

Hitachi Ops Center Common Services

11.0.1

REST API Reference Guide

This manual provides information for how to use the REST API of Hitachi Ops Center Common Services.

© 2020, 2024 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara LLC (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, DB2, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, OS/390, PowerHA, PowerPC, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z15, z16, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, Microsoft Edge, the Microsoft corporate logo, the Microsoft Edge logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found in the product documentation, at <https://www.hitachivantara.com/en-us/company/legal.html>.

Contents

| | |
|--|-----------|
| Preface | 6 |
| Intended audience..... | 6 |
| Product version..... | 6 |
| Release notes..... | 6 |
| Referenced documents..... | 6 |
| Document conventions..... | 7 |
| Accessing product documentation..... | 8 |
| Getting help..... | 8 |
| Comments..... | 8 |
| Chapter 1: Overview of the Common Services REST API | 9 |
| Specifying resources..... | 9 |
| Using a session to perform authentication..... | 9 |
| Response headers..... | 10 |
| Status codes..... | 10 |
| Request and response formats..... | 11 |
| Response when an error occurs..... | 12 |
| Chapter 2: REST API of Common Services | 13 |
| Getting access tokens..... | 13 |
| Getting an access token..... | 13 |
| Getting information about users who obtained an access token..... | 14 |
| Managing external authentication..... | 16 |
| Performing connection and authentication tests for the Active Directory server..... | 16 |
| Getting a list of Active Directory or LDAP servers..... | 19 |
| Getting information about a specific Active Directory or LDAP server..... | 23 |
| Getting a list of realms for Kerberos authentication..... | 28 |
| Getting information about a specific realm for Kerberos authentication..... | 29 |
| Getting Kerberos authentication connection information..... | 30 |
| Checking the number of users to be acquired from an Active Directory or LDAP server..... | 31 |
| Managing identity providers..... | 34 |
| Getting a list of identity providers..... | 34 |
| Getting information about a specific identity provider..... | 39 |

| | |
|---|-----|
| Managing users..... | 45 |
| Getting a list of users..... | 45 |
| Getting information about a specific user..... | 48 |
| Getting a list of the user groups to which a specific user belongs..... | 50 |
| Registering a user..... | 52 |
| Adding a user to a user group..... | 54 |
| Updating the registered information for a user..... | 55 |
| Resetting a user's password..... | 57 |
| Deleting a user from a user group..... | 58 |
| Deleting a user..... | 59 |
| Managing the password policy..... | 60 |
| Getting the password policy..... | 60 |
| Updating the password policy..... | 62 |
| Managing user groups..... | 64 |
| Getting a list of user groups..... | 64 |
| Getting information about a specific user group..... | 66 |
| Getting a list of users who belong to a specific user group..... | 68 |
| Getting a list of roles that can be assigned to a specific user group..... | 70 |
| Getting a list of roles assigned to a specific user group..... | 72 |
| Registering a user group..... | 74 |
| Assigning a role to a user group..... | 75 |
| Updating the registered information for a user group..... | 76 |
| Deleting the role assigned to a user group..... | 78 |
| Deleting a user group..... | 79 |
| Managing linked products..... | 80 |
| Getting a list of products linked with Common Services..... | 80 |
| Getting information about a specific product linked with Common Services..... | 83 |
| Getting license information for a specific product linked with Common Services..... | 86 |
| Getting status information for a specific product linked with Common Services..... | 88 |
| Getting version information for a specific product linked with Common Services..... | 89 |
| Managing data centers..... | 90 |
| Getting a list of data centers..... | 90 |
| Getting information about a specific data center..... | 92 |
| Getting a list of products registered in a specific data center..... | 94 |
| Registering a data center..... | 97 |
| Updating the registered information for a data center..... | 99 |
| Registering a product linked with Common Services in a data center..... | 100 |
| Deleting a product linked with Common Services from a data center..... | 102 |

| | |
|---|-----|
| Deleting a data center..... | 103 |
| Managing the Common Services system information..... | 104 |
| Getting the Common Services version information..... | 104 |
| Session management..... | 105 |
| Obtaining the settings information for session idle timeouts..... | 105 |

Preface

This manual describes how to use the REST API of Hitachi Ops Center Common Services.

Intended audience

This manual is intended for system administrators who use the REST (representational state transfer) API to operate the management functions of Hitachi Ops Center Common Services.

System administrators must have:

- A basic knowledge of the concepts, terms, and functions of Hitachi Ops Center products
- Knowledge of using the REST API to create a program

Product version

This document revision applies to Hitachi Ops Center version 11.0.1.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on the Hitachi Vantara documentation website: <https://docs.hitachivantara.com>.

Referenced documents

The following documents are referenced in this document or contain more information about the features described in this document.

Hitachi Vantara documents







- *Hitachi Ops Center Installation and Configuration Guide*, MK-99OPS001
Hitachi Vantara Support Connect, <https://docs.hitachivantara.com>

Document conventions

This document uses the following typographic conventions:

| Convention | Description |
|---------------------|---|
| Bold | <ul style="list-style-type: none"> Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK. Indicates emphasized words in list items. |
| <i>Italic</i> | <ul style="list-style-type: none"> Indicates a document title or emphasized words in text. Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: <pre>pairdisplay -g group</pre> (For exceptions to this convention for variables, see the entry for angle brackets.) |
| Monospace | Indicates text that is displayed on screen or entered by the user. Example: <code>pairdisplay -g oradb</code> |
| < > angle brackets | Indicates variables in the following scenarios: <ul style="list-style-type: none"> Variables are not clearly separated from the surrounding text or from other variables. Example: <pre>Status-<report-name><file-version>.csv</pre> Variables in headings. |
| [] square brackets | Indicates optional values. Example: [a b] indicates that you can choose a, b, or nothing. |
| { } braces | Indicates required or expected values. Example: { a b } indicates that you must choose either a or b. |
| vertical bar | Indicates that you have a choice between two or more options or arguments. Examples: [a b] indicates that you can choose a, b, or nothing. { a b } indicates that you must choose either a or b. |

This document uses the following icons to draw attention to information:

| Icon | Label | Description |
|---|-----------|--|
|  | Note | Calls attention to additional information. |
|  | Tip | Provides helpful information, guidelines, or suggestions for performing tasks more effectively. |
|  | Important | Highlights information that is essential to the completion of a task. |
|  | Caution | Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash). |
|  | CAUTION | Warns the user of a hazardous situation that, if not avoided, could result in major or minor injury. |
|  | WARNING | Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury. |

Accessing product documentation

Product user documentation is available on the Hitachi Vantara Support Website: <https://docs.hitachivantara.com>. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

The [Hitachi Vantara Support Website](https://support.hitachivantara.com) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

[Hitachi Vantara Community](https://community.hitachivantara.com) is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send comments to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you!

Chapter 1: Overview of the Common Services REST API

The following provides an overview and common specifications of the Common Services REST API.

Specifying resources

In the REST API, the target resource is specified as a URL. In Common Services, the target resource is specified as a continuation of the following base URL:

```
https://host-name-or-IP-address:port-number/portal
```

Specify the host name or IP address of a host that can access Common Services.

For the port number, specify the port number used for Common Services. The default port number is 443.



Note: The Common Services REST API does not support Cross-Origin Resource Sharing (CORS).

Using a session to perform authentication

To run a Common Services REST API request or a request from a REST API provided by a product linking with Common Services, you must first acquire an access token to use the Common Services user authentication. An access token is authentication information that is returned when a session is generated. This authentication information determines whether a request is issued from an authenticated user.

The operational flow for running a REST API request is as follows:

1. Run the Common Services REST API request to acquire an access token.
2. In the Authorization header of the request header, specify the access token in the following format, and run a Common Services REST API request or a request from a REST API provided by another product.

```
Authorization: Bearer access-token
```

Example of specifying an Authorization header:

```
Authorization: Bearer eyJhbxxxx
```

**Note:**

- The validity period of an access token expires five minutes.
- An identify provider user cannot obtain an access token, so they cannot execute a Common Services REST API request.

Response headers

This section describes the response headers returned by the REST API server.

| Header | Description | Default |
|-------------------|--|--------------------------------|
| Content-Type | Indicates the media type of the response data. | application/json;charset=UTF-8 |
| Content-Length | Indicates the size of the response data. If the size of the response data is large, instead of this header, <code>Transfer-Encoding: chunked</code> is returned, indicating that the response data has been divided and then transferred. | None |
| Transfer-Encoding | Indicates the encoding format used when the response data was transferred. When a large amount of response data is divided and then transferred, <code>chunked</code> is returned. | None |
| Location | When an object is registered, this header indicates the URL of the registered object. | None |

Status codes

The REST API uses the following standard HTTP status codes to indicate the processing results.

| HTTP status codes | Description |
|-------------------|-------------|
| 200 | Success |

| HTTP status codes | Description |
|-------------------|---|
| | This indicates that the request was properly processed. |
| 201 | Created This indicates that the request was properly processed and a new resource was successfully created. |
| 204 | No content This indicates that the request was accepted but there was no information to return. |
| 400 | Bad request This indicates that the specification of the request header, the query parameters, or the request body was invalid. |
| 401 | Unauthorized This indicates that the request header did not include the Authorization header or that authentication by using the information specified in the Authorization header failed. |
| 403 | Forbidden This indicates that you do not have permission to perform the operation. |
| 404 | Not found This indicates that the resource specified in the URL could not be found or that you do not have permission to read the resource. |
| 409 | Conflict This indicates that the request could not be completed because of a conflict with the current state of the resource. |
| 500 | Unexpected error This indicates that an unexpected error occurred. |
| 503 | Service Unavailable This indicates that you cannot access the service because of a temporary problem with the server. If you wait a while and then retry the operation, you might be able to access the service. |

Request and response formats

Use the JSON format to specify attribute values when creating or changing a resource. Also, use the JSON format for the results of resource information acquisition.

When creating or adding a resource by using the POST method, or when changing or editing a resource by using the PUT method, specify resource attributes in JSON format. The supported character encoding is UTF-8.

When you use the GET method to collect resource information, responses are returned in JSON format. For API requests that get a list of resources, the response body is an array.

Response when an error occurs

If the processing of a request is not successful, the following error information is returned as a response.

| Attribute | Type | Description |
|----------------|--------|--|
| errorMessage | string | Error message |
| additionalInfo | string | Additional information about the error message |

Output example

```
{
  "errorMessage" : "KAOP20012-E Not Found.",
  "additionalInfo" : "{\"error\":\"Could not find group by id\"}"
}
```

Chapter 2: REST API of Common Services

The following describes the API provided by Common Services.

Getting access tokens

The following describes the API requests for getting an access token to use for REST API authentication.

Getting an access token

You can get an access token to use for REST API authentication.

If you are an identity provider user, you cannot use this API to obtain an access token.

Execution permission

None.

Request line

```
POST base-URL/auth/v1/providers/builtin/token
```

Request message

Object ID

None.

Query parameters

None.

Body

```
{
  "username" : "TestUser",
  "password" : "password"
}
```

| Attribute | Type | Description |
|-----------|--------|--|
| username | string | (Required) Username of the user who wants to acquire an access token |
| password | string | (Required) Password of the user who wants to acquire an access token |

Response message

Body

```
{
  "access_token" : "access token",
  "expires_in" : 300,
  "token_type" : "bearer"
}
```

| Attribute | Type | Description |
|--------------|--------|--|
| access_token | string | Character string that serves as the access token |
| expires_in | int | Period of validity (in seconds) of the access token |
| token_type | string | Access token type A fixed string (<code>bearer</code>) is returned. |

Coding example

```
curl -v -X POST -H "Content-Type:application/json" -s "https://example.com:443/portal/auth/v1/providers/builtin/token" -d @./request.json
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting information about users who obtained an access token

The following request gets information about users who obtained an access token.

Execution permission

None.

Request lineGET *base-URL*/auth/v1/providers/builtin/userinfo**Request message****Object ID**

None.

Query parameters

None.

Body

None.

Response message**Body**

```
{
  "sub": "63583645-fc6f-416d-94a1-1e0719247f4d",
  "name": "john smith",
  "given_name": "john",
  "family_name": "smith",
  "preferred_username": "john_smith",
  "email": "john_smith@example.com",
  "email_verified": false,
  "https://opscenter/user_groups": [
    "92d2677b-a3a2-4643-a908-49ade439e0d4"
  ],
  "https://opscenter/user_is_enabled": true,
  "https://opscenter/roles": [
    "opscenter-user",
    "offline_access",
    "uma_authorization"
  ]
}
```

| Attribute | Type | Description |
|------------|--------|------------------------|
| sub | string | Object ID of the user |
| name | string | Full name of the user |
| given_name | string | First name of the user |

| Attribute | Type | Description |
|---------------------------------------|----------|--|
| family_name | string | Last name of the user |
| preferred_username | string | Username |
| email | string | Email address |
| email_verified | boolean | Whether or not the email address is verified <ul style="list-style-type: none"> ▪ <code>true</code>: Verified ▪ <code>false</code>: Not verified |
| https://opscenter/ user_groups | string[] | ID of the user group that the user belongs to |
| https://opscenter/ user_is_enabled | boolean | Whether the user account is enabled <ul style="list-style-type: none"> ▪ <code>true</code>: The user account is enabled. ▪ <code>false</code>: The user account is disabled. |
| https://opscenter/roles | string[] | ID of the role that was assigned to the user |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/auth/v1/providers/builtin/userinfo"
-H "Authorization:Bearer eyJhbxxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Managing external authentication

The following describes the API requests for managing external authentication.

Performing connection and authentication tests for the Active Directory server

The following request performs connection and authentication tests for the Active Directory server.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
POST base-URL/security/v1/external-user-storage-test-connection
```

Request message

Object ID

None.

Query parameters

None.

