appviewX

API Guide

Version: 2019.4.0

Copyright AppViewX, Inc.

External Reference Links

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
1.0	Initial release of document for Release 2019.4.0	Oct 2019

About this Guide

This guide explains how to use the AppViewX API to perform different functions. It includes descriptions, pointers to code samples, and request/response formats.

Text Conventions

The following text conventions are used in this document:

Convention	Description
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1: API Guide

Overview

The AppViewX API is a programmatic way to get data in and out of the AppViewX subsystems. With access to RESTful AppViewX APIs, you can leverage the raw potential of AppViewX. It provides a powerful way to channel the data into native business applications. This document comprises of module-wise APIs used in AppViewX.

Restful HTTPS Requests

HTTP GET

GET requests, retrieve resource representation/information only and not to modify it.

HTTP POST

POST APIs create new subordinate resources. For example, a file is subordinate to a directory containing it or a row is subordinate to a database table. In terms of REST, POST methods are used to create a new resource into the collection of resources.

HTTP PUT

PUT APIs are used to update existing resources (if a resource does not exist then API may decide whether to create a new resource or not).

HTTP DELETE

DELETE APIs are used to delete resources (identified by the Request-URI).

Description of Server Responses

1. **200** OK - the request was successful (some API calls may return 201 instead).
2. **400** Bad Request - the request is not understood or required parameters are missing.
3. **401** Unauthorized - authentication failed or the user doesn't have permissions for the requested operation.
4. **403** Forbidden - access denied.
5. **404** Not Found - resource not found.
6. **429** Too many requests - the number of requests to the service has crossed the threshold.
7. **504** Gateway timeout - the given request has exceeded the expected time.
8. **503** Service unavailable - the client cannot communicate with the service.

This guide explains how to use the AppViewX API to perform different functions. It includes descriptions, pointers to code samples, and request/response formats.

URI Scheme

- **Host :** {url}
- **BasePath :** /avxapi
- **Schemes :** HTTPS
- **URL :** https://{url}/avxapi

Chapter 2: Prerequisites

Prerequisites

Before using APIs in this guide, make sure the following conditions are met:

- You have provided the gateway key **(gwkey=<gwkey>)** in the URL. APIs won't work without this gateway key.
- There are no spaces in the sample request.

Retrieve a Gateway Key

To retrieve a gateway key,

1. Log in to the CLI of the server where AppViewX is hosted.
2. Go to the directory /<Install_Directory>/conf.
3. Use the command **vim** to open the **appviewx.conf** file
4. Locate the gateway settings information in the file
5. The gateway key is displayed in the field: AppViewX_GATEWAY_KEY= <VALUE>.
6. Use the <VALUE> in the API (gwkey=<gwkey>) field in the URL of the APIs.

Retrieve the Session ID

You can use the following REST service to login. The session ID retrieved from this API can be used to access other APIs.

URL: http://<url>?gwkey=f000ca01&gwsource=API

Type: POST

Example: http://appviewx.eval.com:31443/avxapi/login?gwsource=external

- Method: POST
- Response Format: JSON
- Requires authentication: Yes (User context only)
- Request timeout period: 15 minutes.

Parameters

Param Type	Name	Description	Field Type
Header	username**	Login username	string
Header	Password**	Password for the username	String
Header	Content-Type**	Specifies the nature of the data in the payload (The value of the param should be "application/json")	String
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
** - *Mandatory value*			

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Login failed. Invalid credentials.
200	OK	Login successful
401	Unauthorized	Authentication failed. The reason - Invalid Credentials.

Sample Request/Response

Use Case

Log in to the application with a username and password.

Request URL

http://appviewx.eval.com:31443/avxapi/login?gwsource=external

Request Payload

```
{}
```

Response


```
{
  "response": {
  "status": "SUCCESS",
  "appStatusCode": null,
  "statusDescription": null,
  "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813",
  "availableLoginAttemptCount": 10
  },
  "message": null,
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```

Chapter 3: Commons

Login

Authenticate into the AppViewX application. If success will return a session id which can be used as an authentication token to access the other APIs.

URL: /login

Type: POST

Parameters

Param Type	Name	Description	Field Type
Header	username**	Login username	String
Header	Password**	Password for the username	String
Header	Content-Type**	Specifies the nature of the data in the payload (The value of the param should be "application/json")	String
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	String
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Username or password cannot be null or empty
200	OK	Login successful
401	Unauthorized	Login failed. Invalid Credentials

• Sample Request/Response

Sample Request/Response

Use Case

Log in to the application with a username and password.

Request URL

http://appviewxapi.com/avxapi/login?gwkey=f000ca01&gwsource=test

Request Payload

```
{}
```

Response

```
{
 "response": {
 "status": "SUCCESS",
 "appStatusCode": null,
 "statusDescription": null,
 "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813",
 "availableLoginAttemptCount": null
 },
 "message": null,
 "appStatusCode": null,
 "tags": null,
 "headers": null
}
```

Add Resource

Create a new resource. A resource is a logical entity to group one or more ACL managed entities.

URL: /resource

Type: POST

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String

Param Type	Name	Description	Field Type
Payload	name**	Name of the resource to create. Name cannot be duplicated.	String
Payload	description	Description of the resource	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Mandatory field '<field name>' is missing
201	Created	Resource added successfully
409	Conflict	Resource with the given name already exists

• Sample Request/Response

Sample Request/Response

Use Case

Add a new resource with the name resource_1.

Request URL

http://appviewxapi.com/avxapi/resource?gwkey=f000ca01&gwsource=external

Request Payload

```
{
"payload": {
"name": "resource_1",
"description": "This is a sample resource."
}
}
```

Response

```
{
"response": "Resource added successfully",
"message": "Resource added successfully",
"appStatusCode": null,
"tags": null,
"headers": null
}
```


Search for Resource

Search for resource-based on input filter condition. A resource is a logical entity to group one or more ACL managed entities. The response could be one or more resource(s) matching the input.

URL: /resource-search

Type: POST

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	filterValue	Input filter string value to filter the resources.	String
Payload	sortColumn	Column by which the output has to be sorted	String
Payload	startIndex	Start index to show in output in case if there are more than one matching records	Integer
Payload	maxSize	The number of records to return in a response. maxSize is starting from the start index	Integer
Payload	sortOrder	The order to sort. Possible values are asc and desc	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
200	OK	Matching results found for the given input.
404	OK	No match found for the given input.
400	Bad request	Invalid sort Column

- Sample Request/Response

Sample Request/Response

Use Case

Search a resource with the name Role_admin.

Request URL

http://appviewxapi.com/avxapi/resource-search?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "startIndex" : 1,
 "maxSize" : 3,
 "sortOrder":"asc",
 "sortColumn" : "name",
 "filterValue" : " resource_1"
 }
}
```

Response

```
{
 "response": {
 "data": [
 {
```

```
"name": "Role_admin",
"description": "Super access will have the permissions to access all the resources in AppViewX.",
"state": "A",
"_id": " Role_admin ",
"_keywords": null
}
],
"totalRecords": 1,
"obtainedRecords": 1,
"obtainedRecordRange": {
"start": 1,
"end": 1
}
},
"message": "Matching results found for the given input.",
"appStatusCode": null,
"tags": null,
"headers": null
}
```


The state of a resource indicates if the resource is active or not. ‘A’ stands for active.

Get Resources for User Group

Fetch all the resources for a given user group.

URL: /usergroup-getResources

Type: POST

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string

Param Type	Name	Description	Field Type
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	Name **	Name of the user group	String
Payload	startIndex	Start index to show in output in case if there are more than one matching records	Integer
Payload	maxSize	The number of records to return in a response. maxSize is starting from the start index	Integer

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
200	OK	Matching results found for the given input.
404	Not Found	No matching records found.
400	Bad request	Usergroup name cannot be empty.

Sample Request/Response

Use Case

Get all resources under the user group usergroup_1.

Request URL

http://appviewxapi.com/avxapi/usergroup-getResources?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "startIndex": 1,
```

```
 "maxSize": 0,
 "name": "usergroup_1"
 }
}
```


Response


```
{
"response":{
"data":[
{"name": " resource_0", "description": "Resource for usergroup_0", "state": "A",...},
{"name": "resource_1", "description": " Resource for usergroup_1", "state": "A",...},
{"name": " resource_2", "description": “Resource for usergroup_1”, "state": "A", ,...},
{"name": " resource_3", "description": "Resource for usergroup_1", "state": "A",...}
],
"totalRecords": 4,
"obtainedRecords": 4,
"obtainedRecordRange":{
"start": 1,
"end": 4
}
},
"message": "Matching results found for the given input.",
"appStatusCode": null,
"tags": null,
"headers": null
}
```


The state of a resource indicates if the resource is active or not. ‘A’ stands for active.

Delete Resource

Delete a resource.

URL: /resource

Type: DELETE

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Query	resourceName**	Name of the resource to be deleted.	String

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	ResourceName cannot be empty
200	OK	Resource deleted successfully
404	Not Found	Resource Name does not exist
403	Forbidden	Current user(s) aclIdentifier/resource cannot be deleted

• Sample Request/Response

Sample Request/Response

Use Case

Delete a resource with name resource_1.

Request URL

http://appviewxapi.com/avxapi/resource?resourceName=resource_1&gwkey=f000ca01&gwsource=external

Request Payload

NA

Response

```
{
"response": "Resource deleted successfully",
"message": "Resource deleted successfully",
"appStatusCode": null,
"tags": null,
"headers": null
}
```


Search for Role

Search for a role based on the input filter condition. A role is a logical entity to group one or more Access Control Functions. The response could be one or more resource(s) matching the input.

URL: /role-search

Type: POST

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	filterValue	Input filter value string to filter the role.	String
Payload	sortColumn	Column by which the output has to be sorted	String
Payload	startIndex	Start index to show in output in case if there are more than one matching records	Integer
Payload	maxSize	The number of records to return in a response. maxSize is starting from the start index	Integer
Payload	sortOrder	The order to sort. Possible values are asc and desc	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
200	OK	Matching results found for the given input.
404	OK	No matching records found.
400	Bad request	Invalid sortColumn

- Sample Request/Response

Sample Request/Response

Use Case

Search a role with the name Role_admin.

Request URL

http://appviewxapi.com/avxapi/role-search?gwkey=f000ca01&gwsource=external

Request Payload

```
{
  "payload": {
    "startIndex" : 1,
    "maxSize" : 2,
    "sortColumn" : "name",
    "sortOrder":"asc",
     "filterValue" : "admin"
    }
}
```

Response

```
{
    "response": {
        "data": [
            {
```

```
            "name": "admin",
            "description": "admin",
            "permissions": [
                "certificate:connectorActions:secureConnector",
                "certificate:settings:casettings:custom_ca",
                "certificate:settings:appsettings:view",
                "adc:dashboard:deviceheatmap:modifysettings",
                "certificate:client:adminaccess",
                "adc:deviceGroup:delete"
            ],
            "state": "A",
            "accessControlObjects": null,
            "_id": "admin",
            "_keywords": null
        }
    ],
    "totalRecords": 1,
    "obtainedRecords": 1,
    "obtainedRecordRange": {
        "start": 1,
        "end": 1
    }
  },
  "message": "Matching results found for the given input.",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


The state of a role indicates if the resource is active or not. ‘A’ stands for active.

Add Role

Add a new role to the system.

URL: /role

Type: POST

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	name**	Name of the role.	String
Payload	description	Description of the role	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Role name cannot be null, empty or whitespace alone
201	Created	Role added successfully
409	Conflict	Role with the given name already exists

• Sample Request/Response

Sample Request/Response

Use Case

Add a role with a valid role name.

