REST API Solutions Guide

22.4R1

Copyright Notice

Contents

END USER LICENSE AGREEMENT

The Ivanti product that is the subject of this technical documentation consists of (or is intended for use with) Ivanti software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at https://www.ivanti.com/company/legal/eula. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in [[[Undefined variable Custom.Company_Name]]] technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
italic text	Identifies emphasis
	Identifies variables
	Identifies document titles
`Courier Font`	Identifies command output
	Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Non-printing characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member[member...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.
bold text	Identifies command names, keywords, and command options.

Code Block

Following is an example of Python based code block in the html documentation:

```
def some_function():
interesting = False
print 'This line is highlighted.'
print 'This one is not...'
print '...but this one is.'
```

Notes and Warnings

Note, Attention, and Caution statements might be used in this document.

A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

Requesting Technical Support

Technical product support is available through the Global Support Center (GSC). If you have a support contract, file a ticket with GSC.

- Product warranties—For product warranty information, visit https://forums.ivanti.com/s/all-products

Self-Help Online Tools and Resources

For quick and easy problem resolution, Ivanti provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://forums.ivanti.com/s/contactsupport
- Search for known bugs: https://forums.ivanti.com/s/contactsupport
- Find product documentation: https://forums.ivanti.com/s/contactsupport
- Download the latest versions of software and review release notes: https://forums.ivanti.com/s/contactsupport
- Open a case online in the CSC Case Management tool: https://forums.ivanti.com/s/contactsupport
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://forums.ivanti.com/s/contactsupport

For important product notices, technical articles, and to ask advice:

- Search the Ivanti Knowledge Center for technical bulletins and security advisories: https://forums.ivanti.com/s/searchallcontent
- Ask questions and find solutions at the Community online forum: https://forums.ivanti.com/

Opening a Case with Support Center

You can open a case with support center on the Web or by telephone.

- Use the Case Management tool in the support center at https://forums.ivanti.com/s/contactsupport.

For international or direct-dial options in countries without toll-free numbers, see https://forums.ivanti.com/s/contactsupport

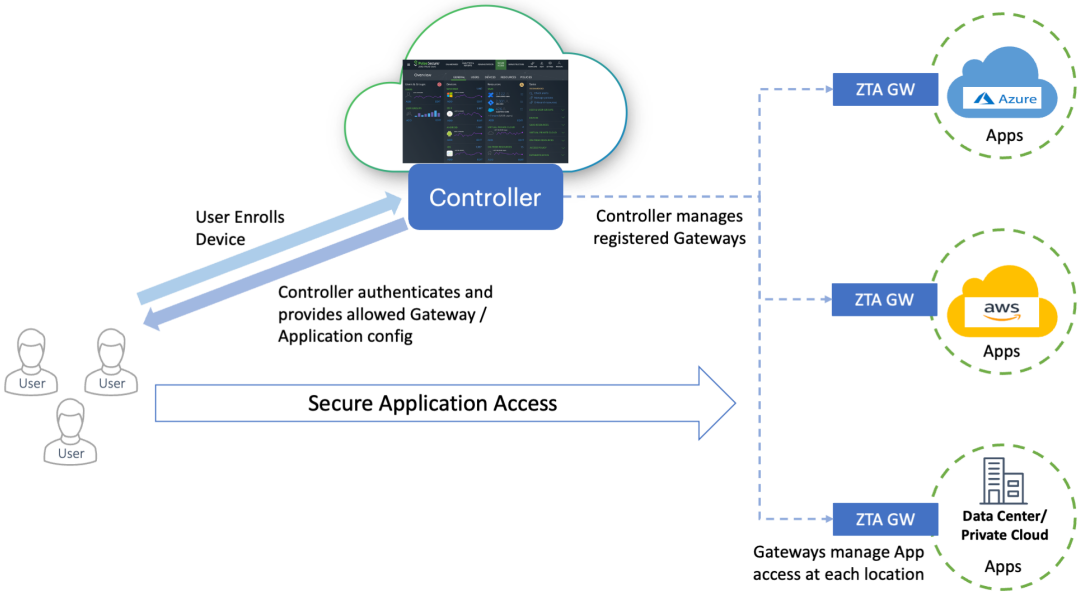
Reporting Documentation Issues

To report any errors or inaccuracies in ivanti technical documentation, or to make suggestions for future improvement, contact ivanti Technical Support (https://forums.ivanti.com/s/contactsupport). Include a full description of your issue or suggestion and the document(s) to which it relates.

Ivanti Neurons for Zero Trust Access Overview

Ivanti Neurons for Zero Trust Access (*nZTA*) is a cloud-based SaaS (software as a service) application that provides fully-managed zero-trust authentication and access control for an organization's application infrastructure. *nZTA* enables administrators to define end-to-end authorization and authentication policies that control application visibility, access, and security for all users and their devices.

The diagram below illustrates the different components in *nZTA*:



A typical *nZTA* deployment

To learn more about *nZTA*, see the *Tenant Admin Guide*.

This guide describes the REST API service running on the *Controller* and includes a list of supported API calls.

Retrieving the Authentication DSID

The Data Set Identification (DSID) is required for API use.

The following CURL command format uses the DSID to query the REST API server:

```
curl -v --cookie "DSID=<value>" <api_request_url>
```

The DSID can be retrieved in two ways:

- Using the *nZTA* API, see Retrieving the DSID Using the API.
- Using a browser, see Retrieving the DSID Using a Browser.

Retrieving the DSID Using the API

You can use the following code to get a DSID token to use across all API calls:

```
      def login(url,username,password):
    tenant_url = url
    return_dict = {'status': 0}
    global user_session, dsid
    login_URL = tenant_url + '/login/admin'
    data = {
        'username': username,
        'password': password,
        'realm': 'ZTA Admin Users',
        'btnSubmit': 'Submit',
        }
    user_session = requests.session()
    r = user_session.get(url=login_URL, verify=False)
    dssignin = user_session.cookies.get('DSSIGNIN')
    data = {'username': username,'password': password,'realm': 'ZTA Admin
Users','btnContinue':
     'Continue the session'}
    login_cgi = url + '/dana-na/auth/' + dssignin + '/login.cgi'
    print login_cgi
    r = user_session.post(url=login_cgi, verify=False, data=data)
    print('login status code: ', +r.status_code)
    print('Login_data: ', user_session.cookies)
    d = str(r.content)
    if 'Continue the session' in d:
        formdatastr = xsauth = None
        try:
            p = r'.*name="FormDataStr" value="(.*?)">'
            x = re.findall(p, d)
            formdatastr = x[0]
        except IndexError:
            print 'Error: unable to get FormDataStr value'
        try:
            p = r'.*name="xsauth" value="(.*?)"'
            x = re.findall(p, d)
            xsauth = x[0]
        except IndexError:
            print 'Error: unable to get xsauth value'
        data = {'FormDataStr': formdatastr, 'xsauth': xsauth,
                'btnContinue': 'Continue the session'}
        login_cgi = url + '/dana-na/auth/' + dssignin + '/login.cgi'
        r = user_session.post(url=login_cgi, verify=False, data=data,
                              allow_redirects=True)
    dsid = user_session.cookies.get('DSID')
    print ('DSID: ', dsid)
```

```
    cookies["DSID"]=dsid
    if dsid is None:
        raise Exception('LoginError: Unable to get DSID cookie')
            # self.cookie = dsid
    session = user_session
```

After the DSID is set in the cookies (refer to code `dsid = user_session.cookies.get('DSID')`) use that session for all other API Calls.

You can use the following CURL command format uses the DSID to query the REST API server:

```
      curl -v --cookie "DSID=<value>" <api_request_url>
```

The following code demonstrates how to get a list of secure access policies using the API. It updates the cookie information for DSID from the above code.

```
        def get_secure_access_policies():
    input_payload = {"type": "application"}
    request_uri = host_url + api_version + "policies/secure-access-
policies"
    output = requests.get(request_uri, params=input_payload,
cookies=cookies)
    status_code = output.status_code
    response_json = output.json()
    print response_json
```

Retrieving the DSID Using a Browser

You can use a browser to access the DSID. The procedure below describes the process for the *Chrome* browser, but any browser that offers similar tools can also be used.

1. Start the *nZTA* user interface in the *Chrome* browser.

   The home page appears.

2. Right-click the main map, and select **Inspect** from the context menu.

   The screen divides horizontally and the element view appears to the right of the screen.

In the *Edge* browser, you click the **...** control, and then click **Other Tools > Developer Tools**. In the *Firefox* browser, you right-click and select **Inspect Element** from the context menu.

3. In the element view, select the **Network** tab.

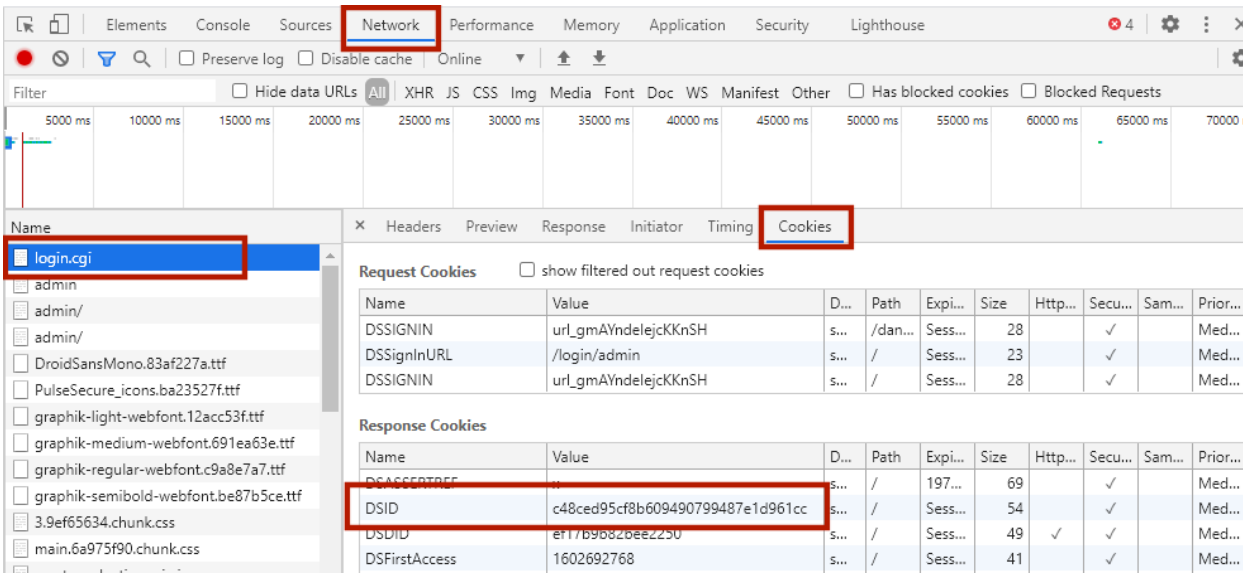
4. Select an element from the list of elements (on the left of the tab). For example, *login*, *admin* or *subscriptions*.

   A tab bar appears (on the right of the tab).

5. Select the **Cookies** tab.

   A list of cookies for the page appears.

6. For the *DSID* entry, copy the DSID value and retain this value for future use. For example:



Element View in Chrome Browser

You can use the following CURL command format uses the DSID to query the REST API server:

```
curl -v --cookie "DSID=<value>" <api_request_url>
```

API Calls

This chapter describes the *Ivanti Neurons for Zero Trust Access* (*nZTA*) entities and the API calls that can be made to them.

- Analytics, see Analytics.
- Applications, see Applications (resources).
- Authentication Servers, see Authentication Server (auth-servers).
- Device Policies, see Device Policies (device-policy/groups).
- Device Policy Rules, see Device Policy Rules (device-policy/rules).
- Gateways, see Gateway (gateways).
- Gateway Settings, see Gateway Settings.
- Gateway Groups, see Gateway Group (groups).
- Hostchecker Levels, see Hostchecker Levels (hostchecker/levels).
- Hostchecker Products, see Hostchecker Products (hostchecker/products).
- Resources, see "Applications" and "User Policies".
- Resource Groups, see Resource Group (resource-groups).
- Role Mapping Rules, see Role Mapping Rules (role-mapping-rules).
- Secure Access Policies, see Secure Access Policy (secure-access-policies).
- Enterprise Integrations Syslog Server Configuration, see Enterprise Integrations Configurations Service (integrations/syslog).
- Users, see Users (users).
- User Rule Groups, see User Rule Groups (user-rule-groups).
- User Policies, see User Policies (resources).
- Lockdown exceptions, see Lockdown Exceptions
- MDM Server, see MDM Server

For all calls, the following CURL command format uses the DSID cookie to query the REST API server:

```
curl -v --cookie "DSID=<value>" <api_request_url>
```

For a worked example of *nZTA* entity use, see Ivanti Neurons for Zero Trust Access Use Case.

Analytics

The *analytics* resource provides API calls for components and elements within the **Insights** analytics pages of the Tenant Admin Portal. Analytics supports the following Network Overview activities:

- Retrieving data for the Summary Ribbon, see Retrieving Analytics Data for the Summary Ribbon.
- Retrieving data for the World Map Gateway Locations view, see Retrieving Analytics Data for the World Map Gateway Location View.
- Retrieving data for the World Map Users view, see Retrieving Analytics Data for the World Map Users View.
- Retrieving data for the Sankey chart view, see Retrieving Analytics Data for the Sankey Chart View.
- Retrieving data for the Top Active Gateways chart, see Retrieving Analytics Data for the Top Active Gateways Chart.
- Retrieving data for the Top Active Applications chart, see Retrieving Analytics Data for the Top Active Applications Chart.
- Retrieving data for the Top Active User Locations chart, see Retrieving Analytics Data for the Top Active User Locations Chart.
- Retrieving data for the Active Anomalies chart, see Retrieving Analytics Data for the Active Anomalies Chart.
- Retrieving data for the Connected Clients Version chart, see Retrieving Analytics Data for the Connected Clients Version Chart.
- Retrieving data for the Non-compliances chart, see Retrieving Analytics Data for the Non-compliances Chart.
- Retrieving data for the Gateways Info-panel, see Retrieving Analytics Data for the Gateways Info-panel.
- Retrieving data for the Users Info-panel, see Retrieving Analytics Data for the Users Info-panel.
- Retrieving data for the Devices Info-panel, see Retrieving Analytics Data for the Devices Info-panel.
- Retrieving data for the Applications Info-panel, see Retrieving Analytics Data for the Applications Info-panel.

- Retrieving data for the Non-compliances Info-panel, see Retrieving Analytics Data for the Non-compliances Info-panel.
- Retrieving data for the Anomalies Info-panel, see Retrieving Analytics Data for the Anomalies Info-panel.

The analytics resource also provides the following Logs activity:

- Retrieving log data, see Retrieving Log Data.

The analytics resource also provides the following Gateways activity:

- Retrieving Gateway metrics, see Retrieving Aggregated Gateway Statistics.

Retrieving Analytics Data for the Summary Ribbon

To retrieve a resource containing Summary Ribbon totals, use the REST API call below:

- **Method:** POST /api/analytics/summary
- **Resource:** Path
- **JSON Data:** JSON data structure representing the **CommonFilterObject** schema (see Schema) - containing date/time period selection, and optional filter for gateway selection.

If processed correctly, a JSON body containing the *analytics/summary* entity is returned. Otherwise, a JSON body containing an error is returned.

Schema

The **CommonFilterObject** schema entity contains the following fields:

```
current_time            integer
                        example: 1580515200
                        The time at which landing page was loaded. This
                        is used to make sure that all the components on
                        landing
                        page have the same reference so that they
                        summarize the same data set.
start_time              integer
                        example:
                        1580515200
```

	Start time (epoch). This needs to be the starting time for the selected time_duration_type below. Selecting current day will result in displaying data from start of the current day (in UTC) e.g., - Selecting day for time_duration_type indicates this value should be start of the calendar day (in UTC) * Selecting week for time_duration_type indicates this value should be start of the calendar week (in UTC) * Selecting month for time_duration_type indicates this value should be start of the calender month (in UTC) * When time_duration_type is active, the start_ time will be ignored. Only (current_time) and (current_time - Active Window Period) will be considered as time duration
time_duration_type	string example: day default: active Details of what unit of time duration need to be considered for the data. Enum: [active, current_day, day, week, month, last_24_ hours, custom]
timezone_offset	integer example: 330
gateway_type	string nullable: true example: pcs default: zta Type of the gateway Enum: [zta, pcs, pps, vtm]
overlay_filter_type	string example: non_compliance_users

```
                        Dashboard overlay text filter type
                        Enum:

                        [ connected_users_in_last_one_hour, non_
                        compliance_users, connected_users_in_more_than_
                        one_day, users_from_most_busy_gateway, users_
                        from_least_busy_gateway, top_risky_users, geo_
                        anomaly_users, user_roles_with_most_non_
                        compliances, top_users_with_auth_failures, users_
                        with_mfa ]
global_filter           {
                              description: Global filter object that is
                              applicable for all pages. If both overlay_
                              filter_type and global_filter are set, only
                              global_fiter would be used
                              gateway_ids  Array [ string ]
                              example: List [ "74h4h3-u43943-4u3o4",
                              "84h4h3-u43943-4u3o5" ]
                              default: List []

                              Filtering based on multiple gateway_ids.
                        }

                        nullable: true
```

Request

The following is an example request:

```
      POST /api/analytics/summary
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648119483,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  [
    {
      "actual_value": 3,
      "description": "Active users",
      "line_graph_color": "green",
      "line_graph_data": [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        1,
        3
      ],
      "name": "users",
      "status": 0,
      "total_value": 1000,
      "trend_delta": 3,
      "trend_direction": "up"
    },
    {
      "actual_value": 3,
      "description": "Active devices",
      "line_graph_color": "green",
      "line_graph_data": [
        0,
        0,
        0,
        0,
        0,
```

```
        0,
        0,
        0,
        0,
        0,
        0,
        1,
        3
      ],
      "name": "devices",
      "status": 100,
      "total_value": 13,
      "trend_delta": 3,
      "trend_direction": "up"
    },
    {
      "actual_value": 2,
      "description": "Active gateways",
      "line_graph_color": "green",
      "line_graph_data": [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        1,
        2
      ],
      "name": "gateways",
      "status": 0,
      "total_value": 6,
      "trend_delta": 2,
      "trend_direction": "up"
    },
```

```
  {
    "actual_value": 7,
    "description": "Active applications",
    "line_graph_color": "green",
    "line_graph_data": [
      0,
      0,
      0,
      0,
      0,
      0,
      0,
      0,
      0,
      0,
      0,
      3,
      4
    ],
    "name": "applications",
    "status": 0,
    "total_value": 43,
    "trend_delta": 7,
    "trend_direction": "up"
  },
  {
    "actual_value": 3,
    "description": "Non-compliances",
    "line_graph_color": "red",
    "line_graph_data": [
      0,
      0,
      0,
      0,
      0,
      0,
      0,
      0,
      0,
      0,
      0,
```

```
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        3
      ],
      "name": "non_compliance",
      "status": 100,
      "total_value": 3,
      "trend_delta": 3,
      "trend_direction": "up"
    },
    {
      "actual_value": 13,
      "description": "Anomalies count",
      "line_graph_color": "red",
      "line_graph_data": [
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        0,
        1,
        0,
        0,
```

```
        0,
        0,
        0,
        0,
        5,
        0,
        0,
        0,
        0,
        4,
        2,
        0,
        0,
        0,
        0,
        0,
        1,
        0
      ],
      "name": "anomalies",
      "status": 100,
      "total_value": 13,
      "trend_delta": 0,
      "trend_direction": "flat"
    }
  ]
}
```


Retrieving Analytics Data for the World Map Gateway Location View

To retrieve a resource containing gateway data-points plotted on a map overlay using geographic coordinates, use the REST API call below:

- **Method:** POST /api/analytics/location_view
- **Resource:** Path

- **JSON Data:** JSON data structure containing map overlay coordinates, date/time period selection, and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains a list of data-points along with summary information and aggregated information. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/analytics/location_view
Authorization:
Content-Type: application/json
Request Body
{
  "top_left_lat": 23,
  "top_left_long": -12,
  "bottom_right_lat": -34,
  "bottom_right_long": 47,
  "current_time": 1648119483,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "response_type": "string",
  "bubble_items": [
    {
      "status": 73,
      "granularity": "city",
      "city": "Austin",
      "country": "USA",
      "continent": "North America",
      "latitude": 48.5,
      "longitude": 71.923,
      "num_gws_good": 1,
      "num_gws_warning": 1,
      "num_gws_critical": 1,
      "num_gws_offline": 1,
      "active_users": {},
      "active_devices": {},
      "active_gateways": {},
      "active_applications": {},
      "num_deviations": {},
      "non_compliance_count": {},
      "critical_errors": {},
      "id": "austin",
      "user_location_bubble_items": [
        {
          "id": "bengaluru",
          "city": "bengaluru",
          "latitude": 48.5,
          "longitude": 71.923,
          "num_active_users": 10
          "num_non_compliance_users": 0
        }
      ]
    }
  ]
}
```

Retrieving Analytics Data for the World Map Users View

To retrieve a resource containing user data-points plotted on a map overlay using geographic coordinates, use the REST API call below:

- **Method:** POST /api/analytics/zta_users_location_view
- **Resource:** Path
- **JSON Data:** JSON data structure containing date/time period selection, and optional filter for gateway selection

If processed correctly, a JSON body is returned that contains a list of data-points along with summary information. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/analytics/location_view
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1580515200,
  "start_time": 1580515200,
  "time_duration_type": "day",
  "timezone_offset": 330,
  "gateway_type": "pcs",
  "overlay_filter_type": "non_compliance_users",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "count": 10,
  "bubble_items": [
    {
      "granularity": "city",
      "city": "Austin",
      "country": "USA",
      "continent": "North America",
      "bubble_color": "Green",
      "latitude": 48.5,
      "longitude": 71.923,
      "avg_risk_score": {
        "count": 9,
        "color": "Green"
      },
      "num_active_users": 176,
      "num_high_risk_users": 21,
      "num_moderate_risk_users": 9,
      "num_low_risk_users": 3,
      "num_no_risk_users": 0
    }
  ]
}
```

Retrieving Analytics Data for the Sankey Chart View

To retrieve a resource containing data-points for plotting a Sankey chart of data flow between user groups, devices, Gateways, and applications, use the REST API call below:

- **Method:** POST /api/analytics/sankey_chart
- **Resource:** Path
- **JSON Data:** JSON data structure representing the **CommonFilterObject** schema (see Schema) - containing date/time period selection, and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains a list of data-points for plotting a Sankey chart. Otherwise, a JSON body containing an error is returned.

Parameters

- `max_items_per_pillar`: (integer - in: query)

  When this value <= 0, all items in each pillar will be returned. Otherwise, only specified maximum number of items per pillar will be returned in response. Default: -1.