Body

To perform only a connection test:

```
{
  "action": "testConnection",
  "connectionUrl": "ldaps://example.com"
}
```

To perform both a connection test and an authentication test:

```
{
  "action": "testAuthentication",
  "connectionUrl": "ldaps://example.com",
  "bindDn": "admin@example.com",
  "bindCredential": "password"
}
```

| Attribute | Type | Description |
|-----------|--------|-------------------------|
| action | string | (Required) Type of test |

| Attribute | Type | Description |
|-----------------------------|--------|--|
| | | <p>Specify either of the following:</p> <ul style="list-style-type: none"> testConnection: Specify this attribute to test whether the connection destination specified by the <code>connectionUrl</code> attribute is accessible. testAuthentication: Specify this attribute to test whether the connection destination specified by the <code>connectionUrl</code> attribute is accessible and whether authentication can be performed by using the authentication information specified by the <code>bindDn</code> and <code>bindCredential</code> attributes. |
| <code>connectionUrl</code> | string | <p>(Required) URL of the connection-destination Active Directory server</p> <p>Specify a URL that starts with <code>ldaps://</code> or <code>ldap://</code>.</p> |
| <code>bindDn</code> | string | <p>(Optional) Bind DN</p> <p>If you specified <code>testAuthentication</code> for the <code>action</code> attribute, you must specify this attribute.</p> |
| <code>bindCredential</code> | string | <p>(Optional) Password for the bind DN</p> <p>If you specified <code>testAuthentication</code> is specified for the <code>action</code> attribute, you must specify this attribute.</p> |

Response message

Body

None.

Coding example

```
curl -v -X POST -H "Content-Type:application/json" -s "https://example.com:443/portal/security/v1/external-user-storage-test-connection" -d @./request.json -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting a list of Active Directory or LDAP servers

The following request gets a list of Active Directory or LDAP servers registered in Common Services.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/external-user-storage
```

Request message

Object ID

None.

Query parameters

None.

Body

None.

Response message

Body

For Active Directory servers

```
[
  {
    "id": "1022c8b2-934e-4097-8112-64b0274a3653",
    "name": "ldap-srv2",
    "priority": 1,
    "userAuthenticationProtocol": "LDAP",
    "vendor": "ACTIVE_DIRECTORY",
    "connectionUrl": "ldaps://vm.ldap-srv2.soft.example.co.jp",
    "baseDn": "CN=Users,DC=ldap-srv2,DC=soft,DC=example,DC=co,DC=jp",
    "bindDn": "admin@ldap-srv2.soft.example.co.jp",
    "bindPassword": null,
    "groupEntryDnList": [
      "CN=admins,CN=Users,DC=ldap-srv2,DC=soft,DC=example,DC=co,DC=jp",
    ]
  }
]
```

```

        "CN=users,CN=Users,DC=ldap-srv2,DC=soft,DC=example,DC=co,
DC=jp"
    ],
    "kerberosRealm": null,
    "enabled": true,
    "defaultGroupMappingEnabled": false,
    "config": {
        "customUserSearchFilter": "(ou=Ops Center*)"
    }
}
]

```

For LDAP servers

```

[
  {
    "id": "1022c8b2-934e-4097-8112-64b0274a3653",
    "name": "ldap-srv2",
    "priority": 1,
    "userAuthenticationProtocol": "LDAP",
    "vendor": "GENERAL",
    "connectionUrl": "ldaps://vm.ldap-srv2.soft.example.co.jp",
    "baseDn": "CN=Users,DC=ldap-srv2,DC=soft,DC=example,DC=co,DC=jp",
    "bindDn": "admin@ldap-srv2.soft.example.co.jp",
    "bindPassword": null,
    "groupEntryDnList": null,
    "kerberosRealm": null,
    "enabled": true,
    "defaultGroupMappingEnabled": true,
    "config": {
      "usernameLDAPAttribute": "userPrincipalName",
      "rdnLDAPAttribute": "cn",
      "customUserSearchFilter": "(ou=Ops Center*)",
      "lastNameLDAPAttribute": "sn",
      "emailLDAPAttribute": "mail",
      "fullNameLDAPAttribute": "cn",
      "searchScope": "2",
      "uuidLDAPAttribute": "objectGUID",
      "userObjectClasses": "person, organizationalPerson"
    }
  }
]

```

| Attribute | Type | Description |
|-----------|--------|-------------|
| id | string | Object ID |
| name | string | Server name |

| Attribute | Type | Description |
|----------------------------|----------|---|
| priority | int | Priority |
| userAuthenticationProtocol | string | Authentication method <ul style="list-style-type: none"> LDAP Kerberos |
| vendor | string | Type of directory service <ul style="list-style-type: none"> ACTIVE_DIRECTORY: Active Directory GENERAL: Not Active Directory |
| connectionUrl | string | URL of the connection-destination Active Directory or LDAP server |
| baseDn | string | BaseDN |
| bindDn | string | Bind DN |
| bindPassword | string | Password for the bind DN |
| groupEntryDnList | string[] | List of DN's of the groups to be synchronized If the value of the <code>vendor</code> attribute is <code>GENERAL</code> , the value <code>null</code> is always returned. |
| kerberosRealm | string | Realm name for Kerberos authentication If the value of the <code>userAuthenticationProtocol</code> attribute is <code>LDAP</code> , the value <code>null</code> is always returned. |
| enabled | boolean | Whether the server setting is enabled <ul style="list-style-type: none"> <code>true</code>: Enabled <code>false</code>: Disabled |
| defaultGroupMappingEnabled | boolean | Whether all the users under the BaseDN of the Active Directory or LDAP server are allocated to the <code>opscenter-users</code> group <ul style="list-style-type: none"> <code>true</code>: The users are allocated to the group. <code>false</code>: The users are not allocated to the group. |
| config | object | Configuration information of the Active Directory or LDAP server |

| Attribute | Type | Description |
|-----------|------|---|
| | | <p>When the <code>vendor</code> attribute is <code>ACTIVE_DIRECTORY</code>, the following configuration information of the Active Directory server is displayed.</p> <ul style="list-style-type: none"> ▪ <code>customUserSearchFilter</code> (string) The search filter for narrowing down the users to be displayed in the Users window of the Hitachi Ops Center Portal <p>When the <code>vendor</code> attribute is <code>GENERAL</code>, the following configuration information of the LDAP server is displayed.</p> <ul style="list-style-type: none"> ▪ <code>usernameLDAPAttribute</code> (string) The LDAP attribute allocated to the user ID ▪ <code>emailLDAPAttribute</code> (string) The LDAP attribute allocated to the email address of the user account ▪ <code>lastNameLDAPAttribute</code> (string) The LDAP attribute allocated to the last name of the user account ▪ <code>fullNameLDAPAttribute</code> (string) The LDAP attribute allocated to the full name of the user account <p>When information is set for the <code>firstNameLDAPAttribute</code> attribute, this attribute is not displayed.</p> <ul style="list-style-type: none"> ▪ <code>firstNameLDAPAttribute</code> (string) The LDAP attribute allocated to the first name of the user account <p>When information is set for the <code>fullNameLDAPAttribute</code> attribute, this attribute is not displayed.</p> <ul style="list-style-type: none"> ▪ <code>rdnLDAPAttribute</code> (string) The LDAP attribute used as the RDN ▪ <code>uuidLDAPAttribute</code> (string) The LDAP attribute used as the UUID |

| Attribute | Type | Description |
|-----------|------|---|
| | | <ul style="list-style-type: none"> ▪ <code>userObjectClasses</code> (string) The object class of the users to be imported ▪ <code>searchScope</code> (string) The range of hierarchy levels in which to search for the users to be imported <ul style="list-style-type: none"> • 1: One level • 2: Subtree ▪ <code>customUserSearchFilter</code> (string) The search filter for narrowing down the users to be imported |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/external-user-storage" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting information about a specific Active Directory or LDAP server

The following request gets information about a specific Active Directory or LDAP server registered in Common Services.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/external-user-storage/object-ID-of-the-server
```

Request message

Object ID of the server

Specify the value of `id` acquired by using the request for getting a list of Active Directory or LDAP servers.

| Attribute | Type | Description |
|-----------|--------|---|
| id | string | (Required) Object ID of the Active Directory or LDAP server |

Query parameters

None.

Body

None.

Response message**Body****For an Active Directory server**

```
{
  "id": "1022c8b2-934e-4097-8112-64b0274a3653",
  "name": "ldap-srv2",
  "priority": 1,
  "userAuthenticationProtocol": "LDAP",
  "vendor": "ACTIVE_DIRECTORY",
  "connectionUrl": "ldaps://vm.ldap-srv2.soft.example.co.jp",
  "baseDn": "CN=Users,DC=ldap-srv2,DC=soft,DC=example,DC=co,DC=jp",
  "bindDn": "admin@ldap-srv2.soft.example.co.jp",
  "bindPassword": null,
  "groupEntryDnList": [
    "CN=admins,CN=Users,DC=ldap-srv2,DC=soft,DC=example,DC=co,DC=jp",
    "CN=users,CN=Users,DC=ldap-srv2,DC=soft,DC=example,DC=co,DC=jp"
  ],
  "kerberosRealm": null,
  "enabled": true,
  "defaultGroupMappingEnabled": false,
  "config": {
    "customUserSearchFilter": "(ou=Ops Center*)"
  }
}
```

For an LDAP server

```
{
  "id": "1022c8b2-934e-4097-8112-64b0274a3653",
  "name": "ldap-srv2",
  "priority": 1,
  "userAuthenticationProtocol": "LDAP",
  "vendor": "GENERAL",
  "connectionUrl": "ldaps://vm.ldap-srv2.soft.example.co.jp",
}
```


Getting information about a specific Active Directory or LDAP server

```

"baseDn": "CN=Users,DC=ldap-srv2,DC=soft,DC=example,DC=co,DC=jp",
"bindDn": "admin@ldap-srv2.soft.example.co.jp",
"bindPassword": null,
"groupEntryDnList": null,
"kerberosRealm": null,
"enabled": true,
"defaultGroupMappingEnabled": true,
"config": {
  "usernameLDAPAttribute": "userPrincipalName",
  "rdnLDAPAttribute": "cn",
  "customUserSearchFilter": "(ou=Ops Center*)",
  "lastNameLDAPAttribute": "sn",
  "emailLDAPAttribute": "mail",
  "fullNameLDAPAttribute": "cn",
  "searchScope": "2",
  "uuidLDAPAttribute": "objectGUID",
  "userObjectClasses": "person, organizationalPerson"
}
}

```

| Attribute | Type | Description |
|----------------------------|----------|---|
| id | string | Object ID of the Active Directory or LDAP server |
| name | string | Server name |
| priority | int | Priority |
| userAuthenticationProtocol | string | Authentication method <ul style="list-style-type: none"> ▪ LDAP ▪ Kerberos |
| vendor | string | Type of directory service <ul style="list-style-type: none"> ▪ ACTIVE_DIRECTORY: Active Directory ▪ GENERAL: Not Active Directory |
| connectionUrl | string | URL of the connection-destination Active Directory or LDAP server |
| baseDn | string | BaseDN |
| bindDn | string | Bind DN |
| bindPassword | string | Password for the bind DN |
| groupEntryDnList | string[] | List of DN's of the groups to be synchronized |

| Attribute | Type | Description |
|--|----------------------|--|
| | | If the value of the <code>vendor</code> attribute is <code>GENERAL</code> , the value <code>null</code> is always returned. |
| <code>kerberosRealm</code> | <code>string</code> | Realm name for Kerberos authentication If the value of the <code>userAuthenticationProtocol</code> attribute is <code>LDAP</code> , the value <code>null</code> is always returned. |
| <code>enabled</code> | <code>boolean</code> | Whether the server setting is enabled <ul style="list-style-type: none"> ▪ <code>true</code>: Enabled ▪ <code>false</code>: Disabled |
| <code>defaultGroupMapping Enabled</code> | <code>boolean</code> | Whether all the users under the BaseDN of the Active Directory or LDAP server are allocated to the <code>opscenter-users</code> group <ul style="list-style-type: none"> ▪ <code>true</code>: The users are allocated to the group. ▪ <code>false</code>: The users are not allocated to the group. |
| <code>config</code> | <code>object</code> | Configuration information of the Active Directory or LDAP server When the <code>vendor</code> attribute is <code>ACTIVE_DIRECTORY</code> , the following configuration information of the Active Directory server is displayed. <ul style="list-style-type: none"> ▪ <code>customUserSearchFilter</code> (string) The search filter for narrowing down the users to be displayed in the Users window of the Hitachi Ops Center Portal When the <code>vendor</code> attribute is <code>GENERAL</code> , the following configuration information of the LDAP server is displayed. <ul style="list-style-type: none"> ▪ <code>usernameLDAPAttribute</code> (string) The LDAP attribute allocated to the user ID ▪ <code>emailLDAPAttribute</code> (string) The LDAP attribute allocated to the email address of the user account ▪ <code>lastNameLDAPAttribute</code> (string) The LDAP attribute allocated to the last name of the user account |

| Attribute | Type | Description |
|-----------|------|---|
| | | <ul style="list-style-type: none"> ▪ <code>fullNameLDAPAttribute</code> (string) The LDAP attribute allocated to the full name of the user account When information is set for the <code>firstNameLDAPAttribute</code> attribute, this attribute is not displayed. ▪ <code>firstNameLDAPAttribute</code> (string) The LDAP attribute allocated to allocated to the first name of the user account When information is set for the <code>fullNameLDAPAttribute</code> attribute, this attribute is not displayed. ▪ <code>rdnLDAPAttribute</code> (string) The LDAP attribute used as the RDN ▪ <code>uuidLDAPAttribute</code> (string) The LDAP attribute used as the UUID ▪ <code>userObjectClasses</code> (string) The object class of the users to be imported ▪ <code>searchScope</code> (string) The range of hierarchy levels in which to search for users to be imported <ul style="list-style-type: none"> • 1: One level • 2: Subtree ▪ <code>customUserSearchFilter</code> (string) The search filter for narrowing down the users to be imported |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/external-user-storage/1022c8b2-934e-4097-8112-64b0274a3653" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting a list of realms for Kerberos authentication

The following request gets a list of realms for Kerberos authentication registered in Common Services.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/kerberos-realm
```

Request message

Object ID

None.

