

# Hitachi Content Platform for Cloud Scale

v2.6

---

## Management API Reference

This document describes the object storage management REST API methods available in the Hitachi Content Platform for cloud scale (HCP for cloud scale) software.

© 2020, 2022 Hitachi Vantara LLC. 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](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, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, Lotus, MVS, OS/390, PowerHA, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, 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> or [https://knowledge.hitachivantara.com/Documents/Open\\_Source\\_Software](https://knowledge.hitachivantara.com/Documents/Open_Source_Software).

**EXPORT CONTROLS** - Licensee will comply fully with all applicable export laws and regulations of the United States and other countries, and Licensee shall not export, or allow the export or re-export of, the Software, API or Materials in violation of any such laws or regulations. By downloading or using the Software, API, or Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any embargoed or restricted country.

---

# Contents

<b>Preface.....</b>	<b>5</b>
About this document.....	5
Intended audience.....	5
Product version.....	5
Release notes.....	5
Related documents.....	5
Document conventions.....	6
Accessing product documentation.....	7
Getting help.....	8
Comments.....	8
<b>Chapter 1: Introducing Hitachi Content Platform for cloud scale.....</b>	<b>9</b>
Getting started with the management APIs.....	9
Input and output formats.....	10
Access and authentication.....	10
Requesting and submitting a CSRF token.....	12
Get CSRF token.....	13
Viewing and using MAPI methods.....	13
Including XSRF tokens in MAPI Swagger requests.....	14
HTTP status response codes.....	15
<b>Chapter 2: Storage component management methods.....</b>	<b>19</b>
Activate storage components.....	19
Configure S3 settings.....	22
Get S3 settings.....	24
Get S3 message queue count.....	26
Set S3 message queue count.....	27
Configure storage component.....	28
Get storage component capacity.....	36
List storage component alerts.....	38
List storage components.....	39
Patch storage component configuration.....	44
Set storage component state.....	51
Test storage component access.....	56
Update storage component configuration.....	59

<b>Chapter 3: Encryption management methods.....</b>	<b>67</b>
Add KMS server.....	67
Delete KMS server.....	71
Get encryption state.....	72
Get KMS server.....	73
List KMS servers.....	75
Promote KMS server.....	78
Rekey.....	80
Set encryption state.....	81
Update KMS server.....	83
Unseal.....	86
Migrate an internal KMS.....	88
<b>Chapter 4: Administrative management methods.....</b>	<b>94</b>
Add license.....	94
Get serial number.....	95
Get system chargeback report.....	96
Get system events.....	99
Get user chargeback report.....	101
List licenses.....	104
Refresh client certificates.....	106
Set serial number.....	107
<b>Chapter 5: User management methods.....</b>	<b>109</b>
Generate S3 user credentials.....	109
List users.....	110
List user buckets.....	112
Revoke OAuth user tokens.....	114
Revoke S3 user credentials.....	116
<b>Chapter 6: Public methods.....</b>	<b>118</b>
Get service port.....	118

---

# Preface

## About this document

This document describes the object storage management REST API methods available in the Hitachi Content Platform for cloud scale (HCP for cloud scale) software.

## Intended audience

This document is intended for people who are managing or administering HCP for cloud scale systems. It assumes you have experience with APIs and some experience writing scripts that issue API methods.

## Product version

This document applies to v2.6 of Hitachi Content Platform for cloud scale.

## 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 Support Website: <https://knowledge.hitachivantara.com/Documents>.

## Related documents

The following list describes documents containing information about v2.6 of HCP for cloud scale. You should have these documents available before using the product. Refer to the latest version of the *Hitachi Content Platform for Cloud Scale Release Notes* for information on document version numbers.

- *Hitachi Content Platform for Cloud Scale Release Notes* (RN-HCPCS004): This document is for customers and describes new features, product documentation, and resolved and known issues, and gives other useful information about this release of the product.
- *Installing Hitachi Content Platform for Cloud Scale* (MK-HCPCS002): This document gives you the information required to install or update the HCP for cloud scale software.

- *Hitachi Content Platform for Cloud Scale Administration Guide (MK-HCPCS008)*: This document explains how to use the HCP for cloud scale Object Storage Management and System Management applications to configure and operate a common object storage interface for clients to interact with; configure HCP for cloud scale for users; enable and disable system features; and monitor the system and its connections.
- *Hitachi Content Platform for Cloud Scale S3 Console Guide (MK-HCPCS009)*: This document is for end users and explains how to use the HCP for cloud scale S3 Console application to use S3 credentials and to simplify the process of creating, monitoring, and maintaining S3 buckets and the objects they contain.
- *Hitachi Content Platform for Cloud Scale Management API Reference (MK-HCPCS007)*: This document is for customers and describes the object storage management application programming interface (API) methods available for customer use.







## Document conventions

This document uses the following typographic conventions:

Convention	Description
<b>Bold</b>	<ul style="list-style-type: none"> <li>▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click <b>OK</b>.</li> <li>▪ Indicates emphasized words in list items.</li> </ul>
<i>Italic</i>	<ul style="list-style-type: none"> <li>▪ Indicates a document title or emphasized words in text.</li> <li>▪ 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></li> </ul> <p>(For exceptions to this convention for variables, see the entry for angle brackets.)</p>
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"> <li>▪ Variables are not clearly separated from the surrounding text or from other variables. Example: <pre>Status-&lt;report-name&gt;&lt;file-version&gt;.csv</pre></li> <li>▪ Variables in headings.</li> </ul>
[ ] square brackets	Indicates optional values. Example: [ a   b ] indicates that you can choose a, b, or nothing.

Convention	Description
{ } 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://knowledge.hitachivantara.com/Documents>. 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/en_us/contact-us.html) 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](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](https://community.hitachivantara.com), register, and complete your profile.

## Comments

Please send comments to [doc.comments@hitachivantara.com](mailto: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: Introducing Hitachi Content Platform for cloud scale

Hitachi Content Platform for cloud scale (HCP for cloud scale) is a software-defined object storage solution that is based on a massively parallel microservice architecture and is compatible with the Amazon S3 application programming interface (API).

HCP for cloud scale is especially well suited to service applications requiring high bandwidth and compatibility with the Amazon S3 API.

HCP for cloud scale has the ability to federate S3-compatible storage from virtually any private or public source, and present the combined capacity in a single, centrally managed, global namespace.

You can install HCP for cloud scale on any server, in the cloud or on premise, that supports the minimum requirements.

HCP for cloud scale lets you manage and scale storage components. You can add storage components, monitor their states, and take them online or offline for maintenance and repair. The HCP for cloud scale system includes functions to send notification of alerts, track and monitor throughput and performance, and trace actions through the system.

## Getting started with the management APIs

HCP for cloud scale includes RESTful HTTP management application programming interfaces (APIs) for the Object Storage Management application and the System Management application. These APIs are separate and use separate ports.

### System Management

You can execute all functions supported in the System Management application using MAPI methods. The System Management methods are served by the Admin service from any HCP for cloud scale node.

All URLs for the System Management MAPI methods have the following base, or root, uniform resource identifier (URI):

```
https://hcpcs_cluster:8000/api/admin/
```

The System Management MAPI is described in Swagger, available from the System Management user interface. Those methods are not described in this document.

## Object Storage Management

You can execute all functions supported in the Object Storage Management application and the S3 Console application using MAPI methods. The Object Storage Management management API (MAPI) supports management of the following:

- Storage components and Amazon Simple Storage Service (Amazon S3) settings
- Storage component encryption
- KMIP (Key Management Interoperability Protocol) servers
- Administrative resources such as serial numbers and system events
- User resources such as S3 user credentials and OAuth tokens
- Public information such as available public ports

The Object Storage Management MAPI methods are served by the MAPI Gateway service from any HCP for cloud scale node.

All URLs for the Object Storage Management MAPI methods have the following base, or root, uniform resource identifier (URI):

```
https://hcpcs_cluster:9099/mapi/v1/
```

The Object Storage Management MAPI is described in the *Management API Reference*. It is also described in Swagger, available from the Object Storage Management user interface.

## Input and output formats

The API accepts and returns JSON.

The REST API accepts and returns JavaScript Object Notation (JSON). It does not support HTTPS 1.0 requests; all HTTPS 1.0 requests are denied. When the body of the request has contents, the MAPI accepts and returns JSON; when the body is empty, JSON format is unnecessary.

## Access and authentication

To use the Object Storage Management or System Management MAPIs, you need a user account that has permission to perform the actions you want.

### Requesting an access token

After you have a user account, you must request an authentication token from the system. To do this, you send an HTTP POST request to the method `/auth/oauth`.

When you generate a new access token, a refresh token also gets generated automatically.

Here's an example using the cURL command-line tool:

```
curl -ik -X POST https://mysystem.example.com:8000/auth/oauth/ \
-d grant_type=password \
-d username=user1 \
```

```
-d password=password1 \
-d scope=* \
-d client_secret=my-secret \
-d client_id=my-client \
-d realm=marketingUsers
```

In response to this request, you receive a JSON response body containing an `access_token` field. The value for this field is the token. For example:

```
{
  "access_token": "eyJr287bjle..."
  "expires_in": 7200
}
```



#### Note:

- To get a list of security realms for the system, send an HTTP GET request to the method `/setup`. For example, to do this with cURL:

```
curl -k -X GET --header 'Accept: application/json' \
'https://mysystem.example.com:8000/api/admin/setup'
```

- To get an access token for the local admin user account, you can omit the realm option for the request, or specify a realm value of Local.

### Submitting the access token

You must specify the access token as part of all REST API requests that you make. You do this by submitting an Authorization header along with the request. Here's an example that uses cURL:

```
curl -X GET --header "Accept:application/json" \
https://mysystem.example.com:8000/api/admin/instances \
--header "Authorization: Bearer eyJr287bjle..."
```

### Changing a password

You can use the MAPI to change the system's password using the following cURL commands, where `$1=server_name`, `$2=current_password`, and `$3=new_password`:

```
TOKEN=$(curl -ik -X POST https://$1.mysystem.com:8000/auth/oauth/ \
-d grant_type=password -d username=admin -d password=$2 \
-d scope=* -d client_secret=client-secret -d client_id=client-id \
-d realm=local 2>&1 | grep access_token | awk -F: '{print $2}' \
| awk -F\" '{print $2}')
```

```
curl -v -X POST --header 'Content-Type: application/json' \
--header "Authorization: Bearer $TOKEN" \
```

```
https://$1.mysystem.com:8000/api/admin/setup/password \
-d '{"password": "'$3''}'
```

## Requesting and submitting a CSRF token

To protect against cross-site-request forgery, the Object Storage Management MAPI requires an XSRF token and a Vert.x web session token in all requests. A MAPI method is provided to return the tokens in cookies for use in subsequent MAPI calls.

The Object Storage Management MAPI requires you to pass the XSRF token in the request header, and the XSRF token and Vert.x web session information as a cookie, within each request. If you do not use the tokens in a request, it will fail with a 401 (invalid) error.



**Tip:** The XSRF token has a limited lifetime, so it's best to obtain a fresh token before issuing every group of requests.

To obtain the token and session information and pass them as part of a request:

### Procedure

1. Use the MAPI method `csrf` to obtain the XSRF token and Vert.x web session information:

```
GET https://10.10.24.195:9099/mapi/v1/csrf
```

The XSRF token is returned as a cookie named `XSRF-TOKEN` and the Vert.x session token is returned as a cookie named `vertx-web.session`.

### Next steps

Use the cookies in subsequent requests.

This example includes a set of commands that does the following:

1. Calls the MAPI method `csrf` and stores the response in a variable named `cookieResponse`
2. Finds the `XSRF-TOKEN` key string in the value stored in `cookieResponse`, extracts the value for that key, and stores it in a variable named `xsrftoken`
3. Finds the `vertx-web.session` key string in the value stored in `cookieResponse`, extracts the value for that key, and stores it in a variable named `vertxsession`
4. Stores the extracted XSRF and Vert.x tokens in a cookie named `cookie`
5. Passes the XSRF token and the cookie as part of a request to obtain S3 authorization, and saves the results in a variable named `token`

```
echo "Generating credentials for ${user}"
cookieResponse=`curl -s -kc - https://${cluster}:9099/mapi/v1/csrf`
xsrftoken=`echo "${cookieResponse}" | grep XSRF-TOKEN | cut -d$'\t' -f 7`
vertxsession=`echo "${cookieResponse}" | grep vertx-web.session | cut -d$'\t' -f 7`
cookie="XSRF-TOKEN=${xsrftoken}; vertx-web.session=${vertxsession}"
token=`curl -s -H "X-XSRF-TOKEN: ${xsrftoken}" -b "${cookie}" \
```

```
-d "grant_type=password&username=${user}&password=password&realm=${realm}" \
http://${cluster}:8889/api/foundry/security/oauth/token | python -mjson.tool \
| grep access_token | cut -d: -f2 | cut -d\" -f2`
```

## Get CSRF token

You can use the method `/csrf` to obtain the XSRF token and Vert.x session token for use in subsequent MAPI calls.