- `apps_details`: (string - in: query)

  Flag capturing whether to return all apps or discovered apps details. Available values : all (default), discovered, non_discovered, default_gateway.

Request

The following is an example request:

```
      POST /api/analytics/sankey_chart?max_items_per_pillar=-1&apps_
details=all
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648119483,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "applications_list": [],
  "device_types_to_gateway_names": [
    {
      "source": "Windows",
      "target": "blackthorn-bng-2",
      "value": 12
    },
    {
      "source": "Windows",
      "target": "az-bkthrn-eastus",
      "value": 4
    }
  ],
  "gateway_names_to_application_names": [
    {
      "source": "blackthorn-bng-2",
      "target": "amazon",
      "value": 4
    },
    {
      "source": "blackthorn-bng-2",
      "target": "atlassian",
      "value": 3
    },
    {
      "source": "blackthorn-bng-2",
      "target": "bngvc.bnglab.psecure.net",
      "value": 3
    },
    {
      "source": "az-bkthrn-eastus",
      "target": "juniper.net",
      "value": 3
    },
    {
      "source": "blackthorn-bng-2",
```

```
      "target": "rdp",
      "value": 1
    },
    {
      "source": "blackthorn-bng-2",
      "target": "telnetresource ip",
      "value": 1
    },
    {
      "source": "az-bkthrn-eastus",
      "target": "community.juniper.net",
      "value": 1
    }
  ],
  "user_groups_to_device_types": [
    {
      "source": "bng group",
      "target": "Windows",
      "value": 12
    },
    {
      "source": "sj group",
      "target": "Windows",
      "value": 4
    }
  ]
}
```


Retrieving Analytics Data for the Top Active Gateways Chart

To retrieve a resource containing data used to create the top Active Gateways chart, use the REST API call below:

- **Method:** POST /api/analytics/widgets/top_gateways
- **Resource:** Path
- **JSON Data:** JSON data structure based on the **FilterObject** schema (see Schema) - containing date/time period selection and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains a list of data-points for plotting the Top Active Gateways chart. Otherwise, a JSON body containing an error is returned.

Schema

The **FilterObject** schema entity contains the following fields:

current_time	integer example: 1580515200 The time at which the Network Overview page was loaded. This is used to make sure that all the components on the page have the same reference so that they summarize the same data set.
start_time	integer example: 1580515200 The start time for the filter period (epoch). This value should represent the starting time for the selected 'time_duration_type'. Note the following: * Selecting "day" for 'time_duration_type' indicates this value should be the start of a specific calendar day (in UTC) * Selecting "week" for 'time_duration_type' indicates this value should be the start of a specific calendar week (in UTC) * Selecting "month" for 'time_duration_type' indicates this value should be the start of a specific calender month (in UTC)
end_time	integer example: 1580515200 The end time for the filter period (epoch). This value should represent the ending time for the selected 'time_duration_time' window. Use this field only when the 'time_duration_type' is set to "custom".

time_duration_type	string example: day Details of what unit of time duration need to be considered for the data. Enum: [active, current_day, day, week, month, last_24_hours, custom]
timezone_offset	string nullable: true example: pcs default: zta Type of the gateway. Enum: [zta, pcs, pps, vtm, null]
user_locations	Array [string] example: List ["Pune", "Bangalore"] default: List [] User access location filters for queries. Filtering based on multiple locations is supported.
user_name	string example: List ["ZTAUser"] User name filter for queries.
period	integer minimum: 0 default: 0 example: 0 Time-range in days (from current_time) for queries. 0 (default) means current values.
gateway_names	Array [string] example: List ["SanJose_Gateway_1", "Paris_Gateway_1"]

	default: List [] Names of the Gateways to be filtered.
application_names	Array [string] example: List ["JIRA", "Confluence"] default: List [] Application name filters for queries.
application_name	string example: List ["Confluence"]
device_types	Array [string] example: List ["Windows", "iOS"] default: List []Device type filters for queries.
geo_filter	Array [number] example: List [90, -180, -90, 180] default: List [90, -180, -90, 180] Geo filter; co-ordinates to be specified in this order [top_left_lat, top_left_long, bottom_right_lat, bottom_right_long]

```
location                    {
                               description: Optional location to filter
                            records.

                               granularity     string
                                               default: city
                                               example: city

                                            Granularity of the location.
                            Following fields will be set for different
                            values of granularity:

                                               city - city, country,
                            continent
                                               country - country,
                            continent
                                               continent - continent

                                               Enum:
                                               [ city, country, continent
                            ]

                               city            string
                                               example: Austin

                                               Name of the city. Set when
                            granularity is city.

                               country         string
                                               example: USA

                                               Name of the country. Set
                            when granularity is city or country.

                               continent       string
                                               example: North America

                                               Name of the continent. Set
                            when granularity is city, country, or
                            continent.
                            }
```

```
overlay_filter_type          string
                             example: non_compliance_users

                             Dashboard overlay text filter type

                             Enum:
                             [ connected_users_in_last_one_hour, non_
                             compliance_users, connected_users_in_more_
                             than_one_day, users_from_most_busy_gateway,
                             users_from_least_busy_gateway, top_risky_
                             users, geo_anomaly_users, user_roles_with_
                             most_non_compliances, top_users_with_auth_
                             failures, users_with_mfa ]
global_filter                {
                               description: Global filter object that is
                             applicable for all pages. If both overlay_
                             filter_type and global_filter are set, only
                             global_fiter would be used

                              gateway_ids  Array [ string ]
                                           example: List [ "74h4h3-u43943-
                             4u3o4", "84h4h3-u43943-4u3o5" ]
                                           default: List []

                                           Filtering based on multiple
                             gateway_ids.
                             }
                             nullable: true
```

Parameters

- `num_gateways`: (integer - in: query)

  The maximum number of Gateways for which data is returned. Default: 10.

Request

The following is an example request:

```
      POST /api/analytics/widgets/top_gateways?num_gateways=10
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648119483,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "gateways": [
    {
      "name": "blackthorn-bng-2",
      "value": 2
    },
    {
      "name": "az-bkthrn-eastus",
      "value": 1
    }
  ],
  "title": "TOP GATEWAYS"
}
```

Retrieving Analytics Data for the Top Active Applications Chart

To retrieve a resource containing data used to create the top Active Applications chart, use the REST API call below:

- **Method:** POST /api/analytics/widgets/top_applications
- **Resource:** Path
- **JSON Data:** JSON data structure based on the **FilterObject** schema (see Schema) - containing date/time period selection and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains a list of data-points for plotting the Top Active Applications chart. Otherwise, a JSON body containing an error is returned.

Parameters

- `num_applications`: (integer - in: query)

  The maximum number of applications for which data is returned. Default: 10.

Request

The following is an example request:

```
      POST /api/analytics/widgets/top_applications?num_applications=10
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648119483,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "applications": [
    {
      "name": "amazon",
      "value": 1
    },
    {
      "name": "atlassian",
      "value": 1
    },
    {
      "name": "bngvc.bnglab.psecure.net",
      "value": 1
    },
    {
      "name": "juniper.net",
      "value": 1
    },
    {
      "name": "community.juniper.net",
      "value": 1
    },
    {
      "name": "rdp",
      "value": 1
    },
    {
      "name": "telnetresource ip",
      "value": 1
    }
  ],
  "title": "TOP APPLICATIONS"
}
```

Retrieving Analytics Data for the Top Active User Locations Chart

To retrieve a resource containing data used to create the Top Active User Locations chart, use the REST API call below:

- **Method:** POST /api/analytics/widgets/top_user_access_locations
- **Resource:** Path
- **JSON Data:** JSON data structure based on the **FilterObject** schema (see Schema) - containing date/time period selection and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains a list of data-points for plotting the Top Active User Locations chart. Otherwise, a JSON body containing an error is returned.

Parameters

- `granularity`: (string - in: query)

  The level of granularity for location identification. Available values : city (default), country, continent.

- `num_locations`: (integer - in: query)

  The maximum number of locations for which data is returned. Default: 10.

Request

The following is an example request:

```
      POST /api/analytics/widgets/top_user_access_
locations?granularity=city&num_locations=10
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648119483,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
       HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "title": "TOP USER ACCESS LOCATIONS",
  "user_access_locations": [
    {
      "name": "bengaluru",
      "value": 2
    },
    {
      "name": "united states",
      "value": 1
    }
  ]
}
```

Retrieving Analytics Data for the Active Anomalies Chart

To retrieve a resource containing data used to create the Active Anomalies chart, use the REST API call below:

- **Method:** POST /api/analytics/widgets/anomalies
- **Resource:** Path
- **JSON Data:** JSON data structure based on the **FilterObject** schema (see Schema) containing date/time period selection and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains a list of data-points for plotting the Active Anomalies chart. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/analytics/widgets/anomalies
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648119483,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "buckets": [
    {
      "name": "Business Hours",
      "value": 8
    },
    {
      "name": "Geolocation",
      "value": 5
    }
  ],
  "chart_timestamp": 1648119483,
  "title": "Anomalies"
}
```

Retrieving Analytics Data for the Connected Clients Version Chart

To retrieve a resource containing data used to create the Connected Clients Version chart, use the REST API call below:

- **Method:** POST /api/analytics/devices/connected_clients
- **Resource:** Path
- **JSON Data:** JSON data structure based on the **FilterObject** schema (see Schema) - containing date/time period selection and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains a list of data-points for plotting the Connected Clients Version chart. Otherwise, a JSON body containing an error is returned.

Parameters

- `count`: (integer - in: query)

  Default: 5.

Request

The following is an example request:

```
      POST /api/analytics/devices/connected_clients?count=5
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648119483,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "users": "active",
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "chart_timestamp": 1648119483,
  "connected_devices": [
    {
      "type": "Windows",
      "values": [
        {
          "count": 2,
          "name": "9.1.14.14887"
        },
        {
          "count": 1,
          "name": "9.1.12.8219"
        }
      ]
    }
  ],
  "title": "Pulse Client Versions"
}
```

Retrieving Analytics Data for the Non-compliances Chart

To retrieve a resource containing data used to create the Non-compliances chart, use the REST API call below:

- **Method:** POST /api/analytics/users/top_non_compliance
- **Resource:** Path
- **JSON Data:** JSON data structure based on the **FilterObject** schema (see Schema) - containing date/time period selection and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains a list of data-points for plotting the Non-compliances chart. Otherwise, a JSON body containing an error is returned.

Parameters

- `count`: (integer - in: query)

  The number of Top Compliance policies for which data is needed based on the number of failures of the corresponding policy. A value of "-1" returns data for all Compliance policies. Default: 8.

- `page_level`: (string - in: query)

  The Insights UI page level/depth for which non-compliance data is to be provided. Available values : L1, L2, L3, L4.

Request

The following is an example request:

```
      POST /api/analytics/users/top_non_compliance?count=8&page_level=L1
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648119483,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "page_level": "L1"
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "chart_timestamp": 1648119483,
  "non_compliance_policies": [
    {
      "name": "antivirus",
      "value": 1
    },
    {
      "name": "commonpolicy",
      "value": 1
    },
    {
      "name": "symantecavlow",
      "value": 1
    }
  ],
  "title": "Non-compliance"
}
```

Retrieving Analytics Data for the Gateways Info-panel

To retrieve a resource containing data used to populate the Gateways Info-panel, use the REST API call below:

- **Method:** POST /api/analytics/widgets/top_gateways/panel
- **Resource:** Path
- **JSON Data:** JSON data structure based on the **FilterObject** schema (see Schema) - containing date/time period selection and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains data used to populate the Gateways Info-panel. Otherwise, a JSON body containing an error is returned.

Parameters

- `max_panel_items`: (integer - in: query)

  The maximum number of items to be returned in the panel output. Default: 500.

- `sort_order`: (string - in: query)

  The sort order to apply. Available values: asc, desc (default).

- `sort_field`: (string - in: query)

  The field to sort by. Available values: active_users_count (default), active_applications_count, non_compliance_count, active_devices_count, active_sessions_count, number_of_issues, gateway_name, city_name.

- `city_name`: (string - in: query)

  The selected city name.

- `search_string`: (string - in: query)

  The search string to apply.

- `status`: (string - in: query)

  Return all Gateways or only those Gateways with this specified status. Available values : all (default), active, offline, online, unregistered.

Request

The following is an example request:

```
      POST /api/analytics/widgets/top_gateways/panel?max_panel_
items=500&sort_order=desc&sort_field=active_users_count&city_
name=bangalore&search_string=gateway1&status=all
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648532792,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "info_panel_items": [
    {
      "id": "feicie-cneineoic-nfeie-32he",
      "gateway_name": "eng-mkn-gw-1",
      "city_name": "bangalore",
      "overall_color": "green",
      "gateway_status": "active",
      "number_of_issues": 10,
      "cpu_line_graph_data": "string",
      "memory_line_graph_data": "string",
      "disk_used_line_graph_data": "string",
      "active_users_count": 10,
      "active_devices_count": 10,
      "active_sessions_count": 10,
      "active_applications_count": 10,
      "non_compliance_count": 10,
      "issues_highest_severity": "CRITICAL",
      "issues_details": [
        {
          "message_id": "NTP12456",
          "raw_message": "NTP server is not reachable",
          "issue_timestamp": 3848462926,
          "number_of_issues": 23
        }
      ],
      "system_uptime": 10748,
      "last_config_update_timestamp": 1063264,
      "ssl_sessions_count": 10,
      "auth_only_sessions_count": 10,
      "active_sync_device_count": 10,
      "is_node_part_of_cluster": true,
      "cluster_properties": {
        "cluster_id": "9ccf22b9fe9ccf22b9fe",
        "cluster_name": "CoaGroup",
        "cluster_type": "Active/Active",
        "cluster_node_type": "active",
```

```
        "cluster_member_type": "leader",
        "is_vip_owner": false,
        "is_node_reachable": true,
        "is_node_enabled": false
      }
    }
  ],
  "count": 10,
  "all_gateway_count": 10,
  "active_gateway_count": 5,
  "offline_gateway_count": 5,
  "online_gateway_count": 5,
  "unregistered_gateway_count": 5
}
```


Retrieving Analytics Data for the Users Info-panel

To retrieve a resource containing data used to populate the Users Info-panel, use the REST API call below:

- **Method:** POST /api/analytics/widgets/top_risky_users/panel
- **Resource:** Path
- **JSON Data:** JSON data structure based on the **FilterObject** schema (see Schema) - containing date/time period selection and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains data used to populate the Users Info-panel. Otherwise, a JSON body containing an error is returned.

Parameters

- `offset`: (integer - in: query)

  The offset from which to fetch panel items. Default: 0.

- `limit`: (integer - in: query)

  The maximum number of panel items to return. Default: 20.

- `sort_order`: (string - in: query)

  The sort order to apply. Available values: asc, desc (default).

- `sort_field`: (string - in: query)

  The field to sort by. Available values: user_risk_score (default), user_name.

- `city_name`: (string - in: query)

  The selected city name.

- `search_string`: (string - in: query)

  The search string to apply.

Request

The following is an example request:

```
      POST /api/analytics/widgets/top_risky_
users/panel?offset=0&limit=20&sort_order=desc&sort_field=user_risk_
score&city_name=bangalore&search_string=user1&status=all
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648532792,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "info_panel_items": [
    {
      "user_name": "user1",
      "timestamp": 1580515200,
      "user_risk_score": 256,
      "non_compliance_count": 25,
      "anomalies_count": 50,
      "activity_deviation_count": 25,
      "user_icon_color": "red",
      "device_location_city": "Austin"
    }
  ],
  "count": 10,
  "total": 20
}
```

Retrieving Analytics Data for the Devices Info-panel

To retrieve a resource containing data used to populate the Devices Info-panel, use the REST API call below:

- **Method:** POST /api/analytics/widgets/top_device_types/panel
- **Resource:** Path
- **JSON Data:** JSON data structure based on the **FilterObject** schema (see Schema) - containing date/time period selection and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains data used to populate the Devices Info-panel. Otherwise, a JSON body containing an error is returned.

Parameters

- `max_panel_items`: (integer - in: query)

  The maximum number of items to be returned in the panel output. Default: 500.

- `sort_order`: (string - in: query)

  The sort order to apply. Available values: asc, desc (default).

- `sort_field`: (string - in: query)

  The field to sort by. Available values: active_users_count (default), active_applications_count, non_compliance_count, deviations_count, devices_count.

- `search_string`: (string - in: query)

  The search string to apply.

Request

The following is an example request:

```
      POST /api/analytics/widgets/top_device_types/panel?max_panel_
items=500&sort_order=desc&sort_field=active_users_count&search_
string=Windows
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648532792,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "info_panel_items": [
    {
      "nvt_items": [
        {
          "name": "active_users_count",
          "trend": "Flat",
          "value": 2
        },
        {
          "name": "active_applications_count",
          "trend": "Flat",
          "value": 7
        },
        {
          "name": "devices_count",
          "trend": "Flat",
          "value": 2
        },
        {
          "name": "non_compliance_count",
          "trend": "Flat",
          "value": 3
        },
        {
          "name": "deviations_count",
          "trend": "Flat",
          "value": 0
        }
      ],
      "status": 100,
      "sub_title": "",
      "title": "windows"
    }
  ]
}
```

Retrieving Analytics Data for the Applications Info-panel

To retrieve a resource containing data used to populate the Applications Info-panel, use the REST API call below:

- **Method:** POST /api/analytics/widgets/top_applications/panel
- **Resource:** Path
- **JSON Data:** JSON data structure based on the **FilterObject** schema (see Schema) - containing date/time period selection and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains data used to populate the Applications Info-panel. Otherwise, a JSON body containing an error is returned.

Parameters

- `max_panel_items`: (integer - in: query)

  The maximum number of items to be returned in the panel output. Default: 500.

- `sort_order`: (string - in: query)

  The sort order to apply. Available values: asc, desc (default).

- `sort_field`: (string - in: query)

  The field to sort by. Available values: active_users_count (default), active_applications_count, non_compliance_count, deviations_count, devices_count.

- `search_string`: (string - in: query)

  The search string to apply.

Request

The following is an example request:

```
      POST /api/analytics/widgets/top_applications/panel?max_panel_
items=500&sort_order=desc&sort_field=active_users_count&search_string=
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648532792,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "info_panel_items": [
    {
      "nvt_items": [
        {
          "name": "active_users_count",
          "trend": "Flat",
          "value": 1
        },
        {
          "name": "active_applications_count",
          "trend": "Flat",
          "value": 1
        },
        {
          "name": "devices_count",
          "trend": "Flat",
          "value": 1
        },
        {
          "name": "application_type",
          "trend": "Flat",
          "value": 0
        },
        {
          "name": "application_port",
          "trend": "Flat",
          "value": 443
        },
        {
          "name": "non_compliance_count",
          "trend": "Flat",
          "value": 0
        },
        {
          "name": "deviations_count",
          "trend": "Flat",
```

```
        "value": 0
      }
    ],
    "status": 0,
    "sub_title": "",
    "title": "pulsesecure.net"
  },
  {
    "nvt_items": [
      {
        "name": "active_users_count",
        "trend": "Flat",
        "value": 1
      },
      {
        "name": "active_applications_count",
        "trend": "Flat",
        "value": 1
      },
      {
        "name": "devices_count",
        "trend": "Flat",
        "value": 1
      },
      {
        "name": "application_type",
        "trend": "Flat",
        "value": 0
      },
      {
        "name": "application_port",
        "trend": "Flat",
        "value": 443
      },
      {
        "name": "non_compliance_count",
        "trend": "Flat",
        "value": 0
      },
      {
```

```
          "name": "deviations_count",
          "trend": "Flat",
          "value": 0
        }
      ],
      "status": 0,
      "sub_title": "",
      "title": "community.juniper.net"
    },
  ]
}
```


Retrieving Analytics Data for the Non-compliances Info-panel

To retrieve a resource containing data used to populate the Non-compliances Info-panel, use the REST API call below:

- **Method:** POST /api/analytics/widgets/non_compliance/panel
- **Resource:** Path
- **JSON Data:** JSON data structure based on the **FilterObject** schema (see Schema) - containing date/time period selection and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains data used to populate the Non-compliances Info-panel. Otherwise, a JSON body containing an error is returned.

Parameters

- `offset`: (integer - in: query)

  The offset from which to fetch panel items. Default: 0.

- `limit`: (integer - in: query)

  The maximum number of panel items to return. Default: 20.

- `sort_order`: (string - in: query)

  The sort order to apply. Available values: asc, desc (default).

- `sort_field`: (string - in: query)

  The field to sort by. Available values: timestamp (default), user_name.

- `search_string`: (string - in: query)

  The search string to apply.

Request

The following is an example request:

```
      POST /api/analytics/widgets/non_
compliance/panel?offset=0&limit=20&sort_order=desc&sort_
field=timestamp&search_string=
Authorization:
Content-Type: application/json
Request Body
{
  "current_time": 1648532792,
  "start_time": 1580515200,
  "time_duration_type": "active",
  "timezone_offset": 330,
  "gateway_type": "zta",
  "global_filter": {
    "gateway_ids": [
      "74h4h3-u43943-4u3o4",
      "84h4h3-u43943-4u3o5"
    ]
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "count": 3,
  "info_panel_items": [
    {
      "application_name": "Zendesk",
      "device_id": "b71af79efc6c43b2b7e9da58071a23da",
      "device_type": "Windows",
      "non_compliance_policy_name": "NetworkPolicy",
      "non_compliance_policy_types_list": [
        "Network"
      ],
      "timestamp": 1648532547,
      "user_name": "cambridgetest1"
    },
    {
      "application_name": "Salesforce",
      "device_id": "a1ee1dc5ee5e4263abaf91599f9dc595",
      "device_type": "Windows",
      "non_compliance_policy_name": "SymantecAVHigh",
      "non_compliance_policy_types_list": [
        "HC"
      ],
      "timestamp": 1648532503,
      "user_name": "sjtest1"
    },
    {
      "application_name": "Box",
      "device_id": "a1ee1dc5ee5e4263abaf91599f9dc595",
      "device_type": "Windows",
      "non_compliance_policy_name": "CommonPolicy",
      "non_compliance_policy_types_list": [
        "Network",
        "HC"
      ],
      "timestamp": 1648532497,
      "user_name": "sjtest1"
    }
```

```
  ],
  "total": 3
}
```

Retrieving Analytics Data for the Anomalies Info-panel

To retrieve a resource containing data used to populate the Anomalies Info-panel, use the REST API call below:

- **Method:** POST /api/analytics/widgets/anomalies/panel
- **Resource:** Path
- **JSON Data:** JSON data structure representing the **AnomaliesPanelFilterObject** schema (see Schema) - containing date/time period selection, and optional filter for gateway selection.

If processed correctly, a JSON body is returned that contains data used to populate the Anomalies Info-panel. Otherwise, a JSON body containing an error is returned.

Schema

The **AnomaliesPanelFilterObject** schema entity contains the following fields:

```
      acknowledged_status          string
                              default: All
                              example: Acknowledged
                              Acknowledged status of anomalies to be
filtered
                              Enum:
                              [ All, Acknowledged, Open ]
```

Parameters

- `offset`: (integer - in: query)

  The offset from which to fetch panel items. Default: 0.

- `limit`: (integer - in: query)

  The maximum number of panel items to return. Default: 20.

- `sort_order`: (string - in: query)

  The sort order to apply. Available values: asc, desc (default).

- `sort_field`: (string - in: query)

  The field to sort by. Available values: timestamp (default), user_name, acknowledged.

- `search_string`: (string - in: query)

  The search string to apply.

Request

The following is an example request:

```
      POST /api/analytics/widgets/anomalies/panel?offset=0&limit=20&sort_
order=desc&sort_field=timestamp&search_string=user1
Authorization:
Content-Type: application/json
Request Body
{
  "acknowledged_status": "Acknowledged"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "info_panel_items": [
    {
      "anomaly_type": "GeoNewLocation",
      "user_name": "John Smith",
      "timestamp": 1587972453,
      "device_id": "27178d97948d46c09c205d30e9cf2afe",
      "session_id": "9ccf22b9fe",
      "device_type": "Windows",
      "anomaly_reason": "Non-familiar user location.",
      "anomaly_id": "e4abbb38ce8d4619891e561cedb7c807",
      "acknowledged": true,
      "active_session": true,
      "browser": "Google Chrome",
      "locations_history": [
        {
          "location_name": "Bangalore",
          "timestamp": 1580515200
        }
      ],
      "current_location": "Bangalore"
    },
    {},
    {
      "anomaly_type": "GeoNewLocation",
      "user_name": "John Smith",
      "timestamp": 1587972453,
      "device_id": "27178d97948d46c09c205d30e9cf2afe",
      "session_id": "9ccf22b9fe",
      "device_type": "Windows",
      "anomaly_reason": "Non-familiar user location.",
      "anomaly_id": "e4abbb38ce8d4619891e561cedb7c807",
      "acknowledged": true,
      "active_session": true,
      "browser": "Google Chrome",
      "application_names": [
        "Microsoft",
```

```
        "Facebook"
      ],
      "details": "Normal access hours range of user is between 9 a.m. to 5
p.m."
    }
  ],
  "count": 20,
  "total": 20
}
```

Retrieving Log Data

To retrieve a resource containing log data, use the REST API call below:

- **Method:** POST /api/analytics/logs/search
- **Resource:** Path
- **JSON Data:** JSON data structure representing the **LogRequestEntity** schema (see Schema), containing log selection criteria.

If processed correctly, a JSON body is returned that contains log data. Otherwise, a JSON body containing an error is returned.

Schema

The **LogRequestEntity** schema entity contains the following fields:

```
name          string
              example: Filter1

              Name to be used
start_time_   integer
es            example: 1576533928

              Start time for logs in seconds since epoch. By default
              start of current day.
end_time_es   integer
              example: 1576533928
```

```
                End time for logs in seconds since epoch. By default
                current time i.e now.
current_        integer
time            example: 1576533928

                Current time for logs in seconds since epoch. By default
                current time i.e now.
timezone_       integer
offset          example: 330

                Offset of the timezone to be used.
offset          integer
                example: 0

                Start offsets for logs, default is 0.
limit           integer
                example: 100

                Number of logs lines to be returned by the query
search_string   string
                example: ZTA

                Search string to be used
```

search_string_columns	Array [string] Selects search string columns to be used in query. Enum: [application_configured_name, application_discovered, application_group_names, application_host, application_id, application_ip, application_location_city, application_name, application_names, application_protocol, application_protocol_display_name, application_request_id, application_status, application_type, application_url, auth_server_name, pulse_client_version, device_location_city, device_id, device_model, device_os_type, device_os_version, device_type, gateway_location_city, gateway_id, gateway_name, gateway_type, message_id, message_type, non_compliance_policy_id, non_compliance_policy_name, non_compliance_policy_types_list, raw_message, realm_name, role_names, session_id, severity, sub_message_type, source_ip, user_group, user_groups_list, user_id, user_name, user_risk_score_category]
sort_by	string nullable: true default: timestamp Field used for sorting logs. Enum:

```
[ timestamp, source_ip, message_id, severity, gateway_id,
gateway_name, session_id, user_name, device_id, raw_
message, user_group, application_name, non_compliance_
policy_name, non_compliance_policy_types_list, device_
location_city, device_location_country, sub_message_type,
user_risk_score, user_risk_score_category, user_anomalies_
count, user_alerts_count, user_activity_deviations_count,
acknowledged, device_type, realm_name, role_names, pulse_
client_version, device_os_type, gateway_location_city,
application_type, application_protocol, application_
protocol_display_name, application_discovered, application_
group_names, application_status, application_bookmark_type,
application_connection_broker, application_desktop_
protocol, application_host, application_ip, application_
location_city, application_url, message, browser, browser_
id, controller, message_type, bandwidth_consumed_str,
connected_time, host_checker_policy_name, host_checker_
failed_reason, session_duration, null ]
```

```
sort_group_   {
by              description: Field used for sorting of grouping logs.

                anyOf -> SortGroupByFieldType string
                         example: application_name
                         default: application_name

                         Group by field type for sorting

                         Enum:
                         [ application_name, application_group, device_
              id, gateway_id, gateway_name, message_id, session_
              id,severity, source_ip, user_name, user_group, unique_
              application_group_names_count, unique_application_ips_
              count, unique_application_location_cities_count, unique_
              application_names_count, unique_application_protocols_
              count, unique_application_protocol_display_names_count,
              unique_application_urls_count, unique_device_ids_count,
              unique_device_location_cities_count, unique_gateway_ids_
              count, unique_gateway_names_count, unique_non_compliance_
              policy_types_count, unique_session_ids_count, unique_
              source_ips_count, unique_user_names_count, unique_user_
              groups_count ]
              }
```

```
group_by      {
                 description: Field used for grouping logs.

                 anyOf -> GroupFieldType string
                          example: application_name
                          default: application_name

                          Group by field type

                          Enum:
                          [ application_discovered, application_group_
              names, application_ip, application_location_city,
              application_name, application_protocol, application_
              protocol_display_name, application_status, application_
              type, pulse_client_version, device_id, device_location_
              city, device_os_type, device_type, gateway_id, gateway_
              location_city, gateway_name, message_type, non_compliance_
              policy_name, non_compliance_policy_types_list, source_ip,
              session_id, severity, sub_message_type, user_name, user_
              group, user_risk_score_category ]
              }
order         string
              default: desc

              Order of sorting specified by sortby field.

              Enum:
              [ asc, desc ]
log_type      string
              default: access
              example: access

              Type of the logs to be exported

              Enum:
              [ access, admin, event ]
```

```
gateway_type      string
                  default: zta
                  example: pcs

                  Gateway Type of the logs to be exported

                  Enum:
                  [ pcs, zta ]

columns           Array [ LogColumns ]
                  default: List [ "timestamp", "message_id", "severity",
                  "session_id", "raw_message" ]

                  Selects columns to be returned by query response.

                  LogColumns string
                  Enum:
```

	[acknowledged, adaptive_auth_reason, application_bookmark_type, application_connection_broker, application_desktop_protocol, application_discovered, application_group_names, application_host, application_ip, application_location_city, application_name, application_protocol, application_protocol_display_name, application_status, application_type, application_url, avg_cpu, avg_disk, avg_memory, avg_throughput, bandwidth_consumed_in_bytes, bandwidth_consumed_str, browser, browser_id, concurrent_users_sessions, connected_time, controller, cpu, device_id, device_location_city, device_location_country, device_os_type, device_type, disk_used_percentage, esap_version, esap_version, gateway_id, gateway_location_city, gateway_location_country, gateway_name, gateway_status, gateway_version, gateway_version, host_checker_failed_reason, host_checker_policy_name, is_session_active, max_concurrent_user_licenses_consumed, message, message_id, message_type, non_compliance_policy_name, non_compliance_policy_types_list, physical_memory, primary_auth_failed_reason, primary_auth_server_name, primary_auth_server_type, pulse_client_version, raw_message, realm_name, role_names, secondary_auth_failed_reason, secondary_auth_server_type, secondary_auth_server_name, secondary_auth_server_user_name, session_created_timestamp, session_duration, session_id, session_type, severity, source_ip, sub_message_type, swap_memory, throughput_value, timestamp, user_activity_deviations_count, user_alerts_count, user_anomalies_count, user_group, user_name, user_risk_score, user_risk_score_category, ALL, null]
group_by_columns	Array [string]

```
default: List [ "unique_gateway_names_count", "unique_user_
names_count", "unique_application_names_count", "summary_
device_types", "summary_message_types", "unique_device_ids_
count", "unique_session_ids_count" ]

Selects group by columns to be returned by query response.

Enum:
[ summary_acknowledged, summary_application_discovered,
summary_application_names, summary_application_types,
summary_application_status, summary_pulse_client_versions,
summary_device_types, summary_device_os_types, summary_non_
compliance_policy_names, summary_non_compliance_policy_
types, summary_message_ids, summary_message_types, summary_
severities, summary_sub_message_types, summary_application_
bookmark_types, summary_application_desktop_protocols,
summary_browsers, summary_esap_versions, summary_gateway_
status, summary_gateway_versions, summary_is_session_
actives, summary_user_risk_score_categories, unique_
application_group_names_count, unique_application_ips_
count, unique_application_location_cities_count, unique_
application_names_count, unique_application_protocols_
count, unique_application_protocol_display_names_count,
unique_application_urls_count, unique_device_ids_count,
unique_device_location_cities_count, unique_gateway_ids_
count, unique_gateway_names_count, unique_session_ids_
count, unique_source_ips_count, unique_user_names_count,
unique_user_groups_count, unique_application_connection_
brokers_count, unique_application_hosts_count, unqiue_
device_ids_count, unique_device_location_countries_count,
unique_gateway_location_cities_count, unique_host_checker_
policy_names_count, unique_message_ids_count, unique_raw_
messages_count, unique_role_names_count, unique_realm_
names_count, max_user_activity_deviations_count, max_user_
alerts_count, max_user_anomalies_count, max_user_risk_
score, avg_user_activity_deviations_count, avg_user_alerts_
count, avg_user_anomalies_count, avg_user_risk_score, avg_
cpu, avg_disk_used_percentage, avg_swap_memory, avg_
throughput_value, max_cpu, max_disk_used_percentage, max_
swap_memory, max_throughput_value, recent_user_activity_
deviations_count, recent_user_alerts_count, recent_user_
anomalies_count, recent_user_risk_score, recent_user_risk_
score_category, ALL ]
```

```
filters      Array [ LogFilterEntity ]

             Represents a collection of filters to be applied.

             LogFilterEntity {
                      description:    Filter to be used

                       filter_by*      string
                                       example: message_ids

                                       Filter by field to be used

                                       Enum:
                                       [ gateway_ids, gateway_location_
             cities, gateway_names, user_names, user_groups, user_risk_
             score_categories, pulse_client_versions, device_ids,
             device_types, device_os_types, device_location_cities,
             device_location_countries, application_bookmark_types,
             application_connection_brokers, application_desktop_
             protocols, application_location_cities, application_names,
             application_group_names, application_hosts, application_
             ips, application_protocols, application_protocol_display_
             names, application_types, application_urls, message_ids,
             session_ids, source_ips, realm_names, role_names,
             severities, non_compliance_policy_names, non_compliance_
             policy_types, message_types, sub_message_types, ignore_sub_
             message_types, application_discovered, acknowledged,
             application_status_list, host_checker_policy_names,
             browsers, browser_ids, is_session_active, controller, raw_
             messages, gateway_statuses, gateway_versions, esap_
             versions, cpus, disk_used_percentages, physical_memories,
             swap_memories, throughput_values, avg_cpus, avg_disks, avg_
             memories, avg_throughputs, max_concurrent_user_licenses_
             consumed ]

                         operator*       string
                                         default: IS
                                         example: IS

                                         operator to be used

                                         Enum:
                                         [ IS, CONTAINS ]
```



```
                         value*          string
                                         example: ZTAGateway
```

Request

The following is an example request:

```
      POST /api/analytics/logs/search
Authorization:
Content-Type: application/json
Request Body
{
  "name": "Filter1",
  "start_time_es": 1576533928,
  "end_time_es": 1576533928,
  "current_time": 1576533928,
  "timezone_offset": 330,
  "offset": 0,
  "limit": 100,
  "search_string": "ZTA",
  "search_string_columns": [
    "application_configured_name"
  ],
  "sort_by": "timestamp",
  "sort_group_by": "application_name",
  "group_by": "application_name",
  "order": "desc",
  "log_type": "access",
  "gateway_type": "zta",
  "columns": [
    "timestamp",
    "message_id",
    "severity",
    "session_id",
    "raw_message"
  ],
  "group_by_columns": [
    "unique_gateway_names_count",
    "unique_user_names_count",
    "unique_application_names_count",
    "summary_device_types",
    "summary_message_types",
    "unique_device_ids_count",
    "unique_session_ids_count"
  ],
  "filters": [
    {
```

```
      "filter_by": "message_ids",
      "operator": "IS",
      "value": "ZTAGateway"
    }
  ]
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "total": 1000,
  "count": 10,
  "offset": 0,
  "log_lines": [
    {
      "timestamp": 1576533928,
      "message_id": "ADM24682",
      "gateway_id": "123e4567-e89b-12d3-a456-426655440000",
      "gateway_name": "Azure-Gateway_1",
      "severity": "INFO",
      "source_ip": "127.0.0.1",
      "raw_message": "Primary authentication successful for admindb/SDP
Admin Auth from\n172.21.8.171\n",
      "user_name": "testuser1",
      "user_group": "testgroup1",
      "session_id": "fa0726e89c",
      "device_id": "965C34BA98C94F4EAE6F2D8564E6CEAC",
      "application_name": "Jira.abc.com",
      "application_group_names": [
        [
          "group-1",
          "group-2"
        ]
      ],
      "application_protocol": "HTTPS",
      "application_protocol_display_name": "Web",
      "application_discovered": false,
      "application_type": "url",
      "application_status": "Green",
      "application_connection_broker": "auto.pcs.com",
      "application_desktop_protocol": "ssh",
      "application_host": "auto.pcs.com",
      "application_ip": "1.2.3.4",
      "application_url": "www.gmail.com",
      "application_location_city": "Bengaluru",
      "application_bookmark_type": "Admin defined",
```

```
    "non_compliance_policy_name": "Jira_access_policy",
    "non_compliance_policy_types_list": [
      [
        "Location",
        "HC"
      ]
    ],
    "message_type": "Anomaly",
    "sub_message_type": "Anomaly",
    "pulse_client_version": "2021.12.1",
    "device_type": "Windows",
    "device_os_type": "Windows 10 Pro",
    "device_location_city": "mumbai",
    "user_risk_score": 10.23,
    "user_risk_score_category": "High",
    "user_alerts_count": 13,
    "user_anomalies_count": 10,
    "user_activity_deviations_count": 5,
    "acknowledged": true,
    "session_type": "local",
    "adaptive_auth_reason": "new_location",
    "controller": true,
    "is_session_active": true,
    "session_duration": "2:20:00",
    "bandwidth_consumed": 1024,
    "bandwidth_consumed_str": "1.00 Kb",
    "connected_time": "2:10:30",
    "role_names": [
      [
        "role-1",
        "role-2"
      ]
    ],
    "session_created_timestamp": 1576533928,
    "browser": "Google Chrome",
    "gateway_status": "online",
    "gateway_version": "21.x Build 1",
    "esap_version": "21.x Build 1",
    "cpu": 26.75,
    "physical_memory": 18.25,
```

```
      "swap_memory": 20.9,
      "disk_used_percentage": 34.5,
      "throughput_value": 67,
      "avg_cpu": 26.75,
      "avg_memory": 18.25,
      "avg_disk": 34.5,
      "avg_throughput": 67,
      "max_concurrent_user_licenses_consumed": 200
    }
  ]
}
```


Retrieving Aggregated Gateway Statistics

To retrieve aggregated usage statistics for a list of Gateways, use the REST API call below:

- **Method:** GET /api/analytics/apm/appstats
- **Resource:** Path
- **JSON Data:** None

If processed correctly, a JSON body containing a *MetricsResponseEntity* resource is returned. Otherwise, a JSON body containing an error is returned.

Parameters

- `metric`: (array[string] - in: query)

  A list of the required metrics. Available values: cpu, file_hits, web_hits, swap_memory, physical_ memory, ssl_connections, in_in_throughput_bps, in_out_throughput_bps, ext_in_throughput_bps, ext_out_throughput_bps, mul_in_throughput_bps, mul_out_throughput_bps, concurrent_users_ sessions, concurrent_users_vpn_sessions, disk_used_percentage, ALL.

- `start_time_es`: (integer - in: query)

  Start time of aggregation since epoch in seconds.

- `end_time_es`: (integer - in: query)

  End time of aggregation since epoch in seconds.

- `bucket_size`: (string - in: query)

  Aggregation based on bucketing. Available values: 5minutes, hours, days.

- `gateway_ids`: (array[string] - in: query)

  A list of the Gateway ID(s) for which data is required. To request data for all Gateways, use the value 'ALL'.

- `agg_type`: (string - in: query)

  The type of aggregation. Available values: SUM, AVG, MAX.

- `location`: (string - in: query)

  The Gateway location to use.

Request

The following is an example request:

```
      GET /api/analytics/apm/appstats?metric=cpu&start_time_
es=1574973734&end_time_es=1574973777&bucket_size=5minutes&gateway_
ids=74h4h3-u43943-4u3o4&agg_type=SUM&location=Bangalore
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "status": {
    "data_points": 0,
    "offset": 0,
    "agg_type": "SUM",
    "gateway_ids": [
      "string"
    ]
  },
  "chart_data": [
    {
      "cpu": 23,
      "file_hits": 32,
      "web_hits": 13,
      "swap_memory": 33,
      "physical_memory": 56,
      "ssl_connections": 3423,
      "in_in_throughput_bps": 1334,
      "in_out_throughput_bps": 423423,
      "ext_in_throughput_bps": 423423,
      "ext_out_throughput_bps": 423423,
      "mul_in_throughput_bps": 423423,
      "mul_out_throughput_bps": 423423,
      "concurrent_users_sessions": 4213,
      "concurrent_users_vpn_sessions": 4213,
      "disk_used_percentage": 56,
      "timestamp_es": 0
    }
  ]
}
```

Applications (resources)

An application is a type of *resources* entity that represents a *nZTA* application. Applications support the following activities:

- Retrieving all applications, see Retrieving an Application.
- Editing an application, see Editing an Application.

> The *resources* entity is also used to represent a *nZTA* user policy. This is enabled by a **type** of "sign-in", see User Policies (resources).

Retrieving an Application

To retrieve all application (*resources*) entities, use the REST API call below:

- **Method:** GET /api/v1/policies/resources
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a *resources* type of "application".

If processed correctly, a JSON body containing a list of all application resources is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/resources
Authorization:
Content-Type: application/json
Request Body
{
   "type": "application"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
   "type": "application",
   "name": "app1",
   "description": "app1",
   "app_config": {
      "access_type": "saml",
      "name": "app1",
      "resource": "https://www.example.com",
      "resource_type": "url",
      "bookmark_config": {
         "name": "app1",
         "type": "web",
         "description": "app1",
         "launch_window": True,
         "url": "https://www.example.com",
         "icon": "/admin/static/media/filename.svg"
      },
      "saml_config": {
         "sp_metadata": "string"
      }
   }
}
```

Editing an Application

To edit an application *resources* entity, use the REST API call below:

- **Method:** PUT /api/v1/policies/resources/{resource_id}
- **Resource:** Path
- **JSON Data:** JSON dictionary representing changed properties for an application *resources* entity.

If processed correctly, a JSON body containing the updated application *resources* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      PUT /api/v1/policies/resources/{resource_id}
Authorization:
Content-Type: application/json
Request Body
{
   "type": "application",
   "name": "app1",
   "description": "app1",
   "app_config": {
      "access_type": "saml",
      "name": "app1",
      "resource": "https://www.example.com",
      "resource_type": "url",
      "bookmark_config": {
         "name": "app1",
         "type": "web",
         "description": "app1",
         "launch_window": True,
         "url": "https://www.intuit.com",
         "icon": "/admin/static/media/filename.svg"
      },
      "saml_config": {
         "sp_metadata": "string"
      }
   }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
   "type": "application",
   "name": "app1",
   "description": "app1",
   "app_config": {
      "access_type": "saml",
      "name": "app1",
      "resource": "https://www.example.com",
      "resource_type": "url",
      "bookmark_config": {
         "name": "app1",
         "type": "web",
         "description": "app1",
         "launch_window": True,
         "url": "https://www.example.com",
         "icon": "/admin/static/media/filename.svg"
      },
      "saml_config": {
         "sp_metadata": "string"
      }
   }
}
```

Authentication Server (auth-servers)

The *auth-servers* entity represents a *nZTA* authentication server. Authentication servers support the following activities:

- Retrieving All Authentication Servers, see Retrieving All Authentication Servers.
- Creating a Local Authentication Server, see Creating a Local Authentication Server.
- Creating a SAML Authentication Server, see Creating a SAML Authentication Server.

Retrieving All Authentication Servers

To retrieve all *auth-servers* entities, use the REST API call below:

- **Method:** GET /api/v1/policies/auth-servers
- **Resource:** Path
- **JSON Data:** No JSON is required for this request.

If processed correctly, a JSON body containing a list of all auth-servers is returned. Otherwise, a JSON body containing an error is returned.

Request

This REST API command always retrieves all *auth-servers* entities.

The following is an example request:

```
      GET /api/v1/policies/auth-servers
Authorization:
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "total": 0,
  "auth_servers": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "type": "Local",
      "name": "string"
    },
    {
      "id": "2c963f64-5717-4562-b3fc-2c963f66afa6",
      "type": "Local",
      "name": "string"
    },
    {
      "id": "66afa664-5717-4562-b3fc-2c963f66afa6",
      "type": "Local",
      "name": "string"
    },
    {
      "id": "63f66a64-5717-4562-b3fc-2c963f66afa6",
      "type": "Local",
      "name": "string"
    }
  ]
}
```

Creating a Local Authentication Server

To create a local authentication server:

- **Method:** POST /api/v1/policies/auth-servers
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new local *auth-servers* entity.

If processed correctly, a JSON body containing the new local *auth-servers* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/v1/policies/auth-servers
Authorization:
Request Body
{
  "type": "Local",
  "name": "string",
  "cert_config": {
    "user_name_template": "string"
  },
  "local_config": {
    "users": [
      {
        "name": "string",
        "full_name": "string",
        "password": "string",
        "password_change_required": true
      }
    ]
  },
  "samlsp_config": {
    "metadata_config_type": "url",
    "metadata_config_url": "string",
    "idp_type": "Azure AD",
    "idp_metadata_xml": "string"
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "type": "Local",
  "name": "string",
  "cert_config": {
    "user_name_template": "string"
   },
  "samlsp_config": {
    "metadata_config_type": "url",
    "metadata_config_url": "string",
    "idp_type": "Azure AD",
    "idp_metadata_xml": "string"
  }
}
```

Creating a SAML Authentication Server

To create a remote SAML authentication server:

- **Method:** POST /api/v1/policies/auth-servers
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new SAML *auth-servers* entity.