Query parameters

None.

Body

None.

Response message

Body

```
[
  {
    "id": "8a44f59a6f87e5d4016f880c544c0000",
    "realm": "LDAP-SRV2.SOFT.EXAMPLE.CO.JP",
    "kdc": [
      "vm.ldap-srv2.soft.example.co.jp"
    ]
  }
]
```

| Attribute | Type | Description |
|-----------|----------|------------------------|
| id | string | Object ID of the realm |
| realm | string | Realm name |
| kdc | string[] | List of KDC servers |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/kerberos-realm" -H
"Authorization:Bearer eyJhbxxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting information about a specific realm for Kerberos authentication

The following request gets information about a specific realm for Kerberos authentication registered in Common Services.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/kerberos-realm/object-ID-of-the-realm
```

Request message**Object ID of the realm**

Specify the value of `id` acquired by using the request for getting information about a list of realms for Kerberos authentication.

| Attribute | Type | Description |
|-----------------|--------|-----------------------------------|
| <code>id</code> | string | (Required) Object ID of the realm |

Query parameters

None.

Body

None.

Response message**Body**

```
{
  "id": "8a44f59a6f87e5d4016f880c544c0000",
  "realm": "LDAP-SRV2.SOFT.EXAMPLE.CO.JP",
```

```

"kdc": [
  "vm.ldap-srv2.soft.example.co.jp"
]
}

```

| Attribute | Type | Description |
|-----------|----------|------------------------|
| id | string | Object ID of the realm |
| realm | string | Realm name |
| kdc | string[] | List of KDC servers |

Coding example

```

curl -v -X GET -s "https://example.com:443/portal/security/v1/kerberos-realm/4028b8816e4ad3ee016e5d76637c0000" -H "Authorization:Bearer eyJhbxxx"

```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting Kerberos authentication connection information

The following request gets Kerberos authentication connection information registered in Common Services.

Execution permission

You must be a system administrator or a security administrator.

Request line

```

GET base-URL/security/v1/kerberos-connection-settings

```

Request message

Object ID

None.

Query parameters

None.

Body

None.

Response message

Body

```
{
  "clockskew" : 0,
  "dnsLookupKdc" : true
}
```

| Attribute | Type | Description |
|--------------|---------|--|
| clockskew | int | Allowable time difference between Common Services and the Kerberos server (in seconds) |
| dnsLookupKdc | boolean | Whether to query the DNS server for KDC information <ul style="list-style-type: none"> ▪ true: Queries the server. ▪ false: Does not query the server. |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/kerberos-connection-
settings" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Checking the number of users to be acquired from an Active Directory or LDAP server

Check the number of users to be acquired from an Active Directory or LDAP server. This number is the number of users to be displayed in the Users window of the Hitachi Ops Center Portal.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
POST base-URL/security/v1/external-user-storage-test-search-limit-exceeded
```

Request message

Object ID

None.

Query parameters

None.

Body

```
{
  "connectionUrl": "ldaps://example.com",
  "bindDn": "cn=Directory Manager",
  "bindPassword": "password",
  "baseDn": "OU=Subtree,DC=example,DC=com",
  "objectClasses": "person, organizationalPerson",
  "searchScope": "1",
  "customUserSearchFilter": "(ou=Ops Center*)",
  "usernameLDAPAttribute": "uid"
}
```

| Attribute | Type | Description |
|---------------|--------|--|
| connectionUrl | string | (Required) URL of the connection-destination Active Directory or LDAP server |
| bindDn | string | (Required) Bind DN |
| bindPassword | string | (Required) Password for the bind DN |
| baseDn | string | (Required) BaseDN |
| objectClasses | string | (Required) For an Active Directory server Specify person, organizationalPerson, user. For an LDAP server The object class of the users to be acquired To specify multiple values, separate the values by using commas. |
| searchScope | string | (Required) For an Active Directory server Specify 2. For an LDAP server The range of hierarchy levels in which to search for users to be acquired |

| Attribute | Type | Description |
|------------------------|--------|--|
| | | Specify either of the following. <ul style="list-style-type: none"> 1: One level 2: Subtree |
| customUserSearchFilter | string | (Optional) The search filter for narrowing down the users to be acquired The syntax of the search filter conforms to RFC 2254. |
| usernameLDAPAttribute | string | (Required) For an Active Directory server Specify <code>sAMAccountName</code> . For an LDAP server LDAP attribute that uniquely identifies the user to be acquired |

Response message

Body

```
{
  "count" : 5,
  "maxValue" : 100
}
```

| Attribute | Type | Description |
|-----------|------|--|
| count | int | The number of users acquired from the Active Directory or LDAP server If the number of users is greater than the value of the <code>maxValue</code> attribute, <code>-1</code> is returned. |
| maxValue | int | The maximum number of users that can be displayed in the Users window of the Hitachi Ops Center Portal |

Coding example

```
curl -v -X POST -H "Content-Type:application/json" -s "https://example.com:443/portal/security/v1/external-user-storage-test-search-limit-exceeded" -d @./request.json -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Managing identity providers

This section describes the API requests related to the management of identity providers.

Getting a list of identity providers

The following request gets a list of identity providers registered in Common Services.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/idp/v1/external-identity-provider
```

Request message**Object ID**

None.

Query parameters

None.

Body

None.

Response message**Body**

When the federation protocol is OIDC

```
[
  {
    "providerType": "ADFS",
```

```

    "protocol": "oidc",
    "alias": "ad5oidc",
    "displayName": "AD5OIDC",
    "fromUrl": "https://adfs.example.com/adfs/.well-known/openid-
configuration",
    "enabled": true,
    "guiOrder": 1,
    "defaultGroupList": [
      {
        "localGroupId": "a39f9e45-5e2e-446b-89d3-93f9e9ec4c31",
        "localGroupName": "opscenter-users"
      }
    ],
    "customGroupList": [
      {
        "idpGroupName": "opscenter-ad5\\opscenter_admins",
        "localGroupId": "9fd2ef28-5077-4816-ade8-526204f4d2ac",
        "localGroupName": "opscenter-administrators"
      }
    ],
    "clientId": "a49d4539-c080-4436-8bcb-113271b5152a",
    "clientSecret": "*****",
    "config": {
      "userInfoUrl": "https://adfs.example.com/adfs/userinfo",
      "validateSignature": "true",
      "redirectURI": "https://example.com:8443/auth/realms/
opscenter/broker/ad5oidc/endpoint",
      "clientId": "a49d4539-c080-4436-8bcb-113271b5152a",
      "tokenUrl": "https://adfs.example.com/adfs/oauth2/token/",
      "jwksUrl": "https://adfs.example.com/adfs/discovery/keys",
      "issuer": "https://adfs.example.com/adfs",
      "useJwksUrl": "true",
      "authorizationUrl": "https://adfs.example.com/adfs/oauth2/
authorize/",
      "clientAuthMethod": "client_secret_post",
      "disableUserInfo": "true",
      "fromUrl": "https://adfs.example.com/adfs/.well-known/openid-
configuration",
      "logoutUrl": "https://adfs.example.com/adfs/oauth2/logout",
      "syncMode": "FORCE",
      "clientSecret": "*****",
      "allowedClockSkew": "300",
      "defaultScope": "https://example.com/openid https://
example.com/allatclaims"
    }
  }
]

```

When the federation protocol is SAML

```
[
  {
    "providerType": "ADFS",
    "protocol": "saml",
    "alias": "ad5saml",
    "displayName": "AD5SAML",
    "fromUrl": "https://adfs.example.com/FederationMetadata/2007-06/
FederationMetadata.xml",
    "enabled": true,
    "guiOrder": 1,
    "defaultGroupList": [
      {
        "localGroupId": "a39f9e45-5e2e-446b-89d3-93f9e9ec4c31",
        "localGroupName": "opscenter-users"
      }
    ],
    "customGroupList": [
      {
        "idpGroupName": "opscenter-ad5\\opscenter_admins",
        "localGroupId": "9fd2ef28-5077-4816-ade8-526204f4d2ac",
        "localGroupName": "opscenter-administrators"
      }
    ],
    "clientId": null,
    "clientSecret": null,
    "config": {
      "redirectURI": "https://example.com:8443/auth/realms/
opscenter/broker/ad5saml/endpoint",
      "samlXmlKeyNameTransformer": "KEY_ID",
      "postBindingLogout": "true",
      "postBindingResponse": "true",
      "singleLogoutServiceUrl": "https://adfs.example.com/
adfs/ls/",
      "claimEmail": "http://schemas.xmlsoap.org/ws/2005/05/
identity/claims/emailaddress",
      "claimFirstname": "http://schemas.xmlsoap.org/ws/2005/05/
identity/claims/givenname",
      "claimGroup": "http://schemas.xmlsoap.org/claims/Group",
      "claimLastname": "http://schemas.xmlsoap.org/ws/2005/05/
identity/claims/surname",
      "xmlSigKeyInfoKeyNameTransformer": "CERT_SUBJECT",
      "metadataEndpoint": "https://example.com:8443/auth/realms/
opscenter/broker/ad5saml/endpoint/descriptor",
      "syncMode": "FORCE",
      "singleSignOnServiceUrl": "https://adfs.example.com/
adfs/ls/",
      "wantAuthnRequestsSigned": "true",
```

```

    "allowedClockSkew": "300",
    "encryptionPublicKey":
"MIIDDDCCAFsGAWIBAgIQPniaLjBZQo1Pp9AouqTIATANBgkqhkiG9w0BAQsFADEBCMUAWPgYD
VQQDEzdBREZTIEVUy3J5cHRpb24gLSB2bTIZnZAlMy5vcmlvb1hZDIuc29mdC5oaXRhY2hpL
mNvLmpwMB4XDTIxMDMyMzA0MTI0MVoXDTI0MMDMyMjA0MTI0MVowQjFAMD4GA1UEAxM3URGUy
BFbmNyeXB0aW9uIC0gdm0yMzcwNTMub3Jpb24tYWQyLnNvZnQuaGl0YWN0aS5jby5qcDCCASI
wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMpfyp71B7YdRjnKir4R1RgJIshmlx9ZmjPZ
YXu+VZ0o7m+r6a+CwuH3zsFJlhu8/
QYhjAthL6iHwyrLdv3YETOrURRzd23BY3q0d9aZ50efaAfh1NfcZ0ltoMkFhOvz39TGjtHL6F
layPkJKRP+AwONZ8VOWkAJIhlmMF3wX8myFHs6Y2cSR5C1bWGZ
+eRlFQP4gJLlribfcZMRCulBhk7FrOe9k4hZd2/
IaqMVZQKEUofqv1r8fpSu99e01pR59hvoJUQE6x12mgmKmqYgMceit
+mCEldw5N311xq8v3Uab12OeudSDYbOJDAuNUwFhx360VJMo6vmZqSpnJlCECAWEAATANBg
kqhkiG9w0BAQsFAAOCAQEAAo7wvasuKX7NtGd8YcHwZ/v/
2k1T0jx1tmuWS0TezKANZSofYmJn7HAYugJa/
VUa18nehvBAPjajjRvArDLsZBAxOzYsn2U4m3XuEzHrtS+40/dBS/
vYGldIfTfupVjCRJZvV35ONFL7sqnXnnxk0PiVTC0r3jY3oIqB8uRELFYEmLgDEEdB3YizH0N
dtzWHdWiChyWTYdZBe3zfizl3UEIOfbZIEmolgXjZquinCOO/
EZKLuJWgbupc17B7RQOhX1ZeKY2OGcL2opqnaBRcib2bTyg6R0E
+ZGm6yOy6pC8pYdbvvKv9uBoys7BB/JgbSnLWXz9nB7c6o/yU6WdCA==",
    "validateSignature": "true",
    "signingCertificate":
"MIIDBjCCAe6gAWIBAgIQMCWzElwV4b9Kq4X13T/i3DANBgkqhkiG9w0BAQsFADA/
MT0wOwYDVQQDEzRBREZTIFNpZ25pbmcgLSB2bTIZnZAlMy5vcmlvb1hZDIuc29mdC5oaXRhY
2hpLmNvLmpwMB4XDTIxMDMyMzA0MTI0MVoXDTI0MMDMyMjA0MTI0NVowPzE9MDSGA1UEAxM0QU
RGUyBTaWduaW5nIC0gdm0yMzcwNTMub3Jpb24tYWQyLnNvZnQuaGl0YWN0aS5jby5qcDCCASI
wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIwQWHRYEJ1MglckuKBBStb
+C1Bz3Ql rzDlcXAPv1/
QQjOpWa20fB0Y1L2RmKtjtVE3AuUNetJXkyfMwOYqVaDcudPj5I6zRve
+ZYE46KgyjDkDSBE2o2saENe74KvZ23G9J+1beKt/
hcmPdXXH6oOQ8c1C40fEXfxoiV2Uw5K3ltOYfa7lSeQ6ywydso/
DYtUrJqK4juq2kV7+hHsrQ7hNndKpAKhouq89KZ1opbxvG/
cdQqWR110NZx2CftZrYxtVu5P4Vz1oBoA+GVvu7CBQoFlZ2dbWruI0oEPj7/ebV
+84HFZYG1NrSMn3D5Da
+6LwReljZEoDwJkNKz3m6cCAWEAATANBgkqhkiG9w0BAQsFAAOCAQEAielrzirZug21oHupUe
zWbaeP7wAYfS8LBIKpbyR+xrtoaJhcdeEUUGwpadT283Yq3AXzRAVJ7rXPVhAGYCOuw
+1kq3WaT+glaTbQJPPAy57WhrhNLRRY3AowohOdCzi5fznTTMbREK4E0hJ1xh4r7Hst
+J1R9hLfMK115DNPKrBMZuiYXa566WIw6F708VLJxRQcTVG9P/
MqecOouch6f91H4zDyNFPrjDmbssdGVCBX2RnVqHhUKJXPVCTTTLDNOqqUZ4Z/wWzuEAhis0/
eyUBs0w3X1BVXyUHaEMIESpGDUSBrBY+Uqv6oR7q0i4Ge+YmfqwpaxKAUrAN0m2ckA==",
    "nameIDPolicyFormat": "urn:oasis:names:tc:SAML:1.1:nameid-
format:WindowsDomainQualifiedName",
    "signatureAlgorithm": "RSA_SHA256",
    "wantAssertionsEncrypted": "true",
    "useJwksUrl": "true",
    "wantAssertionsSigned": "true",
    "fromUrl": "https://adfs.example.com/FederationMetadata/2007-
06/FederationMetadata.xml",

