CSRF_TOKEN_HEADER
Host: localhost:8080
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: 227

{
  "success" : true,
  "value" : {
    "namespaces" : {
      "default" : "https://www.cisco.com/api/schema"
    },
    "data_summary" : {
      "links" : [ ],
      "total_count" : 0,
      "has_more_data" : false
    }
  }
}
```

Path Parameters

Table 13. `/api/v1/sessions/{sessionId}`

| Parameter | Description |
|------------------------|-----------------------------------|
| <code>sessionId</code> | The UUID of the session to delete |

Common Workflows



This document describes the features, operation, and syntax of the Cisco Network Assurance Engine (NAE) REST API as of the current release when written. The features, operation, and syntax of the API are subject to change in future releases, and Cisco cannot guarantee backwards compatibility with prior releases.

Smart Events Workflow

In this workflow example, we fetch the details of a smart event from a specific epoch in our ACI fabric using the Cisco NAE REST API. The summary steps to accomplish this result are as follows:

- Log in to the REST API
- Specify (create) an ACI fabric for analysis
- Start an online analysis on the fabric
- Get a list of the available epochs
- Get a specific epoch (or the latest epoch)
- Get a filtered smart event summary for the epoch
- Get details about a specific smart event

This example assumes that an ACI fabric is installed and operational, has a functioning APIC cluster, and has an available APIC administrator account.

To complete the workflow, perform the following steps:

1. Authenticate and open an API session as described in the [Login Example](#). This step returns a session token that must be included in the subsequent steps.

```
GET /api/v1/whoami
POST /api/v1/login
```

2. Specify the ACI fabric to be analyzed, as demonstrated in [Create a fabric](#). You must specify the hostname or hostnames of an existing fabric, along with the APIC administrator credentials. You may also specify some parameters of the analysis, such as the polling interval. This operation returns the unique fabric ID.

```
POST /api/v1/config-services/assured-networks/aci-fabric
```

3. Using the unique fabric ID, begin an online analysis of the fabric, as demonstrated in [Start Online Analysis](#). Data is collected and analyzed at regular intervals (epochs) that you specified in the previous step.


```
POST /api/v1/config-services/assured-networks/aci-fabric/{FABRIC-ID}/start-analysis
```

4. After a period of time, request a list of the available epochs, as demonstrated in [Get Epochs of an ACI Fabric](#).

```
GET /api/v1/event-services/epochs?$fabric_id={FABRIC-ID}
```

5. Depending on when an event of interest has occurred, request the records of [a specific epoch](#) by its unique epoch ID or of [the latest epoch](#).

```
GET /api/v1/event-services/epochs?$epoch_id={EPOCH-ID}  
or  
GET /api/v1/event-services/epochs?$page=0&$size=1&$sort=-analysis_start_time
```

6. For the chosen epoch, request a summary of the smart events. As shown in [Get An Epoch](#), several request parameters are available to restrict the summary to include only those smart events of interest. The example below returns only critical and major system events for the epoch.

```
GET /api/v1/event-services/smart-events?$epoch_id={EPOCH-ID}&category=SYSTEM&severity=EVENT_SEVERITY_CRITICAL,EVENT_SEVERITY_MAJOR
```

7. Using the unique event ID of a specific smart event in the summary, request its detailed record, as demonstrated in [Get Smart Event Detail](#).

```
GET /api/v1/event-services/smart-events/detail?$event_id={EVENT-ID}
```

Pagination Workflow

This workflow example demonstrates how to fetch the records of a specific epoch that holds multiple pages of event records. We can then use the [Pagination Links](#) in the response structure to fetch the next page and the last page, and we can modify a link to fetch a specific page.

1. Request the records of [a specific epoch](#) by its unique epoch ID.