### HTTP request syntax (URI)

```
GET https://host_ip:9099/mapi/v1/csrf
```

### Request structure

Not applicable.

### Response structure

No applicable.

The XSRF token and Vert.x session token are returned in the response header as cookies with the names `XSRF-TOKEN` and `vertx-web.session`, respectively.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
405	Method Not Allowed	The specified HTTP method is not allowed. Resend using GET.

### Example

Request example:

```
GET https://10.10.24.195:9099/mapi/v1/csrf
```

## Viewing and using MAPI methods

Your system features Swagger, where you can view the MAPI methods for both the Object Storage Management and System Management applications, including the request bodies, request URLs, response bodies, and return codes for each. You can also use these pages to run each MAPI method.

You can use Swagger to experiment with the MAPI through the UI with the Try it out button. However, any requests you submit on the page take effect immediately on the system, so it should *only* be used to test methods *outside* of a production environment.



**Note:** If you specify UUIDs when creating resources, the UUIDs are ignored.

To use the MAPI page to run a method:

### Procedure

1. In either the Object Storage Management App or the System Management App, select the user profile icon, in the upper right portion of the page.
2. Select:
  - In the Object Storage Management App, select **REST API**.
  - In the System Management App, select **REST API - Admin**.

A Swagger page opens for the selected MAPI.

3. Expand the category containing the method you want.
4. Select the row for the method you want.
5. To use an Object Storage Management method, enter the XSRF token in the field **X-XSRF-TOKEN Header**.
6. If the method you want needs a UUID:
  - a. Select the row for the `GET` method for the resource type that you want.
  - b. Click **Try it out**.
  - c. In the JSON response body, copy the value in the field `uuid` for the resource that you want.
7. If the method you want needs a request body:
  - a. In the section **Parameters**, under **Model Schema**, click inside the JSON text box. The JSON text is added to the field **Value**.
  - b. Edit the JSON in the field **Value** as needed.



**Note:** Some methods might need other information in addition to or instead of UUIDs or JSON-formatted text. Some methods need particular string values or need you to browse for and select a file to upload.

8. Click **Execute**.  
The method is executed and the results appear in the section **Responses**.

## Including XSRF tokens in MAPI Swagger requests

Swagger does not automatically populate the X-XSRF-TOKEN header when executing Object Storage Management MAPI requests.

To obtain the token within a browser and include it in a MAPI request through Swagger:

**Procedure**

1. From the user profile icon on the top right of an Object Storage Management window, select **REST API**.  
A Swagger page opens in a new tab.
2. Locate and copy the value of the cookie XSRF-TOKEN:
  - In Chrome, from the **Customize** menu (in the upper right corner), select **More tools > Developer tools**. From the **Developer Tools** window select **Storage > Cookies**. Select and copy the value of the cookie XSRF-TOKEN.
  - In Firefox, from the **Open** menu (in the upper right corner), select **Web Developer > Storage Inspector**. From the **Developer Tools** window select **Cookies**. Select and copy the value of the cookie XSRF-TOKEN.
3. Select the management API you want to execute and then click **Try it out**.
4. In the section **X-XSRF-TOKEN**, paste the value of the cookie into the field **X-XSRF-TOKEN Header**.

**Result**

You can now execute the method.

## HTTP status response codes

When an HTTP request is sent to a server, the server sends back an HTTP response message. The HTTP response message consists of an HTTP header and, optionally, a message body. The response header contains an HTTP status code that gives the status of the request.

When an API request fails, the API returns:

- An HTTP status code
- Conditionally, a system-specific error code
- A JSON-formatted error response body

The following table contains a list of HTTP status codes, their descriptions, and the types of HTTP requests that can generate each status code.

Status code	Meaning	Description	Methods
200	OK	The request was executed successfully.	PATCH POST

Status code	Meaning	Description	Methods
400	Bad Request	<p>The request body contains one or more of these:</p> <ul style="list-style-type: none"> <li>▪ An entry that is not valid</li> <li>▪ A value for an entry that is not valid</li> <li>▪ JSON formatting that is not valid</li> </ul> <p>If the request includes a UUID, the UUID might not be validly formatted.</p>	PATCH POST
401	Unauthorized	<p>Your access is not authorized. Possible reasons:</p> <ul style="list-style-type: none"> <li>▪ No credentials are given with the request.</li> <li>▪ The credentials provided with the request are not valid.</li> <li>▪ A CSRF token is missing or not valid.</li> </ul>	PATCH POST
403	Forbidden	You do not have permission to perform the request.	PATCH POST
404	Not Found	The resource you are trying to retrieve, edit, or delete cannot be found.	PATCH POST



Status code	Meaning	Description	Methods
405	Method Not Allowed	A request was made using a request method not supported by that resource; for example, using GET with a form that needs data to be presented using POST.	PATCH POST
409	Conflict	The resource you are trying to create already exists.	POST
500	Internal Server Error	The system experienced an error.	
501	Unimplemented	An API was invoked that HCP for cloud scale doesn't support.	PATCH POST
503	Service Unavailable	The service is not available. Possible reasons: <ul style="list-style-type: none"> <li>An external KMIP system has not been configured.</li> </ul>	POST

### System-specific error codes

Some API requests return system-specific error codes in addition to an HTTP status code. These error codes are listed in the `errorCodes` field in the JSON response body. This table describes these error codes.

Error code	Description
4000	SSL certificate not trusted.

### JSON response body

REST API error responses have this format:

```
{
  "statusCode": <HTTP-status-code>,
  "errorCode": <system-specific-error-code>,
}
```

```
"errorMessage": <message>,  
"errorProperties": [  
  {  
    "name": <error-property>,  
    "message": <error-property-message>  
  }  
]  
}
```

---

## Chapter 2: Storage component management methods

The management API includes storage component management methods.

Before issuing a MAPI call, request and submit a CSRF token.

For information on CSRF tokens refer to [Requesting and submitting a CSRF token \(on page 12\)](#).



**Note:** If you're working with a storage component that is configured with multiple retries and long timeouts, and if the endpoint for the storage component is unreachable, and if as a result you send multiple verification or activation requests to the endpoint, the MAPI Gateway service can become unresponsive.

If the MAPI Gateway service becomes unresponsive, use the System Management Services function Repair on it.

### Activate storage components

When you define a storage component, it is marked as UNVERIFIED and not available to serve requests until you activate it. The method `storage_component/activate` lets you activate a storage component that is in the UNVERIFIED state.

#### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/storage_component/activate
```

#### Request structure

The request body is:

```
{
  "id": "uuid"
}
```

Parameter	Required	Type	Description
id	Yes	UUID	The UUID of the storage component.

**Response structure**

The response body is:

```
{
  "id": "uuid",
  "storageType": "type",
  "verified": true|false,
  "httpStatus": nnn,
  "errorCode": "code_text",
  "errorMessage": "message_text",
  "daysUntilCertificateExpiration": nnn,
  "state": "state"
}
```

Parameter	Type	Description
id	UUID	The UUID of the storage component.
storageType	String	The type of storage component: <ul style="list-style-type: none"> <li>AMAZON_S3: An Amazon Web Services S3-compatible node</li> <li>HCP_S3: A Hitachi Content Platform node</li> <li>HCPS_S3: An HCP S Series Node</li> <li>GENERIC_S3: An S3-compatible node</li> </ul>
verified	Boolean	If <code>true</code> , the storage component has been activated. If <code>false</code> , it is not verified and awaits administrative action.
httpStatus	32-bit integer	The HTTP status code with which the storage component responded to your request. If 0, the storage component can't be reached. You can use other values to diagnose the issue.
errorCode	String	Any error code associated with the storage component.
errorMessage	String	Any error message associated with the storage component.
daysUntilCertificateExpiration	32-bit integer	Number of days until the current HTTPS certificate expires.

Parameter	Type	Description
state	Enum	<p>The state of the storage component, indicating its availability to serve requests:</p> <ul style="list-style-type: none"> <li>▪ <b>ACTIVE</b>: The storage component is ready for requests.</li> <li>▪ <b>INACTIVE</b>: The storage component is on an administrative pause.</li> <li>▪ <b>INACCESSIBLE</b>: The storage component is not accessible. This condition can be caused by network, authentication, or certificate errors.</li> <li>▪ <b>UNVERIFIED</b>: The storage component has not been activated or has failed to activate.</li> </ul>

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The MAPI metadata ID is not valid.
401	Unauthorized	Access was denied because credentials are not valid.
404	Not Found	The specified storage component does not exist.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/activate
```

JSON request:

```
{
  "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6"
}
```

JSON response:

```
{
  "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
  "storageType": "AMAZON_S3",
  "verified": true,
  "httpStatus": 200,
  "errorCode": null,
  "errorMessage": null,
  "daysUntilCertificateExpiration": 364,
  "state": "ACTIVE"
}
```

## Configure S3 settings

You can configure custom S3 settings for buckets. You can use the method `/s3_settings/set` to configure settings, then use the method `/s3_settings/get` to verify them.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/s3_settings/set
```

### Request structure

The request body is:

```
{
  "maxFileSizeBytes": nnnnnnnnnn,
  "maxBucketsPerUser": buckets,
  "maxBulkDeleteRequestSizeBytes": size,
  "maxBulkDeleteRequestSizeCount": count
}
```

Parameter	Required	Type	Description
maxFileSizeBytes	No	Integer	The maximum size, in bytes, of a single object that can be uploaded to an HCP for cloud scale system. Limit: 5 GB, default: 5 GB.

Parameter	Required	Type	Description
maxBucketsPerUser	No	Integer	The maximum number of buckets that a single user can create and own. Limit: 1000 buckets, default: 100 buckets.
maxBulkDeleteRequestSize Bytes	No	Integer	The maximum, total size of objects, in bytes, allowed in a single bulk deletion. Default: 3 MB.
maxBulkDeleteRequestSize Count	No	Integer	The maximum, total number of objects allowed in a single bulk deletion. Default: 1000 objects.

### Response structure

The response returns the same parameters as the request. The response body structure is:

```
{
  "maxFileSizeBytes": ,
  "maxBucketsPerUser": ,
  "maxBulkDeleteRequestSizeBytes": ,
  "maxBulkDeleteRequestSizeCount":
}
```

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3_settings/set
```

JSON request:

```
{
  "maxBucketsPerUser": 1000
}
```

JSON response:

```
{
  "maxFileSizeBytes": 1099511627776,
  "maxBucketsPerUser": 1000,
  "maxBulkDeleteRequestSizeBytes": 3145728,
  "maxBulkDeleteRequestSizeCount": 1000
}
```

## Get S3 settings

You can retrieve the current S3 settings. You can use the method `/s3_settings/set` to configure settings, then use the method `/s3_settings/get` to verify them.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/s3_settings/get
```

### Request structure

Not applicable.

### Response structure

The response body is:

```
{
  "maxFileSizeBytes": nnnnnnnnnn,
  "maxBucketsPerUser": buckets,
  "maxBulkDeleteRequestSizeBytes": size,
  "maxBulkDeleteRequestSizeCount": count
}
```

Parameter	Required	Type	Description
maxFileSizeBytes	No	Integer	The maximum size, in bytes, of a single object that can be uploaded to an HCP for cloud scale system. Limit: 5 GB, default: 5 GB.



Parameter	Required	Type	Description
maxBucketsPerUser	No	Integer	The maximum number of buckets that a single user can create and own. Limit: 1000 buckets, default: 100 buckets.
maxBulkDeleteRequestSize Bytes	No	Integer	The maximum, total size of objects, in bytes, allowed in a single bulk deletion. Default: 3 MB.
maxBulkDeleteRequestSize Count	No	Integer	The maximum, total number of objects allowed in a single bulk deletion. Default: 1000 objects.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3_settings/get
```

JSON response:

```
{
  "maxFileSizeBytes": 4294967296,
  "maxBucketsPerUser": 100,
  "maxBulkDeleteRequestSizeBytes": 3145728,
  "maxBulkDeleteRequestSizeCount": 1000
}
```

## Get S3 message queue count

The S3 Gateway method `getS3MessageQueueCounts` displays the number of each type of S3 message queue: S3All, S3Notification, S3MirrorOut, and S3MirrorIn.

### HTTP request syntax (URI)

```
POST http://host:9750/components/schemas/MAPIS3MessageQueueCounts
```

### Request structure

The request body is:

```
content:
  '*/*':
    schema:
      $ref: '#/components/schemas/MAPIS3MessageQueueCounts'
    required: true
```

### Response structure

Not applicable.

Parameter	Required	Type	Description
s3AllQueueCount	No	Integer	The number of S3 All message queues.
s3NotificationQueueCount	No	Integer	The number of S3 Notification message queues.
s3MirrorOutQueueCount	No	Integer	The number of S3 MirrorOut message queues.
s3MirrorInQueueCount	No	Integer	The number of S3 MirrorIn message queues.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Invalid	Access was denied because the method is not valid.

Status code	HTTP name	Description
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

## Set S3 message queue count

The S3 Gateway method `setS3MessageQueueCount` sets the number of each type of S3 message queue: S3All, S3Notification, S3MirrorOut, and S3MirrorIn. The call must supply all values.