Request URL

http://appviewxapi.com/avxapi/role?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "name":"role_1",
 "description":"Adding a new role"
 }
}
```

Response

```
{
 "response": "Role added successfully",
 "message": "Role added successfully",
 "appStatusCode": null,
 "tags": null,
 "headers": null
}
```

Get Role

Get the role information.

URL: /role

Type: GET

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Query	roleName **	Name of the role.	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
200	OK	Role Information Retrieved Successfully
400	Bad Request	Role name cannot be empty

• Sample Request/Response

Sample Request/Response

Use Case

Get the information about the role **role_1**.

Request URL

http://appviewxapi.com/avxapi/role?roleName=role_1&gwkey=f000ca01&gwsource=external

Request Payload

NA

Response


```
{
 "response": {
  "name": "role_1",
  "description": "role_1 details",
  "permissions": [
   "permission_1"
  ],
  "state": "A",
  "_id": "log",
  "_keywords": [
   "role used to test role functions.",
   "log",
   "Enabled"
```

```
  ]
 },
 "message": "Role Information Retrieved Successfully",
 "appStatusCode": null,
 "tags": null
}
```


Delete Role

Delete a role.

URL: /role

TYPE: DELETE

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Query	roleName**	Name of the role to delete.	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	RoleName cannot be empty
200	OK	Role deleted successfully
404	Not Found	RoleName does not exist

HTTP Code	Description	Response Message
403	Forbidden	Role(s) which have an active user(s) cannot be deleted

Sample Request/Response

Use Case

Delete a role with name role_1.

Request URL

http://appviewxapi.com/avxapi/role?roleName=role_1&gwkey=f000ca01&gwsource=external

Request Payload

NA

Response


```
{
"response": "Role deleted successfully",
"message": "Role deleted successfully",
"appStatusCode": null,
"tags": null,
"headers": null
}
```


Clone Role

Clone a role.

URL: role-clone

Type: POST

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	String
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	String
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	existingName **	Name of the role to be cloned.	String
Payload	newName**	Name of the cloned new role	String
Payload	description**	Description of the cloned role	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
200	Ok	Clone role successful
404	Not Found	Role Name to be cloned not found
400	Bad Request	The payload cannot be empty or null
400	Bad Request	Source Role Name can not be empty for clone action
400	Bad Request	Role name cannot be left empty or blank
400	Bad Request	Role name cannot be less than 2 characters
400	Bad Request	Role name cannot exceed 64 characters
400	Bad Request	Invalid Description
400	Bad Request	Source role and new role names cannot be empty

• Sample Request/Response

Sample Request/Response

Use Case

Clone a role role_1 to create a new cloned role named clonerole_1.

Request URL

http://appviewxapi.com/avxapi/role-clone?gwkey=f000ca01&gwsource=external

Request Payload

```
{
  "payload": {
    "existingName": "role_1",
    "newName": "clonerole_1",
    "description": "clone test role."
  }
}
```

Response

```
{
"response": "Clone role successful",
"message": "Clone role successful",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Share Dashboard to Role

Share an existing dashboard to one or more existing roles. The sharing can be restricted to read-only or as a read-write.

URL: /dashboard-share-to-roles

Type: PUT

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	readRoles	Name of the roles that need to have only read access to the dashboard.	String
Payload	readWriteRoles	Name of the roles that need to have read-write access to the dashboard.	String
Query	dashboardName**	Name of the dashboard to be shared	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Dashboard name is mandatory
404	Not Found	Dashboard not found
403	Forbidden	Read-write permission not available for the given dashboard

• Sample Request/Response

Sample Request/Response

Use Case

Share a dashboard named dashboard_1 in reading more to the role RO_role and in write mode to the role RW_role.

Request URL

http://appviewxapi.com/avxapi/dashboard-share-to-roles?dashboardName=dashboard_1&gwkey=f000ca01&gwsource=external

Request Payload

```
{
  "payload": {
    "readRoles": [
      "admin"
    ],
    "readWriteRoles": [
      "admin"
    ]
  }
}
```

Response

```
{
"response": "Dashboard shared to the specified roles.",
"message": "Dashboard shared to the specified roles.",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Add a User Group

Add a new user group to the system.

URL: /usergroup

Type: POST

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string

Param Type	Name	Description	Field Type
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	name**	Name of the user group.	String
Payload	description	Description of the user group	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	User group name cannot be null, empty or whitespace alone
201	Created	User group added successfully
409	Conflict	User group with the given name already exists

Sample Request/Response

Use Case

Add a user group with a valid name.

Request URL

http://appviewxapi.com/avxapi/usergroup?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "name": "usergroup_1",
 "description": "Adding user group"
 }
}
```

Response

```
{
 "response": " Usergroup added successfully",
 "message": " Usergroup added successfully",
 "appStatusCode": null,
 "tags": null,
 "headers": null
}
```


Associate Permissions to Role

Assign/Un-assign ACF permissions to a role.

URL: /role-updatePermission

Type: PUT

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	roleName**	Name of the role	String
Payload	assignPermissionList	ACF permissions to be assigned to the role. Refer to the list of possible permissions list for details.	Array
Payload	unassignPermissionList	ACF permissions to be unassigned from the role. Refer to the list of possible permissions list for details.	Array

** - *Mandatory value*

Even if the assignPermissionList and unassignPermissionList contain invalid ACF permission text that cannot be processed, the API would still go-ahead to assign/un-assign any functions in wither list that can be processed.

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Role name cannot be left empty or blank.
202	Accepted	ACF assignment initiated for the given role.
400	Bad request	Permission list cannot be empty

- Sample Request/Response

Sample Request/Response

Use Case

Assign and unassign few ACF permissions to/from the role “role_1”.

Request URL

http://appviewxapi.com/avxapi/role-updatePermission?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "roleName": "role_1",
 "assignPermissionList": [
 "general:accounts:resource:clone",
 "general:accounts:resource:delete"
 ],
 "unassignPermissionList": [
 "general:accounts:resource:delete"
 ]
 }
}
```

Response

```
{
 "response": "ACF assignment initiated for the given role",
 "message": "ACF assignment initiated for the given role",
```

```
 "appStatusCode": null,
 "tags": null,
 "headers": null
}
```


Search User Group

Search / Get the details about a user group. The user group can be filtered by the given input.

URL

/usergroup-search

Type

POST

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Payload	filterValue	Input filter value string to filter the role.	String
Payload	sortColumn	Column by which the output has to be sorted	String
Payload	startIndex	Start index to show in output in case if there are more than one matching records	Integer
Payload	maxSize	The number of records to return in a response. maxSize is starting from the start index	Integer
Payload	sortOrder	Order of sorting. Possible values are asc and desc	String

** - *Mandatory value*

Possible Response MESSAGE & CODE

HTTP Code	Description	Response Message
200	Accepted	Matching results found for the given input.
404	Bad request	No matching records found

Sample Request/Response

Use Case

Get the details about a user group with the name usergroup_1.

Request URL

http://appviewxapi.com/avxapi/usergroup-search?gwkey=f000ca01&gwsource=external

Request Payload

```
{
  "payload": {
    "startIndex" : 1,
    "maxSize" :1,
    "sortColumn" : "name",
    "sortOrder":"asc",
     "filterValue" : "admin usergroup"
    }
}
```

Response

```
{
"response":{
"data":[
{"name": " usergroup_1", "description": "Test user group", "roles":[], "aclIdentifiers":[],...}
],
"totalRecords": 1,
"obtainedRecords": 1,
```

```
"obtainedRecordRange":{
"start": 1,
"end": 1
}
},
"message": "Matching results found for the given input.",
"appStatusCode": null,
"tags": null,
"headers": null
}
```


Delete User Group

Delete a user group.

URL: /userGroup

Type: DELETE

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	userGroupName **	Name of the user group to be deleted	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Invalid Request
200	OK	UserGroup deleted successfully
404	Not Found	UserGroup does not exist
403	Forbidden	Current user(s) usergroup(s) cannot be deleted

• Sample Request/Response

Sample Request/Response

Use Case

Delete a resource with name resource_1.

Request URL

http://appviewxapi.com/avxapi/resource?resourceName=resource_1&gwkey=f000ca01&gwsource=external

Request Payload

NA

Response


```
{
"response": "Resource deleted successfully",
"message": "Resource deleted successfully",
"appStatusCode": null,
"tags": null,
"headers": null
}
```


Associate User Group with Resources

Associate one or more resources to a user group.

URL: /usergroup-updateResource

Type: POST

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (For example, web, external)	String
Payload	filterValue**	Value to filter the name	String
Payload	assignPermissionList	ACF permissions to be assigned to the role	Array
Payload	unassignPermissionList	ACF permissions to be unassigned from the role	Array

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	User group not found.
200	Accepted	Successfully associated user group - resource

• Sample Request/Response

Sample Request/Response

Use Case

Get the details about a user group with the name usergroup_1.

Request URL

http://appviewxapi.com/avxapi/usergroup-updateResource?gwkey=f000ca01&gwsource=external

Request Payload


```
{
  "payload": {
  "name": "testgroup",
  "assignList" : [
  "resource_2"
  ],
  "unassignList": [
  "resource_1"
  ]
}
}
```


Response


```
{
  "response": "Updating usergroup with resource(s) successful",
  "message": "Updating usergroup with resource(s) successful",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


Add User

Creates a new user.

URL: /user

Type: POST

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string

Param Type	Name	Description	Field Type
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Payload	loginName**	Unique names used as the username for authentication. Duplication is not allowed	String
Payload	password**	A password that can be used to authenticate. Note: Not relevant if ‘isExternalAuth’ is set to Y	String
Payload	confirmPassword**	Reconfirm the given password Note: Not relevant if ‘isExternalAuth’ is set to Y	String
Payload	isExternalAuth**	Specify if the user is from an external authentication system like LDAP, Radius, etc. Possible values are ‘Y’ for yes and ‘N’ for No	String
Payload	comment	Comment for the user	String
Payload	preferredContactMode**	Preferred contact mode. Possible values are ‘E’ for email.	String
Payload	email**	Email address	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	The user password cannot be null or empty TBD … more 400
201	Created	User added successfully
409	Conflict	Operation failed. Unable to add a new entity. Entity already exists

• Sample Request/Response

Sample Request/Response

Use Case

Add a new internal user with login name **appviewx**.

Request URL

http://appviewxapi.com/avxapi/user?gwkey=f000ca01&gwsource=external

Request Payload


```
{
  "payload": {
  "loginName": "appviewx",
  "password":"QWRtaW5AMTIz",
  "confirmPassword": "QWRtaW5AMTIz",
  "isExternalAuth" : "N",
  "comment": "This is a test user",
  "preferredContactMode": "E",
  "email": "appviewx@app.com"
}
}
```


Response


```
{
  "response": "User added successfully",
  "message": "User added successfully",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


Associate Roles to a User Group

Associate or disassociate one or more roles to a user group.

URL: platform-assign-roles-to-usergroup

Type: PUT

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	assignRoles	An array of role names to assign	Array
Payload	unassignRoles	An array of role names to unassign	Array
Payload	name**	Name of the user-group for consideration	String

** - *Mandatory value*

Even if the assignRoles and unassignRoles contain invalid role names that cannot be processed, the API would still go-ahead to assign/un-assign any role in the list that can be successfully processed.

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Usergroup Name cannot be null or empty
200	OK	Updating user group with role(s) successful TBD – Change text, multiple cases
409	Conflict	Operation failed. Unable to add a new entity. Entity already exists

• Sample Request/Response

Sample Request/Response

Use Case

role_1, role_2, and role_3 are existing in the application. role_1 and role_2 have to be assigned to the user group *appviewx_usergroup* and role_3 has to be unassigned.

Request URL

http://appviewxapi.com/avxapi/platform-assign-roles-to-usergroup?gwkey=f000ca01&gwsource=external

Request Payload

```
{
  "payload": {
    "loginName": "appviewx",
    "assignUserGroups": [
      "usergroup_1",
          "usergroup_2"
    ],
    "unassignUserGroups": [
      "usergroup_3"
    ]
  }
}
```

Response

```
{
  "response": "Updating usergroup with role(s) successful",
  "message": "Updating usergroup with role(s) successful",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```

Associate User Groups to a User

Associate or disassociate one or more user groups to a user.

URL: /user-updateUsergroups

Type: PUT

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	assignUserGroups	An array of user group names to assign	Array
Payload	unAssignUserGroups	An array of user group names to unassign	Array
Payload	loginName**	Login name of the user	String

** - *Mandatory value*

Even if the assignUserGroups and unAssignUserGroups contain invalid user group names that cannot be processed, the API would still go-ahead to assign/un-assign any user group in the list that can be successfully processed.