If processed correctly, a JSON body containing the new SAML *auth-servers* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/v1/policies/auth-servers
Authorization:
Request Body
{
  "type": "SAML (Azure AD)",
  "name": "auth_server_1",
  "samlsp_config": {
    "idp_metadata_xml": "string"
    "idp_type": "Azure AD",
    "metadata_config_type": "file",
    "metadata_config_url": "string",
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "ab45c43278b42312f00fab4321af54c0543b",
  "type": "SAML (Azure AD)",
  "name": "auth_server_1",
  "samlsp_config": {
    "idp_metadata_xml": "string"
    "idp_type": "Azure AD",
    "metadata_config_type": "file",
    "metadata_config_url": "string",
  }
}
```

Device Policies (device-policy/groups)

The *device-policy/groups* entity represents a *nZTA* device policy configuration.

Hostchecker levels must be created and configured before device policies can be created successfully, see Hostchecker Levels (hostchecker/levels).

Device policies support the following activities:

- Retrieving all device policies, see Retrieving all device policies.
- Retrieving a specific device policy, see Retrieving a specific device policy
- Creating a device policy, see Creating a device policy.
- Editing a device policy, see Editing a device policy.
- Deleting a device policy, see Deleting a device policy.

Retrieving all Device Policies

To retrieve all *device-policy/groups* entities, use the REST API call below:

- **Method:** GET /api/v1/policies/device-policies/device-policy/groups
- **Resource:** Path

If processed correctly, a JSON body containing a list of all *device-policy/groups* entities is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/device-policies/device-policy/groups
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "items": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "name": "string",
      "description": "string",
      "is_default": true,
      "rules": [
        {
          "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "name": "string",
          "description": "string",
          "type": "browser",
          "label": "high",
          "browser_config": {
            "user_agent": "string",
            "mode": "allow"
          },
          "network_config": {
            "ip_address": "string",
            "netmask": "string",
            "mode": "allow"
          },
          "hostchecker_config": {
            "name": "string",
            "type": "predefined",
            "predefined_rule": {
              "type": "antivirus",
              "hostchecker_level_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
              "hostchecker_product_list_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
              "hostchecker_level_name": "string",
              "hostchecker_product_list": {
                "windows": {
                  "products": [
                    "string"
```

```
            ],
            "vendors": [
              "string"
            ]
          },
          "mac": {
            "products": [
              "string"
            ],
            "vendors": [
              "string"
            ]
          }
        },
        "user_settings": {
          "hdd_encryption_settings": {
            "encrypt_drives": [
              "string"
            ]
          }
        }
      },
      "custom_rule": {
        "platform": "windows",
        "type": "process",
        "registry": {
          "root_key": "HKEY_LOCAL_MACHINE",
          "sub_key": "string",
          "type": "string",
          "key": "string",
          "value": "string",
          "is_64_bit": true,
          "remediate": true,
          "monitor": true
        },
        "process": {
          "process_name": "string",
          "md5_checksum": "string",
          "sha256_checksum": "string",
          "monitor": true,
```

```
            "action": "allow"
          },
          "mobile_os_check": {
            "os_version": "string",
            "rule_separator": "above"
          },
          "desktop_os_check": [
            {
              "os_version": "string",
              "service_pack_version": "string"
            }
          ],
          "file": {
            "file_name": "string",
            "md5_checksum": "string",
            "sha256_checksum": "string",
            "monitor": true,
            "action": "allow"
          },
          "cve_check": {
            "check_all": true,
            "cve_list": [
              "string"
            ]
          },
          "mobile_jail_break_root_check_enabled": true,
          "netbios": {
            "allow": true,
            "names": [
              "string"
            ]
          },
          "mac_address": {
            "allow": true,
            "address": [
              "string"
            ]
          }
        }
      },
```

```
          "allow_delete": true,
          "is_default": true
        }
      ]
    }
  ]
}
```

Retrieving a Specific Device Policy

To retrieve a single *device-policy/groups* entity, use the REST API call below:

- **Method:** GET /api/v1/policies/device-policies/device-policy/groups/{id}
- **Resource:** Path

If processed correctly, a JSON body containing the *device-policy/groups* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/device-policies/device-policy/groups/{id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "description": "string",
  "is_default": true,
  "rules": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "name": "string",
      "description": "string",
      "type": "browser",
      "label": "high",
      "browser_config": {
        "user_agent": "string",
        "mode": "allow"
      },
      "network_config": {
        "ip_address": "string",
        "netmask": "string",
        "mode": "allow"
      },
      "hostchecker_config": {
        "name": "string",
        "type": "predefined",
        "predefined_rule": {
          "type": "antivirus",
          "hostchecker_level_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "hostchecker_product_list_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
          "hostchecker_level_name": "string",
          "hostchecker_product_list": {
            "windows": {
              "products": [
                "string"
              ],
              "vendors": [
                "string"
```

```
            ]
          },
          "mac": {
            "products": [
              "string"
            ],
            "vendors": [
              "string"
            ]
          }
        },
        "user_settings": {
          "hdd_encryption_settings": {
            "encrypt_drives": [
              "string"
            ]
          }
        }
      },
      "custom_rule": {
        "platform": "windows",
        "type": "process",
        "registry": {
          "root_key": "HKEY_LOCAL_MACHINE",
          "sub_key": "string",
          "type": "string",
          "key": "string",
          "value": "string",
          "is_64_bit": true,
          "remediate": true,
          "monitor": true
        },
        "process": {
          "process_name": "string",
          "md5_checksum": "string",
          "sha256_checksum": "string",
          "monitor": true,
          "action": "allow"
        },
        "mobile_os_check": {
```

```
          "os_version": "string",
          "rule_separator": "above"
        },
        "desktop_os_check": [
          {
            "os_version": "string",
            "service_pack_version": "string"
          }
        ],
        "file": {
          "file_name": "string",
          "md5_checksum": "string",
          "sha256_checksum": "string",
          "monitor": true,
          "action": "allow"
        },
        "cve_check": {
          "check_all": true,
          "cve_list": [
            "string"
          ]
        },
        "mobile_jail_break_root_check_enabled": true,
        "netbios": {
          "allow": true,
          "names": [
            "string"
          ]
        },
        "mac_address": {
          "allow": true,
          "address": [
            "string"
          ]
        }
      }
    },
    "allow_delete": true,
    "is_default": true
  }
```

```
  ]
}
```

Creating a Device Policy

To create a *device-policy/groups* entity, use the REST API call below:

- **Method:** POST /api/v1/policies/device-policies/device-policy/groups
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new *device-policy/groups* entity.

If processed correctly, a JSON body containing the new *device-policy/groups* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/v1/policies/device-policies/device-policy/groups
Authorization:
Content-Type: application/json
Request Body
{
        "name": "string",
        "description": "string",
        "is_default": true,
        "rules": [
        {
        "additionalProp1": {}
        }
        ],
        "rule_requirements": [
        {
        "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "device_policy_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "all_of_the_above": "string",
        "any_of_the_above": "string",
        "custom_expression_enabled": true,
        "custom_expression": "string",
        "platform": "windows"
        }
        ],
        "remediation": {
        "additionalProp1": {}
        },
        "enable_custom_instructions": true,
        "custom_instructions": "string"
        }
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
       "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
       "name": "string",
       "description": "string",
       "is_default": true,
       "rule_names": [
       "string"
       ],
       "rules": [
       {
       "additionalProp1": {}
       }
       ],
       "rule_requirements": [
       {
       "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
       "device_policy_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
       "all_of_the_above": "string",
       "any_of_the_above": "string",
       "custom_expression_enabled": true,
       "custom_expression": "string",
       "platform": "windows"
       }
       ],
       "remediation": {
       "additionalProp1": {}
       },
       "enable_custom_instructions": true,
       "custom_instructions": "string"
}
```

Editing a Device Policy

To edit a *device-policy/groups* entity, use the REST API call below:

- **Method:** PUT /api/v1/policies/device-policies/device-policy/groups/{id}
- **Resource:** Path
- **JSON Data:** JSON dictionary representing changed properties for a *device-policy/groups* entity.

If processed correctly, a JSON body containing the updated *device-policy/groups* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      PUT /api/v1/policies/device-policies/device-policy/groups/{id}
Authorization:
Content-Type: application/json
Request Body
{
  "name": "string",
  "description": "string"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "description": "string",
  "is_default": true,
  "rules": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "name": "string",
      "description": "string",
      "type": "browser",
      "label": "high",
      "browser_config": {
        "user_agent": "string",
        "mode": "allow"
      },
      "network_config": {
        "ip_address": "string",
        "netmask": "string",
        "mode": "allow"
      },
      "hostchecker_config": {
        "name": "string",
        "type": "predefined",
        "predefined_rule": {
          "type": "antivirus",
          "hostchecker_level_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "hostchecker_product_list_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
          "hostchecker_level_name": "string",
          "hostchecker_product_list": {
            "windows": {
              "products": [
                "string"
              ],
              "vendors": [
                "string"
```

```
            ]
          },
          "mac": {
            "products": [
              "string"
            ],
            "vendors": [
              "string"
            ]
          }
        },
        "user_settings": {
          "hdd_encryption_settings": {
            "encrypt_drives": [
              "string"
            ]
          }
        }
      },
      "custom_rule": {
        "platform": "windows",
        "type": "process",
        "registry": {
          "root_key": "HKEY_LOCAL_MACHINE",
          "sub_key": "string",
          "type": "string",
          "key": "string",
          "value": "string",
          "is_64_bit": true,
          "remediate": true,
          "monitor": true
        },
        "process": {
          "process_name": "string",
          "md5_checksum": "string",
          "sha256_checksum": "string",
          "monitor": true,
          "action": "allow"
        },
        "mobile_os_check": {
```

```
          "os_version": "string",
          "rule_separator": "above"
        },
        "desktop_os_check": [
          {
            "os_version": "string",
            "service_pack_version": "string"
          }
        ],
        "file": {
          "file_name": "string",
          "md5_checksum": "string",
          "sha256_checksum": "string",
          "monitor": true,
          "action": "allow"
        },
        "cve_check": {
          "check_all": true,
          "cve_list": [
            "string"
          ]
        },
        "mobile_jail_break_root_check_enabled": true,
        "netbios": {
          "allow": true,
          "names": [
            "string"
          ]
        },
        "mac_address": {
          "allow": true,
          "address": [
            "string"
          ]
        }
      }
    },
    "allow_delete": true,
    "is_default": true
  }
```

```
  ]
}
```

Deleting a Device Policy

To delete a *device-policy/groups* entity, use the REST API call below:

- **Method:** DELETE /api/v1/policies/device-policies/device-policy/groups/{id}
- **Resource:** Path

If processed correctly, a confirmation is returned. Otherwise, an error is returned.

Request

The following is an example request:

```
      DELETE /api/v1/policies/device-policies/device-policy/groups/{id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 204 Device-policy/groups deleted successfully
Content-Type: application/json
```

Device Policy Rules (device-policy/rules)

The *device-policy/rules* entity represents a *nZTA* policy rule configuration. Device policy rules support the following activities:

- Retrieving all device policy rules, see Retrieving all device policy rules.
- Retrieving a specific device policy rule, see Retrieving a specific device policy rule.
- Creating a device policy rule, see Creating a device policy rule.
- Editing a device policy rule, see Editing a device policy rule.
- Deleting a device policy rule, see Deleting a device policy rule.
- Adding a device policy rule to a device policy, see Adding a device policy rule to a device policy.
- Removing a device policy rule from a device policy, see Removing a device policy rule from a device policy.

> Device rules added or edited through the API are considered *custom* and do not use the "Security Level" field. This field applies only to built-in default device rules.

Retrieving all Device Policy Rules

To retrieve all *device-policy/rules* entities, use the REST API call below:

- **Method:** GET /api/v1/policies/device-policies/device-policy/rules
- **Resource:** Path

If processed correctly, a JSON body containing a list of all *device-policy/rules* entities is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/device-policies/device-policy/rules
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "items": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "name": "string",
      "description": "string",
      "type": "browser",
      "label": "high",
      "browser_config": {
        "user_agent": "string",
        "mode": "allow"
      },
      "network_config": {
        "ip_address": "string",
        "netmask": "string",
        "mode": "allow"
      },
      "hostchecker_config": {
        "name": "string",
        "type": "predefined",
        "predefined_rule": {
          "type": "antivirus",
          "hostchecker_level_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "hostchecker_product_list_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
          "hostchecker_level_name": "string",
          "hostchecker_product_list": {
            "windows": {
              "products": [
                "string"
              ],
              "vendors": [
                "string"
              ]
            },
            "mac": {
              "products": [
```

```
            "string"
          ],
          "vendors": [
            "string"
          ]
        }
      },
      "user_settings": {
        "hdd_encryption_settings": {
          "encrypt_drives": [
            "string"
          ]
        }
      }
    },
    "custom_rule": {
      "platform": "windows",
      "type": "process",
      "registry": {
        "root_key": "HKEY_LOCAL_MACHINE",
        "sub_key": "string",
        "type": "string",
        "key": "string",
        "value": "string",
        "is_64_bit": true,
        "remediate": true,
        "monitor": true
      },
      "process": {
        "process_name": "string",
        "md5_checksum": "string",
        "sha256_checksum": "string",
        "monitor": true,
        "action": "allow"
      },
      "mobile_os_check": {
        "os_version": "string",
        "rule_separator": "above"
      },
      "desktop_os_check": [
```

```
            {
              "os_version": "string",
              "service_pack_version": "string"
            }
          ],
          "file": {
            "file_name": "string",
            "md5_checksum": "string",
            "sha256_checksum": "string",
            "monitor": true,
            "action": "allow"
          },
          "cve_check": {
            "check_all": true,
            "cve_list": [
              "string"
            ]
          },
          "mobile_jail_break_root_check_enabled": true,
          "netbios": {
            "allow": true,
            "names": [
              "string"
            ]
          },
          "mac_address": {
            "allow": true,
            "address": [
              "string"
            ]
          }
        }
      },
      "allow_delete": true,
      "is_default": true
    }
  ]
}
```

Retrieving a Specific Device Policy Rule

To retrieve a single *device-policy/rules* entity, use the REST API call below:

- **Method:** GET /api/v1/policies/device-policies/device-policy/rules/{id}
- **Resource:** Path

If processed correctly, a JSON body containing the *device-policy/rules* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/device-policies/device-policy/rules/{id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "description": "string",
  "type": "browser",
  "label": "high",
  "browser_config": {
    "user_agent": "string",
    "mode": "allow"
  },
  "network_config": {
    "ip_address": "string",
    "netmask": "string",
    "mode": "allow"
  },
  "hostchecker_config": {
    "name": "string",
    "type": "predefined",
    "predefined_rule": {
      "type": "antivirus",
      "hostchecker_level_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "hostchecker_product_list_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
      "hostchecker_level_name": "string",
      "hostchecker_product_list": {
        "windows": {
          "products": [
            "string"
          ],
          "vendors": [
            "string"
          ]
        },
        "mac": {
          "products": [
            "string"
          ],
```

```
        "vendors": [
          "string"
        ]
      }
    },
    "user_settings": {
      "hdd_encryption_settings": {
        "encrypt_drives": [
          "string"
        ]
      }
    }
  },
  "custom_rule": {
    "platform": "windows",
    "type": "process",
    "registry": {
      "root_key": "HKEY_LOCAL_MACHINE",
      "sub_key": "string",
      "type": "string",
      "key": "string",
      "value": "string",
      "is_64_bit": true,
      "remediate": true,
      "monitor": true
    },
    "process": {
      "process_name": "string",
      "md5_checksum": "string",
      "sha256_checksum": "string",
      "monitor": true,
      "action": "allow"
    },
    "mobile_os_check": {
      "os_version": "string",
      "rule_separator": "above"
    },
    "desktop_os_check": [
      {
        "os_version": "string",
```

```
          "service_pack_version": "string"
        }
      ],
      "file": {
        "file_name": "string",
        "md5_checksum": "string",
        "sha256_checksum": "string",
        "monitor": true,
        "action": "allow"
      },
      "cve_check": {
        "check_all": true,
        "cve_list": [
          "string"
        ]
      },
      "mobile_jail_break_root_check_enabled": true,
      "netbios": {
        "allow": true,
        "names": [
          "string"
        ]
      },
      "mac_address": {
        "allow": true,
        "address": [
          "string"
        ]
      }
    }
  },
  "allow_delete": true,
  "is_default": true
}
```


Creating a Device Policy Rule

You can create rules for the following rule types:

- antispyware
- cve_check
- firewall
- hdd_encryption
- mac_address
- netbios
- patch_management
- process
- network
- registry
- file
- antivirus
- os
- jail_break_root

To create a *device-policy/rules* entity, use the REST API call below:

- **Method:** POST /api/v1/policies/device-policies/device-policy/rules
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new *device-policy/rules* entity.

If processed correctly, a JSON body containing the new *device-policy/rules* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/v1/policies/device-policies/device-policy/rules
Authorization:
Content-Type: application/json
Request Body
{
  "name": "string",
  "description": "string",
  "type": "browser",
  "label": "high",
  "browser_config": {
    "user_agent": "string",
    "mode": "allow"
  },
  "network_config": {
    "ip_address": "string",
    "netmask": "string",
    "mode": "allow"
  },
  "hostchecker_config": {
    "name": "string",
    "type": "predefined",
    "predefined_rule": {
      "type": "antivirus",
      "hostchecker_level_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "hostchecker_product_list_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
      "user_settings": {
        "hdd_encryption_settings": {
          "encrypt_drives": [
            "string"
          ]
        }
      },
      "hostchecker_level_name": "string",
      "hostchecker_product_list": {
        "products": [
          "string"
        ],
        "vendors": [
          "string"
```

```
      ]
    },
    "platform": "windows"
  },
  "custom_rule": {
    "platform": "windows",
    "type": "process",
    "registry": {
      "root_key": "HKEY_LOCAL_MACHINE",
      "sub_key": "string",
      "type": "string",
      "key": "string",
      "value": "string",
      "is_64_bit": true,
      "remediate": true,
      "monitor": true
    },
    "process": {
      "process_name": "string",
      "md5_checksum": "string",
      "sha256_checksum": "string",
      "monitor": true,
      "action": "allow"
    },
    "mobile_os_check": {
      "os_version": "string",
      "rule_separator": "above"
    },
    "desktop_os_check": [
      {
        "os_version": "string",
        "service_pack_version": "string"
      }
    ],
    "file": {
      "file_name": "string",
      "md5_checksum": "string",
      "sha256_checksum": "string",
      "monitor": true,
      "action": "allow"
```

```
      },
      "cve_check": {
        "check_all": true,
        "cve_list": [
          "string"
        ]
      },
      "mobile_jail_break_root_check_enabled": true,
      "netbios": {
        "allow": true,
        "names": [
          "string"
        ]
      },
      "mac_address": {
        "allow": true,
        "address": [
          "string"
        ]
      }
    }
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "description": "string",
  "type": "browser",
  "label": "high",
  "browser_config": {
    "user_agent": "string",
    "mode": "allow"
  },
  "network_config": {
    "ip_address": "string",
    "netmask": "string",
    "mode": "allow"
  },
  "hostchecker_config": {
    "name": "string",
    "type": "predefined",
    "predefined_rule": {
      "type": "antivirus",
      "hostchecker_level_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "hostchecker_product_list_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
      "hostchecker_level_name": "string",
      "hostchecker_product_list": {
        "windows": {
          "products": [
            "string"
          ],
          "vendors": [
            "string"
          ]
        },
        "mac": {
          "products": [
            "string"
          ],
```

```
        "vendors": [
          "string"
        ]
      }
    },
    "user_settings": {
      "hdd_encryption_settings": {
        "encrypt_drives": [
          "string"
        ]
      }
    }
  },
  "custom_rule": {
    "platform": "windows",
    "type": "process",
    "registry": {
      "root_key": "HKEY_LOCAL_MACHINE",
      "sub_key": "string",
      "type": "string",
      "key": "string",
      "value": "string",
      "is_64_bit": true,
      "remediate": true,
      "monitor": true
    },
    "process": {
      "process_name": "string",
      "md5_checksum": "string",
      "sha256_checksum": "string",
      "monitor": true,
      "action": "allow"
    },
    "mobile_os_check": {
      "os_version": "string",
      "rule_separator": "above"
    },
    "desktop_os_check": [
      {
        "os_version": "string",
```

```
          "service_pack_version": "string"
        }
      ],
      "file": {
        "file_name": "string",
        "md5_checksum": "string",
        "sha256_checksum": "string",
        "monitor": true,
        "action": "allow"
      },
      "cve_check": {
        "check_all": true,
        "cve_list": [
          "string"
        ]
      },
      "mobile_jail_break_root_check_enabled": true,
      "netbios": {
        "allow": true,
        "names": [
          "string"
        ]
      },
      "mac_address": {
        "allow": true,
        "address": [
          "string"
        ]
      }
    }
  },
  "allow_delete": true,
  "is_default": true
}
```


Editing a Device Policy Rule

To edit a *device-policy/rules* entity, use the REST API call below:

- **Method:** PUT /api/v1/policies/device-policies/device-policy/rules/{id}
- **Resource:** Path
- **JSON Data:** JSON dictionary representing changed properties for a *device-policy/rules* entity.