### HTTP request syntax (URI)

```
POST http://host:9750/components/schemas/MAPIS3MessageQueueCounts
```

### Request structure

The request body is:

```
content:
  /**:
  schema:
    $ref: '#/components/schemas/MAPIS3MessageQueueCounts'
  required: true
```

### Response structure

Not applicable.

Parameter	Required	Type	Description
s3AllQueueCount	Yes	Integer	The number of S3 All message queues.
s3NotificationQueueCount	Yes	Integer	The number of S3 Notification message queues.
s3MirrorOutQueueCount	Yes	Integer	The number of S3 MirrorOut message queues.

Parameter	Required	Type	Description
s3MirrorInQueueCount	Yes	Integer	The number of S3 MirrorIn message queues.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Invalid	Access was denied because the method is not valid.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

## Configure storage component

You can configure a storage component, which exposes the S3 buckets for storage of data on various storage back-end systems. Buckets must already be created on the storage component before you can configure it. Ensure that the buckets are empty.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/storage_component/create
```

### Request structure

The request body is:

```
{
  "storageType": "type",
  "storageComponentConfig": {
    "label": "[label]",
    "host": "url",
    "https": {true|false},
    "port": [nnnnn],
    "bucket": "bucket_name",
```

```

"region": "[region_name]",
"authType": "[V2|V4]",
"siteAffiliation": {
  "id": "uuid"
},
"accessKey": "key",
"secretKey": "key",
"useProxy": [true|false],
"proxyHost": "[host_name]",
"proxyPort": [nnnnn],
"proxyUserName": "[user_name]",
"proxyPassword": "[password]",
"proxyDomain": "[domain_name]",
"usePathStyleAlways": [true|false],
"connectionTimeout": [ms],
"socketTimeout": [ms],
"connectionTTL": [ms],
"maxConnections": [nnnnnnn],
"userAgentPrefix": "[prefix]",
"socketSendBufferSizeHint": [nnnnnnn],
"socketRecvBufferSizeHint": [nnnnnnn],
"managementProtocol": [http|https],
"managementHost": "[host_name]",
"managementUser": "[user_name]",
"managementPassword": "[password]",
"activateNow": [true|false]
}
}

```

Parameter	Required	Type	Description
storageType	Yes	String	The type of storage component: <ul style="list-style-type: none"> <li>AMAZON_S3: An Amazon Web Services S3-compatible node</li> <li>HCP_S3: A Hitachi Content Platform node</li> <li>HCPS_S3: An HCP S Series Node</li> <li>GENERIC_S3: An S3-compatible node</li> </ul>
storageComponent Config	Yes	List	The following storage component configuration values:
label	No	String	The name of the storage component.
host	Yes	String	The URL of the storage component back-end host domain.

Parameter	Required	Type	Description
https	Yes	Boolean	If <code>true</code> , use an HTTPS connection to the back-end system. If <code>false</code> , use an HTTP connection. Default: <code>false</code> .
port	No	Integer	HTTP port of back-end system.
bucket	Yes	String	Name of the bucket. The bucket must already exist.
region	No	String	The S3 region. Default: <code>us-east-1</code> .
authType	No	String	The AWS Signature Version for authenticating all interactions with Amazon S3: <ul style="list-style-type: none"> <li>▪ <code>v2</code></li> <li>▪ <code>v4</code></li> </ul> Default: <code>v4</code> .
siteAffiliation	Yes	UUID	For <code>id</code> , the UUID representing the storage component or the user.
accessKey	Yes		Access key of the S3 credentials for access to the bucket.
secretKey	Yes		Secret key of the S3 credentials for access to the bucket.
useProxy	No	Boolean	If <code>true</code> , a proxy server is defined. If <code>false</code> , it is not. If <code>true</code> , then values are required for <code>proxyHost</code> and <code>proxyHost</code> . Default: <code>false</code> .
proxyHost	No	String	The proxy host, if used.
proxyPort	No	Integer	The proxy port number, if used.
proxyUserName	No	String	The proxy domain user name, if used.
proxyPassword	No	String	The proxy domain password, if used.
proxyDomain	No	String	The proxy domain. Not supported.
usePathStyleAlways	No	Boolean	If <code>true</code> , use path-style syntax to send requests to the back-end system. If <code>false</code> , use virtual-hosted style. Default: <code>true</code> .

Parameter	Required	Type	Description
connectionTimeout	No	32-bit integer	The amount of time, in milliseconds, that the HTTP connection waits to establish a connection before timing out. Default: 10000 ms (10 sec).
socketTimeout	No	32-bit integer	The timeout value, in milliseconds, for reading from a connected socket. Default: 5000 ms (5 sec).
connectionTTL	No	64-bit integer	The connection time to live (TTL) for a request. Default: unlimited (the connection never closes).
maxConnections	No	32-bit integer	The maximum number of open HTTP connections to a storage component. If not specified, the defaults are: <ul style="list-style-type: none"> <li>▪ HCPS_S3: <u>1024</u></li> <li>▪ HCP_S3: <u>50</u></li> <li>▪ AMAZON_S3: <u>50</u></li> <li>▪ GENERIC_S3: <u>50</u></li> </ul>
userAgentPrefix	No	String	The HTTP user agent prefix header, used in requests to a storage component.
socketSendBufferSizeHint	No	32-bit integer	The size hint, in bytes, for the low-level TCP send buffer. If specified, you must also specify <code>socketRecvBufferSizeHint</code> .
socketRecvBufferSizeHint	No	32-bit integer	The size hint, in bytes, for the low-level TCP receive buffer. If specified, you must also specify <code>socketSendBufferSizeHint</code> .
managementProtocol	Yes (for HCP S Series Node)	String	Required for an HCP S Series Node storage component; do not provide for other storage component types. The communication protocol for MAPI requests: <ul style="list-style-type: none"> <li>▪ <code>http</code></li> <li>▪ <code>https</code></li> </ul> There is no default; if you use the parameter you must specify a value.

Parameter	Required	Type	Description
managementHost	Yes (for HCP S Series Node)	String	Required for an HCP S Series Node storage component; do not provide for other storage component types. Type the management system IP address or fully qualified domain name.
managementUser	Yes (for HCP S Series Node)	String	Required for an HCP S Series Node storage component; do not provide for other storage component types. The administrative user name credential. The account must have permissions to execute MAPI methods on the storage component.
managementPassword	Yes (for HCP S Series Node)	String	Required for an HCP S Series Node storage component; do not provide for other storage component types. The password credential. The account must have permissions to execute MAPI methods on the storage component.
activateNow	No	Boolean	If <code>true</code> , activate the storage component immediately. If <code>false</code> , do not activate the storage component. Default: <code>true</code> .

### Response structure

The response returns the same parameters as the request with the following additions. The response body structure is:

```
[
  {
    "id": "uuid",
    "storageType": "",
    "storageComponentConfig": {
      "label": "",
      "host": "",
      "https": ,
      "port": ,
      "bucket": "",
      "region": "",
      "authType": "",
      "siteAffiliation": {
        "id": ""
      }
    }
  }
]
```



```

    "useProxy": ,
    "proxyHost": "",
    "proxyPort": ,
    "proxyUserName": "",
    "proxyPassword": "",
    "proxyDomain": "",
    "usePathStyleAlways": ,
    "connectionTimeout": ,
    "socketTimeout": ,
    "connectionTTL": ,
    "maxConnections": ,
    "userAgentPrefix": "",
    "socketSendBufferSizeHint": ,
    "socketRecvBufferSizeHint": ,
    "managementProtocol": ,
    "managementHost": ,
    "readOnly": ,
    "state": "state"
  }
}
]

```

Parameter	Type	Description
id	UUID	The ID of the storage component.
state	Enum	<p>The state of the storage component, indicating its availability to serve requests:</p> <ul style="list-style-type: none"> <li>▪ <b>ACTIVE:</b> The storage component is ready for requests.</li> <li>▪ <b>INACTIVE:</b> The storage component is on an administrative pause.</li> <li>▪ <b>INACCESSIBLE:</b> The storage component is not accessible. This condition can be caused by network, authentication, or certificate errors.</li> <li>▪ <b>UNVERIFIED:</b> The storage component has not been activated or has failed to activate.</li> </ul>

**Return codes**

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component or parameter.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/create
```

JSON request:

```
{
  "storageType": "AMAZON_S3",
  "storageComponentConfig": {
    "label": "Cloud AWS Bucket",
    "host": "URL of an existing storage component backend",
    "https": true,
    "port": 0,
    "bucket": "string",
    "region": "string",
    "authType": "v2",
    "siteAffiliation": {
      "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6"
    },
    "accessKey": "string",
    "secretKey": "string",
    "useProxy": true,
    "proxyHost": "string",
    "proxyPort": null,
    "proxyUserName": "string",
    "proxyPassword": "string",
    "proxyDomain": "string",
    "usePathStyleAlways": true,
    "connectionTimeout": null,
  }
}
```

```

"socketTimeout": null,
"connectionTTL": null,
"maxConnections": null,
"userAgentPrefix": "string",
"socketSendBufferSizeHint": null,
"socketRecvBufferSizeHint": null,
"activateNow": true
}
}

```

#### JSON response:

```

[
  {
    "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
    "storageType": "AMAZON_S3",
    "storageComponentConfig": {
      "label": "Cloud AWS Bucket",
      "host": "URL of an existing storage component backend",
      "https": true,
      "port": 0,
      "bucket": "string",
      "region": "string",
      "authType": "V2",
      "siteAffiliation": {
        "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6"
      },
      "useProxy": true,
      "proxyHost": "string",
      "proxyPort": 0,
      "proxyUserName": "string",
      "proxyPassword": "string",
      "proxyDomain": "string",
      "usePathStyleAlways": true,
      "connectionTimeout": 0,
      "socketTimeout": 0,
      "connectionTTL": 0,
      "maxConnections": 50,
      "userAgentPrefix": "string",
      "socketSendBufferSizeHint": 0,
      "socketRecvBufferSizeHint": 0,
      "readOnly": true,
      "state": "ACTIVE"
    }
  }
]

```

## Get storage component capacity

The method `storage_component/get_capacity` retrieves capacity information for storage components, and if available the total capacity of the system.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/storage_component/get_capacity
```

### Request structure

Not applicable.

### Response structure

The response body is:

```
[
  {
    "storageCapacities": {
      "uuid": {
        "availableBytes": nnnnn,
        "totalBytes": nnnnn,
        "usedBytes": nnnnn,
        "warnThreshold": nnnnn
      },
      .
      .
      .
      "aggregate": {
        "availableBytes": nnnnn,
        "totalBytes": nnnnn,
        "usedBytes": nnnnn,
        "warnThreshold": nnnnn
      }
    }
  }
]
```

Parameter	Type	Description
id	UUID	The ID of the storage component.
availableBytes	64-bit integer	The available capacity of the storage component in bytes. A returned value of -1 means that the value is not available.

Parameter	Type	Description
totalBytes	64-bit integer	The total capacity of the storage component in bytes. A returned value of -1 means that the value is not available.
usedBytes	64-bit integer	The used capacity of the storage component in bytes. A returned value of -1 means that the value is not available.
warnThreshold	64-bit integer	The threshold for a capacity warning, as compared with the value availableBytes. A returned value of -1 means that the value is not available.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/get_capacity
```

JSON response:

```
[
  {
    "storageCapacities": {
      "494bc750-5f7e-42f3-af7d-64f1024ce2e6": {
        "availableBytes": 1647056204595200,
        "totalBytes": 1993620471152640,
        "usedBytes": 346564266557440,
        "warnThreshold": 598086141345792
      },
      "1954051f-fa79-4e69-bec3-c933bc7dde2a": {
        "availableBytes": -1,
        "totalBytes": -1,
        "usedBytes": -1,
        "warnThreshold": -1
      },
      "aggregate": {
        "availableBytes": -1,
        "totalBytes": -1,

```

```

    "usedBytes": -1,
    "warnThreshold": -1
  }
}
]

```

## List storage component alerts

You can retrieve a list of active storage component alerts. Alerts are triggered by events and remain active until the condition that caused the event is removed. For example, HCP for cloud scale sends an alert when a storage component is unavailable or its certificate is about to expire. When the event is resolved, the alert is cleared.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/alert/list
```

### Request structure

Not applicable.

### Response structure

The response body is:

```

[
  {
    "id": "uuid",
    "timestamp": date_time,
    "category": "STORAGECOMPONENT",
    "description": "alert_description"
  }
  .
  .
  .
]

```

Parameter	Type	Description
id	UUID	The ID of the storage component.
timestamp	64-bit integer	The date and time, in milliseconds since 00:00:00 on 1 January 1970 GMT, when the alert was generated.

Parameter	Type	Description
category	String	Alert category: <ul style="list-style-type: none"> <li>STORAGECOMPONENT</li> </ul>
description	String	The text of the alert.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/alert/list
```

JSON response:

```
[
  {
    "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
    "timestamp": 1571912640205,
    "category": "STORAGECOMPONENT",
    "description": "string"
  }
]
```