```

```

    "postBindingAuthnRequest": "true",
    "forceAuthn": "true",
    "addExtensionsElementWithKeyInfo": "false",
    "principalType": "SUBJECT"
  }
}
]

```

| Attribute | Type | Description |
|------------------|---------|--|
| providerType | string | Provider type A fixed string (ADFS) is returned. |
| protocol | string | Federation protocol <ul style="list-style-type: none"> oidc saml |
| alias | string | Alias name |
| displayName | string | Display name |
| fromUrl | string | OpenID Connect discovery endpoint or metadata endpoint of the identity provider |
| enabled | boolean | Whether the server setting is enabled <ul style="list-style-type: none"> true: Enabled false: Disabled |
| guiOrder | int | Server display sequence in the Identity Provider window A fixed value (1) is returned. |
| defaultGroupList | object | Settings of default group mappers <ul style="list-style-type: none"> localGroupId (string) Object ID of the local user group localGroupName (string) Local user group name |

| Attribute | Type | Description |
|-----------------|--------|---|
| customGroupList | object | Settings of custom group mappers <ul style="list-style-type: none"> idpGroupName (string) Group name of the identity provider localGroupId (string) Object ID of the local user group localGroupName (string) Local user group name |
| clientId | string | Client ID of the identity provider If the value of the <code>protocol</code> attribute is <code>saml</code> , the value <code>null</code> is always returned. |
| clientSecret | string | Client secret of the identity provider If the value of the <code>protocol</code> attribute is <code>oidc</code> , the value <code>*****</code> is always returned. If the value of the <code>protocol</code> attribute is <code>saml</code> , the value <code>null</code> is always returned. |
| config | object | Configuration information of the identity provider |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/idp/v1/external-identity-provider" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting information about a specific identity provider

The following request gets information about a specific identity provider registered in Common Services.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/idp/v1/external-identity-provider/alias-name
```

Request message**Alias name**

Specify the value of `alias` acquired by using the request for getting a list of identity providers.

| Attribute | Type | Description |
|-----------|--------|--|
| alias | string | (Required) Alias name of the identity provider |

Query parameters

None.

Body

None.

Response message**Body****When the federation protocol is OIDC**

```
{
  "providerType": "ADFS",
  "protocol": "oidc",
  "alias": "ad5oidc",
  "displayName": "AD5OIDC",
  "fromUrl": "https://adfs.example.com/adfs/.well-known/openid-configuration",
  "enabled": true,
  "guiOrder": 1,
  "defaultGroupList": [
    {
      "localGroupId": "a39f9e45-5e2e-446b-89d3-93f9e9ec4c31",
      "localGroupName": "opscenter-users"
    }
  ],
  "customGroupList": [
    {
      "idpGroupName": "opscenter-ad5\\opscenter_admins",
      "localGroupId": "9fd2ef28-5077-4816-ade8-526204f4d2ac",
      "localGroupName": "opscenter-administrators"
    }
  ],
}
```



```

"clientId": "a49d4539-c080-4436-8bcb-113271b5152a",
"clientSecret": "*****",
"config": {
  "userInfoUrl": "https://adfs.example.com/adfs/userinfo",
  "validateSignature": "true",
  "redirectURI": "https://example.com:8443/auth/realms/opscenter/
broker/ad5oidc/endpoint",
  "clientId": "a49d4539-c080-4436-8bcb-113271b5152a",
  "tokenUrl": "https://adfs.example.com/adfs/oauth2/token/",
  "jwksUrl": "https://adfs.example.com/adfs/discovery/keys",
  "issuer": "https://adfs.example.com/adfs",
  "useJwksUrl": "true",
  "authorizationUrl": "https://adfs.example.com/adfs/oauth2/
authorize/",
  "clientAuthMethod": "client_secret_post",
  "disableUserInfo": "true",
  "fromUrl": "https://adfs.example.com/adfs/.well-known/openid-
configuration",
  "logoutUrl": "https://adfs.example.com/adfs/oauth2/logout",
  "syncMode": "FORCE",
  "clientSecret": "*****",
  "allowedClockSkew": "300",
  "defaultScope": "https://example.com/openid https://example.com/
allatclaims"
}
}

```

When the federation protocol is SAML

```

{
  "providerType": "ADFS",
  "protocol": "saml",
  "alias": "ad5saml",
  "displayName": "AD5SAML",
  "fromUrl": "https://adfs.example.com/FederationMetadata/2007-06/
FederationMetadata.xml",
  "enabled": true,
  "guiOrder": 1,
  "defaultGroupList": [
    {
      "localGroupId": "a39f9e45-5e2e-446b-89d3-93f9e9ec4c31",
      "localGroupName": "opscenter-users"
    }
  ],
  "customGroupList": [
    {
      "idpGroupName": "opscenter-ad5\\opscenter_admins",
      "localGroupId": "9fd2ef28-5077-4816-ade8-526204f4d2ac",

```

```

        "localGroupName": "opscenter-administrators"
    }
],
"clientId": null,
"clientSecret": null,
"config": {
    "redirectURI": "https://example.com:8443/auth/realms/opscenter/
broker/ad5saml/endpoint",
    "samlXmlKeyNameTransformer": "KEY_ID",
    "postBindingLogout": "true",
    "postBindingResponse": "true",
    "singleLogoutServiceUrl": "https://adfs.example.com/adfs/ls/",
    "claimEmail": "http://schemas.xmlsoap.org/ws/2005/05/identity/
claims/emailaddress",
    "claimFirstname": "http://schemas.xmlsoap.org/ws/2005/05/
identity/claims/givenname",
    "claimGroup": "http://schemas.xmlsoap.org/claims/Group",
    "claimLastname": "http://schemas.xmlsoap.org/ws/2005/05/identity/
claims/surname",
    "xmlSigKeyInfoKeyNameTransformer": "CERT_SUBJECT",
    "metadataEndpoint": "https://example.com:8443/auth/realms/
opscenter/broker/ad5saml/endpoint/descriptor",
    "syncMode": "FORCE",
    "singleSignOnServiceUrl": "https://adfs.example.com/adfs/ls/",
    "wantAuthnRequestsSigned": "true",
    "allowedClockSkew": "300",
    "encryptionPublicKey":
"MIIDDDCCafSgAwIBAgIQPniaLjBZQolPp9AouqTIATANBgkqhkiG9w0BAQsFAADBCMUAWPgYD
VQQDEzdBREZTIEVUyJ3J5cHRpb24gLSB2bTIzNzA1My5vcmlvbilhZDIuc29mdC5oaXRhY2hpL
mNvLmpwMBA4XDTIxMDMyMzA0MTI0MV0xMDMyMjA0MTI0MVowQjFAMD4GA1UEAxM3QURGUy
BFBmNyeXB0aW9uIC0gdm0yMzcwNTMub3Jpb24tYWQyLnNvZnQuaGl0YWN0aS5jby5qcDCCASI
wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMpfyp71B7YdrjnKir4R1RgJIshmlx9ZmjPZ
YXu+VZ0o7m+r6a+CwuH3zsFJlhu/
QYhjAthL6iHwyrLdv3YETOrURRzd23BY3q0d9aZ50efaAfh1NfcZ0ltoMkFhOvz39TGjtHL6F
layPkJKRP+AwONZ8VOWkAJIHlMF3wX8myFHS6Y2cSR5C1bWGZ
+eRLfQP4gjLlribfcZMRCulBhk7FrOe9k4hZd2/
IaqMVZQKEUofqv1r8fpSu99e01pR59hvoJUQE6x12mgmKmQygMceit
+mCEldw5N311xq8vj3Uabl2OeudadSYbOJDAuNUwFhx360VJM06vmZqSpnJlCECAWEAATANBg
kqhkiG9w0BAQsFAAOCAQEAo7wvasuKX7NtGd8YcHwZ/v/
2klT0jxltmuWS0TezKANZSofYmJn7HAYugJa/
VUal8nehvBAPjajjRvArDLsZBAxOzYsn2U4m3XuEzHrts+40/dBS/
vYGldIfTfupVjCRJZvV35ONFL7sqnXnnxk0PiVTC0r3jY3oIqB8uRELFYEmLgDEEdB3YizH0N
dtzWHdWicHyWTYdZBe3zfizl3UEIOfbZIEmolgXjZquiNcOO/
EZKLuJWgbupc17B7RQOhX1ZeKY20GcL2opqnaBRcib2bTyg6R0E
+ZGm6yOy6pC8pYdbvvKv9uBoys7BB/JgbSnLWXz9nB7c6o/yU6WdCA==",
    "validateSignature": "true",
    "signingCertificate": "MIIDBjCCAe6gAwIBAgIQMCWzE1wV4b9Kq4X13T/
i3DANBgkqhkiG9w0BAQsFADA/

```

```

MT0wOwYDVQQDEzRBREZTIFNpZ25pbmcgLSB2bTIZnZAlMy5vcmlvb1hZDIuc29mdC5oaXRhY
2hpLmNvLmpwMB4XDTIxMDMyMzA0MTI0NVoXDTI0MDMyMjA0MTI0NVowPzE9MDSGA1UEAxM0QU
RGUyBTAWduaW5nIC0gdm0yMzcwNTMub3Jpb24tYWQyLnNvZnQuaGl0YWN0aS5jby5qcDCCASI
wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAlwQWHRYEJ1MglckuKBBStb
+C1Bz3Q1rzDlcXAPv1/
QQjOpWa20fB0Y1L2RmKTjtVE3AuUNetJXkYfMwoYqVaDcudPj5I6zRve
+ZYE46KgyjDkDSBE2o2saENe74KvZ23G9J+1beKt/
hcmPdXXH6oOQ8c1C40fEXfxoiV2Uw5K3ltOYfa7lSeQ6ywydso/
DYtUrJqK4juq2kV7+hHsrQ7hNndKpAKhouq89KZ1opbxvG/
cdQqWR110NZx2CftZrYXtVu5P4Vz1oBoA+GVvu7CBQoFlZ2dbWruI0oEPj7/ebV
+84HFZYG1NrSmn3D5Da
+6LwReljZEoDwJkNKz3m6cCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAIElrzirZug21oHupUe
zWbaeP7wAYfs8LBIKpbyR+xrtoaJhcdeEUUGwpadT283Yq3AXzRAVJ7rXPVhAGYCOuw
+1kq3WaT+glaTbQJPPAy57WhrhNLRRY3AowohOdCZi5fznTMMbREK4E0hJ1xh4r7Hst
+J1R9hLfMK115DNPKrBMZuiYXa566WIw6F708VLJxRQcTVG9P/
MqecOOuch6f91H4zDyNFPrjDmbssdGVCBX2RnVqHhUKJXPVCTTTLDNOqqUZ4Z/wWzuEAhis0/
eyUBs0w3X1BVXyHaEMIESpGDUSBrBY+Uqv6oR7q0i4Ge+YmfqwpaxKAUrAN0m2cka==",
    "nameIDPolicyFormat": "urn:oasis:names:tc:SAML:1.1:nameid-
format:WindowsDomainQualifiedName",
    "signatureAlgorithm": "RSA_SHA256",
    "wantAssertionsEncrypted": "true",
    "useJwksUrl": "true",
    "wantAssertionsSigned": "true",
    "fromUrl": "https://adfs.example.com/FederationMetadata/2007-06/
FederationMetadata.xml",
    "postBindingAuthnRequest": "true",
    "forceAuthn": "true",
    "addExtensionsElementWithKeyInfo": "false",
    "principalType": "SUBJECT"
  }
}

```

| Attribute | Type | Description |
|--------------|--------|--|
| providerType | string | Provider type A fixed string (ADFS) is returned. |
| protocol | string | Federation protocol <ul style="list-style-type: none"> ▪ oidc ▪ saml |
| alias | string | Alias name |
| displayName | string | Display name |
| fromUrl | string | OpenID Connect discovery endpoint or metadata endpoint of the identify provider |

| Attribute | Type | Description |
|------------------|---------|---|
| enabled | boolean | Whether the server setting is enabled <ul style="list-style-type: none"> ▪ <code>true</code>: Enabled ▪ <code>false</code>: Disabled |
| guiOrder | int | Server display sequence in the Identify Providers window A fixed value (1) is returned. |
| defaultGroupList | object | Configuration of default group mappers <ul style="list-style-type: none"> ▪ <code>localGroupId</code> (string) Object ID of the local user group ▪ <code>localGroupName</code> (string) Local user group name |
| customGroupList | object | Settings of custom group mappers <ul style="list-style-type: none"> ▪ <code>idpGroupName</code> (string) Group name of the identity provider ▪ <code>localGroupId</code> (string) Object ID of the local user group ▪ <code>localGroupName</code> (string) Local user group name |
| clientId | string | Client ID of the identify provider If the value of the <code>protocol</code> attribute is <code>saml</code> , the value <code>null</code> is always returned. |
| clientSecret | string | Client secret of the identity provider If the value of the <code>protocol</code> attribute is <code>oidc</code> , the value <code>*****</code> is always returned. If the value of the <code>protocol</code> attribute is <code>saml</code> , the value <code>null</code> is always returned. |
| config | object | Configuration information of the identity provider |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/idp/v1/external-identity-provider/ad5oidc" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Managing users

The following describes the API requests for managing users.

Getting a list of users

The following request gets a list of users.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/users
```

Request message**Object ID**

None.