If processed correctly, a JSON body containing the updated *device-policy/rules* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      PUT /api/v1/policies/device-policies/device-policy/rules/{id}
Authorization:
Content-Type: application/json
Request Body
{
  "name": "string",
  "description": "string",
  "type": "browser",
  "label": "high",
  "browser_config": {
    "user_agent": "string",
    "mode": "allow"
  },
  "network_config": {
    "ip_address": "string",
    "netmask": "string",
    "mode": "allow"
  },
  "hostchecker_config": {
    "name": "string",
    "type": "predefined",
    "predefined_rule": {
      "type": "antivirus",
      "hostchecker_level_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "hostchecker_product_list_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
      "user_settings": {
        "hdd_encryption_settings": {
          "encrypt_drives": [
            "string"
          ]
        }
      },
      "hostchecker_level_name": "string",
      "hostchecker_product_list": {
        "products": [
          "string"
        ],
        "vendors": [
          "string"
```

```
      ]
    },
    "platform": "windows"
  },
  "custom_rule": {
    "platform": "windows",
    "type": "process",
    "registry": {
      "root_key": "HKEY_LOCAL_MACHINE",
      "sub_key": "string",
      "type": "string",
      "key": "string",
      "value": "string",
      "is_64_bit": true,
      "remediate": true,
      "monitor": true
    },
    "process": {
      "process_name": "string",
      "md5_checksum": "string",
      "sha256_checksum": "string",
      "monitor": true,
      "action": "allow"
    },
    "mobile_os_check": {
      "os_version": "string",
      "rule_separator": "above"
    },
    "desktop_os_check": [
      {
        "os_version": "string",
        "service_pack_version": "string"
      }
    ],
    "file": {
      "file_name": "string",
      "md5_checksum": "string",
      "sha256_checksum": "string",
      "monitor": true,
      "action": "allow"
```

```
      },
      "cve_check": {
        "check_all": true,
        "cve_list": [
          "string"
        ]
      },
      "mobile_jail_break_root_check_enabled": true,
      "netbios": {
        "allow": true,
        "names": [
          "string"
        ]
      },
      "mac_address": {
        "allow": true,
        "address": [
          "string"
        ]
      }
    }
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "description": "string",
  "type": "browser",
  "label": "high",
  "browser_config": {
    "user_agent": "string",
    "mode": "allow"
  },
  "network_config": {
    "ip_address": "string",
    "netmask": "string",
    "mode": "allow"
  },
  "hostchecker_config": {
    "name": "string",
    "type": "predefined",
    "predefined_rule": {
      "type": "antivirus",
      "hostchecker_level_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "hostchecker_product_list_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
      "hostchecker_level_name": "string",
      "hostchecker_product_list": {
        "windows": {
          "products": [
            "string"
          ],
          "vendors": [
            "string"
          ]
        },
        "mac": {
          "products": [
            "string"
          ],
```

```
        "vendors": [
          "string"
        ]
      }
    },
    "user_settings": {
      "hdd_encryption_settings": {
        "encrypt_drives": [
          "string"
        ]
      }
    }
  },
  "custom_rule": {
    "platform": "windows",
    "type": "process",
    "registry": {
      "root_key": "HKEY_LOCAL_MACHINE",
      "sub_key": "string",
      "type": "string",
      "key": "string",
      "value": "string",
      "is_64_bit": true,
      "remediate": true,
      "monitor": true
    },
    "process": {
      "process_name": "string",
      "md5_checksum": "string",
      "sha256_checksum": "string",
      "monitor": true,
      "action": "allow"
    },
    "mobile_os_check": {
      "os_version": "string",
      "rule_separator": "above"
    },
    "desktop_os_check": [
      {
        "os_version": "string",
```

```
          "service_pack_version": "string"
        }
      ],
      "file": {
        "file_name": "string",
        "md5_checksum": "string",
        "sha256_checksum": "string",
        "monitor": true,
        "action": "allow"
      },
      "cve_check": {
        "check_all": true,
        "cve_list": [
          "string"
        ]
      },
      "mobile_jail_break_root_check_enabled": true,
      "netbios": {
        "allow": true,
        "names": [
          "string"
        ]
      },
      "mac_address": {
        "allow": true,
        "address": [
          "string"
        ]
      }
    }
  },
  "allow_delete": true,
  "is_default": true
}
```


Deleting a Device Policy Rule

To delete a *device-policy/rules* entity, use the REST API call below:

- **Method:** DELETE /api/v1/policies/device-policies/device-policy/rules/{id}
- **Resource:** Path

If processed correctly, a confirmation is returned. Otherwise, an error is returned.

Request

The following is an example request:

```
      DELETE /api/v1/policies/device-policies/device-policy/rules/{id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 204 Device-policy/rules deleted successfully
Content-Type: application/json
```

Adding a Device Policy Rule to a Device Policy

To add a *device-policy/rule* entity to a *device-policy/rule* entity, use the REST API call below:

- **Method:** PUT /api/v1/policies/device-policies/groups/{id}/rules/{rule_id}
- **Resource:** Path

If processed correctly, a confirmation is returned. Otherwise, an error is returned.

Request

The following is an example request:

```
      PUT /api/v1/policies/device-policies/groups/{id}/rules/{rule_id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 204 Rule added to Device Policy successfully
Content-Type: application/json
```

Removing a Device Policy Rule from a Device Policy

To remove a *device-policy/rule* entity from a *device-policy/rule* entity, use the REST API call below:

- **Method:** DELETE /api/v1/policies/device-policies/groups/{id}/rules/{rule_id}
- **Resource:** Path

If processed correctly, a confirmation is returned. Otherwise, an error is returned.

Request

The following is an example request:

```
      DELETE /api/v1/policies/device-policies/groups/{id}/rules/{rule_id}
Authorization:-
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 204 Rule in Device Policy Group deleted successfully
Content-Type: application/json
```

Gateway (gateways)

The *gateways* entity represents a *ZTA Gateway*. Gateways support the following activities:

- Retrieving all gateways, see Retrieving all gateways.
- Creating a gateway, see Creating a gateway.
- Editing a gateway, see Editing a gateway.
- Deleting a gateway, see Deleting a gateway.
- Renewing a client certificate, see Renewing a client certificate.

Retrieving all Gateways

To retrieve all *gateways* entities, use the REST API call below:

- **Method:** GET /api/gateways
- **Resource:** Path

If processed correctly, a JSON body containing a list of all *gateways* entities is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/gateways
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
[
  {
    "id": "e274bf3ebe3841a88ade1630515624c6",
    "name": "string",
    "gateway_type": "pzt_gateway",
    "state": "unregistered",
    "created": "string",
    "updated": "string",
    "type": "string",
    "model": "string",
    "serial_number": "string",
    "appliance_version": "string",
    "sdp_mode": "pzt-gateway",
    "location": {
      "name": "string",
      "city_id": 0
    },
    "notification_channel_status": "online",
    "orchestration": {
      "type": "vsphere",
      "mode": "auto",
      "state": "waiting-to-create"
    },
    "external_ip": "string",
    "external_fqdn": "string",
    "public_ip": "string",
    "public_ips": [
      "xx.xx.xx.xx"
    ],
    "dns_cname": "string",
    "salient_task": {
      "id": "e274bf3ebe3841a88ade1630515624c6",
      "status": "pending",
      "type": "system.operations.appliance.task",
      "group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "created": "string",
      "completed": "string"
```

```
    },
    "group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "is_ready": true,
    "actions": [
      "upgrade"
    ],
    "auto_upgrade": true,
    "capabilities": [
      "readiness"
    ]
  }
]
```

Creating a Gateway

To create a *gateways* entity, use the REST API call below:

- **Method:** POST /api/gateways
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new *gateways* entity.

If processed correctly, a JSON body containing the new *gateways* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/gateways
Authorization:
Content-Type: application/json
Request Body
{
  "name": "test_gateway",
  "orchestration_type": "vsphere"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "e274bf3ebe3841a88ade1630515624c6",
  "name": "test_gateway",
  "state": "unregistered",
  "sdp_mode": "gateway",
  "notification_channel_status": "offline",
  "orchestration": {
    "type": "vsphere",
    "mode": "manual"
  }
}
```

Editing a Gateway

To edit a *gateways* entity, use the REST API call below:

- **Method:** PUT /api/gateways/{gateway_id}
- **Resource:** Path
- **JSON Data:** JSON dictionary representing changed properties for a *gateways* entity.

If processed correctly, a JSON body containing the updated *gateways* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      PUT /api/gateways/{gateway_id}
Authorization:
Content-Type: application/json
Request Body
{
  "group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "e274bf3ebe3841a88ade1630515624c6",
  "name": "string",
  "state": "unregistered",
  "created": "string",
  "updated": "string",
  "type": "string",
  "model": "string",
  "serial_number": "string",
  "appliance_version": "string",
  "sdp_mode": "pzt-gateway",
  "location": {
    "name": "string",
    "city_id": 0
  },
  "notification_channel_status": "online",
  "orchestration": {
    "type": "vsphere",
    "mode": "auto",
    "state": "waiting-to-create"
  },
  "external_ip": "string",
  "external_fqdn": "string",
  "public_ip": "string",
  "salient_task": {
    "id": "e274bf3ebe3841a88ade1630515624c6",
    "status": "pending",
    "type": "system.operations.appliance.task",
    "group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "created": "string",
    "completed": "string"
  },
  "group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "is_ready": true,
  "actions": [
    "upgrade"
  ],
```

```
  "auto_upgrade": true,
  "capabilities": [
    "readiness"
  ]
}
```

Deleting a Gateway

To delete a *gateways* entity, use the REST API call below:

- **Method:** DELETE /api/gateways/{gateway_id}
- **Resource:** Path

If processed correctly, a confirmation is returned. Otherwise, an error is returned.

Request

The following is an example request:

```
      DELETE /api/gateways/{gateway_id}
Authorization:
Content-Type: application/json
Request Body
{
   "id": "e274bf3ebe3841a88ade1630515624c6",
}
```

Response

The following is an example response:

```
        HTTP/1.1 204 Gateway deleted successfully
Content-Type: application/json
```

Renewing a Client Certificate

To renew a certificate for a client, use the REST API call below:

- **Method:** POST /api/gateways/self/certificates/client
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a certificate signing request (CSR).

If processed correctly, a JSON body containing the new client certificate is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/gateways/self/certificates/client
Authorization:
Content-Type: application/json
Request Body
{
   "csr": "string"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
   "certificate": "string",
   "format": "PEM"
}
```

Gateway Settings

Gateway settings are additional properties for a *ZTA Gateway*. Gateway settings support the following activities:

- Retrieving the settings for a gateway, see Retrieving the Settings for a Gateway.
- Editing the settings for a gateway, see Editing Settings for a Gateway.

Retrieving the Settings for a Gateway

To retrieve the settings for a *gateways* entity, use the REST API call below:

- **Method:** GET /api/gateways/{gateway_id}/settings/current
- **Resource:** Path

If processed correctly, a JSON body containing the properties for the *gateways* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/gateways/{gateway_id}/settings/current
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "version": "string",
  "primary_dns": "string",
  "secondary_dns": "string",
  "dns_search_domain": "string",
  "internal_ip_address": "string",
  "internal_subnet": "string",
  "internal_gateway": "string",
  "external_ip_address": "string",
  "external_subnet": "string",
  "external_gateway": "string",
  "management_ip_address": "string",
  "management_subnet": "string",
  "management_gateway": "string",
  "connect_via_mgmt_interface": true,
  "model": "string",
  "rollback_version": "string",
  "use_dhcp": true,
  "previous_version": "string",
  "updated": "string",
  "public_ip_address": "string",
  "public_ip_addresses": [
    "10.1.2.3"
  ],
  "dns_cname": "string"
}
```

Editing Settings for a Gateway

To edit the settings for a *gateways* entity, use the REST API call below:

- **Method:** PUT /api/gateways/self/settings/current
- **Resource:** Path
- **JSON Data:** JSON dictionary representing updated settings

If processed correctly, a JSON body containing the updated properties for the *gateways* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      PUT /api/gateways/self/settings/current
Authorization:
Content-Type: application/json
Request Body
{
  "version": "string",
  "primary_dns": "string",
  "secondary_dns": "string",
  "dns_search_domain": "string",
  "internal_ip_address": "string",
  "internal_subnet": "string",
  "internal_gateway": "string",
  "external_ip_address": "string",
  "external_subnet": "string",
  "external_gateway": "string",
  "management_ip_address": "string",
  "management_subnet": "string",
  "management_gateway": "string",
  "connect_via_mgmt_interface": true,
  "model": "string",
  "rollback_version": "string"
}
```

Response

The following is an example response:

```
        HTTP/1.1 204 Gateway settings updated successfully
Content-Type: application/json
```

Gateway Group (groups)

The groups entity represents a *ZTA Gateway* group. Gateway groups support the following activities:

- Retrieving a gateway groups, see Retrieving a gateway groups.
- Creating a gateway group, see Creating a gateway group.
- Editing a gateway group, see Editing a gateway group.

Retrieving a Gateway Group

To retrieve all gateway groups, use the REST API call below:

- **Method:** GET /api/gateways/groups
- **Resource:** Path

If processed correctly, a JSON body containing a list of all gateway groups is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/gateways/groups
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
   "items": [
      {
         "name": "asia-pacific-grp",
         "description": "Gateway group assigned to Asia Pacific region",
         "load_balancer_ips": [
            "10.1.2.3"
         ],
         "dns_cname": "string",
         "id": "e274bf3ebe3841a88ade1630515624c6",
         "external_fqdn": "string",
         "created": "string",
         "updated": "string",
         "members": [
            "e274bf3ebe3841a88ade1630515624c6"
         ],
         "connected_members": [
            "e274bf3ebe3841a88ade1630515624c6"
         ],
         "ready_members": [
            "e274bf3ebe3841a88ade1630515624c6"
         ]
      }
   ],
   "total": 10
}
```

Creating a Gateway Group

To create a gateway group, use the REST API call below:

- **Method:** POST /api/gateways/groups
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new gateway group.

If processed correctly, a JSON body containing the new gateway group is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/gateways/groups
Authorization:
Content-Type: application/json
Request Body
{
   "name": "asia-pacific-grp",
   "description": "Gateway group assigned to Asia Pacific region",
   "load_balancer_ips": [
      "10.1.2.3"
   ],
   "dns_cname": "string",
   "members": [
      "e274bf3ebe3841a88ade1630515624c6"
   ]
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
   "name": "asia-pacific-grp",
   "description": "Gateway group assigned to Asia Pacific region",
   "load_balancer_ips": [
      "10.1.2.3"
   ],
   "dns_cname": "string",
   "id": "e274bf3ebe3841a88ade1630515624c6",
   "external_fqdn": "string",
   "created": "string",
   "updated": "string",
   "members": [
      "e274bf3ebe3841a88ade1630515624c6"
   ],
   "connected_members": [
      "e274bf3ebe3841a88ade1630515624c6"
   ],
   "ready_members": [
      "e274bf3ebe3841a88ade1630515624c6"
   ]
}
```

Editing a Gateway Group

To edit a gateway group, use the REST API call below:

- **Method:** PUT /api/gateways/groups/{id}
- **Resource:** Path
- **JSON Data:** JSON dictionary representing changed properties for a gateway group.

If processed correctly, a JSON body containing the updated gateway group is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      PUT /api/gateways/groups/{id}
Authorization:
Content-Type: application/json
Request Body
{
   "name": "asia-pacific-grp",
   "description": "Gateway group assigned to Asia Pacific region",
   "load_balancer_ips": [
      "10.1.2.3"
   ],
   "dns_cname": "string"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
   "name": "asia-pacific-grp",
   "description": "Gateway group assigned to Asia Pacific region",
   "load_balancer_ips": [
      "10.1.2.3"
   ],
   "dns_cname": "string",
   "id": "e274bf3ebe3841a88ade1630515624c6",
   "external_fqdn": "string",
   "created": "string",
   "updated": "string",
   "members": [
      "e274bf3ebe3841a88ade1630515624c6"
   ],
   "connected_members": [
      "e274bf3ebe3841a88ade1630515624c6"
   ],
   "ready_members": [
      "e274bf3ebe3841a88ade1630515624c6"
   ]
}
```

Hostchecker Levels (hostchecker/levels)

The *hostchecker/levels* entity represents a *nZTA* hostchecker configuration.

> Hostchecker levels must be created and configured before device policies can be created successfully.

Hostchecker levels support the following activities:

- Retrieving all hostchecker levels, see Retrieving all hostchecker levels.
- Retrieving a specific hostchecker level, see Retrieving a specific hostchecker level.
- Creating a hostchecker level, see Creating a hostchecker level.
- Editing a hostchecker level, see Editing a hostchecker level.
- Deleting a hostchecker level, see Deleting a hostchecker level.

Retrieving all Hostchecker Levels

To retrieve all *hostchecker/levels* entities, use the REST API call below:

- **Method:** GET /api/v1/policies/device-policies/hostchecker/levels
- **Resource:** Path

If processed correctly, a JSON body containing a list of all *hostchecker/levels* entities is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/device-policies/hostchecker/levels
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "items": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "name": "string",
      "antivirus": {
        "check_last_scan": true,
        "last_scan_period": 0,
        "check_definition": true,
        "definition_check_type": "days",
        "remediate_last_scan": true,
        "remediate_download_signatures": true,
        "monitor": true
      },
      "firewall": {
        "remediate": true,
        "monitor": true
      },
      "hdd_encryption": {
        "encrypt_all_drives": true,
        "pass_no_drive_detected": true
      },
      "antispyware": {
        "monitor": true
      },
      "patch_management": {
        "severity": {
          "critical": true,
          "important": true,
          "moderate": true,
          "low": true,
          "unspecified": true
        },
        "category": {
          "security": true,
          "rollup": true,
          "critical": true,
```

```
          "regular": true,
          "driver": true,
          "service_pack": true,
          "unknown": true
        }
      }
    }
  ],
  "total": 0
}
```

Retrieving a Specific Hostchecker Level

To retrieve a single *hostchecker/levels* entity, use the REST API call below:

- **Method:** GET /api/v1/policies/device-policies/hostchecker/levels/{id}
- **Resource:** Path

If processed correctly, a JSON body containing the *hostchecker/levels* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/device-policies/hostchecker/levels/{id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "antivirus": {
    "check_last_scan": true,
    "last_scan_period": 0,
    "check_definition": true,
    "definition_check_type": "days",
    "remediate_last_scan": true,
    "remediate_download_signatures": true,
    "monitor": true
  },
  "firewall": {
    "remediate": true,
    "monitor": true
  },
  "hdd_encryption": {
    "encrypt_all_drives": true,
    "pass_no_drive_detected": true
  },
  "antispyware": {
    "monitor": true
  },
  "patch_management": {
    "severity": {
      "critical": true,
      "important": true,
      "moderate": true,
      "low": true,
      "unspecified": true
    },
    "category": {
      "security": true,
      "rollup": true,
      "critical": true,
      "regular": true,
      "driver": true,
```

```
      "service_pack": true,
      "unknown": true
    }
  }
}
```

Creating a Hostchecker Level

To create a *hostchecker/levels* entity, use the REST API call below:

- **Method:** POST /api/v1/policies/device-policies/hostchecker/levels
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new *hostchecker/levels* entity.

If processed correctly, a JSON body containing the new *hostchecker/levels* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/v1/policies/device-policies/hostchecker/levels
Authorization:
Content-Type: application/json
Request Body
{
  "name": "string",
  "antivirus": {
    "check_last_scan": true,
    "last_scan_period": 0,
    "check_definition": true,
    "definition_check_type": "days",
    "remediate_last_scan": true,
    "remediate_download_signatures": true,
    "monitor": true
  },
  "firewall": {
    "remediate": true,
    "monitor": true
  },
  "hdd_encryption": {
    "encrypt_all_drives": true,
    "pass_no_drive_detected": true
  },
  "antispyware": {
    "monitor": true
  },
  "patch_management": {
    "severity": {
      "critical": true,
      "important": true,
      "moderate": true,
      "low": true,
      "unspecified": true
    },
    "category": {
      "security": true,
      "rollup": true,
      "critical": true,
      "regular": true,
      "driver": true,
```

```
      "service_pack": true,
      "unknown": true
    }
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "antivirus": {
    "check_last_scan": true,
    "last_scan_period": 0,
    "check_definition": true,
    "definition_check_type": "days",
    "remediate_last_scan": true,
    "remediate_download_signatures": true,
    "monitor": true
  },
  "firewall": {
    "remediate": true,
    "monitor": true
  },
  "hdd_encryption": {
    "encrypt_all_drives": true,
    "pass_no_drive_detected": true
  },
  "antispyware": {
    "monitor": true
  },
  "patch_management": {
    "severity": {
      "critical": true,
      "important": true,
      "moderate": true,
      "low": true,
      "unspecified": true
    },
    "category": {
      "security": true,
      "rollup": true,
      "critical": true,
      "regular": true,
      "driver": true,
```

```
      "service_pack": true,
      "unknown": true
    }
  }
}
```

Editing a Hostchecker Level

To edit a *hostchecker/levels* entity, use the REST API call below:

- **Method:** PUT /api/v1/policies/device-policies/hostchecker/levels/{id}
- **Resource:** Path
- **JSON Data:** JSON dictionary representing changed properties for a *hostchecker/levels* entity.

If processed correctly, a JSON body containing the updated *hostchecker/levels* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      PUT /api/v1/policies/device-policies/hostchecker/levels/{id}
Authorization:
Content-Type: application/json
Request Body
{
  "name": "string",
  "antivirus": {
    "check_last_scan": true,
    "last_scan_period": 0,
    "check_definition": true,
    "definition_check_type": "days",
    "remediate_last_scan": true,
    "remediate_download_signatures": true,
    "monitor": true
  },
  "firewall": {
    "remediate": true,
    "monitor": true
  },
  "hdd_encryption": {
    "encrypt_all_drives": true,
    "pass_no_drive_detected": true
  },
  "antispyware": {
    "monitor": true
  },
  "patch_management": {
    "severity": {
      "critical": true,
      "important": true,
      "moderate": true,
      "low": true,
      "unspecified": true
    },
    "category": {
      "security": true,
      "rollup": true,
      "critical": true,
      "regular": true,
      "driver": true,
```

```
      "service_pack": true,
      "unknown": true
    }
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "antivirus": {
    "check_last_scan": true,
    "last_scan_period": 0,
    "check_definition": true,
    "definition_check_type": "days",
    "remediate_last_scan": true,
    "remediate_download_signatures": true,
    "monitor": true
  },
  "firewall": {
    "remediate": true,
    "monitor": true
  },
  "hdd_encryption": {
    "encrypt_all_drives": true,
    "pass_no_drive_detected": true
  },
  "antispyware": {
    "monitor": true
  },
  "patch_management": {
    "severity": {
      "critical": true,
      "important": true,
      "moderate": true,
      "low": true,
      "unspecified": true
    },
    "category": {
      "security": true,
      "rollup": true,
      "critical": true,
      "regular": true,
      "driver": true,
```

```
      "service_pack": true,
      "unknown": true
    }
  }
}
```

Deleting a Hostchecker Level

To delete a *hostchecker/levels* entity, use the REST API call below:

- **Method:** DELETE /api/v1/policies/device-policies/hostchecker/levels/{id}
- **Resource:** Path

If processed correctly, a confirmation is returned. Otherwise, an error is returned.

Request

The following is an example request:

```
      DELETE /api/v1/policies/device-policies/hostchecker/levels/{id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 204 Hostchecker/levels deleted successfully
Content-Type: application/json
```

Hostchecker Products (hostchecker/products)

The *hostchecker/products* entity represents a *nZTA* hostchecker configuration. Hostchecker products support the following activities:

- Retrieving all hostchecker products, see Retrieving all hostchecker products.
- Retrieving a specific hostchecker product, see Retrieving a specific hostchecker product.
- Creating a hostchecker product, see Creating a hostchecker product.
- Editing a hostchecker product, see Editing a hostchecker product.
- Deleting a hostchecker product, see Deleting a hostchecker product.