## List storage components

The method `storage_component/list` retrieves a list of all storage components created in the HCP for cloud scale system along with their component settings.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/storage_component/list
```

### Request structure

Not applicable.

## Response structure

The response body is:

```
[
  {
    "id": "uuid",
    "storageType": "enum",
    "storageComponentConfig": {
      "label": "label",
      "host": "url",
      "https": true|false,
      "port": nnnnn,
      "bucket": "bucket_name",
      "region": "region_name",
      "authType": "V2|V4",
      "siteAffiliation": {
        "id": "uuid"
      },
      "useProxy": true|false,
      "proxyHost": "host_name",
      "proxyPort": nnnnn,
      "proxyUserName": "user_name",
      "proxyPassword": "password",
      "proxyDomain": "domain_name",
      "usePathStyleAlways": true|false,
      "connectionTimeout": ms,
      "socketTimeout": ms,
      "connectionTTL": ms,
      "maxConnections": nnnnnnn,
      "userAgentPrefix": "prefix",
      "socketSendBufferSizeHint": nnnnnnn,
      "socketRecvBufferSizeHint": nnnnnnn,
      "managementProtocol": http|https,
      "managementHost": "host_name",
      "readOnly": true|false,
      "state": "state"
    }
  }
]
```

Parameter	Type	Description
id	UUID	The ID of the storage component.



Parameter	Type	Description
storageType	Enum	The type of storage component: <ul style="list-style-type: none"> <li>AMAZON_S3: An Amazon Web Services S3-compatible node</li> <li>HCP_S3: A Hitachi Content Platform node</li> <li>HCPS_S3: An HCP S Series Node</li> <li>GENERIC_S3: An S3-compatible node</li> </ul>
storageComponentConfig	List	The following storage component configuration values:
label	String	The name of the storage component.
host	String	The URL of the storage component back-end host domain.
https	Boolean	<code>true</code> for HTTPS connection to back-end system, <code>false</code> for HTTP.
port	32-bit integer	HTTP port to back-end system.
bucket	String	The name of the bucket.
region	String	The S3 region.
authType	String	AWS Signature Version, used for authenticating all interactions with Amazon S3: <ul style="list-style-type: none"> <li>v2</li> <li>v4</li> </ul>
siteAffiliation	UUID	The value of <code>id</code> , a UUID representing the storage component or the user.
useProxy	Boolean	If <code>true</code> , a proxy server is defined. If <code>false</code> , a proxy server is not defined.
proxyHost	String	The proxy host, if used; otherwise, <code>null</code> .
proxyPort	32-bit integer	The proxy port number, if used; otherwise, <code>null</code> .
proxyUserName	String	The proxy domain user name, if used; otherwise, <code>null</code> .
proxyPassword	String	The proxy domain password, if used; otherwise, <code>null</code> .

Parameter	Type	Description
proxyDomain	String	The proxy domain, if used; otherwise, <code>null</code> .
usePathStyleAlways	Boolean	If <code>true</code> , use path-style syntax to send requests to the back-end system; if <code>false</code> , use virtual-hosted style.
connectionTimeout	32-bit integer	The amount of time, in milliseconds, that the HTTP connection waits to establish a connection before timing out.
socketTimeout	32-bit integer	The timeout value for reading from a connected socket.
connectionTTL	64-bit integer	The connection time to live (TTL) for a request.
maxConnections	32-bit integer	The maximum number of open HTTP connections to a storage component.
userAgentPrefix	String	The HTTP user agent prefix header, used in requests to a storage component.
socketSendBufferSizeHint	32-bit integer	The size hint, in bytes, for the low-level TCP send buffer.
socketRecvBufferSizeHint	32-bit integer	The size hint, in bytes, for the low-level TCP receive buffer.
managementProtocol	String	The communication protocol for HCP S Series Node MAPI requests: <ul style="list-style-type: none"> <li>▪ <code>http</code></li> <li>▪ <code>https</code></li> </ul>
managementHost	String	The host managing an HCP S Series Node storage component.
readOnly	Boolean	If <code>true</code> , the storage component is marked as read-only. If <code>false</code> , the storage component is available for reading and writing data.
state	Enum	The state of the storage component, indicating its availability to serve requests: <ul style="list-style-type: none"> <li>▪ <code>ACTIVE</code>: The storage component is ready for requests.</li> <li>▪ <code>INACTIVE</code>: The storage component is on an administrative pause.</li> </ul>

Parameter	Type	Description
		<ul style="list-style-type: none"> <li>INACCESSIBLE: The storage component is not accessible. This can be caused by network, authentication, or certificate errors.</li> <li>UNVERIFIED: The storage component has not been activated or has failed to activate.</li> </ul>

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/list
```

JSON response:

```
[
  {
    "id": "8bff981b-5894-43ce-bd41-5a6f548cc241",
    "storageType": "GENERIC_S3",
    "storageComponentConfig": {
      "label": null,
      "host": "172.19.54.102",
      "https": false,
      "port": 9000,
      "bucket": "samplebucket",
      "region": "us-west-2",
      "authType": null,
      "siteAffiliation": {
        "id": "19b96ae2-38dd-4686-b298-b5bebe173e96"
      }
    }
  }
]
```

```

    "useProxy": false,
    "proxyHost": null,
    "proxyPort": null,
    "proxyUserName": null,
    "proxyPassword": null,
    "proxyDomain": null,
    "usePathStyleAlways": true,
    "connectionTimeout": null,
    "socketTimeout": null,
    "connectionTTL": null,
    "maxConnections": 50,
    "userAgentPrefix": null,
    "socketSendBufferSizeHint": null,
    "socketRecvBufferSizeHint": null,
    "managementProtocol": null,
    "managementHost": null,
    "readOnly": false,
    "state": "ACTIVE"
  }
}
]

```

## Patch storage component configuration

You can update the configuration of specific storage component settings. Use the method `/storage_component/list` to verify existing settings or changes. Use the method `/storage_component/update` to update all settings.

### HTTP request syntax (URI)

```
PATCH https://host_ip:9099/mapi/v1/storage_component/update
```

### Request structure

The full request body is:

```

{
  "id": "uuid",
  "storageType": "type",
  "storageComponentConfig": {
    "label": "[label]",
    "host": "url",
    "https": {true|false},
    "port": [nnnnn],
    "bucket": "bucket_name",
    "region": "[region_name]",
    "authType": "[V2|V4]",
    "siteAffiliation": {

```

```

    "id": "uuid"
  },
  "accessKey": "key",
  "secretKey": "key",
  "useProxy": [true|false],
  "proxyHost": "[host_name]",
  "proxyPort": [nnnnn],
  "proxyUserName": "[user_name]",
  "proxyPassword": "[password]",
  "proxyDomain": "[domain_name]",
  "usePathStyleAlways": [true|false],
  "connectionTimeout": [ms],
  "socketTimeout": [ms],
  "connectionTTL": [ms],
  "maxConnections": [nnnnnnn],
  "userAgentPrefix": "[prefix]",
  "socketSendBufferSizeHint": [nnnnnnn],
  "socketRecvBufferSizeHint": [nnnnnnn],
  "managementProtocol": [http|https],
  "managementHost": "[host_name]",
  "managementUser": "[user_name]",
  "managementPassword": "[password]",
  "readOnly":
}
}

```

Parameter	Required	Type	Description
id	Yes	UUID	The ID of the storage component.
storageType	No	String	The type of storage component: <ul style="list-style-type: none"> <li>▪ AMAZON_S3: An Amazon Web Services S3-compatible node</li> <li>▪ HCP_S3: A Hitachi Content Platform node</li> <li>▪ HCPS_S3: An HCP S Series Node</li> <li>▪ GENERIC_S3: An S3-compatible node</li> </ul>
storageComponent Config	No	List	The following storage component configuration values as needed:
label	No	String	The name of the storage component.
host	No	String	The URL of the storage component back-end host domain.

Parameter	Required	Type	Description
https	No	Boolean	If <code>true</code> , use an HTTPS connection to the back-end system. If <code>false</code> , use an HTTP connection.
port	No	32-bit integer	HTTP port of back-end system.
bucket	No	String	The name of the bucket. The bucket must already exist.
region	No	String	The S3 region.
authType	No	String	The AWS Signature Version for authenticating all interactions with Amazon S3: <ul style="list-style-type: none"> <li>▪ v2</li> <li>▪ v4</li> </ul>
siteAffiliation	No	UUID	For <code>id</code> , the UUID representing the storage component or the user.
accessKey	No	String	The access key of the S3 credentials for access to the bucket.
secretKey	No	String	The secret key of the S3 credentials for access to the bucket.
useProxy	No	Boolean	If <code>true</code> , a proxy server is defined. If <code>false</code> , a proxy server is not defined. If <code>true</code> , then you must provide values for <code>proxyHost</code> and <code>proxyPort</code> .
proxyHost	No	String	The proxy host, if used.
proxyPort	No	32-bit integer	The proxy port number, if used.
proxyUserName	No	String	The proxy domain user name, if used.
proxyPassword	No	String	The proxy domain password, if used.
proxyDomain	No	String	The proxy domain. This is not supported.
usePathStyleAlways	No	Boolean	If <code>true</code> , use path-style syntax to send requests to the back-end system. If <code>false</code> , use virtual-hosted style.

Parameter	Required	Type	Description
connectionTimeout	No	32-bit integer	The amount of time, in milliseconds, that the HTTP connection waits to establish a connection before timing out.
socketTimeout	No	32-bit integer	The timeout value for reading from a connected socket.
connectionTTL	No	64-bit integer	The connection time to live (TTL) for a request.
maxConnections	No	32-bit integer	The maximum number of open HTTP connections to a storage component.
userAgentPrefix	No	String	The HTTP user agent prefix header, used in requests to a storage component.
socketSendBufferSize Hint	No	32-bit integer	The size hint, in bytes, for the low-level TCP send buffer. If specified, you must also specify <code>socketRecvBufferSizeHint</code> .
socketRecvBufferSize Hint	No	32-bit integer	The size hint, in bytes, for the low-level TCP receive buffer. If specified, you must also specify <code>socketSendBufferSizeHint</code> .
managementProtocol	Yes (for HCP S Series Node)	String	Required for an HCP S Series Node storage component; do not provide for other storage component types. The communication protocol for MAPI requests: <ul style="list-style-type: none"> <li>▪ <code>http</code></li> <li>▪ <code>https</code></li> </ul> There is no default; if you use the parameter you must specify a value.
managementHost	Yes (for HCP S Series Node)	String	Required for an HCP S Series Node storage component; do not provide for other storage component types. Type the management system IP address or fully qualified domain name.

Parameter	Required	Type	Description
managementUser	Yes (for HCP S Series Node)	String	Required for an HCP S Series Node storage component; do not provide for other storage component types. The administrative user name credential. The account must have permissions to execute MAPI methods on the storage component.
managementPassword	Yes (for HCP S Series Node)	String	Required for an HCP S Series Node storage component; do not provide for other storage component types. The password credential. The account must have permissions to execute MAPI methods on the storage component.
readOnly	No	Boolean	If <code>true</code> , objects can be read and deleted but writes aren't allowed. If <code>false</code> , writes are allowed.

### Response structure

The response returns the same parameters as the request with the following additions. The response body structure is:

```
[
  {
    "id": "uuid",
    "storageType": "",
    "storageComponentConfig": {
      "label": "",
      "host": "",
      "https": ,
      "port": ,
      "bucket": "",
      "region": "",
      "authType": "",
      "siteAffiliation": {
        "id": ""
      },
    },
    "useProxy": ,
    "proxyHost": "",
    "proxyPort": ,
    "proxyUserName": "",
    "proxyPassword": "",
    "proxyDomain": "",
    "usePathStyleAlways": ,
    "connectionTimeout": ,
  }
]
```



```

    "socketTimeout": ,
    "connectionTTL": ,
    "maxConnections": ,
    "userAgentPrefix": "",
    "socketSendBufferSizeHint": ,
    "socketRecvBufferSizeHint": ,
    "managementProtocol": ,
    "managementHost": ,
    "readOnly": ,
    "state": "state"
  }
}
]

```

Parameter	Type	Description
id	UUID	The ID of the storage component.
state	Enum	<p>The state of the storage component, indicating its availability to serve requests:</p> <ul style="list-style-type: none"> <li>▪ <b>ACTIVE</b>: The storage component is ready for requests.</li> <li>▪ <b>INACTIVE</b>: The storage component is on an administrative pause.</li> <li>▪ <b>INACCESSIBLE</b>: The storage component is not accessible. This condition can be caused by network, authentication, or certificate errors.</li> <li>▪ <b>UNVERIFIED</b>: The storage component has not been activated or has failed to activate.</li> </ul>

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component or parameter.
401	Unauthorized	Access was denied because credentials are not valid.