Query parameters

| Parameter | Type | Filter condition |
|-----------|--------|--|
| search | string | String that must be included in the username, first name, last name, or email address of the user. |

Body

None.

Response message**Body**

```
[
  {
    "id": "a010279b-ae66-4c1d-b066-c45d50c9f75a",
    "username": "sysadmin",
    "firstName": "firstName",
    "lastName": null,
    "email": "sysadmin@example.com",
    "dn": null,
    "description": "Built-in user",
    "enabled": true,
    "builtin": true,
    "federatedIdentities": null
  },
  {
    "id": "82576381-e765-4645-a697-782111f8f5b5",
    "username": "user_1",
    "firstName": "1",
    "lastName": "user",
    "email": "user_1@example.com",
    "dn": null,
    "description": "description user_1",
    "enabled": true,
    "builtin": false,
    "federatedIdentities": [
      {
        "alias": "dummy_alias",
        "displayName": "DUMMY DISPLAY NAME"
      }
    ]
  }
]
```

| Attribute | Type | Description |
|-----------|--------|------------------------|
| id | string | Object ID of the user |
| username | string | Username |
| firstName | string | First name of the user |
| lastName | string | Last name of the user |
| email | string | Email address |
| dn | string | Distinguished Name |

| Attribute | Type | Description |
|----------------------------------|----------------------|---|
| | | If the user is not a user acquired from an Active Directory or LDAP server, the value <code>null</code> is always returned. |
| <code>description</code> | <code>string</code> | Description of the user account |
| <code>enabled</code> | <code>boolean</code> | Whether the user account is enabled <ul style="list-style-type: none"> <code>true</code>: The user account is enabled. <code>false</code>: The user account is disabled. |
| <code>builtin</code> | <code>boolean</code> | Whether the user is a built-in user <ul style="list-style-type: none"> <code>true</code>: The user is a built-in user. <code>false</code>: The user is not a built-in user. |
| <code>federatedIdentities</code> | <code>object</code> | Identity provider information If the user is not an identity provider user, <code>null</code> is always returned. |
| <code>alias</code> | <code>string</code> | Alias name that identifies the identity provider This is displayed when the user is an identity provider user. |
| <code>displayName</code> | <code>string</code> | Display name of the identity provider This is displayed when the user is an identify provider user. |

Coding example

When no query parameter is specified:

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/users" -H
"Authorization:Bearer eyJhbxxxx"
```

When a query parameter is specified:

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/users?search=smith" -H
"Authorization:Bearer eyJhbxxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting information about a specific user

The following request gets information about a specific user.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/users/object-ID-of-the-user
```

Request message

Object ID of the user

Specify the value of `id` acquired by using the request for getting information about a list of users.

| Attribute | Type | Description |
|-----------------|--------|----------------------------------|
| <code>id</code> | string | (Required) Object ID of the user |

Query parameters

None.

Body

None.

Response message

Body

```
{
  "id": "a010279b-ae66-4c1d-b066-c45d50c9f75a",
  "username": "sysadmin",
  "firstName": "firstName",
  "lastName": null,
  "email": "sysadmin@example.com",
  "dn": null,
  "description": "Built-in user",
  "enabled": true,
  "builtin": true,
  "federatedIdentities": [
    {
      "alias": "dummy_alias",
      "displayName": "DUMMY DISPLAY NAME"
    }
  ]
}
```



```

]
}

```

| Attribute | Type | Description |
|---------------------|---------|---|
| id | string | Object ID of the user |
| username | string | Username |
| firstName | string | First name of the user |
| lastName | string | Last name of the user |
| email | string | Email address |
| dn | string | Distinguished Name If the user is not a user acquired from an Active Directory or LDAP server, the value <code>null</code> is always returned. |
| description | string | Description of the user account |
| enabled | boolean | Whether the user account is enabled <ul style="list-style-type: none"> ▪ <code>true</code>: The user account is enabled. ▪ <code>false</code>: The user account is disabled. |
| builtin | boolean | Whether the user is a built-in user <ul style="list-style-type: none"> ▪ <code>true</code>: The user is a built-in user. ▪ <code>false</code>: The user is not a built-in user. |
| federatedIdentities | object | Identity provider information If the user is not an identity provider user, <code>null</code> is always returned. |
| alias | string | Alias name that identifies the identity provider This is displayed when the user is an identity provider user. |
| displayName | string | Display name of the identity provider This is displayed when the user is an identify provider user. |

Coding example

```

curl -v -X GET -s "https://example.com:443/portal/security/v1/users/a010279b-ae66-4c1d-b066-c45d50c9f75a" -H "Authorization:Bearer eyJhbxxx"

```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting a list of the user groups to which a specific user belongs

The following request gets a list of the user groups to which a specific user belongs.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/users/object-ID-of-the-user/user-groups
```

Request message

Object ID of the user

Specify the value of `id` acquired by using the request for getting information about a list of users.

| Attribute | Type | Description |
|-----------------|--------|----------------------------------|
| <code>id</code> | string | (Required) Object ID of the user |

Query parameters

None.

Body

None.

Response message

Body

```
[
  {
    "id": "4760d4c0-c593-42fe-b44a-553da4793882",
    "name": "opscenter-administrators",
    "path": "/opscenter-administrators",
    "dn": null,
    "description": null,
    "builtin": true,
    "essential": false,
    "external": false
  }
]
```

```

    },
    {
      "id": "7a773ca8-49cf-4ee2-9456-eb4853b4c6c1",
      "name": "opscenter-users",
      "path": "/opscenter-users",
      "dn": null,
      "description": null,
      "builtin": true,
      "essential": true,
      "external": false
    }
  ]

```

| Attribute | Type | Description |
|-------------|---------|--|
| id | string | Object ID of the user group |
| name | string | User group name |
| path | string | Path |
| dn | string | Distinguished Name If the group is not a group acquired from an Active Directory or LDAP server, the value <code>null</code> is always returned. |
| description | string | Description of the user group |
| builtin | boolean | Whether the user group is a built-in user group <ul style="list-style-type: none"> ▪ <code>true</code>: The user group is a built-in user group. ▪ <code>false</code>: The user group is not a built-in user group. |
| essential | boolean | Whether the user group is an essential user group (<code>opscenter-users</code>) <ul style="list-style-type: none"> ▪ <code>true</code>: The user group is an essential user group. ▪ <code>false</code>: The user group is not an essential user group. |

| Attribute | Type | Description |
|-----------|---------|---|
| external | boolean | Whether the user group was acquired from an external source <ul style="list-style-type: none"> ▪ <code>true</code>: The user group was acquired from an external source. ▪ <code>false</code>: The user group was not acquired from an external source. |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/users/a010279b-ae66-4c1d-b066-c45d50c9f75a/user-groups" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Registering a user

The following request registers a user.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
POST base-URL/security/v1/users
```

Request message

Object ID

None.

Query parameters

None.

Body

```
{
  "username": "John_Smith",
  "firstName": "John",
  "lastName": "Smith",
```

```

"email": "john_smith@example.com",
"description": "John's account",
"enabled": true
}

```

| Attribute | Type | Description |
|-------------|---------|--|
| username | string | (Required) Username Specify a character string that is no more than 255 characters. You can use the following characters: 0-9 A-Z a-z ! # \$ % & ' () * + - . = @ ^ _ \$ |
| firstName | string | (Optional) First name of the user Specify a character string that is no more than 64 characters. |
| lastName | string | (Optional) Last name of the user Specify a character string that is no more than 64 characters. |
| email | string | (Optional) Email address Specify a character string that is no more than 254 characters. |
| description | string | (Optional) Description of the user account Specify a character string that is no more than 128 characters. |
| enabled | boolean | (Required) Whether to enable the user account <ul style="list-style-type: none"> ▪ <code>true</code>: Enables the user account. ▪ <code>false</code>: Disables the user account. |

Response message

Body

None.

Coding example

```

curl -v -X POST -H "Content-Type:application/json" -s "https://example.com:443/portal/security/v1/users" -d @./request.json -H "Authorization:Bearer eyJhbxxx"

```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Adding a user to a user group

The following request adds a user to a user group.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
PUT base-URL/security/v1/users/object-ID-of-the-user/user-groups/object-ID-of-the-user-group
```

Request message

Object ID of the user

Specify the value of `id` acquired by using the request for getting information about a list of users.

| Attribute | Type | Description |
|-----------------|--------|----------------------------------|
| <code>id</code> | string | (Required) Object ID of the user |

Object ID of the user group

Specify the value of `id` acquired by using the request for getting information about a list of user groups.

| Attribute | Type | Description |
|--------------------------|--------|--|
| <code>userGroupId</code> | string | (Required) Object ID of the user group |

Query parameters

None.

Body

None.

Response message

Body

None.

Coding example

```
curl -v -X PUT -s "https://example.com:443/portal/security/v1/users/8b39869a-a778-4a08-a2ff-bf967946e836/user-groups/4760d4c0-c593-42fe-b44a-553da4793882" -H
"Authorization:Bearer eyJhbxxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Updating the registered information for a user

The following request updates the registered information for a user.

The registration information of an identity provider user cannot be updated.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
PUT base-URL/security/v1/users/object-ID-of-the-user
```

Request message**Object ID of the user**

Specify the value of `id` acquired by using the request for getting information about a list of users.

| Attribute | Type | Description |
|-----------------|--------|----------------------------------|
| <code>id</code> | string | (Required) Object ID of the user |

Query parameters

None.

Body

```
{
  "id": "8b39869a-a778-4a08-a2ff-bf967946e836",
  "username": "user_1",
  "firstName": "1",
  "lastName": "user",
  "email": "user_1@email.com",
  "description": "description user_1",
```

```
"enabled": true
}
```

| Attribute | Type | Description |
|-------------|---------|--|
| id | string | (Required) Object ID of the user Specify the value of <code>id</code> acquired by using the request for getting information about a list of users. |
| username | string | (Required) Username Specify the username that corresponds to the object ID of the user. You cannot change the username. |
| firstName | string | (Optional) First name of the user Specify a character string that is no more than 64 characters. |
| lastName | string | (Optional) Last name of the user Specify a character string that is no more than 64 characters. |
| email | string | (Optional) Email address Specify a character string that is no more than 254 characters. |
| description | string | (Optional) Description of the user account Specify a character string that is no more than 128 characters. |
| enabled | boolean | (Optional) Whether to enable the user account <ul style="list-style-type: none"> ▪ <code>true</code>: Enables the user account. ▪ <code>false</code>: Disables the user account. |

Response message

Body

None.

Coding example

```
curl -v -X PUT -H "Content-Type:application/json" -s "https://example.com:443/portal/security/v1/users/8b39869a-a778-4a08-a2ff-bf967946e836" -d @./request.json -H "Authorization:Bearer eyJhbGxxxx"
```




Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Resetting a user's password

The following request resets the password for a user.

The password of an identity provider user cannot be reset.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
PUT base-URL/security/v1/users/object-ID-of-the-user/reset-password
```

Request message

Object ID of the user

Specify the value of `id` acquired by using the request for getting information about a list of users.

| Attribute | Type | Description |
|-----------------|--------|----------------------------------|
| <code>id</code> | string | (Required) Object ID of the user |

Query parameters

None.

Body

```
{
  "type": "password",
  "value": "P@ssw0rd"
}
```

| Attribute | Type | Description |
|--------------------|--------|---|
| <code>type</code> | string | (Required) Type of the authentication information to be reset You must specify <code>password</code> for this attribute. |
| <code>value</code> | string | (Required) New password |

| Attribute | Type | Description |
|-----------|------|---|
| | | Specify a character string that is no more than 256 characters. |

Response message

Body

None.

Coding example

```
curl -v -X PUT -H "Content-Type:application/json" -s "https://example.com:443/portal/security/v1/users/8b39869a-a778-4a08-a2ff-bf967946e836/reset-password" -d @./request.json -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Deleting a user from a user group

The following request deletes a user registered in a user group.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
DELETE base-URL/security/v1/users/object-ID-of-the-user/user-groups/object-ID-of-the-user-group
```

Request message

Object ID of the user

Specify the value of `id` acquired by using the request for getting information about a list of users.

| Attribute | Type | Description |
|-----------|--------|----------------------------------|
| id | string | (Required) Object ID of the user |

Object ID of the user group

Specify the value of `id` acquired by using the request for getting information about a list of user groups.

However, you cannot specify a user group for which `essential` is set to `true`.

| Attribute | Type | Description |
|--------------------------|--------|--|
| <code>userGroupId</code> | string | (Required) Object ID of the user group |

Query parameters

None.

Body

None.

Response message**Body**

None.

Coding example

```
curl -v -X DELETE -s "https://example.com:443/portal/security/v1/users/8b39869a-a778-4a08-a2ff-bf967946e836/user-groups/4760d4c0-c593-42fe-b44a-553da4793882" -H "Authorization:Bearer eyJhbxxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Deleting a user

The following request deletes a user.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
DELETE base-URL/security/v1/users/object-ID-of-the-user
```

Request message**Object ID of the user**

Specify the value of `id` acquired by using the request for getting information about a list of users.

However, you cannot specify a user for which `builtin` is set to `true`.

| Attribute | Type | Description |
|-----------------|--------|----------------------------------|
| <code>id</code> | string | (Required) Object ID of the user |

Query parameters

None.