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Usergroup Name cannot be null or empty
200	OK	Updating user group with a role(s) successful TBD – Change text, multiple cases
409	Conflict	Operation failed. Unable to add a new entity. Entity already exists

• Sample Request/Response

Sample Request/Response

Use Case

"usergroup_1, usergroup_2, and usergroup_3 are existing in the application. usergroup_1 and usergroup_2 have to be assigned to the user with loginname user_1 and usergroup_3 has to be unassigned"

Request URL

http://appviewxapi.com/avxapi/user-updateUsergroups?gwkey=f000ca01&gwsource=external

Request Payload


```
{
  "payload": {
    "loginName": "appviewx",
    "assignUserGroups": [
      "usergroup_1",
          "usergroup_2"
    ],
    "unassignUserGroups": [
      "usergroup_3"
    ]
  }
}
```


Response


```
{
  "response": "Successfully modified user-user group association",
  "message": " Successfully modified user-user group association ",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


Search for a user

Search for a user with filter details.

URL

/user-search

Type

POST

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	filterValue	Input filter value string to filter the role.	String
Payload	sortColumn	Column by which the output has to be sorted	String
Payload	startIndex	Start index to show in output in case if there are more than one matching records	Integer
Payload	maxSize	The number of records to return in a response. maxSize is starting from the start index	Integer
Payload	sortOrder	Order of sorting. Possible values are asc and desc	String

** - *Mandatory value*

Possible Response MESSAGE & CODE

HTTP Code	Description	Response Message
404	Not Found	No matching records found
200	OK	Matching results found for the given input.

Sample Request/Response

Use Case

Search for use with name appviewx_user1.

Request URL

http://appviewxapi.com/avxapi/ user- search?gwkey=f000ca01&gwsource=external

Request Payload


```
{
"payload": {
"startIndex" : 1,
"maxSize" : 2,
"sortColumn" : "loginName",
"sortOrder" :"asc",
"filterValue" : "appviewx_user1"
}
}
```


Response


```
{
"response": {
"data": [
{
"loginName": "appviewx_user1",
"firstName": "Appviewx",
"lastName": "user1",
"comment": Appviewx login user,
"email": "",
"mobile": "",
"preferredContactMode": "",
"isExternalAuth": "N",
"state": "A",
"roles": null,
"swImages": null,
"authenticationMode": "Internal",
"available": "Active",
"lastLogIn": "Online",
"sessionIds": null,
```


"aclIdentifiers": null,

"tenantId": null,

"availableIncorrectAttempt": 10,

"lastLoginTimestamp": 1585669200198,

"adUserGroups": null,

"sso": false,

"date": "2020-04-13 12:05:09",

"_id": "5d258291d7f495bb31691fc4",

"userGroups": null,

"_keywords": null,

"isSSO": false

}

],

"totalRecords": 1,

"obtainedRecords": 1,

"obtainedRecordRange": {

"start": 1,

"end": 1

}

},

"message": "Matching results found for the given input.",

"appStatusCode": null,

"tags": null,

"headers": null

}

Chapter 4: Control Center

- Application Delivery

Application Delivery

- Search Object (Control Center)
- Get Object Hierarchy/Topology
- Get Object Configuration
- Take Device Backup
- Get Backup Details for a Device
- Add Device
- Search Device
- Delete Device
- Sync Configuration
- Manage Device
- Un-manage a Device
- Create Application Widget
- Get Class Management Widget Details
- Delete a Widget
- Action - Enable an Object
- Action - Disable an Object
- Action - Forcedown Object
- Action - Forcedown Active Object
- Action - Graceful Disable Object
- Action - Enable Persistence for Object
- Action - Disable Persistence for Object
- Action Clear Persistence Record
- Action – InService (Activate) Object
- Action - OutOfService (Suspend) Object
- Action - Set Highest Priority
- Action - Set Connection Limit

- Action - Set Loadbalancing Method
- Action - Set Ratio
- Action - Set Service Down Value
- Action - ARP Enable/Disable
- Action - Set Weight
- Action - Set CNAME

Search Object (Control Center)

Search for one or more objects for the given input filter.

URL: /adc-objects-search

Type: POST

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Payload	input**	Input filter key and value to perform the search. Multiple key and value pairs can also be mentioned. **Supported keys :** • deviceName • objectType • vendor • destinationIp • destinationPort • partition • connections • ip	Key:value

Param Type	Name	Description	Field Type
Payload	Filter	**start:** start index of the response to the display. The default value is taken as 1. **max:** number of entries from a start index to display. The default value is taken as 100. **sortColumn :** Sort by column **sortOrder:** Sorting order (asc/desc)	

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Invalid search input
200	OK	Matching results found for the given input
200	OK	No matching results found

• Sample Request/Response

Sample Request/Response

Use Case

View all the Wide IPs in the system.

Request URL

http://appviewxapi.com/avxapi/adc/adc-objects-search?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "input": {
 "objectType": "Wideip"
```

```
 },
 "filter": {
 "start": 1,
 "max": 100, // Max limit allowed is 100
 "sortColumn": "displayName",
 "sortOrder": "asc"
 }
 }
}
```

Response

```
{
 "response": {
  "objects": [
   {
    "resource_id": "gw:@5c0e7af949d8d306e60745d7:@Add.com:@AppTag:@naptr",
    "code": "gw",
    "configData": "gtm wideip naptr /AppTag/Add.com{\npools {\n/AppTag/groupingPoolllll {\norder 0\n}\n    }\n}\n",
    "color": "AVAILABILITY_STATUS_RED",
    "displayName": "Add.com/naptr/f5-v13-112.92.com/F5",
    "description": "",
    "deviceId": "5c0e7af949d8d306e60745d7",
    "partition": "AppTag",
    "ipv6NoErrorNegTtl": "",
     ……
   }
  ],
  "totalRecords": 534,
  "obtainedRecords": 100,
  "obtainedRecordRange": {
   "start": 1,
   "end": 100
  }
 },
 "message": "Matching results found for the given input."
}
```

Get Object Hierarchy/Topology

Get the complete hierarchy of an object from its root object.

URL: /adc-object-hierarchy

Type: POST

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Payload	Object	The composite key values that have to be given to identify an object.	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Invalid Object type
200	OK	Topology successfully retrieved for the given object
404	Not Found	No object found
403	Forbidden	Permission not available for given objects

• Sample Request/Response

Sample Request/Response

Use Case

Get the topology details of the wide IP object with name SetHighestPriority.com in the common partition and on-device bigip-40-152.appviewx.com.

Request URL

http://appviewxapi.com/avxapi/adc-object-hierarchy?gwkey=f000ca01&gwsource=external

Request Payload


```
{
"payload": {
"object":
{
"deviceName": "bigip-40-152.appviewx.com",
"objectType": "wideIp",
"partition": "Common",
"objectName": "SetHighestPriority.com"
}
}
}
```


Response


```
{
  "response": {
    "_id": "gw:@5ba89bbada31ab1b43897071:@SetHighestPriority.com:@Common",
    "last-resort-pool": "none",
    "code": "gw",
                .....
                "color": "AVAILABILITY_STATUS_BLUE",
    "displayName": "SetHighestPriority.com/bigip-40-152.appviewx.com/F5",
    "description": "",
    "persistenceTtl": "",
    "gp": [
      "gp:@5ba89bbada31ab1b43897071:@pool2:@Common",
      "gp:@5ba89bbada31ab1b43897071:@pool1:@Common"
    ],
    "deviceId": "5ba89bbada31ab1b43897071",
    "ipv6NoErrorResponse": "disabled",
```

```
"persistCidrIpv4": "",
"persistCidrIpv6": "",
"partition": "Common",
.........
"children": [
 {
   "_id": "gp:@5ba89bbada31ab1b43897071:@pool1:@Common",
   "code": "gp",
   "configData": "gtm pool /Common/pool1 { }\n",
   "color": "AVAILABILITY_STATUS_BLUE",
   "displayName": "pool1/bigip-40-152.appviewx.com/F5",
   "deviceId": "5ba89bbada31ab1b43897071",
   "deviceName": "bigip-40-152.appviewx.com",
   "partition": "Common",
   "manualResume": "disabled",
   "vendor": "F5",
                        .......
   "alternate": "round-robin",
   "avaliablityRequirement": "all",
   "ttl": "30",
   "maxAddrReturned": "1",
   "gw": [
     "gw:@5ba89bbada31ab1b43897071:@SetHighestPriority.com:@Common",
     "gw:@5ba89bbada31ab1b43897071:@check02.com:@Common",
     "gw:@5ba89bbada31ab1b43897071:@unusedwideip.com:@Common"
   ],
   "qualityofService": {
     "qos-lcs": "30",
     "qos-hit-ratio": "5",
     "qos-hops": "0",
     "qos-packet-rate": "1",
     "qos-topology": "0",
     "qos-vs-score": "0",
     "qos-kilobytes-second": "3",
     "qos-vs-capacity": "0",
     "qos-rtt": "50"
   },
```



```
"limitConnections": "",
"parentName": [
  "unusedwideip.com",
  "check02.com",
  "SetHighestPriority.com"
],
"limitpps": "",
"name": "pool1",
"fallback": "return-to-dns",
"ratioMap": [
  {
    "partition": "Common",
    "name": "SetHighestPriority.com",
    "_id": "gw:@5ba89bbada31ab1b43897071:@SetHighestPriority.com:@Common",
    "order": "0",
    "ratio": "100"
  },
  {
    "partition": "Common",
    "name": "check02.com",
    "_id": "gw:@5ba89bbada31ab1b43897071:@check02.com:@Common",
    "order": "5",
    "ratio": "1"
  },
  {
    "partition": "Common",
    "name": "unusedwideip.com",
    "_id": "gw:@5ba89bbada31ab1b43897071:@unusedwideip.com:@Common",
    "order": "0",
    "ratio": "1"
  }
],
"monitors": [
  "none"
],
"status": "ENABLED",
"statusCode": "UNKNOWN ENABLED",
```



```
  "lastStatusSyncTime": 1546944201401,
  "ratio": "100",
  "order": "0",
  "children": [
  ]
 },
 {
  "_id": "gp:@5ba89bbada31ab1b43897071:@pool2:@Common",
  "code": "gp",
  "configData": "gtm pool /Common/pool2 {\n    fallback-ipv4 10.20.20.30\n}\n",
  "color": "AVAILABILITY_STATUS_BLUE",
  "displayName": "pool2/bigip-40-152.appviewx.com/F5",
  "deviceId": "5ba89bbada31ab1b43897071",
  "deviceName": "bigip-40-152.appviewx.com",
  "partition": "Common",
  "manualResume": "disabled",
  "dashboardObjectName": "pool2(bigip-40-152.appviewx.com)",
  "vendor": "F5",
  "gtr": [
   "gtr:@5ba89bbada31ab1b43897071:@wasdadsa"
  ],
  "dynamicRatio": "disabled",
  "verifyMemberAvailability": "enabled",
  ........
                        "gtt": [
   "gtt:@5ba89bbada31ab1b43897071:@/Common/pool2_wasdadsa"
  ],
  "alternate": "round-robin",
  "avaliablityRequirement": "all",
  "ttl": "30",
  "maxAddrReturned": "1",
  "gw": [
   "gw:@5ba89bbada31ab1b43897071:@SetHighestPriority.com:@Common"
  ],
  "qualityofService": {
   "qos-lcs": "30",
   "qos-hit-ratio": "5",
```

```
      "qos-hops": "0",
      "qos-packet-rate": "1",
      "qos-topology": "0",
      "qos-vs-score": "0",
      "qos-kilobytes-second": "3",
      "qos-vs-capacity": "0",
      "qos-rtt": "50"
    },
    "limitConnections": "",
    "parentName": [
      "SetHighestPriority.com"
    ],
    "limitpps": "",
    "name": "pool2",
    "fallback": "return-to-dns",
    "ratioMap": [
      {
        "partition": "Common",
        "name": "SetHighestPriority.com",
        "_id": "gw:@5ba89bbada31ab1b43897071:@SetHighestPriority.com:@Common",
        "order": "1",
        "ratio": "10"
      }
    ],
    "monitors": [
      "none"
    ],
    "status": "ENABLED",
    "statusCode": "UNKNOWN ENABLED",
    "lastStatusSyncTime": 1546944201401,
    "ratio": "10",
    "order": "1",
    "children": [

    ]
  }
]
```



```
 },
 "message": "Topology successfully retrieved for the given object.",
 "appStatusCode": null,
 "tags": null,
 "headers": null
}
```


Get Object Configuration

Gets the configuration of an object as stored in the AppViewX inventory. Supports both the latest configuration and also the configuration known at a given time if any.

Note: The configuration is not fetched from the device real-time but from the AppViewX inventory.

URL: /adc-object-configuration

Type: POST

Parameters

ParamType	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Payload	input**	Input filter key and value to perform the search. Multiple key and value pairs can also be mentioned. **Supported keys :** • deviceName • objectType • vendor • partition • etc.	Key:value

ParamType	Name	Description	Field Type
Payload	timeStamp	To get the known configuration at the given time mention the time stamp as well. If not mentioned the latest known configuration will be returned.	Long

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Invalid Object type, Invalid Request
200	OK	Configuration found for the given object.
404	Not found	Config data not found for the given object details

Sample Request/Response

Use Case

Get the known object configuration available at the time *1549362738957(time in milliseconds)* for the Virtual server with name Event_test in the partition Test_parti-tion.1 on the device device_1.

Request URL

http://appviewxapi.com/avxapi/adc-object-configuration?gwkey=f000ca01&gwsource=external

Request Payload

```
{
"payload": {
"object": {
"deviceName": "device_1",
"objectType": "VirtualServer",
"partition": "Test_parti-tion.1",
"objectName": "Event_test"
},
"timeStamp": 1549362738957
```

```
}
}
```


Response


```
{
"response": "** Virtual Server - Event_test **\nltm virtual /Test_parti-tion.1/Event_test {\n destination /Common/2.2.2.2:5004\n disabled\n ip-protocol tcp\n mask 255.255.255.255\n profiles {\n /Common/tcp { }\n }\n source 0.0.0.0/0\n translate-address enabled\n translate-port enabled\n}\n\n** Profile - tcp **\nltm profile tcp tcp {\n ack-on-push enabled\n close-wait-timeout 5\n congestion-control high-speed\n deferred-accept disabled\n delayed-acks enabled\n ecn disabled\n fin-wait-timeout 5\n idle-timeout 300\n keep-alive-interval 1800\n limited-transmit enabled\n max-retrans 8\n nagle disabled\n proxy-buffer-high 49152\n proxy-buffer-low 32768\n proxy-mss disabled\n proxy-options disabled\n receive-window-size 65535\n reset-on-timeout enabled\n selective-acks enabled\n send-buffer-size 65535\n slow-start enabled\n syn-max-retrans 3\n time-wait-recycle enabled\n time-wait-timeout 2000\n timestamps enabled\n}\n\n",
"message": "Configuration found for the given object.",
"appStatusCode": null,
"tags": null,
"headers": null
}
```


Take Device Backup

Triggers backup for a device. The backup will be stored in the AppViewX inventory.