Status code	HTTP name	Description
404	Not Found	The specified storage component was not found.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

### Example

Request example:

```
PATCH https://10.10.24.195:9099/mapi/v1/storage_component/update
```

JSON request:

```
{
  "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
  "storageComponentConfig": {
    "label": "Test cloud"
  }
}
```

JSON response:

```
[
  {
    "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
    "storageType": "AMAZON_S3",
    "storageComponentConfig": {
      "label": "Test cloud",
      "host": "172.19.54.102",
      "https": false,
      "port": 9000,
      "bucket": "testbucket",
      "region": "us-west-2",
      "authType": null,
      "siteAffiliation": {
        "id": "19546ae2-38dd-4686-b298-b5beb9173e96"
      },
      "useProxy": false,
      "proxyHost": null,
      "proxyPort": null,
      "proxyUserName": null,
      "proxyPassword": null,
      "proxyDomain": null,
      "usePathStyleAlways": true,
    }
  }
]
```

```

    "connectionTimeout": null,
    "socketTimeout": null,
    "connectionTTL": null,
    "maxConnections": null,
    "userAgentPrefix": null,
    "socketSendBufferSizeHint": null,
    "socketRecvBufferSizeHint": null,
    "readOnly": false,
    "state": "ACTIVE"
  }
}
]

```

## Set storage component state

You can set the state of a storage component to either ACTIVE or INACTIVE.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/storage_component/update_state
```

### Request structure

The request body is:

```

{
  "id": "uuid",
  "storageComponentState": "{ACTIVE|INACTIVE}"
}

```

Parameter	Required	Type	Description
id	Yes	UUID	The ID of the storage component.
storageComponentState	Yes	String	The storage component state: <ul style="list-style-type: none"> <li>ACTIVE: Available to serve requests.</li> <li>INACTIVE: Not available to serve requests (administrative pause).</li> </ul>

### Response structure

The response body structure is:

```

[
  {

```

```

    "id": "uuid",
    "storageType": "",
    "storageComponentConfig": {
      "label": "",
      "host": "",
      "https": ,
      "port": ,
      "bucket": "",
      "region": "",
      "authType": "",
      "siteAffiliation": {
        "id": ""
      },
      "useProxy": ,
      "proxyHost": "",
      "proxyPort": ,
      "proxyUserName": "",
      "proxyPassword": "",
      "proxyDomain": "",
      "usePathStyleAlways": ,
      "connectionTimeout": ,
      "socketTimeout": ,
      "connectionTTL": ,
      "maxConnections": ,
      "userAgentPrefix": "",
      "socketSendBufferSizeHint": ,
      "socketRecvBufferSizeHint": ,
      "managementProtocol": ,
      "managementHost": ,
      "readOnly": ,
      "state": "state"
    }
  }
}
]

```

Parameter	Type	Description
id	UUID	The ID of the storage component.
storageType	Enum	The type of storage component: <ul style="list-style-type: none"> <li>▪ AMAZON_S3: An Amazon Web Services S3-compatible node</li> <li>▪ HCP_S3: A Hitachi Content Platform node</li> <li>▪ HCPS_S3: An HCP S Series Node</li> <li>▪ GENERIC_S3: An S3-compatible node</li> </ul>

Parameter	Type	Description
storageComponentConfig	List	The following storage component configuration values:
label	String	The name of the storage component.
host	String	The URL of the storage component back-end host domain.
https	Boolean	<code>true</code> for HTTPS connection to back-end system, <code>false</code> for HTTP.
port	32-bit integer	HTTP port to back-end system.
bucket	String	The name of the bucket.
region	String	The S3 region.
authType	String	AWS Signature Version, used for authenticating all interactions with Amazon S3: <ul style="list-style-type: none"> <li>▪ v2</li> <li>▪ v4</li> </ul>
siteAffiliation	UUID	The value of <code>id</code> , a UUID representing the storage component or the user.
useProxy	Boolean	If <code>true</code> , a proxy server is defined. If <code>false</code> , a proxy server is not defined.
proxyHost	String	The proxy host, if used; otherwise, <code>null</code> .
proxyPort	32-bit integer	The proxy port number, if used; otherwise, <code>null</code> .
proxyUserName	String	The proxy domain user name, if used; otherwise, <code>null</code> .
proxyPassword	String	The proxy domain password, if used; otherwise, <code>null</code> .
proxyDomain	String	The proxy domain, if used; otherwise, <code>null</code> .
usePathStyleAlways	Boolean	If <code>true</code> , use path-style syntax to send requests to the back-end system; if <code>false</code> , use virtual-hosted style.
connectionTimeout	32-bit integer	The amount of time, in milliseconds, that the HTTP connection waits to establish a connection before timing out.

Parameter	Type	Description
socketTimeout	32-bit integer	The timeout value for reading from a connected socket.
connectionTTL	64-bit integer	The connection time to live (TTL) for a request.
maxConnections	32-bit integer	The maximum number of open HTTP connections to a storage component.
userAgentPrefix	String	The HTTP user agent prefix header, used in requests to a storage component.
socketSendBufferSizeHint	32-bit integer	The size hint, in bytes, for the low-level TCP send buffer.
socketRecvBufferSizeHint	32-bit integer	The size hint, in bytes, for the low-level TCP receive buffer.
managementProtocol	String	The communication protocol for HCP S Series Node MAPI requests: <ul style="list-style-type: none"> <li>▪ http</li> <li>▪ https</li> </ul>
managementHost	String	The host managing an HCP S Series Node storage component.
readOnly	Boolean	If <code>true</code> , the storage component is marked as read-only. If <code>false</code> , the storage component is available for reading and writing data.
state	Enum	The state of the storage component, indicating its availability to serve requests: <ul style="list-style-type: none"> <li>▪ <code>ACTIVE</code>: The storage component is ready for requests.</li> <li>▪ <code>INACTIVE</code>: The storage component is on an administrative pause.</li> <li>▪ <code>INACCESSIBLE</code>: The storage component is not accessible. This can be caused by network, authentication, or certificate errors.</li> <li>▪ <code>UNVERIFIED</code>: The storage component has not been activated or has failed to activate.</li> </ul>

**Return codes**

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component or parameter.
401	Unauthorized	Access was denied because credentials are not valid.
404	Not Found	The specified storage component was not found.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/update_state
```

JSON request:

```
{
  "id": "8bff981b-5894-43ce-bd41-5a6f558cc241",
  "storageComponentState": "INACTIVE"
}
```

JSON response:

```
[
  {
    "id": "8bff981b-5894-43ce-bd41-5a6f558cc241",
    "storageType": "GENERIC_S3",
    "storageComponentConfig": {
      "label": null,
      "host": "172.19.54.102",
      "https": false,
      "port": 9000,
      "bucket": "samplebucket",
      "region": "us-west-2",
      "authType": null,
      "siteAffiliation": {
```

```

    "id": "19b96ae2-38ef-4686-b298-b5bebe173e96"
  },
  "useProxy": false,
  "proxyHost": null,
  "proxyPort": null,
  "proxyUserName": null,
  "proxyPassword": null,
  "proxyDomain": null,
  "usePathStyleAlways": true,
  "connectionTimeout": null,
  "socketTimeout": null,
  "connectionTTL": null,
  "maxConnections": null,
  "userAgentPrefix": null,
  "socketSendBufferSizeHint": null,
  "socketRecvBufferSizeHint": null,
  "managementProtocol": ,
  "managementHost": ,
  "readOnly": false,
  "state": "INACTIVE"
}
}
]

```

## Test storage component access

The method `storage_component/test` tests whether a storage component is accessible.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/storage_component/test
```

### Request structure

The request body is:

```

{
  "id": "uuid"
}

```

Parameter	Required	Type	Description
id	Yes	UUID	The ID of the storage component.



**Response structure**

The response body is:

```
{
  "id": "uuid",
  "storageType": "type",
  "verified": true|false,
  "httpStatus": nnn,
  "errorCode": "code_text",
  "errorMessage": "error_text",
  "daysUntilCertificateExpiration": nnn,
  "state": "state"
}
```

Parameter	Type	Description
id	UUID	The ID of the storage component.
storageType	String	The type of storage component: <ul style="list-style-type: none"> <li>AMAZON_S3: An Amazon Web Services S3-compatible node</li> <li>HCP_S3: A Hitachi Content Platform node</li> <li>HCPS_S3: An HCP S Series Node</li> <li>GENERIC_S3: An S3-compatible node</li> </ul>
verified	Boolean	If <code>true</code> , the storage component is activated. If <code>false</code> , it has not been verified and is awaiting for an administrative action.
httpStatus	Integer	The HTTP status code the storage component responded with. If 0, the storage component can't be reached. Otherwise, the code can help explain why it can't be verified.
errorCode	String	Any error codes associated with the storage component; otherwise, null.
errorMessage	String	Any error messages associated with the storage component; otherwise, null.
daysUntilCertificateExpiration	32-bit integer	The number of days left until the current HTTP certificate expires.

Parameter	Type	Description
state	Enum	<p>The state of the storage component, indicating its availability to serve requests:</p> <ul style="list-style-type: none"> <li>▪ <b>ACTIVE</b>: The storage component is ready for requests.</li> <li>▪ <b>INACTIVE</b>: The storage component is on an administrative pause.</li> <li>▪ <b>INACCESSIBLE</b>: The storage component is not accessible. This condition can be caused by network, authentication, or certificate errors.</li> <li>▪ <b>UNVERIFIED</b>: The storage component has not been activated or has failed to activate.</li> </ul>

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component ID.
401	Unauthorized	Access was denied because credentials are not valid.
404	Not Found	The specified storage component was not found.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/test
```

**JSON request:**

```
{
  "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6"
}
```

**JSON response:**

```
{
  "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
  "storageType": "AMAZON_S3",
  "verified": true,
  "httpStatus": 200,
  "errorCode": null,
  "errorMessage": null,
  "daysUntilCertificateExpiration": null,
  "state": "ACTIVE"
}
```

## Update storage component configuration

You can update the configuration of a storage component, which overwrites the existing settings. Use the method `/storage_component/list` to verify existing settings or changes. Use the method `PATCH /storage_component/update` to update specific settings.

**HTTP request syntax (URI)**

```
POST https://host_ip:9099/mapi/v1/storage_component/update
```

**Request structure**

The request body is:

```
{
  "id": "uuid",
  "storageType": "type",
  "storageComponentConfig": {
    "label": "[label]",
    "host": "url",
    "https": {true|false},
    "port": [nnnnn],
    "bucket": "bucket_name",
    "region": "[region_name]",
    "authType": "[V2|V4]",
    "siteAffiliation": {
      "id": "uuid"
    }
  },
}
```

```

"accessKey": "key",
"secretKey": "key",
"useProxy": [true|false],
"proxyHost": "[host_name]",
"proxyPort": [nnnnn],
"proxyUserName": "[user_name]",
"proxyPassword": "[password]",
"proxyDomain": "[domain_name]",
"usePathStyleAlways": [true|false],
"connectionTimeout": [ms],
"socketTimeout": [ms],
"connectionTTL": [ms],
"maxConnections": [nnnnnnn],
"userAgentPrefix": "[prefix]",
"socketSendBufferSizeHint": [nnnnnnn],
"socketRecvBufferSizeHint": [nnnnnnn],
"managementProtocol": [http|https],
"managementHost": "[host_name]",
"managementUser": "[user_name]",
"managementPassword": "[password]",
"readOnly": {true|false}
}
}

```

Parameter	Required	Type	Description
id	Yes	UUID	The ID of the storage component.
storageType	No	String	The type of storage component: <ul style="list-style-type: none"> <li>▪ AMAZON_S3: An Amazon Web Services S3-compatible node</li> <li>▪ HCP_S3: A Hitachi Content Platform node</li> <li>▪ HCPS_S3: An HCP S Series Node</li> <li>▪ GENERIC_S3: An S3-compatible node</li> </ul>
storageComponent Config	Yes	List	The following storage component configuration values:
label	No	String	The name of the storage component.
host	Yes	String	The URL of the storage component back-end host domain.

Parameter	Required	Type	Description
https	Yes	Boolean	If <code>true</code> , use an HTTPS connection to the back-end system. If <code>false</code> , use an HTTP connection to the back-end system. Default: <code>false</code> .
port	No	Integer	The HTTP port of the back-end system.
bucket	Yes	String	The name of the bucket. The bucket must already exist.
region	No	String	The S3 region. Default: <code>us-east-1</code> .
authType	No	String	The AWS Signature Version for authenticating all interactions with Amazon S3: <ul style="list-style-type: none"> <li>▪ <code>v2</code></li> <li>▪ <code>v4</code></li> </ul>
siteAffiliation	Yes	UUID	For <code>id</code> , the UUID representing the storage component or the user.
accessKey	Yes		The access key of the S3 credentials for access to the bucket.
secretKey	Yes		The secret key of the S3 credentials for access to the bucket.
useProxy	No	Boolean	If <code>true</code> , a proxy server is defined. If <code>false</code> , a proxy server is not defined. If <code>true</code> , then values are required for <code>proxyHost</code> and <code>proxyHost</code> . Default: <code>false</code> .
proxyHost	No	String	The proxy host, if used.
proxyPort	No	Integer	The proxy port number, if used.
proxyUserName	No	String	The proxy domain user name, if used.
proxyPassword	No	String	The proxy domain password, if used.
proxyDomain	No	String	The proxy domain. This is not supported.
usePathStyleAlways	No	Boolean	If <code>true</code> , use path-style syntax to send requests to the back-end system. If <code>false</code> , use virtual-hosted style. Default: <code>true</code> .