Retrieving all Hostchecker Products

To retrieve all *hostchecker/products* entities, use the REST API call below:

- **Method:** GET /api/v1/policies/device-policies/hostchecker/products
- **Resource:** Path

If processed correctly, a JSON body containing a list of all *hostchecker/products* entities is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/device-policies/hostchecker/products
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "items": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "name": "string",
      "windows": {
        "antivirus": {
          "vendors": [
            "string"
          ],
          "products": [
            "string"
          ]
        },
        "firewall": {
          "vendors": [
            "string"
          ],
          "products": [
            "string"
          ]
        },
        "antispyware": {
          "vendors": [
            "string"
          ],
          "products": [
            "string"
          ]
        },
        "hdd_encryption": {
          "vendors": [
            "string"
          ],
          "products": [
            "string"
          ]
```

```
      },
      "patch_management": {
        "vendors": [
          "string"
        ],
        "products": [
          "string"
        ]
      }
    },
    "mac": {
      "antivirus": {
        "vendors": [
          "string"
        ],
        "products": [
          "string"
        ]
      },
      "firewall": {
        "vendors": [
          "string"
        ],
        "products": [
          "string"
        ]
      },
      "antispyware": {
        "vendors": [
          "string"
        ],
        "products": [
          "string"
        ]
      },
      "hdd_encryption": {
        "vendors": [
          "string"
        ],
        "products": [
```

```
            "string"
          ]
        },
        "patch_management": {
          "vendors": [
            "string"
          ],
          "products": [
            "string"
          ]
        }
      }
    }
  ],
  "total": 0
}
```

Retrieving a Specific Hostchecker Product

To retrieve a single *hostchecker/products* entity, use the REST API call below:

- **Method:** GET /api/v1/policies/device-policies/hostchecker/products/{id}
- **Resource:** Path

If processed correctly, a JSON body containing the *hostchecker/products* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/device-policies/hostchecker/products/{id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "windows": {
    "antivirus": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "firewall": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "antispyware": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "hdd_encryption": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "patch_management": {
```

```
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    }
  },
  "mac": {
    "antivirus": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "firewall": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "antispyware": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "hdd_encryption": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
```

```
    },
    "patch_management": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    }
  }
}
```

Creating a Hostchecker Product

To create a *hostchecker/products* entity, use the REST API call below:

- **Method:** POST /api/v1/policies/device-policies/hostchecker/products
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new *hostchecker/products* entity.

If processed correctly, a JSON body containing the new *hostchecker/products* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/v1/policies/device-policies/hostchecker/products
Authorization:
Content-Type: application/json
Request Body
{
  "name": "string",
  "windows": {
    "antivirus": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "firewall": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "antispyware": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "hdd_encryption": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "patch_management": {
```

```
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    }
  },
  "mac": {
    "antivirus": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "firewall": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "antispyware": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "hdd_encryption": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
```

```
    },
    "patch_management": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    }
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "windows": {
    "antivirus": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "firewall": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "antispyware": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "hdd_encryption": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "patch_management": {
```

```
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    }
  },
  "mac": {
    "antivirus": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "firewall": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "antispyware": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "hdd_encryption": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
```

```
    },
    "patch_management": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    }
  }
}
```

Editing a Hostchecker Product

To edit a *hostchecker/products* entity, use the REST API call below:

- **Method:** PUT /api/v1/policies/device-policies/hostchecker/products/{id}
- **Resource:** Path
- **JSON Data:** JSON dictionary representing changed properties for a *hostchecker/products* entity.

If processed correctly, a JSON body containing the updated *hostchecker/products* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      PUT /api/v1/policies/device-policies/hostchecker/products/{id}
Authorization:
Content-Type: application/json
Request Body
{
  "name": "string",
  "windows": {
    "antivirus": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "firewall": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "antispyware": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "hdd_encryption": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "patch_management": {
```

```
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    }
  },
  "mac": {
    "antivirus": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "firewall": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "antispyware": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "hdd_encryption": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
```

```
    },
    "patch_management": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    }
  }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "windows": {
    "antivirus": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "firewall": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "antispyware": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "hdd_encryption": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "patch_management": {
```

```
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    }
  },
  "mac": {
    "antivirus": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "firewall": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "antispyware": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    },
    "hdd_encryption": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
```

```
    },
    "patch_management": {
      "vendors": [
        "string"
      ],
      "products": [
        "string"
      ]
    }
  }
}
```

Deleting a Hostchecker Product

To delete a *hostchecker/products* entity, use the REST API call below:

- **Method:** DELETE /api/v1/policies/device-policies/hostchecker/products/{id}
- **Resource:** Path

If processed correctly, a confirmation is returned. Otherwise, an error is returned.

Request

The following is an example request:

```
      DELETE /api/v1/policies/device-policies/hostchecker/products/{id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 204 Hostchecker/products deleted successfully
Content-Type: application/json
```

Resource Group (resource-groups)

The resource-groups entity represents a *nZTA* group of resources (both sign-in resources and applications). Resource groups support the following activities:

- Retrieving all resource groups, see Retrieving All Resource Groups.
- Creating a resource group, see Creating a Resource Group.
- Editing a resource group, see Editing a Resource Group.

Retrieving All Resource Groups

To retrieve a resource_groups entity, use the REST API call below:

- **Method:** GET /api/v1/policies/resource-groups
- **Resource:** Path

If processed correctly, a JSON body containing a list of all resource-groups entities is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/resource-groups
Authorization:
```

Response

The following is an example response:

```
        {
   "items": [
      {
         "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
         "name": "string",
         "type": "sign_in",
         "resources": [
            {
               "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
               "name": "string",
               "type": "sign_in",
               "description": "string",
               "sign_in_config": {
                  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
                  "policy_type": "admin",
                  "url_pattern": "string",
                  "realm": "string",
                  "primary_auth_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
                  "secondary_auth_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
                  "primary_authorization_server_id": "3fa85f64-5717-4562-
b3fc-2c963f66afa6"
               },
               "app_config": {
               "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
               "name": "string",
               "access_type": "application",
               "resource_type": "fqdn",
               "resource": "string",
               "bookmark_config": {
                  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
                  "name": "string",
                  "type": "web",
                  "description": "string",
                  "launch_window": true,
                  "url": "string",
                  "icon": "string"
               },
               "saml_config": {
```

```
                    "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
                    "sp_metadata": "string"
                }
            }
        ]
    }
]
}
```

Creating a Resource Group

To create a resource_group entity, use the REST API call below:

- **Method:** POST /api/v1/policies/resource-groups
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new resource-groups entity.

If processed correctly, a JSON body containing the new resource-groups is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/v1/policies/resource-groups
Authorization:
Content-Type: application/json
Request Body
{
   "name": "string",
   "type": "string",
   "resources": [
      {
         "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
         "name": "string",
         "type": "sign_in",
         "description": "string",
         "sign_in_config": {
            "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
            "policy_type": "admin",
            "url_pattern": "string",
            "realm": "string",
            "primary_auth_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
            "secondary_auth_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
            "primary_authorization_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6"
         },
         "app_config": {
            "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
            "name": "string",
            "access_type": "application",
            "resource_type": "fqdn",
            "resource": "string",
            "bookmark_config": {
               "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
               "name": "string",
               "type": "web",
               "description": "string",
               "launch_window": true,
               "url": "string",
               "icon": "string"
            },
```

```
            "saml_config": {
               "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
               "sp_metadata": "string"
            }
         }
      }
   ]
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
   "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
   "name": "string",
   "type": "sign_in",
   "resources": [
      {
         "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
         "name": "string",
         "type": "sign_in",
         "description": "string",
         "sign_in_config": {
            "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
            "policy_type": "admin",
            "url_pattern": "string",
            "realm": "string",
            "primary_auth_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
            "secondary_auth_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
            "primary_authorization_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6"
         },
         "app_config": {
            "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
            "name": "string",
            "access_type": "application",
            "resource_type": "fqdn",
            "resource": "string",
            "bookmark_config": {
               "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
               "name": "string",
               "type": "web",
               "description": "string",
               "launch_window": true,
               "url": "string",
               "icon": "string"
            },
```

```
            "saml_config": {
            "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
            "sp_metadata": "string"
            }
         }
      }
   ]
}
```

Editing a Resource Group

To edit a resource-group entity, use the REST API call below:

- **Method:** PUT /api/v1/policies/resource-groups/<id>
- **Resource:** Path
- **JSON Data:** JSON dictionary representing changed properties for a resource-groups entity.

If processed correctly, a JSON body containing the updated resources-group entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      PUT /api/v1/policies/resource-groups/{id}
Authorization:
Content-Type: application/json
Request Body
{
   "name": "string",
   "type": "string",
   "resources": [
      {
         "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
         "name": "string",
         "type": "sign_in",
         "description": "string",
         "sign_in_config": {
            "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
            "policy_type": "admin",
            "url_pattern": "string",
            "realm": "string",
            "primary_auth_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
            "secondary_auth_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
            "primary_authorization_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6"
         },
         "app_config": {
            "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
            "name": "string",
            "access_type": "application",
            "resource_type": "fqdn",
            "resource": "string",
            "bookmark_config": {
               "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
               "name": "string",
               "type": "web",
               "description": "string",
               "launch_window": true,
               "url": "string",
               "icon": "string"
            },
```

```
            "saml_config": {
               "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
               "sp_metadata": "string"
            }
         }
      }
   ]
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
   "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
   "name": "string",
   "type": "sign_in",
   "resources": [
      {
         "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
         "name": "string",
         "type": "sign_in",
         "description": "string",
         "sign_in_config": {
            "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
            "policy_type": "admin",
            "url_pattern": "string",
            "realm": "string",
            "primary_auth_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
            "secondary_auth_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6",
            "primary_authorization_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6"
         },
         "app_config": {
            "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
            "name": "string",
            "access_type": "application",
            "resource_type": "fqdn",
            "resource": "string",
            "bookmark_config": {
               "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
               "name": "string",
               "type": "web",
               "description": "string",
               "launch_window": true,
               "url": "string",
               "icon": "string"
            },
```

```
            "saml_config": {
               "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
               "sp_metadata": "string"
            }
         }
      }
   ]
}
```

Role Mapping Rules (role-mapping-rules)

The *role-mapping-rules* entity represents a *nZTA* role mapping rule. Role mapping rules support the following activities:

- Retrieving role map rules, see Retrieving All Role Mapping Rules.
- Creating a role mapping rule, see Creating a Role Mapping Rule.

Retrieving All Role Mapping Rules

To retrieve a list of all *role-mapping-rules* entities, use the REST API call below:

- **Method:** GET /api/v1/policies/role-mapping-rules
- **Resource:** Path

If processed correctly, a JSON body containing a list of all *role-mapping-rules* entities is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/role-mapping-rules
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "items": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "type": "username",
      "name": "string",
      "attribute": "string",
      "value": "string"
    }
  ]
}
```

Creating a Role Mapping Rule

To create a *role-mapping-rules* entity, use the REST API call below:

- **Method:** POST /api/v1/policies/role-mapping-rules
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new *role-mapping-rules* entity.

If processed correctly, a JSON body containing the new *role-mapping-rules* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/v1/policies/role-mapping-rules
Authorization:
Content-Type: application/json
Request Body
{
  "type": "username",
  "name": "string",
  "attribute": "string",
  "value": "string"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "type": "username",
  "name": "string",
  "attribute": "string",
  "value": "string"
}
```

Secure Access Policy (secure-access-policies)

The *secure-access-policies* entity represents a *nZTA* secure access policy. Secure access policies support the following activities:

- Retrieving All Secure Access Policies, see Retrieving All Secure Access Policies.
- Creating a Secure Access Policy, see Creating a Secure Access Policy.

Retrieving All Secure Access Policies

To retrieve all *secure-access-policies* entities, use the REST API call below:

- **Method:** GET /api/v1/policies/secure-access-policies
- **Resource:** Path

If processed correctly, a JSON body containing a list of all *secure-access-policies* entities is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/secure-access-policies
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "items": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "type": "sign_in",
      "resource_type": "single",
      "resource_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "resource_group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "device_policy_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "gateway_type": "single",
      "gateway_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "gateway_group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "user_rule_group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "resource_config": {
        "name": "string"
      },
      "resource_group_config": {
        "name": "string"
      },
      "device_policy_config": {
        "name": "string"
      },
      "user_rule_group_config": {
        "name": "string",
        "role_config": {
          "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "type": "admin",
          "name": "string",
          "redirect_url": "string"
        }
      }
    }
  ]
}
```

Creating a Secure Access Policy

To create a *secure-access-policies* entity, use the REST API call below:

- **Method:** POST /api/v1/policies/secure-access-policies
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new secure-access-policies entity.

If processed correctly, a JSON body containing the new secure-access-policies entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/v1/policies/secure-access-policies
Authorization:
Content-Type: application/json
Request Body
{
  "type": "sign_in",
  "resource_type": "single",
  "resource_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "resource_group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "device_policy_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "gateway_type": "single",
  "gateway_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "gateway_group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "user_rule_group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "type": "sign_in",
  "resource_type": "single",
  "resource_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "resource_group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "device_policy_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "gateway_type": "single",
  "gateway_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "gateway_group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "user_rule_group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "resource_config": {
    "name": "string"
  },
  "resource_group_config": {
    "name": "string"
  },
  "device_policy_config": {
    "name": "string"
  },
  "user_rule_group_config": {
    "name": "string",
    "role_config": {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "type": "admin",
      "name": "string",
      "redirect_url": "string"
    }
  }
}
```

Enterprise Integrations Configurations Service (integrations/syslog)

The *integrations/syslog* entity holds information about third party Enterprise Integrations Syslog Server configurations. This entity support the following activities:

- Retrieving the Enterprise Integrations Syslog forwarding configuration details, grouped by log type, see Retrieving the Enterprise Integrations Syslog Forwarding Configuration.
- Creating an Enterprise Integrations Syslog forwarding configuration, see Adding Enterprise Integrations Syslog Forwarding Configuration Details.
- Retrieving a List of Enterprise Integrations Syslog forwarding configurations, see Retrieving a List of Enterprise Integrations Syslog Configurations.
- Retrieving a specific Enterprise Integrations Syslog forwarding configuration, see Retrieving a Specific Enterprise Integrations Syslog Configuration.
- Editing an Enterprise Integrations Syslog forwarding configuration, see Editing an Enterprise Integrations Syslog Configuration.
- Removing an Enterprise Integrations Syslog forwarding configuration, see Removing an Enterprise Integrations Syslog Configuration.

Retrieving the Enterprise Integrations Syslog Forwarding Configuration

To retrieve an *integrations/syslog* entity, use the REST API call below:

- **Method:** GET /api/integrations/syslog
- **Resource:** Path

If processed correctly, a JSON body is returned that contains a list of syslog servers categorized by log type (access, event, admin). Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/integrations/syslog
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "access": [
    {
      "name": "string",
      "server": "string",
      "log_types": [
        "access"
      ],
      "facility": "LOCAL0",
      "protocol": "TLS",
      "certificate_id": "3fa85f6457174562b3fc2c963f66afa6",
      "filter_id": "123e4567e89b12d3a456426614174000",
      "gateway_ids": [
        "123e4567e89b12d3a456wr6614175643"
      ],
      "proxy_gateway_id": "123e4567e89b12d3a456wr6614175643",
      "id": "824411c22bf94e719ea757f8f3fd818e",
      "filter_name": "string",
      "created": "2021-01-27T00:00:00+00:00",
      "updated": "2021-01-27T00:00:00+00:00"
    }
  ],
  "admin": [
    {
      "name": "string",
      "server": "string",
      "log_types": [
        "access"
      ],
      "facility": "LOCAL0",
      "protocol": "TLS",
      "certificate_id": "3fa85f6457174562b3fc2c963f66afa6",
      "filter_id": "123e4567e89b12d3a456426614174000",
      "gateway_ids": [
        "123e4567e89b12d3a456wr6614175643"
      ],
      "proxy_gateway_id": "123e4567e89b12d3a456wr6614175643",
```

```
      "id": "824411c22bf94e719ea757f8f3fd818e",
      "filter_name": "string",
      "created": "2021-01-27T00:00:00+00:00",
      "updated": "2021-01-27T00:00:00+00:00"
    }
  ],
  "events": [
    {
      "name": "string",
      "server": "string",
      "log_types": [
        "access"
      ],
      "facility": "LOCAL0",
      "protocol": "TLS",
      "certificate_id": "3fa85f6457174562b3fc2c963f66afa6",
      "filter_id": "123e4567e89b12d3a456426614174000",
      "gateway_ids": [
        "123e4567e89b12d3a456wr6614175643"
      ],
      "proxy_gateway_id": "123e4567e89b12d3a456wr6614175643",
      "id": "824411c22bf94e719ea757f8f3fd818e",
      "filter_name": "string",
      "created": "2021-01-27T00:00:00+00:00",
      "updated": "2021-01-27T00:00:00+00:00"
    }
  ]
}
```


Adding Enterprise Integrations Syslog Forwarding Configuration Details

To add an *integrations/syslog* entity containing a syslog forwarding configuration, use the REST API call below:

- **Method:** POST /api/integrations/syslog
- **Resource:** Path

- **JSON Data:** JSON dictionary representing a new integrations/syslog entity.

If processed correctly, a JSON body containing the new integrations/syslog entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/integrations/syslog
Authorization:
Content-Type: application/json
Request Body
{
  "name": "string",
  "server": "string",
  "log_types": [
    "access"
  ],
  "facility": "LOCAL0",
  "protocol": "TLS",
  "certificate_id": "3fa85f6457174562b3fc2c963f66afa6",
  "filter_id": "123e4567e89b12d3a456426614174000",
  "gateway_ids": [
    "123e4567e89b12d3a456wr6614175643"
  ],
  "proxy_gateway_id": "123e4567e89b12d3a456wr6614175643"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "name": "string",
  "server": "string",
  "log_types": [
    "access"
  ],
  "facility": "LOCAL0",
  "protocol": "TLS",
  "certificate_id": "3fa85f6457174562b3fc2c963f66afa6",
  "filter_id": "123e4567e89b12d3a456426614174000",
  "gateway_ids": [
    "123e4567e89b12d3a456wr6614175643"
  ],
  "proxy_gateway_id": "123e4567e89b12d3a456wr6614175643",
  "id": "824411c22bf94e719ea757f8f3fd818e",
  "filter_name": "string",
  "created": "2021-01-27T00:00:00+00:00",
  "updated": "2021-01-27T00:00:00+00:00"
}
```

Retrieving a List of Enterprise Integrations Syslog Configurations

To retrieve a list of Enterprise Integrations Syslog Server configurations, use the REST API call below:

- **Method:** GET /api/integrations/syslog/ui
- **Resource:** Path

If processed correctly, a JSON body containing a list of all *integrations/syslog/ui* entities is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/integrations/syslog/ui
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "total": 0,
  "items": [
    {
      "name": "string",
      "server": "string",
      "log_types": [
        "access"
      ],
      "facility": "LOCAL0",
      "protocol": "TLS",
      "certificate_id": "3fa85f6457174562b3fc2c963f66afa6",
      "filter_id": "123e4567e89b12d3a456426614174000",
      "gateway_ids": [
        "123e4567e89b12d3a456wr6614175643"
      ],
      "proxy_gateway_id": "123e4567e89b12d3a456wr6614175643",
      "id": "824411c22bf94e719ea757f8f3fd818e",
      "filter_name": "string",
      "created": "2021-01-27T00:00:00+00:00",
      "updated": "2021-01-27T00:00:00+00:00"
    }
  ]
}
```

Retrieving a Specific Enterprise Integrations Syslog Configuration

To retrieve a single *integrations/syslog* entity, use the REST API call below:

- **Method:** GET /api/integrations/syslog/{syslog_id}
- **Resource:** Path

If processed correctly, a JSON body containing the *integrations/syslog* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/integrations/syslog/{syslog_id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "name": "string",
  "server": "string",
  "log_types": [
    "access"
  ],
  "facility": "LOCAL0",
  "protocol": "TLS",
  "certificate_id": "3fa85f6457174562b3fc2c963f66afa6",
  "filter_id": "123e4567e89b12d3a456426614174000",
  "gateway_ids": [
    "123e4567e89b12d3a456wr6614175643"
  ],
  "proxy_gateway_id": "123e4567e89b12d3a456wr6614175643",
  "id": "824411c22bf94e719ea757f8f3fd818e",
  "filter_name": "string",
  "created": "2021-01-27T00:00:00+00:00",
  "updated": "2021-01-27T00:00:00+00:00"
}
```

Editing an Enterprise Integrations Syslog Configuration

To edit an *integrations/syslog* entity, use the REST API call below:

- **Method:** PUT /api/integrations/syslog/{syslog_id}
- **Resource:** Path
- **JSON Data:** JSON dictionary representing changed properties for a *integrations/syslog* entity.

If processed correctly, a JSON body containing the updated *integrations/syslog* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      PUT /api/integrations/syslog/{syslog_id}
Authorization:
Content-Type: application/json
Request Body
{
  "name": "string",
  "server": "string",
  "log_types": [
    "access"
  ],
  "facility": "LOCAL0",
  "protocol": "TLS",
  "certificate_id": "3fa85f6457174562b3fc2c963f66afa6",
  "filter_id": "123e4567e89b12d3a456426614174000",
  "gateway_ids": [
    "123e4567e89b12d3a456wr6614175643"
  ],
  "proxy_gateway_id": "123e4567e89b12d3a456wr6614175643"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "name": "string",
  "server": "string",
  "log_types": [
    "access"
  ],
  "facility": "LOCAL0",
  "protocol": "TLS",
  "certificate_id": "3fa85f6457174562b3fc2c963f66afa6",
  "filter_id": "123e4567e89b12d3a456426614174000",
  "gateway_ids": [
    "123e4567e89b12d3a456wr6614175643"
  ],
  "proxy_gateway_id": "123e4567e89b12d3a456wr6614175643",
  "id": "824411c22bf94e719ea757f8f3fd818e",
  "filter_name": "string",
  "created": "2021-01-27T00:00:00+00:00",
  "updated": "2021-01-27T00:00:00+00:00"
}
```

Removing an Enterprise Integrations Syslog Configuration

To remove an *integrations/syslog* entity, use the REST API call below:

- **Method:** DELETE /api/integrations/syslog/{syslog_id}
- **Resource:** Path

If processed correctly, a confirmation is returned. Otherwise, an error is returned.

Request

The following is an example request:

```
      DELETE /api/integrations/syslog/{syslog_id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 204 No Content
Content-Type: application/json
```

Users (users)

The users entity represents a *nZTA* user. Users support the following activities:

- Retrieving a user, see Retrieving a User.
- Creating a user, see Creating a User.
- Retrieving user settings, see Retrieving User Settings.
- Updating user settings, see Updating User Settings.