URL: /adc-device-backup

Type: POST

Parameters

Param Type	Name	Description	Field type
Header	sessionId **	Session Id received after login	string
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Payload	backupName**	The name of the backup group. A group can have more than one backups. If the backup group name is already existing in the system,	String

Param Type	Name	Description	Field type
		then the backup will happen only if one of the following conditions are met. • The backup group is not configured yet with any devices. In this case, the device will be automatically added to the group. • The backup group is already configured with the given device.	
Payload	deviceName**	Name of the device	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	Device backup triggered successfully
403	Forbidden	Cannot access resource, permission not available.
403	Forbidden	Action cannot be performed on unmanaged device object(s)
400	Bad request	Respective vendor's device is not supported. Action cannot be performed
400	Bad request	Mismatch in backup type, cannot add a device to the existing group as it already has a device group configured
404	Not found	Device not available for the given details

Sample Request/Response

Use Case

Trigger a backup for the device ADC_GTM_1 with a backup name bkp_1. The backup for the device will be generated under the group bkp_1.

Request URL

http://appviewxapi.com/avxapi/ /adc-device-backup?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "backupName": "bkp_1",
 "deviceName": "ADC_GTM_1"
 }
}
```

Response

```
{
 "response": "Backup triggered for device ADC_GTM_1",
 "message": "Device backup triggered successfully."
}
```

Get Backup Details for a Device

List the archive details for an ADC device.

URL: /adc-device-archives

Type: GET

Parameters

ParamType	Name	Description	Field type
Header	sessionId **	Session Id received after login	string
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Payload	deviceName **	Name of the device.	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
200	OK	Archive details retrieved successfully
400	Bad Request	The device name is mandatory
404	Not Found	Device not available for the given details

Sample Request/Response

Use Case

Get the list of archives for the device with name bigip.40.151.bkp.com.

Request URL

http://appviewxapi.com/avxapi/adc-device-archives?deviceName=bigip.40.151.bkp.com&gwkey=f000ca01&gwsource=external

Request Payload

NA

Response


```
{
"response": {
"bigip.40.151.payoda.com": [
"chunkSize": 261120,
"length": 80179309,
"md5": "d0619f9065684875c6962ac9c75fe85c",
"filename": "F5_V11_40.152_1561354799000.tar.gz",
"metadata": {
"timeStamp": "1561354837000",
"deviceId": "5d0c8e1e7b4c057a5f656df9"
},
"_id": "5d106255785d7112c022657c"
},
"chunkSize": 261120,
"length": 80169090,
"md5": "1347ffa90124c26ab0a1e9205bd7aea6",
```

"filename": "F5_V11_40.152_1561293025000.tar.gz",

"metadata": {

"timeStamp": "1561293067000",

"deviceId": "5d0c8e1e7b4c057a5f656df9"

},

"_id": "5d0f710b785d7112c0224402"

},

"chunkSize": 261120,

"length": 80157312,

"md5": "a14dc63a72dbbb7d0cb8677cd0afc328",

"filename": "F5_V11_40.152_1561206626000.tar.gz",

"metadata": {

"timeStamp": "1561206663000",

"deviceId": "5d0c8e1e7b4c057a5f656df9"

},

"_id": "5d0e1f87785d7112c02219be"

},

"name": null,

"chunkSize": 261120,

"length": 80145137,

"md5": "930503177ff8f7a77f56dbf0e5db8bd4",

"filename": "F5_V11_40.152_1561120224000.tar.gz",

"metadata": {

"timeStamp": "1561120267000",

"deviceId": "5d0c8e1e7b4c057a5f656df9"

},

"_id": "5d0cce0b71aea9331507308b"

},

"message": “Archive details retrieved successfully”

"appStatusCode": null,

"tags": null,

"headers": null

}

Add Device

Add an ADC device.

URL: /adc-device-add

Type: POST

Parameters

Param Type	Name	Description	Field type
Header	sessionId **	Session Id received after login	string
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The device has been successfully added and configuration parse is triggered.
409	Conflict	Device(s) Already Exists
400	Bad request	Validation error [NOTE: Mandatory parameters will be dynamic basic based on vendor and version]

Sample Request/Response

Use Case

Add an F5 device with IP address 192.168.112.92 with both LTM and GTM modules with user name and password with the name f5-v13-112.92.com.

Request URL

http://appviewxapi.com/avxapi/ /adc-device-add/gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
```

```
 "name": "f5-v13-112.92.com",
 "communicationAddressType": "ip",
 "ip": "192.168.112.92",
 "vendor": "F5",
 "module": [
 "LTM",
 "BIG-IP DNS"
 ],
 "credentialType": "Manual Entry",
 "userName": "admin",
 "password": "YXBwdGFnQDEyMw=="
 }
}
```


Response


```
{
 "response": "Device is added to the inventory.",
 "message": "Device has been successfully added and configuration parse is triggered.",
 "appStatusCode": null,
 "tags": null,
 "headers": null
}
```


Search Device

Search for device

URL: /adc-device-search

Type: POST

Parameters

ParamType	Name	Description	FieldType
Header	sessionId **	Session Id received after login	string

ParamType	Name	Description	FieldType
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Payload	Input	Key value for the search. Possible keys are : "name","ip","vendor","subsystem","version","dataCenter"	Key:Value

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
200	OK	Matching results found for the given input

Sample Request/Response

Use Case

Get all the ADC F5 devices.

Request URL

http://appviewxapi.com/avxapi/avxapi/adc-device-search?gwkey=f000ca01&gwsource=external

Request Payload

```
{
"payload": {
"input": {
"vendor": "F5"
}
}
}
```

Response

```
{
   "response": {
      "devices": [
```

```
            "name": "192.168.112.93",
            "ip": "192.168.112.93",
            "fqdn": null,
            "deviceType": [
                "LTM",
                "GTM"
            ],
            "module": [
                "LTM",
                "BIG-IP DNS"
            ],
            "dataCenter": "",
            "vendor": "F5",
            "version": "v13",
            "detailedVersion": "13.0.0 build 0.0.1645",
            "subsystem": "LoadBalancer",
            "category": "ADC",
            .....

    ],
    "totalRecords": 2,
    "obtainedRecords": 1,
    "obtainedRecordRange": {
        "start": 1,
        "end": 1
  },
  "message": "Matching results found for the given input.",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```


Delete Device

Delete a device from inventory.

URL: /adc-device

Type: Delete

Parameters

ParamType	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Query Param	adc-device**	Name of the device	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
200	OK	Device(s) deleted successfully
400	Bad request	All the given devices are invalid
400	Bad request	Invalid Device Name. The device name cannot be null or empty

Sample Request/Response

Use Case

Delete the device with name ADC_GTM_1 and device with the name ADC_GTM_2.

Request URL

http://appviewxapi.com/avxapi/adc-device?deviceName=ADC_GTM_1,ADC_GTM_2&gwkey=f000ca01&gwsource=external

Request Payload

NA

Response


```
{
 "response": "Device(s) deleted succesfully.",
 "message": "Device(s) deleted succesfully.",
 "appStatusCode": null,
 "tags": {
 "Deleted Device(s)": [
 "ADC_GTM_1",
    “ADC_GTM_2”
 ],
 "Invalid Device(s)": [
 ]
 }
}
```


Sync Configuration

Sync the device configuration details in AppViewX inventory with the details from the device.

URL: /adc-device-config-sync

Type: POST

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Payload	deviceName	Name of the device	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
404	Not found	Invalid Device Name
400	Bad request	This field should not be null/empty and should match pattern …
403	Forbidden	Config fetch not allowed for Unmanaged/Queued devices and Device(s) on which other operations are already in progress
202	Accepted	Config sync triggered successfully

Sample Request/Response

Use Case

Perform sync configuration for the device ADC_GTM_1

Request URL

http://appviewxapi.com/avxapi/adc-device-config-sync?gwkey=f000ca01&gwsource=external

Request Payload

```
{
  "payload": {
  "deviceName": "ADC_GTM_1"
  }
}
```

Response

```
{
  "response": "Config sync triggered for given device - ADC_GTM_1",
  "message": "Config sync triggered successfully.",
  "tags": null
}
```

Manage Device

Change an ADC device from an unmanaged state to managed state. The device goes through a configuration sync process before getting managed.

URL: /adc-device-manage

Type: PUT

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Payload	deviceName**	Name of the device(s) to manage	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	State change to manage the device has been initiated
403	Forbidden	Selected device(s) are not in the unmanaged state. The operation cannot be performed
400	Bad Request	The device name is mandatory. Value cannot be null or empty
404	Not Found	Device not found

Sample Request/Response

Use Case

Change the state of devices ADC_DEVICE_1 and ADC_DEVICE_2 from unmanaged to managed.

Request URL

http://appviewxapi.com/avxapi/adc-device-manage?gwkey=f000ca01&gwsource=external

Request Payload

```
{
"payload": {
              "deviceName": [
            "ADC_DEVICE_1",
            " ADC_DEVICE_1"
             ]
}
```

Response

```
202 Accepted
{
"response": "State change to manage the device has been initiated.",
"message": "State change to manage the device has been initiated.",
"appStatusCode": null,
"tags": null,
"headers": null
}
```

Un-manage a Device

Change an ADC device from managed state to un-managed state.

URL: /adc-device-unmanage

Type: PUT

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string

Param Type	Name	Description	Field Type
Query	gwsource**	Source from which the request is triggered (for exapmle: web, external)	String
Payload	deviceName**	Name of the device(s) to unmanage	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	State change to unmanage the device has been initiated
403	Forbidden	Selected device(s) are in in-progress/un-managed state. Operation cannot be performed.
400	Bad Request	The device name is mandatory. Value cannot be null or empty
404	Not Found	Device not found

Sample Request/Response

Use Case

Change the state of devices ADC_DEVICE_1 and ADC_DEVICE_2 from managed to unmanaged.

Request URL

http://appviewxapi.com/avxapi/adc-device-unmanage?gwkey=f000ca01&gwsource=external

Request Payload

```
{
"payload": {
            "deviceName": [
          "ADC_DEVICE_1",
          " ADC_DEVICE_1"
           ]
```

```
}
```

Response

```
202 Accepted

{

"response": "State change to unmanage the device has been initiated.",

"message": "State change to unmanage the device has been initiated.",

"appStatusCode": null,

"tags": null,

"headers": null

}
```

Create Application Widget

Create and configure an application widget.

URL: /dashboard-widget-applicationview

Type: POST

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	name**	Name of the widget	String
Payload	action.name	Readable name of the action	String

Param Type	Name	Description	Field Type
Payload	action.type	Type of action. Limited to the actions that are supported in AppviewX	String
Payload	vendor	Device vendor	String
Payload	hierarchy	Hierarchy to display	String
Payload	selectedList.resourceId	Resource id of the object	String
Payload	selectedList.actions	Actions on the object	String[]

** - *Mandatory value*

The input supports up to three hierarchical levels of groups. group, subGroup1, subGroup2, subGroup3 are static keys.

group

subGroup1

subGroup2

subGroup3

Possible Response Message and Code

HTTP Code	Description	Response Message
200	OK	Application widget is created under the given dashboard
400	Bad request	

Sample Request/Response

Use Case

- Create an application widget with a name appwidget and with a group group_1.
- group_1 to have two actions configured – enable and disable.
- group_1 to have two virtual servers – virtualserver_1 and virtualserver_2 configured in it.
- Both the virtual servers to display all the hierarchal children in the group (hierarchy: all)
- Virtualserver_1 and virtualserver_2 to have actions - enable(en) and disable(dis) configured.

- group_1 to have child group group_2 inside it
- group_2 to have two wide IP inside – wideip_1 and wideip_2
- Both the wide IPs to display all the hierarchal children in the group (hierarchy: all)
- wideip_1 and wideip_2 to be configured with actions enable persistence(enPer) and disable persistence(disPer)
- group_2 to be configured with actions enable persistence(enPer) and disable persistence(disPer)

Request URL

http://appviewxapi.com/avxapi//dashboard-widget-applicationview?dashboardName=test&gwkey=f000ca01&gwsource=externalRequest payload

Request


```
{
  "payload": {
    "name": "appwidget",
    "group": [
      {
        "name": "main",
        "action": [
          {
            "name": "en",
            "type": "Enable"
          },
          {
            "name": "dis",
            "type": "Disable"
          }
        ],
        "objects": [
          {
            "vendor": "F5",
            "objectType": "VirtualServer",
            "hierarchy": "All",
            "selectedList": [
              {
                "resourceId": "virtualserver_1",
```

```
          "actions": [
            "en",
            "dis"
          ]
        },
        {
          "resourceId": "virtualserver_2",
          "actions": [
            "en",
            "dis"
          ]
        }
      ]
    }
  ],
  "subGroup1": [
    {
      "name": "grp_sub1",
      "action": [
        {
          "name": "enPer",
          "type": "EnablePersistence"
        },
        {
          "name": "disPer",
          "type": "DisablePersistence"
        }
      ],
      "objects": [
        {
          "vendor": "F5",
          "objectType": "wideIp",
          "hierarchy": "All",
          "selectedList": [
            {
              "resourceId": "wideip_1",
              "actions": [
```

```
                "enPer",
                "disPer"
              ]
             },
             {
              "resourceId": "wideip_2",
              "actions": [
                "enPer",
                "disPer"
              ]
             }
            ]
           }
          ]
         }
        ]
       }
      ]
     }
    ]
}
```

Response

```
{
  "response": "Application widget is created under the given dashboard.",
  "message": "Application widget is created under the given dashboard.",
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```

Get Class Management Widget Details

Get the details for a given class management widget.