Parameter	Required	Type	Description
connectionTimeout	No	32-bit integer	The amount of time, in milliseconds, that the HTTP connection waits to establish a connection before timing out.
socketTimeout	No	32-bit integer	The timeout value for reading from a connected socket.
connectionTTL	No	64-bit integer	The connection time to live (TTL) for a request.
maxConnections	No	32-bit integer	The maximum number of open HTTP connections to a storage component. If not specified, the defaults are: <ul style="list-style-type: none"> <li>▪ HCPS_S3: <u>1024</u></li> <li>▪ HCP_S3: <u>50</u></li> <li>▪ AMAZON_S3: <u>50</u></li> <li>▪ GENERIC_S3: <u>50</u></li> </ul>
userAgentPrefix	No	String	The HTTP user agent prefix header, used in requests to a storage component.
socketSendBufferSizeHint	No	32-bit integer	The size hint, in bytes, for the low-level TCP send buffer. If specified, you must also specify <code>socketRecvBufferSizeHint</code> .
socketRecvBufferSizeHint	No	32-bit integer	The size hint, in bytes, for the low-level TCP receive buffer. If specified, you must also specify <code>socketSendBufferSizeHint</code> .
managementProtocol	Yes (for HCP S Series Node)	String	Required for an HCP S Series Node storage component; do not provide for other storage component types. The communication protocol for MAPI requests: <ul style="list-style-type: none"> <li>▪ http</li> <li>▪ https</li> </ul> There is no default; if you use the parameter you must specify a value.

Parameter	Required	Type	Description
managementHost	Yes (for HCP S Series Node)	String	Required for an HCP S Series Node storage component; do not provide for other storage component types. Type the management system IP address or fully qualified domain name.
managementUser	Yes (for HCP S Series Node)	String	Required for an HCP S Series Node storage component; do not provide for other storage component types. The administrative user name credential. The account must have permissions to execute MAPI methods on the storage component.
managementPassword	Yes (for HCP S Series Node)	String	Required for an HCP S Series Node storage component; do not provide for other storage component types. The password credential. The account must have permissions to execute MAPI methods on the storage component.
readOnly	No	Boolean	If <code>true</code> , objects can be read and removed but writes aren't allowed. If <code>false</code> , writes are allowed.

### Response structure

The response returns the same parameters as the request with one addition. The response body structure is:

```
[
  {
    "id": "",
    "storageType": "",
    "storageComponentConfig": {
      "label": "",
      "host": "",
      "https": ,
      "port": ,
      "bucket": "",
      "region": "",
      "authType": "",
      "siteAffiliation": {
        "id": ""
      },
    },
    "useProxy": ,
  }
]
```

```

    "proxyHost": "",
    "proxyPort": ,
    "proxyUserName": "",
    "proxyPassword": "",
    "proxyDomain": "",
    "usePathStyleAlways": ,
    "connectionTimeout": ,
    "socketTimeout": ,
    "connectionTTL": ,
    "maxConnections": ,
    "userAgentPrefix": "",
    "socketSendBufferSizeHint": ,
    "socketRecvBufferSizeHint": ,
    "managementProtocol": ,
    "managementHost": ,
    "readOnly": true|false,
    "state": "state"
  }
}
]

```

Parameter	Type	Description
state	Enum	<p>The state of the storage component, indicating its availability to serve requests:</p> <ul style="list-style-type: none"> <li>▪ <b>ACTIVE</b>: The storage component is ready for requests.</li> <li>▪ <b>INACTIVE</b>: The storage component is on an administrative pause.</li> <li>▪ <b>INACCESSIBLE</b>: The storage component is not accessible. This can be caused by network, authentication, or certificate errors.</li> <li>▪ <b>UNVERIFIED</b>: The storage component has not been activated or has failed to activate.</li> </ul>



**Return codes**

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component or parameter.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/storage_component/update
```

JSON request:

```
{
  "storageType": "AMAZON_S3",
  "storageComponentConfig": {
    "label": "Cloud AWS Bucket",
    "host": "172.19.54.102",
    "https": false,
    "port": 9000,
    "bucket": "testbucket",
    "region": "us-west-2",
    "authType": "v2",
    "siteAffiliation": {
      "id": "3fa85f64-1024-4562-bffc-2c963f66afa6"
    },
  },
  "useProxy": false,
  "proxyHost": ,
  "proxyPort": ,
  "proxyUserName": ,
  "proxyPassword": ,
  "proxyDomain": ,
  "usePathStyleAlways": true,
  "connectionTimeout": ,
  "socketTimeout": ,
  "connectionTTL": ,
}
```

```

    "maxConnections": ,
    "userAgentPrefix": ,
    "socketSendBufferSizeHint": ,
    "socketRecvBufferSizeHint": ,
    "readOnly":
  }
}

```

**JSON response:**

```

[
  {
    "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6",
    "storageType": "AMAZON_S3",
    "storageComponentConfig": {
      "label": "Cloud AWS Bucket",
      "host": "URL of an existing storage component backend",
      "https": false,
      "port": 0,
      "bucket": "string",
      "region": "string",
      "authType": "V2",
      "siteAffiliation": {
        "id": "3fa85f64-1024-4562-b3fc-2c963f66afa6"
      },
      "useProxy": true,
      "proxyHost": "string",
      "proxyPort": 0,
      "proxyUserName": "string",
      "proxyPassword": "string",
      "proxyDomain": "string",
      "usePathStyleAlways": true,
      "connectionTimeout": 0,
      "socketTimeout": 0,
      "connectionTTL": 0,
      "maxConnections": 50,
      "userAgentPrefix": "string",
      "socketSendBufferSizeHint": 0,
      "socketRecvBufferSizeHint": 0,
      "readOnly": false,
      "state": "ACTIVE"
    }
  }
]

```

## Chapter 3: Encryption management methods

The management API includes methods for storage component encryption and key management server management.

Before issuing a MAPI call, request and submit a CSRF token.

For information on CSRF tokens refer to [Requesting and submitting a CSRF token \(on page 12\)](#).

### Add KMS server

You can configure the connection to an external KMS server.

#### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/kmip/add_server
```



**Note:** The first KMS server you configure is designated as the primary server, and any other servers you configure are designated as secondary servers. Use the method `promote_server` to designate another KMS server as the primary server.

#### Request structure

The request body is:

```
{
  "name": "name",
  "host": "{hostname|ip_addr}",
  ["port": [nnnnn],]
  "isTLS12Enabled": {true|false},
  "httpsCiphers": "cipher_1[,...,cipher_n]"
}
```

Parameter	Required	Type	Description
name	Yes	String	The user-assigned name of the KMS server you want to add. Type up to 63 Unicode characters. The server name must be unique.

Parameter	Required	Type	Description
host	Yes	String	The host name or IP address of the KMS server.
port	No	Integer	The port number of the KMS server. Default: 5956
isTLS12Enabled	Yes	Boolean	true if TLS v1.2 is enabled, false otherwise. <b>Note:</b> TLS v1.2 support is provided for backward compatibility only.
httpsCiphers	Yes	String	A string of comma-separated cyphers. The default group supports interoperability with a range of commercial key managers.  Default: TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_AES_256_GCM_SHA384, TLS_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

### Response structure

The response returns the same parameters as the request with the following additions. The response body structure is:

```
{
  "name": "label",
  "host": "host_name",
  "port": nnnnn,
  "isPrimary": {true|false},
  "isTLS12Enabled": {true|false},
  "httpsCiphers": "cipher_1[,...,cipher_n]",
}
```

```

"isOnline": {true|false},
"uuid": "uuid"
}

```

Parameter	Type	Description
name	String	The name of the KMS server.
host	String	The host name or IP address of the KMS server.
port	32-bit integer	The port number of the KMS server.
isPrimary	Boolean	<code>true</code> if server is primary (read/write access), <code>false</code> if server is secondary (read-only access).
isTLS12Enabled	Boolean	<code>true</code> if TLS v1.2 is enabled, <code>false</code> otherwise.
httpsCiphers	String	A string of comma-separated cyphers.
isOnline	Boolean	<code>true</code> if server is online, <code>false</code> if server is offline.
uuid	UUID	The UUID of the server.

**Return codes**

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component or parameter.
401	Unauthorized	Access was denied because credentials are not valid.
404	Not Found	The KMS server was not found.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.
500	Internal Server Error	The system was unable to set the requested object in the database.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/kmip/add_server
```

JSON request:

```
{
  "name": "myServer",
  "host": "kmip.company.com",
  "port": 5678,
  "isTLS12Enabled": false,
  "httpsCiphers": "TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384"
}
```

JSON response:

```
{
  "name": "myServer",
  "host": "kmip.company.com",
  "port": 5678,
  "isPrimary": true,
  "isTLS12Enabled": false,
}
```

```

"httpsCiphers": "TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384"
  "isOnline": true,
  "uuid": "uuid"
}

```

## Delete KMS server

You can delete the connection to an external secondary KMS server. The server is not deleted, only the connection to the server.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/kmip/delete_server
```

### Request structure

```
"name": "name"
```

Parameter	Required	Type	Description
name	Yes	String	The user-assigned name of the secondary KMS server you want to delete. Type up to 63 Unicode characters.

### Response structure

Not applicable.

### Return codes



**Note:** Before deleting the connection to a secondary KMS server, the system checks the KEKs currently on the reachable online servers. If each KEK on the server is contained in the set of currently available KEKs, the connection to the server is deleted and the method succeeds. However, if the server contains a KEK not available on at least one of the other servers, the connection is not deleted and the method fails.

Status code	HTTP name	Description
200	OK	The request was executed successfully.

Status code	HTTP name	Description
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.
503	Service Unavailable	An external KMS system has not been configured.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/knip/delete_server
```

JSON request:

```
"name": "myServer"
```

## Get encryption state

You can get the state of encryption for the HCP for cloud scale system.

**HTTP request syntax (URI)**

```
POST https://host_ip:9099/mapi/v1/s3_encryption/get
```

**Request structure**

Not applicable.

**Response structure**

The response body structure is:

```
{
  MAPIS3EncryptionSetting {
    "value": "{true|false}"
  }
}
```



Parameter	Type	Description
MAPIS3EncryptionSetting	Boolean	true if encryption is on, false otherwise.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3_encryption/get
```

JSON response:

```
{
  MAPIS3EncryptionSetting {
    "value": "true"
  }
}
```

## Get KMS server

You can get information about an individual external KMS server.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/kmip/get_server
```

### Request structure

```
"name"
```

Parameter	Required	Type	Description
name	Yes	String	The user-assigned name of the KMS server you want to get information about. Type up to 63 Unicode characters.

### Response structure

The response body structure is:

```
{
  "name": "label",
  "host": "host_name",
  "port": nnnnn,
  "isPrimary": {true|false},
  "isTLS12Enabled": {true|false},
  "httpsCiphers": "cipher_1[,...,cipher_n]",
  "isOnline": {true|false},
  "uuid": "uuid"
}
```

Parameter	Type	Description
name	String	The name of the KMS server.
host	String	The host name or IP address of the KMS server.
port	Integer	The port number of the KMS server.
isPrimary	Boolean	true if server is primary (read/write access), false if server is secondary (read-only access).
isTLS12Enabled	Boolean	true if TLS v1.2 is enabled, false otherwise.
httpsCiphers	String	A string of comma-separated cyphers.
isOnline	Boolean	true if server is online, false if server is offline.
uuid	UUID	The UUID of the server.

**Return codes**

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed. Resend using POST.
503	Service Unavailable	External KMS servers have not been set up. Configure connection to an external KMS server and resend.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/knip/get_server
```

JSON request:

```
"myServer"
```

JSON response:

```
{
  "name": "myServer",
  "host": "myHost_0",
  "port": 5678,
  "isPrimary": true,
  "isTLS12Enabled": false,
  "httpsCiphers": "TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384"
  "isOnline": true,
  "uuid": "uuid",
}
```

**List KMS servers**

You can get information about all configured external KMS servers.

**HTTP request syntax (URI)**

```
POST https://host_ip:9099/mapi/v1/kmip/list_servers
```

**Request structure**

Not applicable.

**Response structure**

The response body structure is:

```
[
  {
    "name": "label",
    "host": "host_name",
    "port": nnnnn,
    "isPrimary": {true|false},
    "isTLS12Enabled": {true|false},
    "httpsCiphers": "cipher_1[, ..., cipher_n]",
    "isOnline": {true|false},
    "uuid": "uuid"    }
  .
  .
  .
]
```

Parameter	Type	Description
name	String	The name of the KMS server.
host	String	The host name or IP address of the KMS server.
port	Integer	The port number of the KMS server.
isPrimary	Boolean	true if server is primary (read/write access), false if server is secondary (read-only access).
isTLS12Enabled	Boolean	true if TLS v1.2 is enabled, false otherwise.
httpsCiphers	String	A string of comma-separated cyphers.
isOnline	Boolean	true if server is online, false if server is offline.
uuid	UUID	The UUID of the server.