Body

None.

Response message**Body**

None.

Coding example

```
curl -v -X DELETE -s "https://example.com:443/portal/security/v1/users/8b39869a-a778-4a08-a2ff-bf967946e836" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Managing the password policy

The following describes the API requests for managing the password policy.

Getting the password policy

The following request gets the password policy for Common Services.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/password-policy
```

Request message**Object ID**

None.

Query parameters

None.

Body

None.

Response message**Body**

```
{
  "length": 8,
  "upperCase": 1,
  "lowerCase": 1,
  "digits": 1,
  "specialChars": 1,
  "bruteForceProtected": true,
  "failureFactor": 5
}
```

| Attribute | Type | Description |
|--------------|------|---|
| length | int | Minimum number of characters required for a password |
| upperCase | int | Minimum number of uppercase characters required in a password |
| lowerCase | int | Minimum number of lowercase characters required in a password |
| digits | int | Minimum number of numeric characters required in a password |
| specialChars | int | Minimum number of symbols required in a password |

| Attribute | Type | Description |
|---------------------|---------|--|
| bruteForceProtected | boolean | Whether to lock a user account after a certain number of unsuccessful login attempts <ul style="list-style-type: none"> ▪ <code>true</code>: Locks the account. ▪ <code>false</code>: Does not lock the account. |
| failureFactor | int | Number of unsuccessful login attempts allowed before a user account is locked |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/password-policy" -H
"Authorization:Bearer eyJhbxxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Updating the password policy

The following request updates the password policy for Common Services.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
PUT base-URL/security/v1/password-policy
```

Request message

Object ID

None.

Query parameters

None.

Body

```
{
  "length": 8,
  "upperCase": 1,
```

```

"lowerCase": 1,
"digits": 1,
"specialChars": 1,
"bruteForceProtected": true,
"failureFactor": 5
}

```

| Attribute | Type | Description |
|---------------------|---------|---|
| length | int | (Required) Minimum number of characters required for a password Specify a value in the range from 1 to 256. |
| upperCase | int | (Required) Minimum number of uppercase characters required in a password Specify a value in the range from 0 to 256. If you do not want to set a minimum for the number of uppercase characters, specify 0. |
| lowerCase | int | (Required) Minimum number of lowercase characters required in a password Specify a value in the range from 0 to 256. If you do not want to set a minimum for the number of lowercase characters, specify 0. |
| digits | int | (Required) Minimum number of numeric characters required in a password Specify a value in the range from 0 to 256. If you do not want to set a minimum for the number of numeric characters, specify 0. |
| specialChars | int | (Required) Minimum number of symbols required in a password Specify a value in the range from 0 to 256. If you do not want to set a minimum for the number of symbols, specify 0. |
| bruteForceProtected | boolean | (Required) Whether to lock a user account after a certain number of unsuccessful login attempts <ul style="list-style-type: none"> ▪ <code>true</code>: Locks the account. ▪ <code>false</code>: Does not lock the account. |
| failureFactor | int | (Optional) Number of unsuccessful login attempts allowed before a user account is locked |

| Attribute | Type | Description |
|-----------|------|---|
| | | Specify a value in the range from 1 to 256. If you specified <code>true</code> for the <code>bruteForceProtected</code> attribute, you must specify this attribute. |

Response message**Body**

None.

Coding example

```
curl -v -X PUT -H "Content-Type:application/json" -s "https://example.com:443/portal/security/v1/password-policy" -d @./request.json -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Managing user groups

The following describes the API requests for managing user groups.

Getting a list of user groups

You can get a list of user groups.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/user-groups
```

Request message**Object ID**

None.

Query parameters

| Parameter | Type | Filter condition |
|-----------|--------|--|
| search | string | String that must be included in the name of the user group |

Body

None.

Response message**Body**

```
[
  {
    "id": "caf4dd60-5213-430a-907c-17c98c3dca5e",
    "name": "opscenter-administrators",
    "path": "/opscenter-administrators",
    "dn": null,
    "description": null,
    "builtin": true,
    "essential": false,
    "external": false
  }
]
```

| Attribute | Type | Description |
|-------------|---------|---|
| id | string | Object ID of the user group |
| name | string | User group name |
| path | string | Path |
| dn | string | Distinguished Name If the group is not a group acquired from an Active Directory or LDAP server, the value <code>null</code> is always returned. |
| description | string | Description of the user group |
| builtin | boolean | Whether the user group is a built-in user group <ul style="list-style-type: none"> ▪ <code>true</code>: The user group is a built-in user group. ▪ <code>false</code>: The user group is not a built-in user group. |

| Attribute | Type | Description |
|-----------|---------|---|
| essential | boolean | Whether the user group is an essential user group (opscenter-users) <ul style="list-style-type: none"> ▪ <code>true</code>: The user group is an essential user group. ▪ <code>false</code>: The user group is not an essential user group. |
| external | boolean | Whether the user group was acquired from an external source <ul style="list-style-type: none"> ▪ <code>true</code>: The user group was acquired from an external source. ▪ <code>false</code>: The user group was not acquired from an external source. |

Coding example

When no query parameter is specified:

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/user-groups" -H
"Authorization:Bearer eyJhbxxx"
```

When a query parameter is specified:

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/user-groups?
search=smith" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting information about a specific user group

You can get information about a specific user group.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/user-groups/object-ID-of-the-user-group
```

Request message**Object ID of the user group**

Specify the value of `id` acquired by using the request for getting information about a list of user groups.

| Attribute | Type | Description |
|-----------------|--------|--|
| <code>id</code> | string | (Required) Object ID of the user group |

Query parameters

None.

Body

None.

Response message**Body**

```
{
  "id": "caf4dd60-5213-430a-907c-17c98c3dca5e",
  "name": "opscenter-administrators",
  "path": "/opscenter-administrators",
  "dn": null,
  "description": null,
  "builtin": true,
  "essential": false,
  "external": false
}
```

| Attribute | Type | Description |
|--------------------------|--------|---|
| <code>id</code> | string | Object ID of the user group |
| <code>name</code> | string | User group name |
| <code>path</code> | string | Path |
| <code>dn</code> | string | Distinguished Name If the group is not a group acquired from an Active Directory or LDAP server, the value <code>null</code> is always returned. |
| <code>description</code> | string | Description of the user group |

| Attribute | Type | Description |
|-----------|---------|--|
| builtin | boolean | Whether the user group is a built-in user group <ul style="list-style-type: none"> ▪ <code>true</code>: The user group is a built-in user group. ▪ <code>false</code>: The user group is not a built-in user group. |
| essential | boolean | Whether the user group is an essential user group (<code>opscenter-users</code>) <ul style="list-style-type: none"> ▪ <code>true</code>: The user group is an essential user group. ▪ <code>false</code>: The user group is not an essential user group. |
| external | boolean | Whether the user group was acquired from an external source <ul style="list-style-type: none"> ▪ <code>true</code>: The user group was acquired from an external source. ▪ <code>false</code>: The user group was not acquired from an external source. |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/user-groups/caf4dd60-5213-430a-907c-17c98c3dca5e" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting a list of users who belong to a specific user group

The following request gets a list of users who belong to a specific user group.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/user-groups/object-ID-of-the-user-group/users
```

Request message**Object ID of the user group**

Specify the value of `id` acquired by using the request for getting information about a list of user groups.

| Attribute | Type | Description |
|-----------------|--------|--|
| <code>id</code> | string | (Required) Object ID of the user group |

Query parameters

None.

Body

None.

Response message**Body**

```
[
  {
    "id": "a010279b-ae66-4c1d-b066-c45d50c9f75a",
    "username": "sysadmin",
    "firstName": "firstName",
    "lastName": null,
    "email": "sysadmin@example.com",
    "dn": null,
    "description": "Built-in user",
    "enabled": true,
    "builtin": true
  }
]
```

| Attribute | Type | Description |
|------------------------|--------|------------------------|
| <code>id</code> | string | Object ID of the user |
| <code>username</code> | string | Username |
| <code>firstName</code> | string | First name of the user |
| <code>lastName</code> | string | Last name of the user |
| <code>email</code> | string | Email address |
| <code>dn</code> | string | Distinguished Name |

| Attribute | Type | Description |
|--------------------------|----------------------|---|
| | | If the user is not a user acquired from an Active Directory or LDAP server, the value <code>null</code> is always returned. |
| <code>description</code> | <code>string</code> | Description of the user account |
| <code>enabled</code> | <code>boolean</code> | Whether the user account is enabled <ul style="list-style-type: none"> <code>true</code>: The user account is enabled. <code>false</code>: The user account is disabled. |
| <code>builtin</code> | <code>boolean</code> | Whether the user is a built-in user <ul style="list-style-type: none"> <code>true</code>: The user is a built-in user. <code>false</code>: The user is not a built-in user. |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/user-groups/4760d4c0-c593-42fe-b44a-553da4793882/users" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting a list of roles that can be assigned to a specific user group

The following request gets a list of roles that can be assigned to a specific user group.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/user-groups/object-ID-of-the-user-group/role-mappings/portal/available
```

Request message

Object ID of the user group

Specify the value of `id` acquired by using the request for getting information about a list of user groups.

| Attribute | Type | Description |
|-----------|--------|--|
| id | string | (Required) Object ID of the user group |

Query parameters

None.

Body

None.

Response message**Body**

```
[
  {
    "id": "e219126f-c858-4fc6-8ad9-9622cc8bddf7",
    "name": "opscenter-security-administrator",
    "description": null,
    "builtin": true,
    "essential": false
  },
  {
    "id": "6eb98bb9-43cc-4062-a25c-185e78afa438",
    "name": "opscenter-system-administrator",
    "description": null,
    "builtin": true,
    "essential": false
  }
]
```

| Attribute | Type | Description |
|-------------|---------|---|
| id | string | Object ID of the role |
| name | string | Role name |
| description | string | Description of the role |
| builtin | boolean | Whether the role is a built-in role <ul style="list-style-type: none"> ▪ <code>true</code>: The role is a built-in role. ▪ <code>false</code>: The role is not a built-in role. |

| Attribute | Type | Description |
|-----------|---------|--|
| essential | boolean | Whether the role is an essential role (opscenter-user) <ul style="list-style-type: none"> ▪ true: The role is an essential role. ▪ false: The role is not an essential role. |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/user-groups/7a773ca8-49cf-4ee2-9456-eb4853b4c6c1/role-mappings/portal/available" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting a list of roles assigned to a specific user group

The following request gets a list of roles assigned to a specific user group.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/user-groups/object-ID-of-the-user-group/role-mappings/portal
```

Request message

Object ID of the user group

Specify the value of id acquired by using the request for getting information about a list of user groups.

| Attribute | Type | Description |
|-----------|--------|--|
| id | string | (Required) Object ID of the user group |

Query parameters

None.

Body

None.

Response message**Body**

```
[
  {
    "id": "6eb98bb9-43cc-4062-a25c-185e78afa438",
    "name": "opscenter-system-administrator",
    "description": null,
    "builtin": true,
    "essential": false
  },
  {
    "id": "8c9db2e1-9abb-4f9a-a6a0-d0486faa75c1",
    "name": "opscenter-user",
    "description": null,
    "builtin": true,
    "essential": true
  }
]
```

| Attribute | Type | Description |
|-------------|---------|--|
| id | string | Object ID of the role |
| name | string | Role name |
| description | string | Description of the role |
| builtin | boolean | Whether the role is a built-in role <ul style="list-style-type: none"> ▪ true: The role is a built-in role. ▪ false: The role is not a built-in role. |
| essential | boolean | Whether the role is an essential role (opscenter-user) <ul style="list-style-type: none"> ▪ true: The role is an essential role. ▪ false: The role is not an essential role. |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/user-groups/4760d4c0-c593-42fe-b44a-553da4793882/role-mappings/portal" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Registering a user group

The following request registers a user group.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
POST base-URL/security/v1/user-groups
```

Request message

Object ID

None.

Query parameters

None.

Body

```
{
  "name": "group_1",
  "description": "description group_1"
}
```

| Attribute | Type | Description |
|-------------|--------|---|
| name | string | (Required) Name of the user group Specify a character string that is no more than 255 characters. You can use the following characters: 0-9 A-Z a-z ! # \$ & ' () + - . = @ [] ^ _ ` { } ~ \$ space character You cannot specify space character at the start or end. |
| description | string | (Optional) Description of the user group Specify a character string that is no more than 255 characters. |

Response message**Body**

None.

Coding example

```
curl -v -X POST -H "Content-Type:application/json" -s "https://example.com:443/portal/security/v1/user-groups" -d @./request.json -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Assigning a role to a user group

The following request assigns a role to a user group.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
POST base-URL/security/v1/user-groups/object-ID-of-the-user-group/role-mappings/portal/role-name
```

Request message**Object ID of the user group**

Specify the value of `id` acquired by using the request for getting information about a list of user groups.

| Attribute | Type | Description |
|-----------------|--------|--|
| <code>id</code> | string | (Required) Object ID of the user group |

Role name

Specify the value of `name` acquired by using the request for getting information about a list of roles that can be assigned to a specific user group.

| Attribute | Type | Description |
|-----------------------|--------|----------------------|
| <code>roleName</code> | string | (Required) Role name |

Query parameters

None.

Body

None.

Response message**Body**

None.

Coding example

```
curl -v -X POST -s "https://example.com:443/portal/security/v1/user-groups/baf760bc-c789-4cb9-a9cb-662b0b2e4be1/role-mappings/portal/opscenter-security-administrator" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Updating the registered information for a user group

The following request updates the registered information for a user group.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
PUT base-URL/security/v1/user-groups/object-ID-of-the-user-group
```

Request message**Object ID of the user group**

Specify the value of `id` acquired by using the request for getting information about a list of user groups.

| Attribute | Type | Description |
|-----------|--------|--|
| id | string | (Required) Object ID of the user group |

Query parameters

None.

Body