```
GET /api/v1/event-services/epochs?$epoch_id={EPOCH-ID}
```

2. In the response structure, examine the links in `value.data_summary.links`. In the example below, the "total_page_count" indicates that there are 20 pages of records found for this epoch. This response contains the first page, which is page 0. The structure contains direct links for you to request the first page, the next page, or the last page.

```

"data_summary" : {
  "links" : [ {
    "rel" : "first",
    "href" : "https://localhost/api/v1/event-services/epochs?$page=0&$size=1"
  }, {
    "rel" : "self",
    "href" : "https://localhost/api/v1/event-services/epochs?$page=0&$size=1"
  }, {
    "rel" : "next",
    "href" : "https://localhost/api/v1/event-services/epochs?$page=1&$size=1"
  }, {
    "rel" : "last",
    "href" : "https://localhost/api/v1/event-services/epochs?$page=19&$size=1"
  } ],
  "total_count" : 20,
  "has_more_data" : true,
  "page_size" : 1,
  "current_page_number" : 0,
  "total_page_count" : 20
}

```

- To view the next page of records, send a GET request to the link contained in the "href" field associated with "rel":"next". The response structure of the each subsequent page will in turn contain links to the previous, next, and last pages.

```
GET /api/v1/event-services/epochs?$page=1&$size=1
```

- To view the last page of records, send a GET request to the link contained in the "href" field associated with "rel":"last":

```
GET /api/v1/event-services/epochs?$page=19&$size=1
```

- To view the a specific page of records, such as page 5, modify a link by setting the \$page URL parameter to the desired page number (note that the pages are numbered from 0). Send a GET request to the resulting link, as in this example for page 5:

```
GET /api/v1/event-services/epochs?$page=5&$size=1
```

Password Reset Workflow

This workflow example demonstrates how to recover from a lost user password. This is a two-step procedure in which the user obtains a one-time token from the Cisco NAE appliance and then submits the token along with a new password.



This procedure is for resetting a password when the current password has been forgotten. For a normal password change by a user, use the [Change User Password API](#).

1. To initiate the password recovery, send a [Forgot Password](#) request with the unique ID of the user in the URL:

```
POST /api/v1/config-services/users/{USER-ID}/forgot-password
```

2. In the `value.data_summary.links` field of the response structure, locate the "href" field associated with "rel":"resetPassword". This field contains a [Reset Password](#) URL that includes a one-time token for resetting the password, as shown in this example:

```
{
  "rel" : "resetPassword",
  "href" : "https://localhost/api/v1/config-services/users/3e00b524-8e2c-4233-a32f-120da7d6e540/reset-password"
}
```

3. Send a POST request to the URL with a message body containing the new password, as shown in this example:

```
POST /api/v1/config-services/users/{TOKEN}/reset-password
{
  "new_password" : "xjZXZBYaiCsRa0c",
  "confirm_password" : "xjZXZBYaiCsRa0c"
}
```



The Forgot Password API also generates an email with a GUI link for resetting the password. The link in the email contains the one-time token as a URL parameter. Because an email is generated, SMTP must be configured and enabled in the appliance. For information about configuring SMTP, see *Cisco Network Assurance Engine Getting Started Guide*.

Status and Error Codes

HTTP Status Codes

For any REST API request, the response from the Cisco NAE REST API server contains an HTTP status code that indicates whether the request was successful, along with other information related to the request. The following table lists supported HTTP status codes.

| HTTP Status Code | HTTP method | Description |
|------------------|----------------------|--|
| 101 | Web Socket request | The server has accepted a protocol upgrade request to open a websocket connection to the Cisco NAE REST API server. |
| 200 | GET/PUT/PATCH/DELETE | The request was completed successfully. Additional details about the request are contained in the response payload, as explained in Response Payload Structure . |
| 201 | POST | The request was completed successfully and a resource has been created. The Location header in the response contains the URL for the resource. |
| 202 | GET/POST/PUT/DELETE | A request for a long running operation has been accepted and the operation is being completed asynchronously. This exchange is used infrequently in GET operations and is more commonly used in POST/PUT/DELETE. The body of the HTTP response contains additional information for tracking the progress of the request. |
| 304 | GET/POST/PUT/DELETE | The requested content has not been modified since a previous request. |
| 400 | POST/PUT/DELETE | A write operation is rejected due to validation errors detected by the server. |
| 401 | GET/POST/PUT/DELETE | The requested operation is rejected because it requires authentication that was not provided by the user. |

| HTTP Status Code | HTTP method | Description |
|-------------------------|---------------------|---|
| 403 | GET/POST/PUT/DELETE | The requested operation is rejected because the user does not have the necessary permissions to access the resource. |
| 404 | GET/PUT/DELETE | The requested operation is rejected because the specified resource does not exist. |
| 405 | GET/POST/PUT/DELETE | The requested operation is rejected because the specified resource does not support that operation. |
| 409 | POST/PUT/DELETE | The requested operation is rejected due to a conflict, such as an attempt to create a resource that already exists. |
| 415 | POST/PUT/DELETE | The requested operation is rejected because the specified resource does not support the uploaded media type of the request. |
| 429 | GET/POST/PUT/DELETE | The requested operation is rejected because the client has sent too many requests in a given time period. |
| 500 | GET/POST/PUT/DELETE | The requested operation is rejected due to an internal server error. The response payload may contain additional information about the error. This condition may require assistance from your Cisco representative. |
| 502 | GET/POST/PUT/DELETE | An invalid response was received from the server. |
| 503 | GET/POST/PUT/DELETE | The server is currently unable to handle the request due to a temporary overloading or maintenance of the server. |
| 504 | GET/POST/PUT/DELETE | The requested operation timed out while waiting for a response from the server. |

Cisco NAE Status and Error Codes

The response structure returned by an API query may contain one or more status or error codes in

the `messages` field. The following tables show some of the more common code categories and codes.

System Codes

| Code | Description |
|------|--|
| 5000 | The requested resource {0} does not exist on this server |
| 5001 | The request failed with the following error: {0}. Contact your administrator |
| 5002 | The requested page size {0} is greater than system supported maximum limit. Only maximum of {1} values will be returned |
| 5003 | Invalid value specified for request param {0} |
| 5004 | Invalid HTTP method {0} for request |
| 5005 | The request made to the server is not valid |
| 5006 | The input provided to the REST API method is not valid. |
| 5007 | Unknown query param(s) {0} specified |
| 5008 | {0} must not be greater than {1} |
| 5009 | {0} cannot be in the future |
| 5010 | {0} param must be specified along with {1} |
| 5011 | Invalid value specified for param {0}. Valid values are: {1} |
| 5012 | {0} param is incompatible with {1} param. Specify only one of them. |
| 5013 | No epochs found in the given time range. |
| 5015 | {0} object is created. |
| 5016 | {0} request is accepted, but not complete. |
| 5017 | Param(s) {0} must be specified in request url |
| 5018 | The requested resource: {0} does not exist on this server given the provided parameters |
| 5019 | The param EPG_PAIR requires one comma to separate the EPG DNs |