**Return codes**

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed. Resend using POST.
503	Service Unavailable	External KMS servers have not been set up. Configure connection to an external KMS server and resend.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/kmip/list_servers
```

JSON response:

```
[
  servers: {
    myName=class MAPIKMIPServer {
      "name": "myName",
      "host": "myHost_0",
      "port": 9876,
      "isPrimary": true,
      "isTLS12Enabled": false,
      "httpsCiphers": "TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "isOnline": true,
      "uuid": "uuid"},
    myName_0=class MAPIKMIPServer {
      "name": "myName_0",
      "host": "myHost_0",
      "port": 5678,
      "isPrimary": true,
      "isTLS12Enabled": false,
      "httpsCiphers": "TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "isOnline": true,
      "uuid": "uuid"},}
```

```
}
]
```

## Promote KMS server

You can promote a configured secondary external KMS server to the primary server. Any primary server is demoted to a secondary server.

Any external KMS server designated as a secondary server can be promoted to a primary server. Promoting a secondary server demotes the existing primary server to secondary status.

Normally, key encryption keys (KEKs) are synchronized between the primary server and any secondary servers. If a secondary server is promoted but has an incomplete set of KEKs, HCP for cloud scale tries to populate missing KEKs using cached KEKs. If the promoted server cannot produce a KEK and the KEK is not cached, then all data associated with the missing KEK remains unavailable until the previous primary server is repaired and populates the newly promoted primary server with the missing KEK.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/kmip/promote_server
```

### Request structure

```
"name": "name"
```

Parameter	Required	Type	Description
name	Yes	String	The user-assigned name of the KMS server you want to promote. Type up to 63 Unicode characters.

### Response structure

The response body structure is:

```
{
  "name": "label",
  "host": "host_name",
  "port": nnnnn,
  "isPrimary": {true|false},
  "isTLS12Enabled": {true|false},
  "httpsCiphers": "cipher_1[,...,cipher_n]",
  "isOnline": {true|false},
```

```
"uuid": "uuid"
}
```

Parameter	Type	Description
name	String	The name of the KMS server.
host	String	The host name or IP address of the KMS server.
port	Integer	The port number of the KMS server.
isPrimary	Boolean	true.
isTLS12Enabled	Boolean	true if TLS v1.2 is enabled, false otherwise.
httpsCiphers	String	A string of comma-separated cyphers.
isOnline	Boolean	true if server is online, false if server is offline.
uuid	UUID	The UUID of the server.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed. Resend using POST.
503	Service Unavailable	External KMS servers have not been set up. Configure connection to an external KMS server and resend.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/kmip/promote_server "MyServer"
```

**JSON request:**

```
"name": "myServer"
```

**JSON response:**

```
{
  "name": "myServer",
  "host": "myHost_0",
  "port": 9876,
  "isPrimary": true,
  "isTLS12Enabled": false,
  "httpsCiphers": "TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
  "isOnline": true,
  "uuid": "uuid"
}
```

## Rekey

You can generate new key encryption keys (KEKs) for all storage components.

**HTTP request syntax (URI)**

```
POST https://host_ip:9099/mapi/v1/s3_encryption/rekey
```

**Request structure**

```
{
  "code": "{KEY_COMPROMISE|SUPERSEDED}",
  "message": "reason"
}
```

Parameter	Required	Type	Description
code	Yes	Enum	KEY_COMPROMISE if rekey is requested because a key was compromised, SUPERSEDED if rekey is requested per policy or another reason.
message	No	String	Text details on the reason for asking for new keys.



**Response structure**

Not applicable.

**Return codes**

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	Encryption is not enabled on the HCP for cloud scale system.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed. Resend using POST.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3_encryption/rekey
```

JSON request:

```
{
  "code": "SUPERSEDED",
  "message": "Retire existing keys 2022-12-31"
}
```

## Set encryption state

You can start encryption globally for the HCP for cloud scale system. Starting encryption initializes, configures, and unseals the key management server and returns an initial root token and a set of unseal keys. Once encryption is started, it can't be removed. The best practice is to encrypt and securely store the initial root token and unseal keys separately.

**HTTP request syntax (URI)**

```
POST https://host_ip:9099/mapi/v1/s3_encryption/set
```

**Request structure**

Not applicable.

## Response structure

The response body structure is:

```
{
  "value": {true|false},
  "rootToken": "root_token",
  "unsealKeys": ["unseal_key_1", "unseal_key_2", "unseal_key_3", "unseal_key_4",
"unseal_key_5"]
}
```

Parameter	Type	Description
value	Boolean	true if encryption is on, false otherwise.
rootToken	Hex	The initial root token, used to authenticate login to the key management server.
unsealKeys	Hex	A set of unseal keys. A quorum of unseal keys is required to restart the key management server.

## Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.
503	Service Unavailable	The key management system has not been set up.

## Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3_encryption/set
```

JSON response:

```
{
  "value":true,
  "rootToken":"s.FBZngLG9RcyjBzddCxTwoMkk",
  "unsealKeys":[
    "f7a0652cbe07d573a7eeab127ff102454c33adc9402e49622ffa5b5f43cec0794e",
    "4d7e620a694cb607dd1e503027f82880f376edfb1024548d0121572a3dc989c685",
    "6c6081054e26ec55824eb97481acd1f31d660d99e4ba158ca4248e39a8d4de1e16",
    "5dd42c8c60d60469d675dbaad15ff2a78d262cb42e2f9a798aa0b09f368b8caff4",
    "fdc2f29b4359a550916b43071501dab257b73f911960c7fc793f1a279f71091482"]
}
```

## Update KMS server

You can update selected configuration values for an external KMS server.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/kmip/update_server
```

### Request structure

The request body is:

```
{
  "name": "name",
  "host": "{hostname|ip_addr}",
  ["port": [nnnnn],]
  "isTLS12Enabled": {true|false},
  "httpsCiphers": "cipher_1[,...,cipher_n",
  "uuid": "uuid"
}
```

Parameter	Required	Type	Description
name	Yes	String	The user-assigned name of the KMS server you want to update. Type up to 63 Unicode characters. The server name must be unique.
host	Yes	String	The host name or IP address of the KMS server.
port	No	Integer	The port number of the KMS server. Default: 5956

Parameter	Required	Type	Description
isTLS12Enabled	Yes	Boolean	true if TLS v1.2 is enabled, false otherwise.  <b>Note:</b> TLS v1.2 support is provided for backward compatibility only.
httpsCiphers	Yes	String	A string of comma-separated cyphers. The default group supports interoperability with a range of commercial key managers.  Default: TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_AES_256_GCM_SHA384, TLS_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
uuid	Yes	UUID	The UUID of the server.

### Response structure

The response returns the same parameters as the request with the following additions. The response body structure is:

```
{
  "name": "label",
  "host": "host_name",
  "port": nnnnn,
  "isPrimary": {true|false},
  "isTLS12Enabled": {true|false},
  "httpsCiphers": "cipher_1[, ..., cipher_n]",
  "isOnline": {true|false},
  "uuid": "uuid"
}
```

Parameter	Type	Description
name	String	The name of the KMS server.
host	String	The host name or IP address of the KMS server.
port	32-bit integer	The port number of the KMS server.
isPrimary	Boolean	<code>true</code> if server is primary (read/write access), <code>false</code> if server is secondary (read-only access).
isTLS12Enabled	Boolean	<code>true</code> if TLS v1.2 is enabled, <code>false</code> otherwise.
httpsCiphers	String	A string of comma-separated cyphers.
isOnline	Boolean	<code>true</code> if server is online, <code>false</code> if server is offline.
uuid	UUID	The UUID of the server.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component or parameter.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.
503	Service Unavailable	External KMS servers are not defined.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/kmip/update_server
```

**JSON request:**

```
{
  "name": "myServer",
  "host": "kmip.company.com",
  "port": 5956,
  "isTLS12Enabled": false,
  "httpsCiphers": "TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384"
}
```

**JSON response:**

```
{
  "name": "myServer",
  "host": "kmip.company.com",
  "port": 5956,
  "isPrimary": true,
  "isTLS12Enabled": false,
  "httpsCiphers": "TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
  "isOnline": true,
  "uuid": "uuid"
}
```

## Unseal

You can unseal all the instances of the key management server for the HCP for cloud scale system.

**HTTP request syntax (URI)**

```
POST https://host_ip:9099/mapi/v1/s3_encryption/unseal
```

**Request structure**

The request body is:

```
{
  "unsealKey1": "string",
  "unsealKey2": "string",
  "unsealKey3": "string"
}
```

Parameter	Required	Type	Description
unsealKey1, unsealKey2, unsealKey3	Yes	String	An unseal key. You must provide three unseal keys in the request.

### Response structure

Not applicable.

### Return codes

Status code	HTTP name	Description
000	Provides an empty response body	Occurs when a vault instance is restarted and the vault ends up in various intermediate states between unsealed, partially unsealed, and fully sealed.
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid unseal key.
400	KMS Unseal Failure	The request was unable to unseal the KMS instance, as all available instances are already unsealed.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.
503	Service Unavailable	External KMS servers have not been set up. Configure connection to an external KMS server and resend.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3_encryption/unseal
```

JSON request:

```
{
  "unsealKey1": "f7a0652cbe07d573a7eeab127ff102454c33adc9402e49622ffa5b5f43cec0794e",
  "unsealKey2": "4d7e620a694cb607dd1e503027f82880f376edfb1024548d0121572a3dc989c685",
  "unsealKey3": "6c6081054e26ec55824eb97481acd1f31d660d99e4ba158ca4248e39a8d4de1e16"
}
```

## Migrate an internal KMS

Administrators with the appropriate permissions can migrate their internal KMS to an external HCP for cloud scale system.

**Pre-requisites:**

- The system must have a valid DARE license.
- The internal KMS must already be configured
- The internal KMS must be unsealed.
- The external KMS must be available, with the client certificate already loaded.
- The admin user must have the `migrate_server` permissions from the MAPI KMIP permissions group assigned to them.

**HTTP request syntax (URI)**

```
POST https://host_ip:9099/mapi/v1/kmip/migrate_server
```

**Request structure**

The request body is:

```
{
  "name": "string",
  "host": "string",
  "port": 0,
  "isTLS12Enabled": true,
  "kmipProtocol": string,
  "httpsCiphers": "string"
}
```



Parameter	Required	Type	Description
name	Yes	String	The user-assigned name of the KMS server you want to update. Type up to 63 Unicode characters.  The server name must be unique.
host	Yes	String	The hostname or IP address of the KMS server.
port	No	Integer	The port number of the KMS server.  Default: 5956
isTLS12Enabled	Yes	Boolean	<code>true</code> if TLS v1.2 is enabled, <code>false</code> otherwise.  <b>Note:</b> TLS v1.2 support is provided for backward compatibility only.
KMIP protocol version	Yes	String	The KMIP protocol version identifier used in KMIP exchanges.  Default: 5956
httpsCiphers	Yes	String	A string of comma-separated cyphers. The default group supports interoperability with a range of commercial key managers.  Defaults include: <i>TLS_RSA_WITH_AES_128_CBC_SHA256,</i> <i>TLS_RSA_WITH_AES_256_CBC_SHA256,</i> <i>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,</i> <i>SSL_RSA_WITH_3DES_EDE_CBC_SHA,</i> <i>TLS_AES_256_GCM_SHA384,</i> <i>TLS_AES_128_GCM_SHA256,</i> <i>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,</i> <i>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,</i> <i>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,</i> <i>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</i>

### Response structure

The response returns the same parameters as the request with the following additions. The response body structure is:

```
{
  "name": "string",
  "host": "string",
  "port": 0,
  "isPrimary": true,
  "isTLS12Enabled": true,
  "httpsCiphers": "string",
  "isOnline": true,
  "uuid": "string"
}
```

Parameter	Type	Description
name	String	The user-assigned name of the KMS server you want to update. Type up to 63 Unicode characters. The server name must be unique.
host	String	The hostname or IP address of the KMS server.
port	32-bit integer	The port number of the KMS server. Default: 5956
isTLS12Enabled	Boolean	<i>true</i> if TLS v1.2 is enabled, <i>false</i> otherwise.
KMIP protocol version	String	A string of comma-separated cyphers.

Parameter	Type	Description
httpsCiphers	String	<p>A string of comma-separated cyphers. The default group supports interoperability with a range of commercial key managers.</p> <p>Defaults include:</p> <p><i>TLS_RSA_WITH_AES_128_CBC_SHA256,</i>  <i>TLS_RSA_WITH_AES_256_CBC_SHA256,</i>  <i>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,</i>  <i>SSL_RSA_WITH_3DES_EDE_CBC_SHA,</i>  <i>TLS_AES_256_GCM_SHA384,</i><i>TLS_AES_128_GCM_SHA256,</i>  <i>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,</i>  <i>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,</i>  <i>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,</i>  <i>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</i></p>
isPrimary	Boolean	<code>true</code> marks the KMIP servers as primary (read/write permissions), <code>false</code> marks it as secondary (read-only permissions).
uuid	String	The UUID of the KMS server.