URL: /dashboard-widget

Type: GET

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Query	dashboardName **	Name of the dashboard.	String
Query	widgetName**	Name of the class management widget	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
200	OK	Class management widget details retrieved successfully
400	Bad Request	Dashboard name is mandatory
404	Not Found	Dashboard not available for the given name
404	Not Found	Widget not found

Sample Request/Response

Use Case

Get the details of the class management widget with name class_widget under the dashboard dashboard_1.

Request URL

http://appviewxapi.com/avxapi/dashboard-widget?dashboardName=dashboard_1&widgetName=class_widget&gwkey=f000ca01&gwsource=external

Request Payload

NA

Response


```
{
  "response": {
    "name": "Class_test",
    "subsystem": "adc",
    "userDefined": true,
    "applicableFor": null,
    "disabled": false,
    "size": {
      "width": 634,
      "height": 120
    },
    "keywords": [],
    "componentName": "Class_test",
    "description": null,
    "settings": {
      "actionlist": {
        "Grp1": {
          "Internal-class": {
            "action": "ModifyClass",
            "hostProfile": "",
            "actionGroupName": "Grp1",
            "className": "aol/gs-f5-pe16.appviewx.com/F5",
            "classId": "lc:@5d089e6bf923c36659327582:@aol:@Common",
            "deviceId": "gs-f5-pe16.appviewx.com(5d089e6bf923c36659327582)",
            "stringValueAssociationCheck": true,
            "selectedStringValueObject": [
              {
                "keyData": "1.2.2.1:=99",
                "String": "1.2.2.1",
                "Value": "99",
                "type": null,
                "Mask": "255.255.255.255",
                "Type": "Host"
```

```
  },
  .....
  {
    "keyData": "99.99.99.99:=9",
    "String": "99.99.99.99",
    "Value": "9",
    "type": "Address",
    "Mask": null,
    "Type": null
  }
],
"availableStringValueObject": [],
"deviceAssociationCheck": true,
"selectedDeviceObject": [


    "name": "gs-f5-pe16.appviewx.com",
    "id": "5d089e6bf923c36659327582"

],
"availableDeviceObject": [

    "name": "192.168.112.93",
    "id": "5d0782c7b84fd170beec8132"
  },

    "name": "bigip39.payoda.com",
    "id": "5d075eff289791373cc03c4f"
  },

    "name": "192.168.40.152 - Device- Cyberark**",
    "id": "5d075de4b84fd170beec811a"
  },

    "name": "192.168.112.78",
    "id": "5d07830db84fd170beec8134"
```

```
        ],
        "defaultExecuted": true,
        "msg": "",
        "isRuntimeCheck": true
      },
      "view-int": {
        "action": "ViewClass",
        "hostProfile": "",
        "actionGroupName": "Grp1",
        "className": "private_net/192.168.40.152 - Device- Cyberark**/F5",
        "classId": "lc:@5d075de4b84fd170beec811a:@private_net:@Common",
        "deviceId": "192.168.40.152%20-%20Device-%20Cyberark**(5d075de4b84fd170beec811a)",
        .....
      },
      "view-int1": {
        "action": "ViewClass",
        "hostProfile": "",
        "actionGroupName": "Grp1",
        "className": "images/bigip39.payoda.com/F5",
        "classId": "lc:@5d075eff289791373cc03c4f:@images:@Common",
        "deviceId": "bigip39.payoda.com(5d075eff289791373cc03c4f)",
        .....
  },
  "settings": [


    "name": "Class_test",
      "parent": "",
      "hierarchy": "",
      "level": "group",
      "nodeLevel": 0,
      "actions": [],
      "children": [],
      "actionStatus": null,
      "className": null,
      "id": "Class_test"
    },
```

```
        "name": "Grp1",
        "parent": "Class_test",
        "hierarchy": "",
        "level": "group",
        "nodeLevel": 1,
        "actions": [
          "view-int",
          "view-int1",
          "Internal-class"
        ],
        "children": [],
        "actionStatus": null,
        "classActionName": null,
        "id": "Grp1"
      }
  },
  "classLog": null,
  "viaImport": false,
  "StdCustomFlag": "ClassManagement",
  "_id": "5d08967ff923c36659323e29"
 },
 "message": “Class management widget details retrieved successfully”,
 "appStatusCode": null,
 "tags": null,
 "headers": null
}
```


Delete a Widget

Delete a dashboard widget.

URL: /dashboard-widget

Type: POST

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Query	dashboardName**	Name of the dashboard.	String
Query	widgetName**	Name of the widget	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
200	OK	Widget deleted successfully
400	Bad Request	Dashboard name/widget name is mandatory
404	Not Found	Dashboard not available for the given name
403	Forbidden	Permission not available for dashboard
404	Not Found	Widget not found

Sample Request/Response

Use Case

Delete a widget named widget_1 from the dashboard dashboard_1.

Request URL

http://appviewxapi.com/avxapi/dashboard-widget?dashboardName=dashboard_1&widgetName=widget_1&gwkey=f000ca01&gwsource=external

Request Payload

NA

Response


```
{
"response": "Widget deleted successfully.",
"message": "Widget deleted successfully.",
"appStatusCode": null,
"tags": null,
"headers": null
}
```


Action - Enable an Object

Enable one or more ADC objects for which the action applies to.

Supported on the following object types:

- **F5 –** wideip, wideip pool, wideip pool member, vip, vip pool member, LTM node, GTM server, virtual address
- **A10 –** Fqdn, ServiceIP, SLB_VSV, SLB Server, SLB VS
- **Cisco –** GSLB Answer, SLB virtual server, SLB real server
- **Citrix –** GSLB virtual server, GSLB services, SLB virtual servers, SLB service group, SLB service
- **Akamai –** Datacenter
- **Radware –** Virtual server, Server group, Real server: port, Real server

URL: /adc-device-object-action-enable

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Trigger enables action on objects with resource id wideip_1 and wideip_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-enable?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "objectIds": [
 "wideip_1",
 " wideip_2"
 ]
```

```
 }
}
```

Response

```
{
 "response": "Action triggered successfully.",
 "message": "Action triggered for the following 2 objects : wideip_1,wideip_2"
}
```

Action - Disable an Object

Disable one or more ADC objects for which the action applies to.

Supported on the following object types:

- **F5 –** wideip, wideip pool, wideip pool member, vip, vip pool member, LTM node, GTM server, virtual address
- **A10 –** Fqdn, ServiceIP, SLB_VSV, SLB Server, SLB VS
- **Cisco –** GSLB Answer, SLB virtual server, SLB real server
- **Citrix –** GSLB virtual server, GSLB services, SLB virtual servers, SLB service group, SLB service
- **Akamai –** Datacenter
- **Radware –** Virtual server, Server group, Real server: port, Real server

URL: /adc-device-object-action-disable

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string

Param Type	Name	Description	Field Type
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Trigger disable action on objects with resource id wideip_1 and wideip_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-disable?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "objectIds": [
 "obj_1",
 " obj_2"
 ]
 }
}
```

Response

```
{
 "response": "Action triggered successfully.",
 "message": "Action triggered for the following 2 objects : obj_1,obj_2"
}
```

Action - Forcedown Object

Force down one or more ADC objects for which the action applies to.

Supported on the following object types:

- **F5 –** Vip pool member

URL

/adc-device-object-action-forcedown

Type

PUT

Parameter

Param Type	Name	Description	Field type
Header	sessionId **	Session Id received after login	string
Query	gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Trigger forcedown action on objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-forcedown?gwkey=f000ca01&gwsource=external

Request Payload

```
{
  "payload": {
  "objectIds": [
  "obj_1",
  " obj_2"
  ]
  }
}
```

Response

```
{
  "response": "Action triggered successfully.",
  "message": "Action triggered for the following 2 objects : obj_1,obj_2"
}
```

Action - Forcedown Active Object

Force down active one or more ADC objects for which the action applies to. Applicable only for F5 LTM pool member objects.

Supported on the following object types:

• **AVI** – Server

URL: /adc-device-object-action-gracefuldisable

Type: PUT

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Trigger graceful disable action on objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-forcedown?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "objectIds": [
 "obj_1",
 " obj_2"
 ]
 }
}
```

Response

```
{
 "response": "Action triggered successfully.",
 "message": "Action triggered for the following 2 objects : obj_1,obj_2"
}
```

Action - Graceful Disable Object

Force down active one or more ADC objects for which the action applies to. Applicable only for F5 LTM pool member objects.

Supported on the following object types:

- **AVI** – Server

URL: /adc-device-object-action-gracefuldisable

Type: PUT

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Trigger graceful disable action on objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-forcedown?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "objectIds": [
 "obj_1",
 " obj_2"
 ]
```

```
 }
}
```

Response

```
{
 "response": "Action triggered successfully.",
 "message": "Action triggered for the following 2 objects : obj_1,obj_2"
}
```

Action - Enable Persistence for Object

Enable persistence on one or more ADC objects for which the action applies to.

Supported on the following object types:

- **F5 –** Wideip

URL: /adc-device-object-action-enablepersistence

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Trigger enable persistence action on objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-enablepersistence?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "objectIds": [
 "obj_1",
 " obj_2"
 ]
 }
}
```

Response

```
{
 "response": "Action triggered successfully.",
 "message": "Action triggered for the following 2 objects : obj_1,obj_2"
}
```

Action - Disable Persistence for Object

Disable persistence on one or more ADC objects for which the action applies to.

Supported on the following object types:

• **F5 –** Wideip

URL: /adc-device-object-action-disablepersistence

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Trigger disable persistence action on objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-enablepersistence?gwkey=f000ca01&gwsource=external

Request Payload

```
{
  "payload": {
  "objectIds": [
  "obj_1",
  " obj_2"
  ]
  }
}
```

Response

```
{
  "response": "Action triggered successfully.",
  "message": "Action triggered for the following 2 objects : obj_1,obj_2"
}
```

Action Clear Persistence Record

Clear persistence on one or more ADC objects for which the action applies to.

Supported on the following object types:

- **F5 –** Virtual Server, Virtual Server pool

URL: /adc-device-object-action-clearpersistencerecords

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Trigger clear persistence action on objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action- clearpersistencerecords?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "objectIds": [
 "obj_1",
 " obj_2"
```

```
 ]
 }
}
```

Response

```
{
 "response": "Action triggered successfully.",
 "message": "Action triggered for the following 2 objects : obj_1,obj_2"
}
```

Action – InService (Activate) Object

InService(activate) action on one or more ADC objects for which the action applies to.

Supported on the following object types:

- **Cisco –** GSLB Answer, SLB virtual server, SLB real server

URL: /adc-device-object-action-activate

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Trigger activates action on objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-activate?gwkey=f000ca01&gwsource=external

Request Payload

```
{
  "payload": {
  "objectIds": [
  "obj_1",
  " obj_2"
  ]
  }
}
```

Response

```
{
  "response": "Action triggered successfully.",
  "message": "Action triggered for the following 2 objects : obj_1,obj_2"
}
```

Action - OutOfService (Suspend) Object

OutOfService(suspend) action on one or more ADC objects for which the action applies to. .

Supported on the following object types:

• **Cisco –** GSLB Answer, SLB virtual server, SLB real server

URL: /adc-device-object-action-suspend

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Trigger suspend action on objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/ adc-device-object-action-suspend?gwkey=f000ca01&gwsource=external

Request Payload

```
{
  "payload": {
  "objectIds": [
  "obj_1",
  " obj_2"
  ]
  }
}
```

Response

```
{
  "response": "Action triggered successfully.",
  "message": "Action triggered for the following 2 objects : obj_1,obj_2"
}
```

Action - Set Highest Priority

Set highest priority action on one or more ADC objects for which the action applies to.