```
{
  "id": "baf760bc-c789-4cb9-a9cb-662b0b2e4be1",
  "name": "name",
  "description": "description"
}
```

| Attribute | Type | Description |
|-------------|--------|---|
| id | string | (Required) Object ID of the user group Specify the value of <code>id</code> acquired by using the request for getting information about a list of user groups. |
| name | string | (Optional) User group name Specify a character string that is no more than 255 characters. You can use the following characters: 0-9 A-Z a-z ! # \$ & ' () + - . = @ [] ^ _ ` { } ~ \$ space character You cannot specify space character at the start or end. |
| description | string | (Optional) Description of the user group Specify a character string that is no more than 255 characters. |

Response message**Body**

None.

Coding example

```
curl -v -X PUT -H "Content-Type:application/json" -s "https://example.com:443/portal/security/v1/user-groups/baf760bc-c789-4cb9-a9cb-662b0b2e4be1" -d @./request.json -H "Authorization:Bearer eyJhbxxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Deleting the role assigned to a user group

The following request deletes the role assigned to a user group.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
DELETE base-URL/security/v1/user-groups/object-ID-of-the-user-group/role-mappings/portal/role-name
```

Request message

Object ID of the user group

Specify the value of `id` acquired by using the request for getting information about a list of user groups.

| Attribute | Type | Description |
|-----------|--------|--|
| id | string | (Required) Object ID of the user group |

Role name

Specify the value of `name` acquired by using the request for getting information about a list of roles that can be assigned to a specific user group.

However, you cannot specify the `opscenter-user` role.

| Attribute | Type | Description |
|-----------|--------|----------------------|
| roleName | string | (Required) Role name |

Query parameters

None.

Body

None.

Response message

Body

None.

Coding example

```
curl -v -X DELETE -s "https://example.com:443/portal/security/v1/user-groups/baf760bc-c789-4cb9-a9cb-662b0b2e4be1/role-mappings/portal/opscenter-security-administrator" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Deleting a user group

The following request deletes a user group.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
DELETE base-URL/security/v1/user-groups/object-ID-of-the-user-group
```

Request message**Object ID of the user group**

Specify the value of `id` acquired by using the request for getting information about a list of user groups.

However, you cannot specify a user group for which `builtin` is set to `true`.

| Attribute | Type | Description |
|-----------------|--------|--|
| <code>id</code> | string | (Required) Object ID of the user group |

Query parameters

None.

Body

None.

Response message**Body**

None.

Coding example

```
curl -v -X DELETE -s "https://example.com:443/portal/security/v1/user-groups/baf760bc-c789-4cb9-a9cb-662b0b2e4be1" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Managing linked products

The following describes the API requests for managing products linked with Common Services.

Getting a list of products linked with Common Services

The following request gets a list of products linked with Common Services.

Execution permission

None.

Request line

```
GET base-URL/app/v1/application-services
```

Request message**Object ID**

None.

Query parameters

None.

Body

None.

Response message**Body**

```
[
  {
    "id": "8a11a1bf6d7012db016dd878c5e50001",
    "type": "AUTOMATOR",
    "displayType": "Hitachi Ops Center Automator",
```



```

    "abbreviatedDisplayType": "Automator",
    "name": "example.com",
    "description": "",
    "scheme": "https",
    "hostname": "example.com",
    "port": 22016,
    "baseUri": "https://example.com:22016/Automation",
    "loginScreenUri": "https://example.com:22016/Automation/login",
    "licenseRegistrationScreenUri": "https://example.com:22016/Automation/
license.htm",
    "authorizationManagementScreenUri": "https://example.com:22016/
Automation/main.htm?module=administrations",
    "clientConfigurationUri": "https://example.com:22016/Automation/v1/
application/ClientConfigurations",
    "oidcEnabled": true,
    "oidcRedirectUris": [
        "https://example.com:22016/Automation/callback"
    ],
    "internalVersion": 1,
    "statusCheckDisabled": false
},
{
    "id": "3c6be9db-41b0-4fce-a38d-413f0c5b101a",
    "type": "STORAGE_NAVIGATOR",
    "displayType": "Hitachi Device Manager Storage Navigator",
    "abbreviatedDisplayType": "Storage Navigator",
    "name": "SN",
    "description": "description",
    "scheme": "sdlauncher",
    "hostname": "localhost",
    "port": 8082,
    "baseUri": "sdlauncher://localhost:8082",
    "loginScreenUri": "sdlauncher://localhost:8082/dev/storage/
xxxxxxxxxxxx/index.do",
    "licenseRegistrationScreenUri": "",
    "authorizationManagementScreenUri": "",
    "clientConfigurationUri": "",
    "oidcEnabled": false,
    "oidcRedirectUris": [],
    "internalVersion": 1,
    "statusCheckDisabled": true,
    "attributes": {
        "serial": "8901234",
        "model": "VSP 5600"
    }
},
{
    "id": "3fb742cd-f888-48ba-99e5-aad089c61753",
    "type": "VSP_ONE_BLOCK_ADMINISTRATOR",

```

```

    "displayType": "VSP One Block Administrator",
    "abbreviatedDisplayType": "VSP One Block Administrator",
    "name": "Salamander plus",
    "description": "description",
    "scheme": "https",
    "hostname": "localhost",
    "port": 443,
    "baseUri": "https://localhost:443",
    "loginScreenUri": "https://localhost/",
    "licenseRegistrationScreenUri": "",
    "authorizationManagementScreenUri": "",
    "clientConfigurationUri": "",
    "oidcEnabled": false,
    "oidcRedirectUris": [],
    "internalVersion": 1,
    "statusCheckDisabled": true,
    "attributes": {
      "serial": "1234567",
      "model": "VSP One B28"
    }
  ]

```

| Attribute | Type | Description |
|------------------------|--------|--|
| id | string | Object ID of the product |
| type | string | Product type |
| displayType | string | Display type |
| abbreviatedDisplayType | string | Product abbreviation |
| name | string | Product name |
| description | string | Description of the product |
| scheme | string | Communication protocol <ul style="list-style-type: none"> ▪ http ▪ https ▪ sdlauncher (This is set if Storage Navigator is used.) |
| hostname | string | Host name of the server running the product |
| port | int | Port number of the product |
| baseUri | string | Base URI of the product |

| Attribute | Type | Description |
|----------------------------------|----------|--|
| loginScreenUri | string | URI of the login screen for the product |
| licenseRegistrationScreenUri | string | URI of the license registration screen for the product |
| authorizationManagementScreenUri | string | URI of the authorization management screen for the product |
| clientConfigurationUri | string | URI of the configuration screen for the product |
| oidcEnabled | boolean | Whether single sign-on can be used <ul style="list-style-type: none"> ▪ <code>true</code>: Can be used. ▪ <code>false</code>: Cannot be used. |
| oidcRedirectUris | string[] | Redirect URI |
| internalVersion | int | Internal version of the product |
| statusCheckDisabled | boolean | Whether to use Common Services to check the product's heartbeat <ul style="list-style-type: none"> ▪ <code>true</code>: Do not check the product's heartbeat. ▪ <code>false</code>: Check the product's heartbeat. |
| attributes | object | Information about the attributes of storage systems managed by Storage Navigator or VSP One Block Administrator |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/app/v1/application-services" -H
"Authorization:Bearer eyJhbxxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting information about a specific product linked with Common Services

The following request gets information about a specific product linked with Common Services.

Execution permission

None.

Request lineGET *base-URL/app/v1/application-services/object-ID-of-the-product***Request message****Object ID of the product**

Specify the value of `id` acquired by using the request for getting information about the products linked with Common Services.

| Attribute | Type | Description |
|-----------------|--------|-------------------------------------|
| <code>id</code> | string | (Required) Object ID of the product |

Query parameters

None.

Body

None.

Response message**Body**

```
{
  "id": "3fb742cd-f888-48ba-99e5-aad089c61753",
  "type": "VSP_ONE_BLOCK_ADMINISTRATOR",
  "displayType": "VSP One Block Administrator",
  "abbreviatedDisplayType": "VSP One Block Administrator",
  "name": "Salamander plus",
  "description": "description",
  "scheme": "http",
  "hostname": "localhost",
  "port": 80,
  "baseUri": "http://localhost:80",
  "loginScreenUri": "http://localhost/",
  "licenseRegistrationScreenUri": "",
  "authorizationManagementScreenUri": "",
  "clientConfigurationUri": "",
  "oidcEnabled": false,
  "oidcRedirectUris": [],
  "internalVersion": 1,
  "statusCheckDisabled": true,
  "attributes": {
    "serial": "1234567",
  }
}
```

```

    "model": "VSP One B28"
  }
}

```

| Attribute | Type | Description |
|----------------------------------|----------|--|
| id | string | Object ID of the product |
| type | string | Product type |
| displayType | string | Display type |
| abbreviatedDisplayType | string | Product abbreviation |
| name | string | Product name |
| description | string | Description of the product |
| scheme | string | Communication protocol <ul style="list-style-type: none"> ▪ http ▪ https ▪ sdlauncher (This is set if Storage Navigator is used.) |
| hostname | string | Host name of the server running the product |
| port | int | Port number of the product |
| baseUri | string | Base URI of the product |
| loginScreenUri | string | URI of the login screen for the product |
| licenseRegistrationScreenUri | string | URI of the license registration screen for the product |
| authorizationManagementScreenUri | string | URI of the authorization management screen for the product |
| clientConfigurationUri | string | URI of the configuration screen for the product |
| oidcEnabled | boolean | Whether single sign-on can be used <ul style="list-style-type: none"> ▪ true: Can be used. ▪ false: Cannot be used. |
| oidcRedirectUris | string[] | Redirect URI |
| internalVersion | int | Internal version of the product |

| Attribute | Type | Description |
|---------------------|---------|--|
| statusCheckDisabled | boolean | Whether to use Common Services to check the product's heartbeat <ul style="list-style-type: none"> ▪ <code>true</code>: Do not check the product's heartbeat. ▪ <code>false</code>: Check the product's heartbeat. |
| attributes | object | Information about the attributes of storage systems managed by Storage Navigator or VSP One Block Administrator |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/app/v1/application-services/8a11a1bf6d7012db016dd878c5e50001" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting license information for a specific product linked with Common Services

The following request gets license information for a specific product linked with Common Services.

Execution permission

None.

Request line

```
GET base-URL/app/v1/application-services/object-ID-of-the-product/license
```

Request message

Object ID of the product

Specify the value of `id` acquired by using the request for getting information about the products linked with Common Services.

| Attribute | Type | Description |
|-----------|--------|-------------------------------------|
| id | string | (Required) Object ID of the product |

Query parameters

None.

Body

None.

Response message**Body**

```
{
  "status" : "NOT_ACTIVATED"
}
```

| Attribute | Type | Description |
|-----------|--------|--|
| status | string | Status of the license <ul style="list-style-type: none"> ▪ NOT_ACTIVATED: A license is not set up. ▪ ACTIVATED: A license has been set up. ▪ ACTIVATED_WITH_ISSUES: There is a problem with the license that was set. (Possible reasons include the license being expired or the license capacity being exceeded.) ▪ UNKNOWN: The license status is unknown. |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/app/v1/application-services/8a11a1bf6d7012db016dd878c5e50001/license" -H "Authorization:Bearer eyJhbxxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting status information for a specific product linked with Common Services

The following request gets status information for a specific product linked with Common Services.

Execution permission

None.

Request line

```
GET base-URL/app/v1/application-services/object-ID-of-the-product/status
```

Request message

Object ID of the product

Specify the value of `id` acquired by using the request for getting information about the products linked with Common Services.

| Attribute | Type | Description |
|-----------|--------|-------------------------------------|
| id | string | (Required) Object ID of the product |

Query parameters

None.

Body

None.

Response message

Body

```
{
  "connectionStatus" : "ONLINE",
  "trustRelationshipStatus" : "ESTABLISHED"
}
```

| Attribute | Type | Description |
|------------------|--------|---|
| connectionStatus | string | Status of connection with Common Services <ul style="list-style-type: none"> ▪ ONLINE: Connected ▪ OFFLINE: Not connected |

| Attribute | Type | Description |
|-------------------------|--------|--|
| trustRelationshipStatus | string | <p>Single sign-on status</p> <ul style="list-style-type: none"> ▪ ESTABLISHED: Single sign-on is possible. ▪ NOT_ESTABLISHED: Single sign-on is not possible. ▪ NOT_SUPPORTED: The single sign-on function is not supported. ▪ UNKNOWN: The status of the single sign-on setting is unknown. |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/app/v1/application-services/8a11a1bf6d7012db016dd878c5e50001/status" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting version information for a specific product linked with Common Services

The following request gets version information for a specific product linked with Common Services.

Execution permission

None.

Request line

```
GET base-URL/app/v1/application-services/object-ID-of-the-product/version
```

Request message

Object ID of the product

Specify the value of `id` acquired by using the request for getting information about the products linked with Common Services.

| Attribute | Type | Description |
|-----------|--------|-------------------------------------|
| id | string | (Required) Object ID of the product |

Query parameters

None.

Body

None.

Response message**Body**

```
{
  "displayVersion" : "10.0.1-01",
  "internalVersion" : 1
}
```

| Attribute | Type | Description |
|-----------------|--------|-------------------|
| displayVersion | string | Displayed version |
| internalVersion | int | Internal version |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/app/v1/application-services/8a44f59a6f785e31016f78651c820000/version" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Managing data centers

The following describes the API requests for managing data centers.

Getting a list of data centers

The following request gets a list of data centers.

Execution permission

None.

Request lineGET *base-URL*/app/v1/datacenters**Request message****Object ID**

None.

Query parameters

None.

Body

None.