| 5020 | {field} is a required field and cannot be null |
| 5021 | The requested resource: {0} does not exist on this server because there are no epochs in the database. |
| 5022 | {0} must not be an empty string. |
| 5023 | Specified value {0} for input {1} is not valid |
| 5024 | The number of {0} returned by the request {1} is larger than the maximum {2} supported by the server. Apply some filters to reduce the returned result set and try again |
| 5025 | {0} is an unsupported filter or sort parameter |
| 5026 | {validatedValue} is not a valid input param |
| 5027 | Installation has already been completed |
| 5030 | The requested resource is already being modified |
| 5032 | The requested resource already exists |

| Code | Description |
|------|---|
| 5033 | Invalid Parameter Syntax |
| 5034 | Could not download the file. {0} |
| 5035 | Datastore storage path db.storage.path must be set correctly in properties file |
| 5036 | Could not persist {0} for {1} |
| 5037 | Information not found. Unsupported char(s) included in search parameter. |
| 5038 | One or more IP addresses or host names are invalid. |
| 5039 | Requested Operation is allowed only for Super Admins |
| 5040 | Requested Operation is allowed only for users from Local domain |
| 5041 | No data found with the provided request params. |
| 5042 | Missing required query param(s) {0} |
| 5050 | Request payload contained an unrecognized field : {0} |
| 5051 | The input JSON syntax was not valid. Error message:{0} |
| 5053 | Required request body is missing |

Authentication Codes

| Code | Description |
|------|--|
| 7000 | The One Time Password (OTP) password was either not specified or has expired and is no longer valid |
| 7001 | The session has either expired or is not valid |
| 7002 | Invalid username and/or password |
| 7003 | The user is already authenticated to this session |
| 7004 | The user is not authorized to make this request |
| 7005 | User is not authenticated. Use One Time Password found in the response header {0} within the next {1} minutes to login |
| 7006 | The password was not changed because the old and the new passwords did not match. |
| 7007 | CSRF token verification failed. |
| 7008 | X-NAE-CSRF-TOKEN header is missing. |
| 7009 | Cannot authenticate the credentials against the given authentication domain. |
| 7010 | Account is locked. Please contact your administrator |
| 7011 | Username and Password are mandatory fields. Provide valid credentials |
| 7012 | The password is expired. You must change your password before proceeding |

User Management Codes

| Code | Description |
|------|---|
| 9000 | The user with username {0} already exists |

| Code | Description |
|------|--|
| 9002 | The user with username {0} cannot change the password of the user {1} |
| 9003 | The user with username {0} cannot create user. Only a Super Admin can create users |
| 9004 | The length of the password must be between {min} and {max} characters |
| 9005 | The current password is incorrect. |
| 9006 | The new password does not match the confirm password |
| 9007 | The password for user {0} has been successfully changed |
| 9010 | Token has expired or is invalid. |
| 9011 | Password recovery is already in progress for {0}. Wait for {1} minutes before reattempting recovery if you have lost your password recovery token. |
| 9012 | Change password request failed due to {0} |
| 9013 | The email address already exists. It might be assigned to an inactive or deleted user. |
| 9014 | The user with username {0} cannot change the email address of the user {1} |
| 9015 | User {0} cannot delete user. Only Super admin can delete users. |
| 9016 | User {0} does not exist |
| 9017 | Super admin can not be deleted |
| 9018 | {0} operation failed as either user is not ready for update or account is locked. |
| 9019 | Username must have 4 to 30 alphanumeric characters with optional single dots placed in between words |
| 9020 | Maximum {0} users are allowed to be added. |
| 9021 | Invalid email address |
| 9022 | value must be greater than {value} day |
| 9023 | Invalid password. Allowed characters are {0}. The length of the password must be between {1} and {2} characters |

Epoch Codes

| Code | Description |
|-------|---|
| 11000 | Invalid epoch {0}. Epoch must be a long value or \$latest |
| 11001 | Invalid epoch {0} for specified fabric {1} |

Session Codes

| Code | Description |
|-------|---|
| 25003 | Cannot delete the current logged in session |

Related Documentation

The following companion guides provide documentation for Cisco NAE:

- *Cisco Network Assurance Engine Release Notes*
- *Cisco Network Assurance Engine Getting Started Guide*
- *Cisco Network Assurance Engine Fundamentals Guide*
- *Cisco Network Assurance Engine Smart Events Reference Guide*

A complete and interactive REST API reference is embedded in the Cisco NAE at this URL:

https://<Your_NAE_Appliance>/api/v1/swagger-ui.html

For information about the REST API reference, see [About The REST API Reference \(Swagger\)](#).

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to cisconae-docfeedback@cisco.com. We appreciate your feedback.