Supported on the following object types:

- **F5 –** GTM wideip pool

URL: /adc-device-object-action-priority

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string

Param Type	Name	Description	Field Type
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Set the highest priority action on objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/ adc-device-object-action-priority?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "objectIds": [
 "obj_1",
 " obj_2"
 ]
 }
}
```

Response

```
{
 "response": "Action triggered successfully.",
 "message": "Action triggered for the following 2 objects : obj_1,obj_2"
}
```

Action - Set Connection Limit

Set connection limit action on one or more ADC objects for which the action applies to.

Supported on the following object types:

- **F5 –** LTM servers

URL: /adc-device-object-action-connectionlimit

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	String
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	String
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/ get the resource id	String[]
Payload	connectionLimit	Connection limit to set	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Set a connection limit of 4 on objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-connectionlimit?gwkey=f000ca01&gwsource=external

Request Payload

```
{
  "payload": {
  "objects": [
  {
  "_id": “obj_1",
  "parent_id": "parent_1"
  },
  {
  "_id" : "obj_2",
  "parent_id":"parent_2"
  }
  ],
  "ratio": "9"
  }
}
```

Response

```
{
  "response": "Action triggered successfully.",
  "message": "Action triggered for the following 2 objects : obj_1,obj_2"
```

```
}
```

Action - Set Loadbalancing Method

Set the load balancing method on one or more ADC objects for which the action applies to.

Supported on the following object types:

- **F5 –** LTM pools
- **Citrix** – GSLB Virtual Server, SLB Virtual Server

A10 - SLB Service Group

URL: /adc-device-object-action-lbmethod

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]
Payload	lbmode	Load balancing mode to set.	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

• Sample Request/Response

Sample Request/Response

Use Case

Set load balancing method of the round-robin on objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-lbmethod?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "objects": [
 {
"_id": “obj_1",
 "parent_id": "parent_1"
 },
 {
 "_id" : ”obj_2",
 "parent_id":”parent_2"
 }
 ],
 "lbMode": "round-robin"
 }
}
```

Response

```
{ "response": "Action triggered successfully.", "message": "Action triggered for the following 2 objects : obj_1,obj_2" }
```

Action - Set Ratio

Set connection limit action on one or more ADC objects for which the action applies to.

Supported on the following object types:

- **F5** – GTM pool, GTM pool member, LTM pool member
- **AVI** - GSLB Pool Member, Server
- **Akamai** - Datacenter

URL: /adc-device-object-action-ratio

Type: PUT

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	String
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	String
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]
Payload	ratio	Ratio to set	Integer

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action

HTTP Code	Description	Response Message
403	Forbidden	No given object(s) have Read or Write permission

- Sample Request/Response

Sample Request/Response

Use Case

Set the weight of objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-weight?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "objectIds": [
 “obj_1", "obj_2"
 ],
 "weight": "3"
 }
}
```

Response

```
{ "response": "Action triggered successfully.", "message": "Action triggered for the following 2 objects : obj_1,obj_2" }
```

Action - Set Service Down Value

Set service down the value on one or more ADC objects for which the action applies to.

Supported on the following object types:

- **F5** – LTM pool

URL: /adc-device-object-action-servicedown

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]
Payload	serviceDown	Service down value to set	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform an action
403	Forbidden	No given object(s) have Read or Write permission

• Sample Request/Response

Sample Request/Response

Use Case

Set service down value ‘drop’ on objects with resource id obj_1 with parent object parent_1 and obj_2 with parent object parent_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-servicedown?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "objects": [
 {
 "_id": "obj_1",
 "parent_id": "parent_1"
 },
 {
 "_id": "obj_2",
 "parent_id": "parent_2"
 }
 ],
 "serviceDown": "drop"
 }
}
```

Response

```
{ "response": "Action triggered successfully.", "message": "Action triggered for the following 2 objects : obj_1,obj_2" }
```

Action - ARP Enable/Disable

ARP enable/disable on one or more ADC objects for which the action applies to. .

Supported on the following object types:

- **F5** – Virtual address
- **A10** – Virtual server

URL: /adc-device-object-action-arp

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]
Payload	arp	Action. Possible values are 'ENABLED, DISABLED'	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered for the following <#> objects …
400	Bad request	No objects found to perform the action
403	Forbidden	No given object(s) have Read or Write permission

• Sample Request/Response

Sample Request/Response

Use Case

ARP enable/disable on objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-arp?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
```

```
"objectIds": [
"obj_1", "obj_2"
],
"arp": "DISABLED"
}
}
```

Response

```
{ "response": "Action triggered successfully.", "message": "Action triggered for the following 2 objects : obj_1,obj_2" }
```

Action - Set Weight

Set weight on one or more ADC objects for which the action applies to.

Supported on the following object types:

- **Citrix** – SLB service group member, SLB service, Service
- **A10** – Service group member, Server

URL: /adc-device-object-action-weight

Type:PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	String
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	String
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]
Payload	weight	Weight to set	Integer

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	The action triggered the following <#> objects …
400	Bad request	No objects found to perform an action
403	Forbidden	No given object(s) have Read or Write permission

• Sample Request/Response

Sample Request/Response

Use Case

Set the weight of objects with resource id obj_1 and obj_2.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-weight?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "objectIds": [
 “obj_1", "obj_2"
 ],
 "weight": "3"
 }
}
```

Response

```
{ "response": "Action triggered successfully.", "message": "Action triggered for the following 2 objects : obj_1,obj_2" }
```

Action - Set CNAME

Set CNAME on one or more ADC objects for which the action applies to.

Supported on the following object types:

• Akamai - Property

URL: /adc-device-object-action-cname

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	String
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	String
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	objectIds**	Resource id of the objects. Note: Use the search API to search/get the resource id	String[]
Payload	cname	CNAME to set	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	Action triggered for the following <#> objects …
400	Bad request	No objects found to perform an action
403	Forbidden	No given object(s) have Read or Write permission

Sample Request/Response

Use Case

Set CNAME of www.example.com on objects with resource id obj_1.

Request URL

http://appviewxapi.com/avxapi/adc-device-object-action-cname?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "payload": {
 "objectIds": [obj_1],
 "cname": "www.example.com"
 }
}
```

Response

```
{ "response": "Action triggered successfully.", "message": "Action triggered for the following 1 objects : obj_1" }
```

Chapter 5: Login

Authenticate into the AppViewX application. If success will return a session id which can be used as an authentication token to access the other APIs.

URL: /login

Type: POST

Parameter

Param Type	Name	Description	Field Type
Header	username**	Login username	string
Header	Password**	Password for the username	String
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	String
Query	gwsource**	Source from which the request is triggered (Eg: web, external)	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Username or password cannot be null or empty
200	OK	Login successful
401	Unauthorized	Login failed. Invalid Credentials

Sample Request/Response

Use case

Log in to the application with a username and password.

Request URL

http://appviewxapi.com/avxapi/login?gwkey=f000ca01&gwsource=test

Request payload

```
{}
```

Response


```
{
  "response": {
  "status": "SUCCESS",
  "appStatusCode": null,
  "statusDescription": null,
  "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813",
  "availableLoginAttemptCount": null
  },
  "message": null,
  "appStatusCode": null,
  "tags": null,
  "headers": null
}
```

Chapter 6: X509_Certificate

Create a Certificate

Create a new certificate. The API will submit a request to create a certificate. In case the work order has manual approvals or other manual intervention needed, those have to be done with respective APIs.

URL: /certificate/create

Type: POST

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session ID received after login	String
Query	Gwkey	Tenant Key. It is needed only in case of multi-tenant installations	String
Query	gwsource**	Source from which the request is triggered (for example, web and external)	String
Payload	csrGenerationSource	How a CSR is generated. Possible values: appviewx, HSM, ENDPOINT, and uploadCSR	String
Payload	certificateGroup	Group to which the certificate has to belong to.	JSON

Param Type	Name	Description	Field Type
Payload	caConnectorInfo	Info about the CA connector	JSON

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	The group name is not available
202	Accepted	Certificate submission triggered successfully.
409	Conflict	CSR parameters already available for the selected CA

• Sample Request/Response

Sample Request/Response

Use Case

Create an AppViewX CA certificate with common name *gyttest.appviewx.com*.

Request URL

http://appviewxapi.com/ avxapi/certificate/create?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "csrGenerationSource": "appviewx",
 "certificateGroup": {
 "name": "Default"
 },
 "caConnectorInfo": {
 "certificateAuthority": "AppViewX",
 "caSettingName": "AppViewX CA",
 "certificateType": "",
```

```
"csrParameters": {
"commonName": "gyttest.appviewx.com",
"encryptedChallengePassword": "",
"hashFunction": "SHA160",
"keyType": "RSA",
"bitLength": "4096",
"certificateCategories": [
"Server",
"Client"
],
"enhancedSANTypes": {
"dNSNames": [
"gyt.appviewx.com"
]
}
},
"validityInDays": 365,
"vendorSpecificDetails": {}
}
}
```


Response


```
{
"response": {
"resourceId": "5c4ae31272a0d0030e375be5",
"requestId": "4132"
},
"message": "CA connector added and certificate submitted successfully.",
"appStatusCode": null,
"headers": null
}
```


Download Certificate

Download a certificate. Supported only for **.pem** certificate type.

URL: /certificate/download

Type: GET

Parameters

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Param	resourceId**	Unique resource ID / UUID of the certificate	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
200	OK	NA
404	Not Found	No matching record found
400	Bad request	Mandatory field is missing or invalid – <>

• Sample Request/Response

Sample Request/Response

Use Case

Download a certificate with resource id 5c487011db4496588e04930e. Use the search API to search and get the resource id of a certificate.

Request URL

http:// appviewxapi.com/ avxapi/certificate/download?
gwkey=f000ca01&gwsource=external&resourceId=5c487011db4496588e04930e

Request Payload

NA

Response

NA

Renew Certificate

Renew a given certificate.

URL: /certificate/action

Type: PUT

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	action**	Possible value: “Renew”	String
Payload	resourceId	Unique resource ID / UUID of the certificate	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	Renew action triggered successfully.
400	Bad request	Please provide a valid action

HTTP Code	Description	Response Message
404	Not found	No matching records found

- Sample Request/Response

Sample Request/Response

Use Case

Renew a certificate with resource Id 5c4ae31272a0d0030e375be5. Use the search API to search and get the resource id of a certificate.

Request URL

http:// appviewxapi.com/avxapi/certificate/action?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "action":"Renew",
 "resourceId":"5c4ae31272a0d0030e375be5"
}
```

Response

```
{
"response": {
 "resourceId": "5c4ae31272a0d0030e375be5",
 "message": "Renew action performed successfully.",
 "requestId": "4132"
 },
 "message": "Renew has been done successfully"
....
}
```

Search/Get Certificate Inventory

Search for one or more certificates against the given searchable input. The complete detail of the matching certificate is returned.

URL: /certificate/search

Type: POST

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String
Payload	Input	Search key and value for searching a certificate. Does accept multiple entries. **Possible keys** • **commonName** – Common name • **serialNumber** – Serial number • **resourceId** – Resource Id / UUID of the certificate • **issuer.certificateAuthority** – Certificate Authority • **category** – Certificate category (Possible values: Client, Server, Code Signing, Device, Others). Defaults to Server • **startDate –** Mention the start date and end date to get the certificates expiring within the range. • **endDate -** Mention the start date and end date to get the certificates expiring within the range.	String
Payload	filter.start	Start index from which the response has to be available (Eg: If the response has to skip the first 100 and show the next 50, then start index has to be 101)	Integer
Payload	filter.max	The number of entries from the start index to be made available. (Eg: If the response has to have skipped the first 100 and show the next 50, then start index has to be 101 and max has to be 50)	Integer
Payload	sortColumn	Sort by column	

Param Type	Name	Description	Field Type
Payload	sortOrder	Ascending or descending order of sort (Possible values: asc, desc	

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
200	OK	Matching results found for the given input
404	Not found	No matching records found for the given input

• Sample Request/Response

Sample Request/Response

Use Case

Search for the details of the certificate with the common name ‘appviewx.com’ and serial number ‘5F:59:A7:83:B2:86:69:DF’.

Request URL

http://appviewxapi.com/avxapi/certificate/search?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 “input”: {
 “ commonName:”appviewx.com”,
“serialNumber”:”5F:59:A7:83:B2:86:69:DF”
 },
 "filter": {
 "start": 10,
 "max": 100,
 "sortColumn": "commonName",
 "sortOrder": "asc"
```

```
}
}
```

Response

```
{
 "response": {
 "httpStatusCode": 200,
 "response": {
 "objects": [
 {
 "commonName": "aruna.appviewx.com",
 "serialNumber": "C2:AA:C2:BC:01:8E:5B:48",
 "issuerCommonName": "AppViewX Intermediate CA",
 "status": "Managed",
 "associatedObjects": [],
 "discoverySources": [
 "192.168.112.88:8443"
 ],
 .....
 "missingParamsForAutoRenew": "CSR parameters are available for certificate renewal",
 "suspendedCertificate": false,
 "mailAddress": "aruna.sn@appviewx.com",
 "privatekeyAvaliable": false,
 "resourceId": "5c90dbfe72a6365d8baa83c7"
 }
 ],
 "totalRecords": 1,
 "obtainedRecords": 1,
 "obtainedRecordRange": {
 "start": 1,
 "end": 1
 }
 },
 "message": "Matching results found for the given input.",
 "appStatusCode": null,
 "tags": null
 },
```

```
"message": null,
"appStatusCode": null,
"tags": {},
"headers": null
}
```


Push Certificate

Push a certificate to an end device. A request is generated for pushing the certificate against the mentioned profile. We need to mention the details of the application connector which acts as an interface with the end device.