Retrieving a User

To retrieve the current user, use the REST API call below:

- **Method:** GET /users/self
- **Resource:** Path

If processed correctly, a JSON body containing the current user is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /users/self
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
   "first_name": "John",
   "last_name": "Doe",
   "email": "john.doe@example.com",
   "id": "0cd145e28d483a6d57e9d73b6d78b7fe58377950",
   "username": "john.doe",
   "created": "2020-09-21T00:00:00+00:00",
   "updated": "2020-09-22T00:00:00+00:00"
}
```

Creating a User

To create a user entity, use the REST API call below:

- **Method:** POST /users/self
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new user entity.

If processed correctly, a JSON body containing the new user entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /users/self
Authorization:
Content-Type: application/json
Request Body
{
   "first_name": "John",
   "last_name": "Doe",
   "email": "john.doe@example.com"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
   "first_name": "John",
   "last_name": "Doe",
   "email": "john.doe@example.com",
   "id": "0cd145e28d483a6d57e9d73b6d78b7fe58377950",
   "username": "john.doe",
   "created": "2020-09-21T00:00:00+00:00",
   "updated": "2020-09-22T00:00:00+00:00"
}
```

Retrieving User Settings

To retrieve the current user settings, use the REST API call below:

- **Method:** GET /users/self/settings/ui
- **Resource:** Path

If processed correctly, a JSON body containing the current user settings is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /users/self/settings/ui
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
   "version": "785bb486534129fd8ec732a1aa647b02d8e33491",
   "settings": {
     "on_login": {
       "show_welcome_wizard": false
     }
   }
}
```

Updating User Settings

To update user settings, use the REST API call below:

- **Method:** PUT /users/self/settings/ui
- **Resource:** Path
- **JSON Data:** JSON dictionary representing new user settings.

If processed correctly, a JSON body containing user settings is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /users/self/settings/ui
Authorization:
Content-Type: application/json
Request Body
{
   "previous_version": "h2kbb486534c49fd8ec732a1aa647b02d8e338ua",
   "settings": {
      "on_login": {
         "show_welcome_wizard": true
      }
   }
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
   "version": "785bb486534129fd8ec732a1aa647b02d8e33491",
   "settings": {
      "on_login": {
        "show_welcome_wizard": false
      }
   }
}
```

User Rule Groups (user-rule-groups)

The *user-rule-groups* entity represents a *nZTA* user rule group. User rule groups support the following activities:

Retrieving All User Rule Groups

To retrieve all *user-rule-groups* entities, use the REST API call below:

- **Method:** GET /api/v1/policies/user-rule-groups
- **Resource:** Path

If processed correctly, a JSON body containing a list of all *user-rule-groups* entities is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/user-rule-groups
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "items": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "name": "string",
      "description": "string",
      "sign_in_policy_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "sign_in_config": {
        "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "policy_type": "admin",
        "url_pattern": "string",
        "realm": "string",
        "use_as_saml_idp": true,
        "primary_auth_server_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "primary_auth_server_config": {
          "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "type": "Local",
          "name": "string"
        },
        "secondary_auth_server_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "secondary_auth_server_config": {
          "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "type": "Local",
          "name": "string"
        },
        "primary_authorization_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6"
      },
      "role_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "role_config": {
        "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "type": "admin",
        "name": "string",
        "redirect_url": "string"
      },
      "rules": [
        {
```

```
          "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "name": "string",
          "type": "username",
          "attribute": "string",
          "value": "string"
        }
      ]
    }
  ]
}
```

Creating a User Rule Group

To create a *user-rule-groups* entity, use the REST API call below:

- **Method:** POST /api/v1/policies/user-rule-groups
- **Resource:** Path
- **JSON Data:** JSON dictionary representing a new *user-rule-groups* entity.

If processed correctly, a JSON body containing the new *user-rule-groups* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/v1/policies/user-rule-groups
Authorization:
Content-Type: application/json
Request Body
{
  "name": "string",
  "description": "string",
  "role_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "sign_in_policy_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "rules": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "name": "string",
      "type": "username",
      "attribute": "string",
      "value": "string"
    }
  ]
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "description": "string",
  "sign_in_policy_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "sign_in_config": {
    "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "policy_type": "admin",
    "url_pattern": "string",
    "realm": "string",
    "use_as_saml_idp": true,
    "primary_auth_server_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "primary_auth_server_config": {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "type": "Local",
      "name": "string"
    },
    "secondary_auth_server_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "secondary_auth_server_config": {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "type": "Local",
      "name": "string"
    },
    "primary_authorization_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6"
  },
  "role_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "role_config": {
    "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "type": "admin",
    "name": "string",
    "redirect_url": "string"
  },
  "rules": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "name": "string",
```

```
      "type": "username",
      "attribute": "string",
      "value": "string"
    }
  ]
}
```

User Policies (resources)

A user policy is a type of *resources* entity that represents a *nZTA* user policy. User policies support the following activities:

- Retrieving all user policies, see Retrieving All User Policies.
- Editing a user policy, see Editing a User Policy.

> The *resources* entity is also used to represent a *nZTA* application. This is enabled by a **type** of "application", see Applications (resources).

Retrieving All User Policies

To retrieve all user policy (*resources*) entities, use the REST API call below:

- **JSON Data:** JSON dictionary representing a *resources* type of sign-in.
- **Resource:** Path
- **Method:** GET /api/v1/policies/resources

If processed correctly, a JSON body containing a list of all user policy resources is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/resources
Authorization:
Content-Type: application/json
Request Body
{
   "type": "sign_in"
}
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "items": [
    {
      "name": "string",
      "type": "sign_in",
      "description": "string",
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "sign_in_config": {
        "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "policy_type": "admin",
        "url_pattern": "string",
        "realm": "string",
        "use_as_saml_idp": true,
        "primary_auth_server_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "primary_auth_server_config": {
          "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "type": "Local",
          "name": "string"
        },
        "secondary_auth_server_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "secondary_auth_server_config": {
          "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "type": "Local",
          "name": "string"
        },
        "primary_authorization_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6"
      },
      "app_config": {
        "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "name": "string",
        "access_type": "application",
        "resource_type": "fqdn",
        "resource": "string",
        "bookmark_config": {
          "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "name": "string",
```

```
          "type": "web",
          "description": "string",
          "launch_window": true,
          "url": "string",
          "icon": "string"
        },
        "saml_config": {
          "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "sp_metadata": "string"
        }
      }
    }
  ]
}
```


Editing a User Policy

To edit a user policy *resources* entity, use the REST API call below:

- **JSON Data:** JSON dictionary representing changed properties for a user policy *resources* entity.
- **Resource:** Path
- **Method:** PUT /api/v1/policies/resources/{resource_id}

If processed correctly, a JSON body containing the updated user policy *resources* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      PUT /api/v1/policies/resources/{resource_id}
Authorization:
Content-Type: application/json
Request Body
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "name": "string",
  "type": "sign_in",
  "description": "string",
  "sign_in_config": {
    "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "policy_type": "admin",
    "url_pattern": "string",
    "realm": "string",
    "use_as_saml_idp": true,
    "primary_auth_server_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "primary_auth_server_config": {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "type": "Local",
      "name": "string"
    },
    "secondary_auth_server_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "secondary_auth_server_config": {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "type": "Local",
      "name": "string"
    },
    "primary_authorization_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6"
  },
  "app_config": {
    "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "name": "string",
    "access_type": "application",
    "resource_type": "fqdn",
    "resource": "string",
    "bookmark_config": {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "name": "string",
      "type": "web",
```

```
      "description": "string",
      "launch_window": true,
      "url": "string",
      "icon": "string"
    },
    "saml_config": {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "sp_metadata": "string"
    }
  }
}
```

Response

The following is an example response:

```
      HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
  "name": "string",
  "type": "sign_in",
  "description": "string",
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "sign_in_config": {
    "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "policy_type": "admin",
    "url_pattern": "string",
    "realm": "string",
    "use_as_saml_idp": true,
    "primary_auth_server_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "primary_auth_server_config": {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "type": "Local",
      "name": "string"
    },
    "secondary_auth_server_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "secondary_auth_server_config": {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "type": "Local",
      "name": "string"
    },
    "primary_authorization_server_id": "3fa85f64-5717-4562-b3fc-
2c963f66afa6"
  },
  "app_config": {
    "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
    "name": "string",
    "access_type": "application",
    "resource_type": "fqdn",
    "resource": "string",
    "bookmark_config": {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "name": "string",
      "type": "web",
      "description": "string",
```

```
      "launch_window": true,
      "url": "string",
      "icon": "string"
    },
    "saml_config": {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "sp_metadata": "string",
      "attributes": [
        {
          "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "attribute": "string",
          "value": "string",
          "resource_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
        }
      ]
    }
  }
}
```

Retrieving Lockdown Exceptions

To retrieve Lockdown exceptions, use the REST API call below:

- **Method:** GET /api/clients/ui/lockdown/exceptions
- **Resource:** Path

If processed correctly, a JSON body containing the *exceptions* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/clients/ui/lockdown/exceptions
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
       "total": 0,
       "count": 0,
       "items": [
       {
       "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
       "name": "string",
       "description": "string",
       "platform": "Windows",
       "type": "Program",
       "rule_action": "Allow",
       "created": "string",
       "updated": "string",
       "is_default": true,
       "direction": "Inbound",
       "exception_order": 0,
       "port": {
       "protocol": "string",
       "remote_port": "string",
       "local_port": "string"
       },
       "program": {
       "program_path": "string",
       "sha256": "string"
       },
       "custom": {
       "program_path": "string",
       "sha256": "string",
       "protocol": "string",
       "local_port": "string",
       "remote_port": "string",
       "local_resource": "string",
       "remote_resource": "string"
       },
       "program_path": "string",
       "protocol": "TCP",
       "local_port": "string",
```

```
        "remote_port": "string",
        "local_resource": "string",
        "remote_resource": "string"
        }
        ]
}
```

MDM Server

A MDM is a type of *server* entity that represents a *nZTA* server. MDM supports the following activities:

- Retrieving all MDM Servers, see Retrieving All MDM Server.
- Create MDM Server, see Creating a MDM Server.
- Retrieving MDM Servers by ID, see Retrieving a MDM Server by ID.
- Editing a MDM Server, see Editing a MDM Server.

Retrieving All MDM Servers

To retrieve MDM Servers, use the REST API call below:

- **Method:** GET /api/v1/policies/mdm-servers
- **Resource:** Path

If processed correctly, a JSON body containing the *MDM server* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/mdm-servers
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
        HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
       "total": 0,
       "mdm_servers": [
       {
       "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
       "name": "string",
       "type": "Ivanti Cloud",
       "ivanti_cloud_config": {
       "server_url": "string",
       "viewer_url": "string",
       "request_timeout": 0,
       "admin_user_name": "string",
       "admin_password": "string",
       "admin_password_hash": "string",
       "device_identifier_template": "CN",
       "device_identifier_type": "UUID"
       },
       "microsoft_intune_config": {
       "national_clouds": "string",
       "tenant_id": "string",
       "client_id": "string",
       "client_secret": "string",
       "request_timeout": 0,
       "device_identifier_template": "CN",
       "device_identifier_type": "deviceID",
       "device_identity": "certificate"
       }
       }
       ]
```

Creating a MDM Server

To Create a MDM Server entity, use the REST API call below:

- **JSON Data:** JSON dictionary representing changed properties for a MDM Server entity.
- **Resource:** Path

- **Method:** POST /api/v1/policies/mdm-servers

If processed correctly, a JSON body containing the new *MDM Server* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      POST /api/v1/policies/mdm-servers
Authorization:
Content-Type: application/json
Request Body
{
       "name": "string",
       "type": "Ivanti Cloud",
       "ivanti_cloud_config": {
       "server_url": "string",
       "viewer_url": "string",
       "request_timeout": 0,
       "admin_user_name": "string",
       "admin_password": "string",
       "admin_password_hash": "string",
       "device_identifier_template": "CN",
       "device_identifier_type": "UUID"
       },
       "microsoft_intune_config": {
       "national_clouds": "string",
       "tenant_id": "string",
       "client_id": "string",
       "client_secret": "string",
       "request_timeout": 0,
       "device_identifier_template": "CN",
       "device_identifier_type": "deviceID",
       "device_identity": "certificate"
       }
}
```

Response

The following is an example response:

```
      HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
       "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
       "name": "string",
       "type": "Ivanti Cloud",
       "ivanti_cloud_config": {
       "server_url": "string",
       "viewer_url": "string",
       "request_timeout": 0,
       "admin_user_name": "string",
       "admin_password": "string",
       "admin_password_hash": "string",
       "device_identifier_template": "CN",
       "device_identifier_type": "UUID"
       },
       "microsoft_intune_config": {
       "national_clouds": "string",
       "tenant_id": "string",
       "client_id": "string",
       "client_secret": "string",
       "request_timeout": 0,
       "device_identifier_template": "CN",
       "device_identifier_type": "deviceID",
       "device_identity": "certificate"
       }
}
```

Retrieving a MDM Server by ID

To retrieve a MDM Server by ID entity, use the REST API call below:

- **JSON Data:** JSON dictionary representing changed properties for a MDM Server by ID entity.
- **Resource:** Path

- **Method:** GET/api/v1/policies/mdm-servers/{mdm_server_id}

If processed correctly, a JSON body containing the *MDM Server by ID* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      GET /api/v1/policies/mdm-servers/{mdm_server_id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
      HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
       "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
       "name": "string",
       "type": "Ivanti Cloud",
       "ivanti_cloud_config": {
       "server_url": "string",
       "viewer_url": "string",
       "request_timeout": 0,
       "admin_user_name": "string",
       "admin_password": "string",
       "admin_password_hash": "string",
       "device_identifier_template": "CN",
       "device_identifier_type": "UUID"
       },
       "microsoft_intune_config": {
       "national_clouds": "string",
       "tenant_id": "string",
       "client_id": "string",
       "client_secret": "string",
       "request_timeout": 0,
       "device_identifier_template": "CN",
       "device_identifier_type": "deviceID",
       "device_identity": "certificate"
       }
}
```

Editing a MDM Server

To edit a MDM Server entity, use the REST API call below:

- **JSON Data:** JSON dictionary representing changed properties for a MDM Server entity.
- **Resource:** Path
- **Method:** PUT /api/v1/policies/mdm-servers/{mdm_server_id}

If processed correctly, a JSON body containing the edited *MDM Server* entity is returned. Otherwise, a JSON body containing an error is returned.

Request

The following is an example request:

```
      PUT /api/v1/policies/mdm-servers/{mdm_server_id}
Authorization:
Content-Type: application/json
Request Body
{
       "name": "string",
       "type": "Ivanti Cloud",
       "ivanti_cloud_config": {
       "server_url": "string",
       "viewer_url": "string",
       "request_timeout": 0,
       "admin_user_name": "string",
       "admin_password": "string",
       "admin_password_hash": "string",
       "device_identifier_template": "CN",
       "device_identifier_type": "UUID"
       },
       "microsoft_intune_config": {
       "national_clouds": "string",
       "tenant_id": "string",
       "client_id": "string",
       "client_secret": "string",
       "request_timeout": 0,
       "device_identifier_template": "CN",
       "device_identifier_type": "deviceID",
       "device_identity": "certificate"
       }
}
```

Response

The following is an example response:

```
      HTTP/1.1 200 OK
Content-Type: application/json
Response Body
{
       "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
       "name": "string",
       "type": "Ivanti Cloud",
       "ivanti_cloud_config": {
       "server_url": "string",
       "viewer_url": "string",
    "request_timeout": 0,
       "admin_user_name": "string",
       "admin_password": "string",
       "admin_password_hash": "string",
       "device_identifier_template": "CN",
       "device_identifier_type": "UUID"
       },
       "microsoft_intune_config": {
       "national_clouds": "string",
       "tenant_id": "string",
       "client_id": "string",
       "client_secret": "string",
       "request_timeout": 0,
       "device_identifier_template": "CN",
       "device_identifier_type": "deviceID",
       "device_identity": "certificate"
       }
}
```

Deleting a MDM Server

To delete a *MDM Server* entity, use the REST API call below:

- Method: DELETE /api/v1/policies/mdm-servers/{mdm_server_id}
- Resource: Path

If processed correctly, a confirmation is returned. Otherwise, an error is returned.

Request

The following is an example request:

```
DELETE /api/v1/policies/mdm-servers/{mdm_server_id}
Authorization:
Content-Type: application/json
```

Response

The following is an example response:

```
HTTP/1.1 204 Deleted MDM Server successfully
Content-Type: application/json
```

Ivanti Neurons for Zero Trust Access Use Case

This chapter of the document will provide code snippets for different API call which can help tenant admins to configure secure access policy. These steps involve authenticating the API then adding all required components including user and user rules and finally configure Secure Access Policy using all the other components.

Steps automated in example use case:

- Preparing to configure the *nZTA* system, see Preparing to Configure the System.
- Adding a gateway, see Adding a ZTA Gateway.
- Adding an application, see Adding an Application.
- Adding a device rule and device policy, see Adding a Device Rule and Policy.
- Adding an auth server, see Adding an Authentication Server.
- Adding a user (local user), see Adding a Local User.
- Adding a user rule, see Adding a User Rule.
- Adding a user rule to a group, see Adding a User Rule.
- Adding a secure access policy, see Adding a Secure Access Policy.

Preparing to Configure the System

This section explains how to prepare to configure the *nZTA* system using its REST API.

The following Python modules needs to be imported to enable the code snippets in this chapter:

```
      import requests
import json
```

The following parameters are required to enable the code snippets in this chapter:

```
      SSLCertverify = False
apiHeaders = {'Content-type': 'application/json', 'Accept':
'application/json'}
headers = {"Content-Type": "application/json"}
user_name = 'admin'
passwrd = 'admin_password'
api_version = 'api/v1/'
api = 'api/'
host_url = 'https://<tenant_domain_name>/'
cookies = {"DSID": ""}
```

You can use the following CURL command format uses the DSID to query the REST API server:

```
        curl -v --cookie "DSID=<value>" <api_request_url>
```

Adding a *ZTA Gateway*

Adding a gateway involves multiple API calls, including getting `city_id` and using that to add the gateway. You can then get the gateway ID to enable gateway configuration.

```
        def add_gateways():
    '''
    Get country code to get the city_id which is one of the parameters
needed for adding gateway.
    '''
    get_country_code_url = host_url + api + "locations/countries"
    country_list = requests.get(get_country_code_url,cookies=cookies)
    country_list_json = country_list.json()
    country_id = "241"
    for country_details in country_list_json["items"]:
        if country_details["country"]["name"] == "United States":
            country_id = country_details["country"]["id"]
     # one we get the country ID use that ID to get the list of cities with
respective ID, following request will illustrates process of getting city_
id
    state_id = "3512"
    get_state_code_url = host_url + api + "locations/states?country="+str
(country_id)
    state_code_json = requests.get(get_state_code_url,cookies=cookies)
    state_list_json = state_code_json.json()
    for state_details in state_list_json["items"]:
        #print state_details
        if state_details["state"]["name"] == "California":
            state_id = state_details["state"]["id"]
    # following api call is get the city id using country and state id
which are retrived from previous two calls. This logic will filter for San
Jose city to get the city_id
    get_city_code_url = host_url + api + "locations/cities?country="+str
(country_id)+"&state="+str(state_id)
    city_list = requests.get(get_city_code_url,cookies=cookies)
    city_list_json = city_list.json()
    city_id="12631"
    for cities in city_list_json["items"]:
        if cities["city"]["name"] == "San Jose":
            city_id = cities["city"]["id"]
    # following step will help us add a gateway to Controller using API
call
    input_gateways = {"name": "gw4","orchestration": {"type": "vsphere"}}
    gateway_location = {}
    gateway_location["city_id"] = city_id
```

```
    input_gateways["location"]=gateway_location
    # input_gateways variable input all the required parameters such as
gateway name, orchestration type and city id for gateway api which is post
method.
    request_uri = host_url + api + "gateways"
    output = requests.post(request_uri, data=json.dumps(input_gateways),
cookies=cookies, headers=headers)
    status_code = output.status_code
    response_json = output.json()
    print response_json
    gateway_id=response_json["id"]
    input_data='{"service_account_id":None,"appliance_config":{"external_
gateway":"192.168.114.251","external_ip_address":"192.168.14.11","external_
subnet":"255.255.255.0","external_vlan":"-1","internal_fqdn":"","internal_
gateway":"172.96.14.1","internal_ip_address":"172.96.14.60","internal_
subnet":"255.255.255.0",
"internal_vlan":"-1","management_gateway":"172.96.14.1","management_ip_
address":"172.96.14.61","management_subnet":"255.255.255.0","management_
vlan":"-1","primary_dns":"142.21.0.15",
"private_domain_name":"psecure.net","secondary_dns":"8.8.8.8","dns_search_
domain":"psecure.net","public_ip_address":"192.168.14.11",},"deployment_
config":None,}'
    request_uri = request_uri + "/" + gateway_id + "/" + "orchestration"
    print request_uri
    output = requests.post(request_uri, data=json.dumps(input_data),
cookies=cookies, headers=headers)
    print output.json
```

Adding an Application

To add an application, use a policies/resources API call with the type set to "application". For example:

```
      def add_application():
    input_data =
{"type":"application","name":"app1","description":"app1","app_config":
{"access_type"
:"application","name":"app1","resource":"https://www.intuit.com","resource_
type":"url","bookmark_config":
{"name":"app1","type":"web","description":"app1","launch_
window":True,"url":"https://www.intuit.com","icon":""}}}
    add_application_url = host_url+api_version+"policies/resources"
    print add_application_url
    add_application_output = requests.post(add_application_
url,data=json.dumps(input_data),cookies=cookies, headers=headers)
    print add_application_output.text
```

Output for this code is below:

```
        {
   "allow_delete": true,
   "app_config": {
      "access_type": "application",
      "bookmark_config": {
         "description": "app1",
         "icon": "",
         "id": "3ddf5e1b0d35d3f8ca8da7ded4f6f0a",
         "launch_window": true,
         "name": "app1",
         "type": "web",
         "url": "https://www.intuit.com"
      }
      "id": "4899a9fe06e64316a17891fff401bc6a",
      "name": "app1",
      "resource": "https://www.intuit.com",
      "resource_type": "url"
   }
   "description": "app1",
   "id": "4899a9fe06e64316a17891fff401bc6a",
   "name": "app1",
   "type": "application"
}
```

Adding a Device Rule and Policy

Create a device rule:

```
      def create_device_rule():
    input_data = {
       "name":"device_rule_1",
       "description":"device_rule_1",
       "network_config": {
          "ip_address":"192.168.1.1",
          "netmask":"255.255.255.0",
          "mode":"allow"
       },
       "label":"moderate",
       "type":"network"
    }
    add_device_rule_url = host_url+api_version+"policies/device-
policies/rules"
    add_device_rule_output = requests.post(add_device_rule_
url,data=json.dumps(input_data),cookies=cookies, headers=headers)
    print add_device_rule_output.text
```