Response message**Body**

```
[
  {
    "id": "8a11a1bf6d4378d9016d67206ee70005",
    "name": "Bangkok",
    "description": "",
    "attributes": {
      "city": "Bangkok (Krung Thep Maha Nakhon, Thailand)",
      "latitude": "13.7500",
      "longitude": "100.5166"
    }
  },
  {
    "id": "8a11a1bf6d4378d9016d6723704e000a",
    "name": "Tokyo Data Center",
    "description": "",
    "attributes": {
      "city": "Hachioji (Tokyo, Japan)",
      "latitude": "35.6577",
      "longitude": "139.3261"
    }
  }
]
```

| Attribute | Type | Description |
|-----------|--------|------------------------------|
| id | string | Object ID of the data center |

| Attribute | Type | Description |
|-------------|--------|--|
| name | string | Data center name |
| description | string | Description |
| attributes | object | Information about the attributes of the data center Information defined by the user when registering or updating the data center is returned. |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/app/v1/datacenters" -H
"Authorization:Bearer eyJhbxxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting information about a specific data center

The following request gets information about a specific data center.

Execution permission

None.

Request line

```
GET base-URL/app/v1/datacenters/object-ID-of-the-data-center
```

Request message

Object ID of the data center

Specify the value of `id` acquired by using the request for getting information about a list of data centers.

| Attribute | Type | Description |
|-----------|--------|---|
| id | string | (Required) Object ID of the data center |

Query parameters

None.

Body

None.

Response message**Body**

```
{
  "id": "8a11a1bf6d4378d9016d6723704e000a",
  "name": "Tokyo Data Center",
  "description": "",
  "attributes": {
    "city": "Hachioji (Tokyo, Japan)",
    "latitude": "35.6577",
    "longitude": "139.3261"
  }
}
```

| Attribute | Type | Description |
|-------------|--------|--|
| id | string | Object ID of the data center |
| name | string | Data center name |
| description | string | Description |
| attributes | object | Information about the attributes of the data center Information defined by the user when registering or updating the data center is returned. |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/app/v1/datacenters/8a11a1bf6d4378d9016d6723704e000a" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Getting a list of products registered in a specific data center

The following request gets a list of products registered in a specific data center.

Execution permission

None.

Request line

```
GET base-URL/app/v1/datacenters/object-ID-of-the-data-center/application-services
```

Request message

Object ID of the data center

Specify the value of `id` acquired by using the request for getting information about a list of data centers.

| Attribute | Type | Description |
|-----------------|--------|---|
| <code>id</code> | string | (Required) Object ID of the data center |

Query parameters

None.

Body

None.

Response message

Body

```
[
  {
    "id": "8a11a1bf6d7012db016dd878c5e50001",
    "type": "AUTOMATOR",
    "displayType": "Hitachi Ops Center Automator",
    "abbreviatedDisplayType": "Automator",
    "name": "example.com",
    "description": "",
    "scheme": "https",
    "hostname": "example.com",
    "port": 22016,
    "baseUri": "https://example.com:22016/Automation",
    "loginScreenUri": "https://example.com:22016/Automation/login",
    "licenseRegistrationScreenUri": "https://example.com:22016/Automation/
license.htm",
    "authorizationManagementScreenUri": "https://example.com:22016/
```

```
Automation/main.htm?module=administrations",
  "clientConfigurationUri": "https://example.com:22016/Automation/v1/
application/ClientConfigurations",
  "oidcEnabled": true,
  "oidcRedirectUris": [
    "https://example.com:22016/Automation/callback"
  ],
  "internalVersion": 1,
  "statusCheckDisabled": false
},
{
  "id": "3c6be9db-41b0-4fce-a38d-413f0c5b101a",
  "type": "STORAGE_NAVIGATOR",
  "displayType": "Hitachi Device Manager Storage Navigator",
  "abbreviatedDisplayType": "Storage Navigator",
  "name": "SN",
  "description": "description",
  "scheme": "sdlauncher",
  "hostname": "localhost",
  "port": 8082,
  "baseUri": "sdlauncher://localhost:8082",
  "loginScreenUri": "sdlauncher://localhost:8082/dev/storage/
xxxxxxxxxxxx/index.do",
  "licenseRegistrationScreenUri": "",
  "authorizationManagementScreenUri": "",
  "clientConfigurationUri": "",
  "oidcEnabled": false,
  "oidcRedirectUris": [],
  "internalVersion": 1,
  "statusCheckDisabled": true,
  "attributes": {
    "serial": "8901234",
    "model": "VSP 5600"
  }
},
{
  "id": "3fb742cd-f888-48ba-99e5-aad089c61753",
  "type": "VSP_ONE_BLOCK_ADMINISTRATOR",
  "displayType": "VSP One Block Administrator",
  "abbreviatedDisplayType": "VSP One Block Administrator",
  "name": "Salamander plus",
  "description": "description",
  "scheme": "https",
  "hostname": "localhost",
  "port": 443,
  "baseUri": "https://localhost:443",
  "loginScreenUri": "https://localhost/",
  "licenseRegistrationScreenUri": "",
  "authorizationManagementScreenUri": ""
}
```

```

    "clientConfigurationUri": "",
    "oidcEnabled": false,
    "oidcRedirectUris": [],
    "internalVersion": 1,
    "statusCheckDisabled": true,
    "attributes": {
      "serial": "1234567",
      "model": "VSP One B28"
    }
  ]

```

| Attribute | Type | Description |
|----------------------------------|--------|--|
| id | string | Object ID of the product |
| type | string | Product type |
| displayType | string | Display type |
| abbreviatedDisplayType | string | Product abbreviation |
| name | string | Product name |
| description | string | Description of the product |
| scheme | string | Communication protocol <ul style="list-style-type: none"> ▪ http ▪ https ▪ sdlauncher (This is set if Storage Navigator is used.) |
| hostname | string | Host name of the server running the product |
| port | int | Port number of the product |
| baseUri | string | Base URI of the product |
| loginScreenUri | string | URI of the login screen for the product |
| licenseRegistrationScreenUri | string | URI of the license registration screen for the product |
| authorizationManagementScreenUri | string | URI of the authorization management screen for the product |
| clientConfigurationUri | string | URI of the configuration screen for the product |

| Attribute | Type | Description |
|---------------------|----------|--|
| oidcEnabled | boolean | Whether single sign-on can be used <ul style="list-style-type: none"> ▪ <code>true</code>: Can be used. ▪ <code>false</code>: Cannot be used. |
| oidcRedirectUri | string[] | Redirect URI |
| internalVersion | int | Internal version of the product |
| statusCheckDisabled | boolean | Whether to use Common Services to check the product's heartbeat <ul style="list-style-type: none"> ▪ <code>true</code>: Do not check the product's heartbeat. ▪ <code>false</code>: Check the product's heartbeat. |
| attributes | object | Information about the attributes of storage systems managed by Storage Navigator or VSP One Block Administrator |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/app/v1/datacenters/8a11a1bf6d4378d9016d67206ee70005/application-services" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Registering a data center

The following request registers a data center.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
POST base-URL/app/v1/datacenters
```

Request message**Object ID**

None.

Query parameters

None.

Body

```
{
  "name": "Yokohama",
  "description": "Data center of Yokohama city",
  "attributes": {
    "city": "Yokohama (Kanagawa, Japan)",
    "latitude": "35.3200",
    "longitude": "139.5800"
  }
}
```

| Parameter | Type | Description |
|-------------|--------|--|
| name | string | (Required) Data center name You cannot use the following characters: / \ ^ \$. * + ? () [] { } You cannot specify space character at the start or end. |
| description | string | (Optional) Description |
| attributes | object | (Optional) Information about the attributes of the data center You can define a pair of any key and any value as a map. |

Response message**Body**

None.

Coding example

```
curl -v -X POST -H "Content-Type:application/json" -s "https://example.com:443/portal/app/v1/datacenters" -d @./request.json -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Updating the registered information for a data center

The following request updates the registered information for a data center.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
PUT base-URL/app/v1/datacenters/object-ID-of-the-data-center
```

Request message

Object ID of the data center

Specify the value of `id` acquired by using the request for getting information about a list of data centers.

| Attribute | Type | Description |
|-----------------|--------|---|
| <code>id</code> | string | (Required) Object ID of the data center |

Query parameters

None.

Body

```
{
  "id": "8a11a1bf6f1c0a95016f8d41c4d7000a",
  "name": "Yokohama",
  "description": "Data center of Yokohama city",
  "attributes": {
    "city": "Yokohama (Kanagawa, Japan)",
    "latitude": "35.3200",
    "longitude": "139.5800"
  }
}
```

| Parameter | Type | Description |
|-----------------|--------|---|
| <code>id</code> | string | (Required) Object ID of the data center |

| Parameter | Type | Description |
|--------------------------|--------|---|
| | | Specify the value of <code>id</code> acquired by using the request for getting information about a list of data centers. |
| <code>name</code> | string | (Optional) Data center name You cannot use the following characters: <code>/ \ ^ \$. * + ? () [] { } </code> You cannot specify space character at the start or end. |
| <code>description</code> | string | (Optional) Description |
| <code>attributes</code> | object | (Optional) Information about the attributes of the data center You can define a pair of any key and any value as a map. |

Response message

Body

None.

Coding example

```
curl -v -X PUT -H "Content-Type:application/json" -s "https://example.com:443/portal/app/v1/datacenters/8a11a1bf6f1c0a95016f8d41c4d7000a" -d @./request.json -H "Authorization:Bearer eyJhbxxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Registering a product linked with Common Services in a data center

The following request registers a product linked with Common Services in a data center.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
PUT base-URL/app/v1/datacenters/object-ID-of-the-data-center/application-services/
application-service-ID
```

Request message

Object ID of the data center

Specify the value of `id` acquired by using the request for getting information about a list of data centers.

| Attribute | Type | Description |
|-----------------|--------|---|
| <code>id</code> | string | (Required) Object ID of the data center |

Application service ID

Specify the value of `id` acquired by using the request for getting information about a list of products linked with Common Services.

| Attribute | Type | Description |
|-------------------------------------|--------|-------------------------------------|
| <code>application-service-id</code> | string | (Required) Object ID of the product |

Query parameters

None.

Body

None.

Response message

Body

None.

Coding example

```
curl -v -X PUT -s "https://example.com:443/portal/app/v1/datacenters/
8a44f59a6f785e31016f7957f7db0005/application-services/
8a44f59a6f785e31016f78651c820000" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Deleting a product linked with Common Services from a data center

The following request deletes a product linked with Common Services from a data center.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
DELETE base-URL/app/v1/datacenters/object-ID-of-the-data-center/application-services/
application-service-ID
```

Request message

Object ID of the data center

Specify the value of `id` acquired by using the request for getting information about a list of data centers.

| Attribute | Type | Description |
|-----------------|--------|---|
| <code>id</code> | string | (Required) Object ID of the data center |

Application service ID

Specify the value of `id` acquired by using the request for getting information about a list of products linked with Common Services.

| Attribute | Type | Description |
|-------------------------------------|--------|-------------------------------------|
| <code>application-service-id</code> | string | (Required) Object ID of the product |

Query parameters

None.

Body

None.

Response message

Body

None.

Coding example

```
curl -v -X DELETE -s "https://example.com:443/portal/app/v1/datacenters/
8a44f59a6f785e31016f7957f7db0005/application-services/
8a44f59a6f785e31016f78651c820000" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Deleting a data center

The following request deletes a registered data center.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
DELETE base-URL/app/v1/datacenters/object-ID-of-the-data-center
```

Request message

Object ID of the data center

Specify the value of `id` acquired by using the request for getting information about a list of data centers.

| Attribute | Type | Description |
|-----------------|--------|---|
| <code>id</code> | string | (Required) Object ID of the data center |

Query parameters

None.

Body

None.

Response message

Body

None.

Coding example

```
curl -v -X DELETE -s "https://example.com:443/portal/app/v1/datacenters/8a44f59a6f7d6b59016f7ee8cc210001" -H "Authorization:Bearer eyJhbxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Managing the Common Services system information

The following describes the API requests for managing the Common Services system information.

Getting the Common Services version information

The following requests gets information about the Common Services version.

Execution permission

None.

Request line

```
GET base-URL/system/v1/version
```

Request message

Object ID

None.

Query parameters

None.

Body

None.

Response message

Body

```
{
  "version" : "10.1.0",
  "build" : "20191218163524"
}
```

| Attribute | Type | Description |
|-----------|--------|-----------------|
| version | string | Product version |
| build | string | Build version |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/system/v1/version" -H
"Authorization:Bearer eyJhbxxxx"
```




Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Session management

The API described here is related to session management.

Obtaining the settings information for session idle timeouts

You can obtain the settings information for session idle timeouts.

Execution permission

You must be a system administrator or a security administrator.

Request line

```
GET base-URL/security/v1/session-settings
```

Request message

Object ID

None.

Query parameters

None.

Body

None.

Response message

Body

```
{
  "idleTimeout": 1200
  "autoRefreshWithoutTimeout": true
}
```

| Attribute | Type | Description |
|-------------|------|-----------------------------------|
| idleTimeout | int | The idle timeout period (seconds) |

| Attribute | Type | Description |
|---------------------------|---------|--|
| autoRefreshWithoutTimeout | boolean | Whether a timeout occurs for windows that support automatic refresh. <ul style="list-style-type: none"> ▪ true: Timeout does not occur. ▪ false: Timeout occurs. |

Coding example

```
curl -v -X GET -s "https://example.com:443/portal/security/v1/session-settings" -H
"Authorization:Bearer eyJhbxxxx"
```



Tip: Because this request uses SSL communication, you must either run the `curl` command with the root certificate of the Common Services server certificate specified for the `--cacert` option, or run the command with the `-k` option specified. (The `-k` option runs the command by ignoring SSL errors.)

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA



HitachiVantara.com/contact