URL: /certificate/pushToDevice

Type: POST

Parameter

Param Type	Name	Description	Field Type
Header	sessionId **	Session Id received after login	string
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	string
Query	gwsource**	Source from which the request is triggered (for example,web, external)	String
Payload	certificateDetails. certificateType	Type of certificate. Possible values	

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
202	Accepted	<> connector(s) saved and push operation has been triggered

HTTP Code	Description	Response Message
400	Bad request	Invalid value - <>
404	Not found	No matching records found

• Sample Request/Response

Sample Request/Response

Use Case

Push certificate with resourceid/UUID 5c3583a018593f0c9f5c3ca9 to the profiles profile_1 and profile_2.

Request URL

http:// appviewxapi.com/avxapi/certificate/pushToDevice?gwkey=f000ca01&gwsource=external

Request Payload

```
{
 "generalInformation": {
 "name": "sample f5 connector"
 },
 "certificateDetails": {
 "certificateType": "PEM-.crt",
 "certificateFileName": "sample.crt",
 "privateKeyFileName": "sample.key",
 "pushRootAndIntermediateCertificates": "false",
 "intermediateCertificateFileName": []
 },
 "certificateId": "5c3583a018593f0c9f5c3ca9",
 "selectedProfiles": [
 "profile_1",
 "profile_2"
 ]
}
```

Response

```
"response": [
 {
 "connectorId": "connector_1",
 "requestId": "33"
 },
 {
 "connectorId": "41.150:@wom-default-serverssl:@Common:@d1a1682be60768a97dab9be03612cce797566c7a",
 "requestId": "34"
 }
 ],
 "message": "2 connector(s) saved and push opertaion has been triggered."
 ……
}
```


Login

Authenticate into the AppViewX application. If success will return a session id which can be used as an authentication token to access the other APIs.

URL: /login

Type: POST

Parameters

Param Type	Name	Description	Field Type
Header	username**	Login username	String
Header	Password**	Password for the username	String
Header	Content-Type**	Specifies the nature of the data in the payload (The value of the param should be "application/json")	String
Query	Gwkey	Tenant Key. Needed only in case of multitenant installations	String
Query	gwsource**	Source from which the request is triggered (for example, web, external)	String

** - *Mandatory value*

Possible Response Message and Code

HTTP Code	Description	Response Message
400	Bad request	Username or password cannot be null or empty
200	OK	Login successful
401	Unauthorized	Login failed. Invalid Credentials

- Sample Request/Response

Sample Request/Response

Use Case

Log in to the application with a username and password.

Request URL

http://appviewxapi.com/avxapi/login?gwkey=f000ca01&gwsource=test

Request Payload

```
{}
```

Response

```
{
 "response": {
 "status": "SUCCESS",
 "appStatusCode": null,
 "statusDescription": null,
 "sessionId": "ce7f1a14-2bf9-4e4a-89a8-bc780a255813",
 "availableLoginAttemptCount": null
 },
 "message": null,
 "appStatusCode": null,
 "tags": null,
```

```
  "headers": null

}
```

Chapter 7: References

- Possible Access Control Functions (ACF) Permissions

Possible Access Control Functions (ACF) Permissions

The Possible Access Control Functions (ACF) permission entries possible and valid with AppViewX.

- Application Delivery - Backup
- Application Delivery - Control Center
- Application Delivery - Dashboard/Widget
- Application Delivery - Device/Device Inventory
- Application Delivery - Orphan Objects
- Appvision
- Design
- Domain Name System (DNS)
- Firewall
- General
- Mobile Device Management (MDM)
- Proxy
- Router
- Server
- SSH
- Switch
- Web Application Firewall (WAF)
- Workflow
- X.509 Certificate

Application Delivery - Backup

"adc:backup_restore:backupNow",

"adc:backup_restore:backupSettings",

"adc:backup_restore:create_modify",

"adc:backup_restore:delete",

"adc:backup_restore:deviceCompare",

"adc:backup_restore:deviceRestore",

"adc:backup_restore:download",

"adc:backup_restore:objectCompare",

"adc:backup_restore:objectRestore",

"adc:backup_restore:environmentCompare:*",

"adc:backup_restore:environmentCompare:view_compare",

"adc:backup_restore:environmentCompare:import_export",

"adc:backup_restore:environmentCompare:delete",

Application Delivery - Control Center

"adc:controlCenter:actions:CNAME",

"adc:controlCenter:actions:RATIO",

"adc:controlCenter:actions:SERVICEDOWN",

"adc:controlCenter:actions:arp",

"adc:controlCenter:actions:clearPersistenceConnections",

"adc:controlCenter:actions:delete",

"adc:controlCenter:actions:enable/disable/forcedown",

"adc:controlCenter:actions:enable_disable_persistence",

"adc:controlCenter:actions:export",

"adc:controlCenter:actions:forcedownActive",

"adc:controlCenter:actions:lbmode",

"adc:controlCenter:actions:viewPersistenceConnections",

"adc:controlCenter:actions:viewSourceConnections",

"adc:controlCenter:applicationView",

"adc:controlCenter:infrastructureView",

Application Delivery - Dashboard/Widget

"adc:dashboard:applicationWidget:add_delete",

"adc:dashboard:applicationWidget:executeActions",

"adc:dashboard:applicationWidget:modifySettings",

"adc:dashboard:classManagementWidget:*",

"adc:dashboard:classManagementWidget:add_delete",

"adc:dashboard:classManagementWidget:executeActions",

"adc:dashboard:classManagementWidget:modifySettings",

"adc:dashboard:defaultdashboard_widget:*",

"adc:dashboard:defaultdashboard_widget:view",

"adc:dashboard:deviceheatmap:add_delete",

"adc:dashboard:deviceheatmap:modifysettings",

"adc:dashboard:scriptExecutionWidget:add_delete",

"adc:dashboard:scriptExecutionWidget:executeScripts",

"adc:dashboard:scriptExecutionWidget:modifySettings",

"adc:dashboard:trafficGridWidget:add_delete",

"adc:dashboard:trafficGridWidget:modifySettings",

"adc:dashboard:trafficGridWidget:monitorTrafficPercentage",

"adc:dashboard:trafficStatisticsWidget:*",

"adc:dashboard:trafficStatisticsWidget:add_delete",

"adc:dashboard:trafficStatisticsWidget:modifySettings",

Application Delivery - Device/Device Inventory

"adc:deviceGroup:add_modify",

"adc:deviceGroup:delete",

"adc:deviceGroup:view",

"adc:inventory:add_modify",

"adc:inventory:credentialLibrary",

"adc:inventory:delete",

"adc:inventory:export",

"adc:inventory:fetchConfig",

"adc:inventory:generateiHealthReport",

"adc:inventory:import",

"adc:inventory:manage_unmanage",

"adc:inventory:view",

Application Delivery - Orphan Objects

"adc:orphanObjects:delete",

"adc:orphanObjects:view"

Appvision

"appvision:apps:create",

"appvision:apps:delete",

"appvision:apps:view",

"appvision:configurator:*",

"appvision:configurator:create",

"appvision:configurator:delete",

"appvision:configurator:modify",

"appvision:configurator:view"

Design

"design:report:view",

"design:report:viewall",

"design:report:create_modify",

"design:report:clone",

"design:report:delete",

"design:rules:view",

"design:rules:create_modify",

"design:rules:clone",

"design:rules:delete"

Domain Name System (DNS)

"dns:inventory:add_modify",

"dns:inventory:credentialLibrary",

"dns:inventory:delete",

"dns:inventory:export",

"dns:inventory:manage_unmanage",

"dns:inventory:view"

Firewall

"firewall:controlCenter:securityRules:create",

"firewall:controlCenter:securityRules:modify",

"firewall:controlCenter:securityRules:delete",

"firewall:controlCenter:natRules:create",

"firewall:controlCenter:natRules:modify",

"firewall:controlCenter:natRules:delete",

"firewall:controlCenter:natRules:view",

"firewall:controlCenter:routeRules:create",

"firewall:controlCenter:routeRules:delete",

"firewall:controlCenter:routeRules:modify",

"firewall:controlCenter:routeRules:view",

"firewall:controlCenter:securityRules:risksettings",

"firewall:controlCenter:securityRules:traceroute",

"firewall:controlCenter:securityRules:view",

"firewall:dashboard:defaultdashboard_widget:*",

"firewall:dashboard:defaultdashboard_widget:view",

"firewall:inventory:add_modify",

"firewall:inventory:credentialLibrary",

"firewall:inventory:delete",

"firewall:inventory:export",

"firewall:inventory:fetchConfig",

"firewall:inventory:import",

"firewall:inventory:manage_unmanage",

"firewall:inventory:view",

"firewall:backup_restore:backupNow",

"firewall:backup_restore:backupSettings",

"firewall:backup_restore:compare",

"firewall:backup_restore:deviceRestore",

"firewall:backup_restore:create_modify",

"firewall:backup_restore:delete",

"firewall:backup_restore:download"

General

"general:accounts:roles:add_modify",

"general:accounts:roles:delete",

"general:accounts:roles:enable_disable",

"general:accounts:roles:view",

"general:accounts:users:add_modify",

"general:accounts:users:delete",

"general:accounts:users:enable_disable",

"general:accounts:users:import",

"general:accounts:users:view",

"general:accounts:usrGrp:add_modify",

"general:accounts:usrGrp:delete",

"general:accounts:usrGrp:enable_disable",

"general:accounts:usrGrp:clone",

"general:accounts:usrGrp:view",

"general:alert:adc",

"general:alert:appviewx",

"general:alert:cert",

"general:alert:syslog",

"general:alert:clear",

"general:alert:secureSH",

"general:alert:settings",

"general:cloud:inventory:add_modify",

"general:cloud:inventory:delete",

"general:cloud:inventory:view",

"general:collection:create_modify",

"general:collection:export",

"general:collection:import",

"general:collection:view",

"general:dashboard:create_delete",

"general:dashboard:import",

"general:dashboard:share",

"general:dashboard:defaultdashboard:*",

"general:dashboard:defaultdashboard:view",

"general:logging:appviewx",

"general:logging:audit",

"general:logging:cert",

"general:logging:adc",

"general:logging:secureSH",

"general:logging:selfAudit",

"general:logging:settings",

"general:logging:syslog",

"general:others:inventory:add_modify",

"general:others:inventory:delete",

"general:others:inventory:view",

"general:provisioning:request:cloneRequest",

"general:provisioning:request:cloneWorkorder",

"general:provisioning:request:createRequest",

"general:provisioning:request:deleteRequest",

"general:provisioning:request:pre-validation",

"general:provisioning:request:rollbackWorkorder",

"general:provisioning:request:viewAllRequests",

"general:provisioning:request:viewRequest",

"general:provisioning:request:viewWorkOrder",

"general:provisioning:template:create_modify",

"general:provisioning:template:create_viewHelperScript",

"general:provisioning:template:delete",

"general:provisioning:template:enable_disable",

"general:provisioning:template:exportTemplate_helperScript",

"general:provisioning:template:importTemplate_helperScript",

"general:provisioning:template:view",

"general:commandProfile:add_modify",

"general:commandProfile:delete",

"general:commandProfile:view",

"general:hsm:inventory:add_modify",

"general:hsm:inventory:delete",

"general:hsm:inventory:view",

"general:accounts:roles:clone",

"general:accounts:resource:add_modify",

"general:accounts:resource:clone",

"general:accounts:resource:delete",

"general:accounts:resource:enable_disable",

"general:accounts:resource:view"

Mobile Device Management (MDM)

"mdm:inventory:view",

"mdm:inventory:delete",

"mdm:inventory:add_modify",

"mdm:inventory:manage_unmanage",

"mdm:inventory:import",

"mdm:inventory:export",

"mdm:inventory:fetchConfig"

Proxy

"proxy:backup_restore:backupNow",

"proxy:backup_restore:backupSettings",

"proxy:backup_restore:compare",

"proxy:backup_restore:create_modify",

"proxy:backup_restore:delete",

"proxy:backup_restore:deviceRestore",

"proxy:backup_restore:download",

"proxy:controlCenter",

"proxy:inventory:add_modify",

"proxy:inventory:credentialLibrary",

"proxy:inventory:delete",

"proxy:inventory:export",

"proxy:inventory:import",

"proxy:inventory:manage_unmanage",

"proxy:inventory:view"

Router

"router:inventory:add_modify",

"router:inventory:credentialLibrary",

"router:inventory:delete",

"router:inventory:export",

"router:inventory:import",

"router:inventory:manage_unmanage",

"router:inventory:view"

Server

"server:inventory:add_modify",

"server:inventory:credentialLibrary",

"server:inventory:delete",

"server:inventory:export",

"server:inventory:import",

"server:inventory:manage_unmanage",

"server:inventory:view"