Create a device policy using the device rule:

```
        def add_device_policy2_device_rule():
    input_data = {
       "name": "device_policy_1",
       "description": "device_policy_1"
    }
    add_policy_device_rule_url = host_url+api_version+"policies/device-
policies/groups"
    add_policy_device_rule_output = requests.post(add_policy_device_rule_
url,data=json.dumps(input_data),cookies=cookies, headers=headers)
    print add_policy_device_rule_output.text
```

Adding an Authentication Server

Create an authentication server:

```
        def add_local_auth_server():
    input_data = {
       "name": "auth_server_1",
       "type": "Local",
       "local_config": {
          "users": []
       }
    }
    add_local_auth_server_url= host_url+api_version+"policies/auth-servers"
    add_local_auth_server_output = requests.post(add_local_auth_server_
url,data=json.dumps(input_data),cookies=cookies, headers=headers)
    print add_local_auth_server_output.text
```

Adding a Local User

Add a user to the local authentication server:

```
      def add_user_AuthServers():
    #global auth_server_id
    # get list of auth servers
    auth_server_id = ""
    get_authserver_request_uri = host_url + api_version + "policies/auth-
servers"
    auth_servers = requests.get(get_authserver_request_uri,cookies=cookies,
headers=headers)
    for server_details in json.loads(auth_servers.text)["auth_servers"]:
        if server_details["name"] == "auth_server_1":
            auth_server_id = server_details["id"]
# API call uses auth_server_id to update auth_server with new user details.
    input_data = {"name": "newuser1", "full_name": "newuser1", "password":
"dana123"}
    request_uri = host_url + api_version + "policies/auth-servers" + "/" +
auth_server_id + "/users"
    add_user_response = requests.post(request_uri,data=json.dumps(input_
data),cookies=cookies, headers=headers)
    print add_user_response.text
```

Update the user authentication policy to use the auth server:

```
        def update_user_auth_policy():
    input_payload = {
       "type": "sign_in"
    }
    auth_server_id = ""
    default_user_policies_uri = host_url + api_version +
"policies/resources"
    get_default_user_policies_response = requests.get(default_user_
policies_uri,params=input_payload,cookies=cookies)
    # for this response we will get user_policy_id which for type sing in
and realm ZTA users and update the primary_auth_server_id value with auth
server ID.
    # get the Auth server ID with name auth_server_1, this auth server we
added in previous steps.
    get_authserver_request_uri = host_url + api_version + "policies/auth-
servers"
    auth_servers = requests.get(get_authserver_request_uri,cookies=cookies,
headers=headers)
    for server_details in json.loads(auth_servers.text)["auth_servers"]:
        if server_details["name"] == "auth_server_1":
            auth_server_id = server_details["id"]
    # now update the input_payload for updating user signin policy primary_
auth_server_id during the put call.
    for user_policy_details in json.loads(get_default_user_policies_
response.text)["items"]:
        if user_policy_details["sign_in_config"]["realm"] == "ZTA Users":
            request_uri = default_user_policies_uri + "/" + user_policy_
details["id"]
            input_data = user_policy_details
            input_data["sign_in_config"]["primary_auth_server_id"] = auth_
server_id
            update_user_policy_details_output = requests.put(request_uri,
data=json.dumps(input_data), cookies=cookies, headers=headers)
            print update_user_policy_details_output.text
```

Adding a User Rule

Create a user rule:

```
      def add_user_rule():
    input_data = {
       "name":"user_rule_1",
       "type":"username",
       "value":"user_rule_1",
       "attribute":"is"
    }
    request_uri = host_url + api_version + "policies/role-mapping-rules"
    output_add_user_rule = requests.post(request_uri, data=json.dumps
(intput_data), cookies=cookies, headers=headers)
    print output_add_user_rule.text
```

The output of this code is below:

```
        {
   "attribute": "is",
   "id": "8970619481ba470c82c114a20bee3a07",
   "name": "user_rule_1",
   "type": "username",
   "value": "user_rule_1"
}
```

Adding a User Rule to a Group

Create a user group of type User Signin Policy, and add the above user rule to the group:

```
      def add_user_group():
    input_payload = {
       "type": "sign_in"
    }
    auth_server_id = ""
    default_user_policies_uri = host_url + api_version +
"policies/resources"
    get_default_user_policies_response = requests.get(default_user_
policies_uri,params=input_payload,cookies=cookies)
    user_policy_id = ""
    # now update the input_payload for updating user signin policy primary_
auth_server_id during the put call.
    for user_policy_details in json.loads(get_default_user_policies_
response.text)["items"]:
        if user_policy_details["sign_in_config"]["realm"] == "ZTA Users":
           user_policy_id = user_policy_details["id"]
    input_data = {
       "name":"user_group_1",
       "sign_in_policy_id":"",
       "description":"user_group_1",
       "rules":[]
    }
    input_data["sign_in_policy_id"] = user_policy_id
    request_uri = host_url + api_version + "policies/user-rule-groups"
    output_add_user_rule = requests.post(request_uri, data=json.dumps
(input_data), cookies=cookies, headers=headers)
    print output_add_user_rule.text
```

The output of this code is below:

```
        {
   "allow_delete": true,
   "description": "user_group_1",
   "id": "3e99edd4e5534ca6a322a404e8c26d4a",
   "name": "user_group_1",
   "role_config": {
      "id": "612dc9de1e5148748a378742a5d2311e",
      "name": "user_group_1",
      "redirect_url": "/user",
      "type"L "user"
   }
   "role_id": "612dc9de1e5148748a378742a5d2311e",
   "sign_in_config": {
      "id": "21ff78e93fda4b0c86e7af96dfa75680",
      "policy_type": "user",
      "primary_auth_server_config": {
         "id": "0a867da874cd426cbe6acd2efba149ec",
         "name": "auth_server_1",
         "type": "Local"
      }
      "primary_auth_server_id": "0a867da874cd426cbe6acd2efba149ec",
      "realm": "ZTA Users",
      "url_pattern": "*/login/",
      "use_as_saml_idp": false
   }
   sign_in_policy_id": "21ff78e93fda4b0c86e7af96dfa75680"
}
```

Adding a Secure Access Policy

Finally, publish a secure access policy using all of the above:

```
      def add_secure_access_policy():
    input_data = {
       "type":"application",
       "resource_type":"single",
       "user_rule_group_id":"",
       "gateway_type":"single",
       "gateway_id":"",
       "resource_id":"",
       "device_policy_id":""
    }
    # all values in following 4 lines derived from different API calls made
in all previous examples
    input_data["user_rule_group_id"] = "3e99edd4e5534ca6a322a404e8c26d4a"
    input_data["gateway_id"] = "edb5fc9969304619b6cb976a2a6101e6"
    input_data["resource_id"] = "4899a9fe06e64316a17891fff401bc6a"
    input_data["device_policy_id"] = "e639512d55fb47e5940d9b8053916629"
    request_uri = host_url + api_version + "policies/secure-access-
policies"
    output_add_secureaccess_policy = requests.post(request_uri,
data=json.dumps(input_data), cookies=cookies, headers=headers)
    print output_add_secureaccess_policy.text
```

The output of this code is below:

```
      {
   "device_policy_config": {
      "name": "device_policy_1"
   }
   "device_policy_id": "e639512d55fb47e5940d9b8053916629",
   "gateway_id": "edb5fc9969304619b6cb976a2a6101e6",
   "gateway_type": "single",
   "id": "1b87430b470a44cda082fb638fa87ae2",
   "resource_config": {
      "name": "app1"
   }
   "resource_id": "4899a9fe06e64316a17891fff401bc6a",
   "resource_type": "single",
   "type": "application",
   "user_rule_group_config": {
      "name": "user_group_1",
      "role_config": {
         "id": "612dc9de1e5148748a378742a5d2311e",
         "name": "user_group_1",
         "redirect_url": "/user",
         "type": "user"
      }
   }
   "user_rule_group_id": "3e99edd4e5534ca6a322a404e8c26d4a"
}
```

Additional References

To see a list of the default secure access policies:

```
      Input Payload : {'type': 'application'}
Request URI : ``https://<tenant_domain>/api/v1/policies/secure-access-
policies``
Returned Status Code : 200
Returned JSON Response : {'items': [], 'total': 0}
```

To retrieve the default User Auth Server ID:

```
      Input Payload : {}
Request URI : ``https://<tenant_domain>/api/v1/policies/auth-servers``
Returned Status Code : 200
Returned JSON Response : {
   'auth_servers': [{
      'id': '4a02312f7b1f4dd89f5350966feb528d',
      'name': 'Admin Auth',
      'type': 'Local'
      }, {
      'id': '706960d40e43451786f6f5d6c598d7fa',
      'name': 'User Auth',
      'type': 'Local'
      }],
   'total': 2
   }
```

Retrieving a list of the default user policies:

```
      Input Payload : {'type': 'sign_in'}
Request URI : https://<tenant_domain>/api/v1/policies/resources
Returned Status Code : 200
Returned JSON Response : {
   'items': [{
      'description': 'Admin Signin',
      'id': 'f87680b7292242b9af247fec1b17347c',
      'name': 'Admin Signin',
      'sign_in_config': {
         'id': 'f87680b7292242b9af247fec1b17347c',
         'policy_type': 'admin',
         'primary_auth_server_id': '4a02312f7b1f4dd89f5350966feb528d',
         'realm': 'ZTA Admin Users',
         'url_pattern': '*/login/admin/',
         'use_as_saml_idp': False
      },
      'type': 'sign_in'
   }, {
      'description': 'Enrollment Signin',
      'id': 'cb8753de76fb45d581e07d4bc700cb67',
      'name': 'Enrollment Signin',
      'sign_in_config': {
         'id': 'cb8753de76fb45d581e07d4bc700cb67',
         'policy_type': 'enroll',
         'primary_auth_server_id': '706960d40e43451786f6f5d6c598d7fa',
         'realm': 'ZTA Enrollment',
         'url_pattern': '*/login/enroll/',
         'use_as_saml_idp': False
      },
      'type': 'sign_in'
   }, {
      'description': 'User Signin',
      'id': '21ff78e93fda4b0c86e7af96dfa75680',
      'name': 'User Signin',
      'sign_in_config': {
         'id': '21ff78e93fda4b0c86e7af96dfa75680',
         'policy_type': 'user',
         'primary_auth_server_id': '706960d40e43451786f6f5d6c598d7fa',
         'realm': 'ZTA Users',
         'url_pattern': '*/login/',
```

```
         'use_as_saml_idp': False
      },
      'type': 'sign_in'
   }],
   'total': 3
}
```

Adding a new user authentication server "auth_server_1" of type "local":

```
      Input Payload : {
   'name': 'auth_server_1',
   'type': 'Local',
   'local_config': {
      'users': []
   }
}
Request URI : ``https://<tenant_domain>/api/v1/policies/auth-servers``
Returned Status Code : 200
Returned JSON Response : {
   'allow_delete': True,
   'id': '0b634b96bcb04dc98072cf28c5129a91',
   'name': 'auth_server_1',
   'type': 'Local'
}
```

Editing the user policy user signin by changing auth server to "auth_server_1":

```
      Input Payload : {
   'name': 'User Signin',
   'description': 'User Signin',
   'sign_in_config': {
      'policy_type': 'user',
      'primary_auth_server_id': '0b634b96bcb04dc98072cf28c5129a91',
      'realm': 'ZTA Users',
      'url_pattern': '*/login/',
      'use_as_saml_idp': False
   },
   'type': 'sign_in',
   'id': '21ff78e93fda4b0c86e7af96dfa75680'
}
Request URI : ``https://<tenant_
domain>/api/v1/policies/resources/21ff78e93fda4b0c86e7af96dfa75680``
Returned Status Code : 200
Returned JSON Response : {
   'allow_delete': False,
   'description': 'User Signin',
   'id': '21ff78e93fda4b0c86e7af96dfa75680',
   'name': 'User Signin',
   'sign_in_config': {
      'id': '21ff78e93fda4b0c86e7af96dfa75680',
      'policy_type': 'user',
      'primary_auth_server_config': {
         'id': '0b634b96bcb04dc98072cf28c5129a91',
         'name': 'auth_server_1',
         'type': 'Local'
      },
      'primary_auth_server_id': '0b634b96bcb04dc98072cf28c5129a91',
      'realm': 'ZTA Users',
      'role_mapping_rules': [{
          'attribute': 'is',
          'id': 'bb77d22ae3b440bbb3d464f0df50f4af',
          'name': 'AllUsers',
          'type': 'username',
          'value': '*'
      }],
      'url_pattern': '*/login/',
      'use_as_saml_idp': False
```

```
   },
   'type': 'sign_in'
}
```

Adding user rule "user_rule_1" of type "username" for an expression matching:

```
      Input Payload : {
   'name': 'user_rule_1',
   'type': 'username',
   'value': 'user_rule_1',
   'attribute': 'is'
}
Request URI : ``https://<tenant_domain>/api/v1/policies/role-mapping-
rules``
Returned Status Code : 200
Returned JSON Response : {
   'attribute': 'is',
   'id': 'b48d02408ad14992bfde266e9b5a43a8',
   'name': 'user_rule_1',
   'type': 'username',
   'value': 'user_rule_1'
}
```

Adding a user group "user_group_1" of authentication policy type "user":

```
      Input Payload : {
   'name': 'user_group_1',
   'sign_in_policy_id': '21ff78e93fda4b0c86e7af96dfa75680',
   'description': 'user_group_1',
   'rules': []
}
Request URI : ``https://<tenant_domain>/api/v1/policies/user-rule-groups``
Returned Status Code : 200
Returned JSON Response : {
   'allow_delete': True,
   'description': 'user_group_1',
   'id': '71bc234b6c8f46a9806dfdc0e33df05d',
   'name': 'user_group_1',
   'role_config': {
      'id': 'a44e4ac7ae114e009fd2f2bd457c1480',
      'name': 'user_group_1',
      'redirect_url': '/user',
      'type': 'user'
   },
   'role_id': 'a44e4ac7ae114e009fd2f2bd457c1480',
   'sign_in_config': {
      'id': '21ff78e93fda4b0c86e7af96dfa75680',
      'policy_type': 'user',
      'primary_auth_server_config': {
         'id': '0b634b96bcb04dc98072cf28c5129a91',
         'name': 'auth_server_1',
         'type': 'Local'
      },
      'primary_auth_server_id': '0b634b96bcb04dc98072cf28c5129a91',
      'realm': 'ZTA Users',
      'url_pattern': '*/login/',
      'use_as_saml_idp': False
      },
   'sign_in_policy_id': '21ff78e93fda4b0c86e7af96dfa75680'
}
```

Editing user group "user_group_1" by adding user rule "user_rule_1":

```
      Input Payload :  {}
Request URI :  ``https://<tenant_domain>/api/v1/policies/user-rule-
groups/71bc234b6c8f46a9806dfdc0e33df05d/rule/b48d02408ad14992bfde266e9b5a43
a8``
Returned Status Code :  204
```

Editing user authentication server "auth_server_1" by adding user "newuser1":

```
      Input Payload : {
   'name': 'newuser1',
   'full_name': 'newuser1',
   'password': 'dana123'
   }
Request URI : ``https://<tenant_domain>/api/v1/policies/auth-
servers/0b634b96bcb04dc98072cf28c5129a91/users``
Returned Status Code : 200
```

Adding device policy rule "device_rule_1" of type network rule:

```
      Input Payload : {
   'name': 'device_rule_1',
   'description': 'device_rule_1',
   'network_config': {
      'ip_address': '192.168.1.1',
      'netmask': '255.255.255.0',
      'mode': 'allow'
   },
   'label': 'moderate',
   'type': 'network'
}
Request URI : ``https://<tenant_domain>/api/v1/policies/device-
policies/rules``
Returned Status Code : 200
Returned JSON Response : {
   'description': 'device_rule_1',
   'id': 'aab467febf0b45af99be71f25cb0fdbc',
   'label': 'moderate',
   'name': 'device_rule_1',
   'network_config': {
      'id': '98e55fe902b64d6abe45ec38012a64af',
      'ip_address': '192.168.1.1',
      'mode': 'allow',
      'netmask': '255.255.255.0'
   },
   'network_config_id': '98e55fe902b64d6abe45ec38012a64af',
   'type': 'network'
}
```

Adding device policy "device_policy_1":

```
      Input Payload : {}
Request URI : ``https://<tenant_domain>/api/v1/policies/device-
policies/groups/deb6e20a2f1a4c5dac98772525a7d350/rules/aab467febf0b45af99be
71f25cb0fdbc``
Returned Status Code : 204
```

Editing device policy "device_policy_1" by adding device policy rule "device_rule_1":

```
      Input Payload : {
   'name': 'device_policy_1',
   'description': 'device_policy_1'
}
Request URI : ``https://<tenant_domain>/api/v1/policies/device-
policies/groups``
Returned Status Code : 200
Returned JSON Response : {
   'description': 'device_policy_1',
   'id': 'deb6e20a2f1a4c5dac98772525a7d350',
   'name': 'device_policy_1',
   'rules': []
}
```

Adding a new Application "app1":

```
      Input Payload : {
   'type': 'application',
   'name': 'app1',
   'description': 'app1',
   'app_config': {
      'access_type': 'application',
      'name': 'app1',
      'resource': 'https://www.intuit.com',
      'resource_type': 'url',
      'bookmark_config': {
         'name': 'app1',
         'type': 'web',
         'description': 'app1',
         'launch_window': True,
         'url': 'https://www.intuit.com',
         'icon': '/admin/static/media/intuit512.2fdd1f2f.svg'
      }
   }
}
Request URI : ``https://<tenant_domain>/api/v1/policies/resources``
Returned Status Code : 200
Returned JSON Response : {
   'allow_delete': True,
   'app_config': {
      'access_type': 'application',
      'bookmark_config': {
         'description': 'app1',
         'icon': '/admin/static/media/intuit512.2fdd1f2f.svg',
         'id': '79418be3ce3a4ae4895d2d0223c2bf49',
         'launch_window': True,
         'name': 'app1',
         'type': 'web',
         'url': 'https://www.intuit.com'
      },
      'id': 'd3328c9a86ed42d0aa1d90432e4f7fb7',
      'name': 'app1',
      'resource': 'https://www.intuit.com',
      'resource_type': 'url'
   },
   'description': 'app1',
```

```
   'id': 'd3328c9a86ed42d0aa1d90432e4f7fb7',
   'name': 'app1',
   'type': 'application'
}
```

Adding a new gateway "gw1" of type vsphere with manual settings:

```
      Input Payload : {
   'name': 'gw1',
   'orchestration': {
      'type': 'vsphere'
   },
   'location': {
      'city_id': 97
   }
}
Request URI : ``https://<tenant_domain>/api/gateways``
Returned Status Code : 200
Returned JSON Response : {
   'auto_upgrade': True,
   'created': '2020-09-10T05:29:39Z',
   'id': 'b7c3fca3993a4addaa4fe08958afa013',
   'is_ready': False,
   'location': {
      'city_id': 97
   },
   'name': 'gw1',
   'notification_channel_status': 'offline',
   'orchestration': {
      'mode': 'manual',
      'type': 'vsphere'
   },
   'sdp_mode': 'pzt-gateway',
   'state': 'unregistered',
   'updated': '2020-09-10T05:29:39Z'
}
```

```
      Input Payload : {
   'service_account_id': None,
   'appliance_config': {
      'external_gateway': '<ip_address>',
      'external_ip_address': '<ip_address>',
      'external_subnet': '255.255.255.0',
      'external_vlan': '-1',
      'internal_fqdn': '',
      'internal_gateway': '<ip_address>',
      'internal_ip_address': '<ip_address>',
      'internal_subnet': '255.255.255.0',
      'internal_vlan': '-1',
      'management_gateway': '<ip_address>',
      'management_ip_address': '<ip_address>',
      'management_subnet': '255.255.255.0',
      'management_vlan': '-1',
      'primary_dns': '<ip_address>',
      'private_domain_name': 'psecure.net',
      'secondary_dns': '<ip_address>',
      'dns_search_domain': '<domain>',
      'public_ip_address': '<ip_address>'
   },
   'deployment_config': None
}
Request URI : ``https://<tenant_
domain>/api/gateways/b7c3fca3993a4addaa4fe08958afa013/orchestration``
Returned Status Code : 200
Returned JSON Response : {
   'appliance_config': {
      'dns_search_domain': 'psecure.net',
      'external_fqdn': '<server>',
      'external_gateway': '1<ip_address>',
      'external_ip_address': '1<ip_address>',
      'external_subnet': '255.255.255.0',
      'internal_fqdn': '',
      'internal_gateway': '<ip_address>',
      'internal_ip_address': '<ip_address>',
      'internal_subnet': '255.255.255.0',
      'management_gateway': '<ip_address>',
      'management_ip_address': '<ip_address>',
```

```
      'management_subnet': '255.255.255.0',
      'primary_dns': '<ip_address>',
      'private_domain_name': 'psecure.net',
      'public_ip_address': '<ip_address>',
      'secondary_dns': '<ip_address>',
      'use_dhcp': True,
      'wins_server': 'localhost'
   },
   'appliance_id': 'b7c3fca3993a4addaa4fe08958afa013'
}
```

Adding a new Secure Access Policy for the above configurations:

```
      Input Payload : {
   'type': 'application',
   'resource_type': 'single',
   'user_rule_group_id': '71bc234b6c8f46a9806dfdc0e33df05d',
   'gateway_type': 'single',
   'gateway_id': 'b7c3fca3993a4addaa4fe08958afa013',
   'resource_id': 'd3328c9a86ed42d0aa1d90432e4f7fb7',
   'device_policy_id': 'deb6e20a2f1a4c5dac98772525a7d350'
}
Request URI : ``https://<tenant_domain>/api/v1/policies/secure-access-
policies``
Returned Status Code : 200
Returned JSON Response : {
   'device_policy_config': {
      'name': 'device_policy_1'
   },
   'device_policy_id': 'deb6e20a2f1a4c5dac98772525a7d350',
   'gateway_id': 'b7c3fca3993a4addaa4fe08958afa013',
   'gateway_type': 'single',
   'id': 'c90a3e348a0f4fed868d5acd09655aa6',
   'resource_config': {
      'name': 'app1'
   },
   'resource_id': 'd3328c9a86ed42d0aa1d90432e4f7fb7',
   'resource_type': 'single',
   'type': 'application',
   'user_rule_group_config': {
      'name': 'user_group_1',
      'role_config': {
         'id': 'a44e4ac7ae114e009fd2f2bd457c1480',
         'name': 'user_group_1',
         'redirect_url': '/user',
         'type': 'user'
      }
   },
   'user_rule_group_id': '71bc234b6c8f46a9806dfdc0e33df05d'
}
```