SSH

"ssh:controlCenter",

"ssh:dashboard:defaultdashboard_widget:*",

"ssh:dashboard:defaultdashboard_widget:view",

"ssh:hostInventory:createModify",

"ssh:hostInventory:delete",

"ssh:hostInventory:export",

"ssh:hostInventory:manageUnmanage",

"ssh:hostInventory:view",

"ssh:hostLevelAction:associateHost",

"ssh:hostLevelAction:delete:otherOwnedKeys",

"ssh:hostLevelAction:delete:userOwnedKeys",

"ssh:hostLevelAction:keyPushToDevice:toAllUser",

"ssh:hostLevelAction:keyPushToDevice:toLoggedInUser",

"ssh:hostLevelAction:modifyConnector",

"ssh:hostLevelAction:rollback",

"ssh:hostLevelAction:sessionTermination",

"ssh:hostgroup:assignUnassign",

"ssh:hostgroup:createModify",

"ssh:hostgroup:delete",

"ssh:keyInventory:create",

"ssh:keyInventory:discovery",

"ssh:keyInventory:midnightkeySyncResult",

"ssh:keyInventory:modify",

"ssh:keyInventory:upload",

"ssh:keyInventory:viewAllKeys",

"ssh:keyInventory:viewUserOwnedKeys",

"ssh:keyLevelAction:changeStatus",

"ssh:keyLevelAction:delete",

"ssh:keyLevelAction:downloadPrivateKey",

"ssh:keyLevelAction:downloadPublicKey",

"ssh:keyLevelAction:export",

"ssh:keyLevelAction:renew",

"ssh:keyLevelAction:rollback",

"ssh:keyLevelAction:rotate",

"ssh:keygroup:assignUnassign",

"ssh:keygroup:createModify",

"ssh:keygroup:delete",

"ssh:policy:createModify",

"ssh:policy:delete",

"ssh:policy:editDefaultPolicy",

"ssh:policy:view"

Switch

"switch:inventory:add_modify",

"switch:inventory:credentialLibrary",

"switch:inventory:delete",

"switch:inventory:export",

"switch:inventory:import",

"switch:inventory:manage_unmanage",

"switch:inventory:view"

Web Application Firewall (WAF)

"waf:controlCenter:view",

"waf:controlCenter:risksettings",

"waf:controlCenter:policies:create",

"waf:controlCenter:policies:modify",

"waf:controlCenter:policies:delete",

"waf:controlCenter:policies:download",

"waf:controlCenter:complianceSettings:view",

"waf:controlCenter:complianceSettings:modify",

"waf:inventory:add_modify",

"waf:inventory:credentialLibrary",

"waf:inventory:delete",

"waf:inventory:export",

"waf:inventory:fetchConfig",

"waf:inventory:import",

"waf:inventory:manage_unmanage",

"waf:inventory:view",

"waf:backup_restore:compare",

"waf:backup_restore:backupNow",

"waf:backup_restore:deviceRestore",

"waf:backup_restore:delete",

"waf:backup_restore:download",

"waf:backup_restore:create_modify",

"waf:backup_restore:backupSettings",

"waf:dashboard:Defaultdashboard_widget:view",

"waf:learning_suggestions:accept",

"waf:learning_suggestions:delete",

"waf:learning_suggestions:ignore"

Workflow

"workflow:inventory:clone",

"workflow:inventory:create_modify",

"workflow:inventory:delete",

"workflow:inventory:export",

"workflow:inventory:import",

"workflow:inventory:view",

"workflow:inventory:sharedFolder",

"workflow:request:trigger",

"workflow:request:viewAllRequests",

"workflow:request:viewRoleRequests",

"workflow:request:viewMyRequests",

"workflow:request:clone",

"workflow:request:schedule",

"workflow:request:rollback",

"workflow:request:abort",

"workflow:request:pauseResume"

X.509 Certificate

"certificate:applicationConnectoractions:dissociateDevice",

"certificate:applicationConnectoractions:pushToDevices_retry",

"certificate:applicationConnectoractions:rollback",

"certificate:certificatediscovery:*",

"certificate:certificatediscovery:abort",

"certificate:certificatediscovery:columns",

"certificate:certificatediscovery:createeditrediscover",

"certificate:certificatediscovery:delete",

"certificate:certificatediscovery:view",

"certificate:certificatediscovery:export",

"certificate:certificatediscovery:ignore",

"certificate:certificatediscovery:manage",

"certificate:certificatediscovery:monitor",

"certificate:certificatediscovery:rule:*",

"certificate:certificatediscovery:rule:add_modify",

"certificate:certificatediscovery:rule:delete",

"certificate:certificatediscovery:rule:view",

"certificate:client:adminaccess",

"certificate:client:changestatus",

"certificate:client:columns",

"certificate:client:delete",

"certificate:client:export",

"certificate:client:uploadcertificate",

"certificate:client:view",

"certificate:clientcertificateactions:*",

"certificate:clientcertificateactions:deletecertificate",

"certificate:clientcertificateactions:downloadcertificate",

"certificate:clientcertificateactions:reissue",

"certificate:clientcertificateactions:regenerate",

"certificate:clientcertificateactions:renew",

"certificate:clientcertificateactions:resubmit",

"certificate:clientcertificateactions:revoke",

"certificate:clientcertificateactions:submit",

"certificate:clientcertificateactions:suspend",

"certificate:clientcertificateactions:reinstate",

"certificate:connectorActions:add_modify",

"certificate:connectorActions:delete",

"certificate:connectorActions:secureConnector",

"certificate:controlCenter:clientcertificate",

"certificate:controlCenter:servercertificate",

"certificate:controlCenter:codesigningcertificate",

"certificate:dashboard:defaultdashboard_widget:*",

"certificate:dashboard:defaultdashboard_widget:servercertificate",

"certificate:dashboard:defaultdashboard_widget:clientcertificate",

"certificate:dashboard:defaultdashboard_widget:codesigningcertificate",

"certificate:group:assigngroup",

"certificate:group:create_modify",

"certificate:group:delete",

"certificate:group:editDefault",

"certificate:group:unassigngroup",

"certificate:group:viewgroup",

"certificate:intermediate:bulkdownload",

"certificate:intermediate:view",

"certificate:policy:add_modify",

"certificate:policy:delete",

"certificate:policy:editDefaultPolicy",

"certificate:policy:viewpolicy",

"certificate:root:bulkdownload",

"certificate:root:view",

"certificate:server:bulkdownload",

"certificate:server:changestatus",

"certificate:server:columns",

"certificate:server:delete",

"certificate:server:export",

"certificate:server:generatecsrmanually",

"certificate:server:sslchecker",

"certificate:server:uploadcertificate",

"certificate:server:view",

"certificate:servercertificateactions:*",

"certificate:servercertificateactions:deletecertificate",

"certificate:servercertificateactions:downloadCertificate",

"certificate:servercertificateactions:downloadCsr",

"certificate:servercertificateactions:downloadKey",

"certificate:servercertificateactions:reissue",

"certificate:servercertificateactions:regenerate",

"certificate:servercertificateactions:renew",

"certificate:servercertificateactions:resubmit",

"certificate:servercertificateactions:revoke",

"certificate:servercertificateactions:submit",

"certificate:servercertificateactions:uploadCertificate",

"certificate:servercertificateactions:uploadKey",

"certificate:servercertificateactions:suspend",

"certificate:servercertificateactions:reinstate",

"certificate:settings:appsettings:modifysettings",

"certificate:settings:appsettings:view",

"certificate:settings:casettings:custom_ca",

"certificate:settings:casettings:modifysettings",

"certificate:settings:casettings:view",

"certificate:settings:passwordvaultsettings:*",

"certificate:settings:passwordvaultsettings:modifysettings",

"certificate:settings:passwordvaultsettings:view",

"certificate:settings:secureconnectorpasswordrecovery",

"certificate:renewcertificate",

"certificate:caswitch",

"certificate:settings:jobscheduler:modifysettings",

"certificate:settings:jobscheduler:view",

"certificate:codesigning:changestatus",

"certificate:codesigning:columns",

"certificate:codesigning:delete",

"certificate:codesigning:export",

"certificate:codesigning:uploadcertificate",

"certificate:codesigning:view",

"certificate:codesigning:bulkdownload",

"certificate:codesigningcertificateactions:*",

"certificate:codesigningcertificateactions:deletecertificate",

"certificate:codesigningcertificateactions:downloadcsr",

"certificate:codesigningcertificateactions:downloadkey",

"certificate:codesigningcertificateactions:downloadcertificate",

"certificate:codesigningcertificateactions:regenerate",

"certificate:codesigningcertificateactions:renew",

"certificate:codesigningcertificateactions:resubmit",

"certificate:codesigningcertificateactions:revoke",

"certificate:codesigningcertificateactions:submit",

"certificate:codesigningcertificateactions:suspend",

"certificate:codesigningcertificateactions:reinstate"

Chapter 8: Object_CodeObject_Type

- Object Code/Object Type

Object Code/Object Type

Supported Object type/code

Vendor	Object Code	Object Type	Description
F5	vs	Virtual Server	LTM Virtual server
F5	lpm	Pool Member	LTM pool member
F5	lm	LTM Monitor	LTM Monitor
F5	lpr	Profile	Profile
F5	lr	LTM iRule	LTM i-rule
F5	ltmpersistence	LTM Persistence	LTM Persistence
F5	gw	WideIP	GTM Wide IP
F5	gpm	Pool Member	GTM pool member
F5	gp	GTM Pool	GTM pool
F5	gm	GTM Monitor	GTM monitor
F5	gs	GTM Server	GTM Server
F5	gr	GTM iRule	GTM i-rule
Citrix	citrixvs	SLB Virtual Server	SLB virtual server
Citrix	citrixsg	Service Group	Service Group
Citrix	citrixsv	SLB Service	SLB Service
Citrix	citrixcsvs	CS Virtual Server	CS Virtual Server
Citrix	citrixcspolicylabel	CS Policy Label	CS Policy Label
Citrix	citrixcspolicy	CS Policy	CS Policy
Citrix	citrixcsaction	CS Action	CS Action
Citrix	citrixmonitor	Citrix Monitor	Citrix Monitor

Vendor	Object Code	Object Type	Description
Citrix	citrixserver	Server	Server
Citrix	citrixgslbvs	GSLB Virtual Server	GSLB Virtual Server
Citrix	citrixgslbsv	GSLB Service	GSLB Service
Citrix	citrixgslbsite	GSLB Site	GSLB Site
Akamai	akagp	akagp	akagp
Akamai	Akadc	Akadc	Akadc
Akamai	akags	akags	akags
A10	a10vs	Virtual Server	Virtual Server
A10	a10sg	Service Group	Service Group
A10	a10sr	Service Group Member	Service Group Member
A10	a10hm	SLB Health Monitor	SLB Health Monitor
A10	a10fx	aFlex	aFlex
A10	a10cl	Class	Class
A10	a10tm	Template	Template
A10	a10node	Server	Server
A10	a10snatpool	SnatPool	A10 SNAT pool
A10	a10zn	FQDN	FQDN
A10	a10sip	Service IP	Service IP
A10	a10hm	GSLB Health Monitor	GSLB Health Monitor
A10	a10p	Policy	Policy
Radware	radwarevs	Virtual Server	Virtual Server
Radware	radwarevsv	Virtual Service	Virtual Service
Radware	radwaresg	SLB Server Group	SLB Server Group
Radware	radwaresgrs	Group Real Server	Group Real Server
Radware	radwarers	Real Server	Real Server
Radware	radwarehc	Health Check	Health Check

Vendor	Object Code	Object Type	Description
Radware	radwareappshape	App Shape++	App Shape++
Radware	radwarecomppol	Compression Policy	Compression Policy
Radware	radwaresslpol	SSL Policy	SSL Policy
Radware	radwarecachepol	Caching Policy	Caching Policy
Radware	radwarenwclass	Network Class	Network Class
Radware	radwaredataclass	Data Class	Data Class
Radware	radwarecntclass	Content Class	Content Class
Radware	radwarefqdn	FQDN	FQDN
Radware	radwaregslbsg	GSLB Server Group	GSLB Server Group
Radware	radwaregslbsgrs	Group Real Server	Group Real Server
Radware	radwaregslbrs	Real Server	Real Server
Radware	radwarehc	Health Check	Health Check
Radware	radwarenetwork	Network	Network
Radware	radwarerule	Rule	Rule
AVI	avivsv	Virtual Service	Virtual Service
AVI	avipool	Pool	Pool
AVI	aviserver	Server	Server
AVI	aviAppProfile	Application Profile	Application Profile
AVI	aviNwProfile	Network Profile	Network Profile
AVI	aviAnlProfile	Analytical Profile	Analytical Profile
AVI	aviSslProfile	Ssl Profile	Ssl Profile
AVI	aviAppPerProfile	Application Persistence Profile	Application Persistence Profile
AVI	aviPkiProfile	Pki Profile	Pki Profile
AVI	aviMonitor	Monitor	Monitor
AVI	aviIpGroup	Ip Group	Ip Group
AVI	aviNsRule	Network Security Rule	Network Security Rule

Vendor	Object Code	Object Type	Description
AVI	aviHttpSecRule	Http Security Rule	Http Security Rule
AVI	aviHttpReqRule	Http Request Rule	Http Request Rule
AVI	aviHttpResRule	Http Response Rule	Http Response Rule
AVI	aviDataScript	Data Script	Data Script
Cisco	slbvs	Virtual Server	Virtual Server
Cisco	slbsf	Server Farm	Server Farm
Cisco	Slbrs	Real Server	Real Server