**Return codes**

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid storage component or parameter.
401	Unauthorized	Access was denied because credentials are not valid.
403	Forbidden	License error.
405	Method Not Allowed	The specified HTTP method is not allowed for a storage component. Resend using POST.
500	Internal Service Error	There is a problem with the KMS server.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/kmip/update_server
```

JSON request:

```
{
  "name": "myServer",
  "host": "kmip.company.com",
  "port": 5956,
  "isTLS12Enabled": true,
  "kmipProtocol": 1.4,
  "httpsCiphers": "TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384"
}
```

JSON response:

```
{
  "name": "myServer",
  "host": "kmip.company.com",
  "port": 5956,
  "isTLS12Enabled": true,
  "kmipProtocol": 1.4,
  "httpsCiphers": "TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,
```

```
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",  
  "isPrimary": true,  
  "uuid": "uuid"  
}
```

---

## Chapter 4: Administrative management methods

The management API includes administrative management methods.

Before issuing a MAPI call, request and submit a CSRF token.

For information on CSRF tokens refer to [Requesting and submitting a CSRF token \(on page 12\)](#).

### Add license

The method `license/add` adds a license for the system. You must provide a valid license file for the licensed function to function. The method decrypts, validates, and stores the license file.

#### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/license/add
```

#### Request structure

The request body is:

```
{
  "value": "license_file"
}
```

Parameter	Required	Type	Description
value	Yes	String	The file path of your HCP for cloud scale license.

#### Response structure

Not applicable.

**Return codes**

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials were noit valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/license/add
```

JSON request:

```
{
  "value": "hcpcs_license.plk"
}
```

## Get serial number

You can retrieve the current serial number of your HCP for cloud scale system.

**HTTP request syntax (URI)**

```
POST https://host_ip:9099/mapi/v1/serial_number/get
```

**Request structure**

Not applicable.

**Response structure**

The response body is:

```
{
  "value": "serial_number"
}
```

Parameter	Type	Description
value	String	The serial number of your HCP for cloud scale system.

#### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

#### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/serial_number/get
```

JSON response:

```
{
  "value": "SerialNumber48692"
}
```

## Get system chargeback report

The method `chargeback/system/get_report` lets a user with system-level permission generate a chargeback report on storage usage for any or all buckets defined in the system.

#### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/chargeback/system/get_report
```



## Request structure

The request structure is:

```
{
  "userName": "name",
  "startDateTime": "yyyy-mm-ddT hh:mm:ssZ",
  "endDateTime": "yyyy-mm-ddT hh:mm:ssZ",
  "granularity": "granularity",
  "bucketList": ["string"],
  "header": true|false,
  "reportedFields": [
    "field"
  ]
}
```

## Response structure

The response is a stream in comma-separated value (CSV) format.

Parameter	Required	Type	Description
userName	No	String	Report bucket usage by the specified display name. Either a user name or a bucket list is required.
startDateTime	No	Date-Time	The starting UTC date and time for the report, in the format <i>yyyy-mm-ddT hh:mm:ssZ</i> . Truncated to the beginning of the specified hour.
endDateTime	No	Date-Time	The ending UTC date and time for the report, in the format <i>yyyy-mm-ddT hh:mm:ssZ</i> . Truncated to the beginning of the specified hour. The default is the current hour.
granularity	No	Enum	The granularity of detail in the report: <ul style="list-style-type: none"> <li>▪ HOURLY: Report hourly data</li> <li>▪ DAILY (default): Report daily data</li> <li>▪ MONTHLY: Report monthly data</li> </ul>
bucketList	No	String	A list of buckets to include in the report. Either a user name or a bucket list is required. The default is all buckets in the specified scope. Limited to the number of buckets allowed per user.

Parameter	Required	Type	Description
header	No	Boolean	If <code>true</code> , include column headers as the first line of the response. If <code>false</code> , omit the column headers. The default is <code>false</code> .
reportedFields	No	String	A comma-separated list of available fields to include in the report: <ul style="list-style-type: none"> <li>▪ <code>BUCKET_OWNER</code>: bucket owner</li> <li>▪ <code>BUCKET_NAME</code>: bucket name</li> <li>▪ <code>STORAGE_CLASS</code>: storage class (STANDARD)</li> <li>▪ <code>CAPACITY_IN_BYTE_HOURS</code>: capacity in byte-hours</li> <li>▪ <code>CAPACITY_IN_GB_MONTHS</code>: capacity in gigabyte-months</li> <li>▪ <code>TOTAL_OBJECTS</code>: object count</li> <li>▪ <code>WRITES</code>: total writes</li> <li>▪ <code>DELETES</code>: total deletions</li> <li>▪ <code>WRITTEN_MB</code>: bytes written</li> <li>▪ <code>DELETED_MB</code>: bytes deleted</li> </ul> The default is to return all fields.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

## Examples

The following example returns a daily report for all buckets owned by the user `Jimmy` for a specific date range in November 2020.

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/chargeback/system/get_report
```

JSON request:

```
{
  "userName": "Jimmy",
  "startDateTime": "2020-11-02T00:00Z",
  "endDateTime": "2020-11-04T00:00Z",
  "granularity": "DAILY",
  "header": true
}
```

Response:

```
Bucket Capacity Report for user: Jimmy@example.org; Requested by: admin; Reporting
period: 2020-11-02T00:00Z - 2020-11-04T00:00Z; Granularity: daily; System name:
hcpcs.company.com
YYYY-MM-DD,Bucket Owner,Bucket Name,Storage Class,Byte-Hour,GB-Month,Total Objects,
Writes,Deletes,Written MB,Deleted MB
2020-11-02,Jimmy@example.org,bucket2,Standard,202970940,0,4,28,0,193,0
2020-11-02,Jimmy@example.org,bucket1,Standard,103229940,0,-11916,11927,11917,86,11
2020-11-03,Jimmy@example.org,bucket1,Standard,112383590,0,72,74,0,32,0
2020-11-04,Jimmy@example.org,bucket1,Standard,229915961,0,21,1121,0,3,0
```

## Get system events

The method `system/info` retrieves the 100 most recent system events.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/system/info
```

### Request structure

Not applicable.

### Response structure

The response body is:

```
{
  "events": [
    {
```

```

    "severity": "INFO|WARNING|SEVERE",
    "subject": "event_subject",
    "message": "event_message",
    "subsystem": "event_subsystem",
    "timestamp": date_time
  },
  .
  .
  .
]
}

```

Parameter	Type	Description
severity	String	The severity of the event: <ul style="list-style-type: none"> <li>▪ INFO</li> <li>▪ WARNING</li> <li>▪ SEVERE</li> </ul>
subject	String	Summary of the event.
message	String	Details about the event.
subsystem	String	The event category (for example, User, Bucket, or S3 settings).
timestamp	64-bit integer	The date and time, in milliseconds since 00:00:00 on 1 January 1970 GMT, when the event was generated.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/system/info
```

JSON response:

```
{
  "events": [
    {
      "severity": "INFO",
      "subject": "User admin@company.com authenticated",
      "message": "User admin@company.com with Id d3c01db4-ac18-4d90-a321-899bb210baf7 authenticated successfully to the Administration App.",
      "subsystem": "User",
      "timestamp": 1559547959735
    },
    {
      "severity": "INFO",
      "subject": "Unexpectedly failed authentication request by user admin@company.com",
      "message": "An authentication request unexpectedly failed for username admin@company.com.",
      "subsystem": "User",
      "timestamp": 1559547646844
    }
  ]
}
```

## Get user chargeback report

The method `chargeback/user/get_report` lets a user generate a chargeback report on storage usage for any or all buckets defined in the system that the user owns.

**HTTP request syntax (URI)**

```
POST https://host_ip:9099/mapi/v1/chargeback/user/get_report
```

**Request structure**

The request structure is:

```
{
  "startDateTime": "yyyy-mm-ddThh.mm.ssZ",
  "endDateTime": "yyyy-mm-ddThh.mm.ssZ",
  "granularity": "granularity",
  "bucketList": ["string"],
  "header": true|false,
```

```

"reportedFields": [
  "field"
]
}

```

### Response structure

The response is a stream in comma-separated value (CSV) format.

Parameter	Required	Type	Description
startDateTime	No	Date-Time	The starting UTC date and time for the report, in the format <code>yyyy-mm-ddThh.mm.ssZ</code> . Truncated to the beginning of the specified hour.
endDateTime	No	Date-Time	The ending UTC date and time for the report, in the format <code>yyyy-mm-ddThh.mm.ssZ</code> . Truncated to the beginning of the specified hour. The default is the current hour.
granularity	No	Enum	The granularity of detail in the report: <ul style="list-style-type: none"> <li>▪ HOURLY: Report hourly data</li> <li>▪ DAILY (default): Report daily data</li> <li>▪ MONTHLY: Report monthly data</li> </ul>
bucketList	No	String	A list of buckets to include in the report. The default is all buckets that the user owns. Limited to the number of buckets allowed per user.
header	No	Boolean	If <code>true</code> , include column headers as the first line of the response. If <code>false</code> , omit the column headers. The default is <code>false</code> .
reportedFields	No	String	A comma-separated list of available fields to include in the report: <ul style="list-style-type: none"> <li>▪ BUCKET_OWNER: bucket owner</li> <li>▪ BUCKET_NAME: bucket name</li> <li>▪ STORAGE_CLASS: storage class (STANDARD)</li> <li>▪ CAPACITY_IN_BYTE_HOURS: capacity in byte-hours</li> </ul>

Parameter	Required	Type	Description
			<ul style="list-style-type: none"> <li>▪ CAPACITY_IN_GB_MONTHS: capacity in gigabyte-months</li> <li>▪ TOTAL_OBJECTS: object count</li> <li>▪ WRITES: total writes</li> <li>▪ DELETES: total deletions</li> <li>▪ WRITTEN_MB: bytes written</li> <li>▪ DELETED_MB: bytes deleted</li> </ul> <p>The default is to return all fields.</p>

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

### Example

The following example returns a daily report for all buckets owned by the user (Jimmy) for a specific date range in November 2020.

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/chargeback/system/get_report
```

JSON request:

```
{
  "startDateTime": "2020-11-02T00:00Z",
  "endDateTime": "2020-11-04T00:00Z",
  "granularity": "DAILY",
  "header": true
}
```

**Response:**

```
Capacity Report for user: Jimmy@example.org; Reporting period: 2020-11-02T00:00Z -
2020-11-04T00:00Z; Granularity: daily; System name: hcpcs.company.com
YYYY-MM-DD, Bucket Owner, Bucket Name, Storage Class, Byte-Hour, GB-Month, Total Objects,
Writes, Deletes, Written MB, Deleted MB
2020-11-02, Jimmy@example.org, bucket2, Standard, 202970940, 0, 4, 28, 0, 193, 0
2020-11-02, Jimmy@example.org, bucket1, Standard, 103229940, 0, -11916, 11927, 11917, 86, 11
2020-11-03, Jimmy@example.org, bucket1, Standard, 112383590, 0, 72, 74, 0, 32, 0
2020-11-04, Jimmy@example.org, bucket1, Standard, 229915961, 0, 21, 1121, 0, 3, 0
```

## List licenses

You can retrieve information about the current licenses for your HCP for cloud scale system.

**HTTP request syntax (URI)**

```
POST https://host_ip:9099/mapi/v1/license/list
```

**Request structure**

Not applicable.

**Response structure**

The response body is:

```
{
  "featureName": "feature",
  "uploadDate": "date_time",
  "expirationDate": "date_time0",
  "valid": {true|false},
  "message": "message"
}
```

Parameter	Type	Description
featureName	String	Name of the licensed feature.
uploadDate		The date and time, in the format <i>Ddd Mmm dd hh:mm:ss TMZ yyyy</i> , when the license was uploaded.
expirationDate		The date and time, in the format <i>Ddd Mmm dd hh:mm:ss TMZ yyyy</i> , when the license expires.



Parameter	Type	Description
valid	Boolean	If <code>true</code> , the license is valid. If <code>false</code> , the license is invalid.
message	String	State of the license: <ul style="list-style-type: none"> <li>▪ License is expired</li> <li>▪ License is valid</li> <li>▪ License not set</li> </ul>

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/license/list
```

JSON response:

```
{
  "featureName": "DARE",
  "uploadDate": "Tue Jun 16 00:00:00 GMT 2020",
  "expirationDate": "Sat Oct 24 10:24:54 GMT 2020",
  "valid": true,
  "message": "License is valid"
}
```

## Refresh client certificates

If your system uses the HTTPS protocol and you change an SSL certificate, you need to update the certificates on storage components. Additionally, the following services need to be restarted when a client certificate is added or changed:

- MAPI Gateway
- S3 Gateway
- S3 Notifications
- Sync-From
- Sync-To

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/certificates/refresh
```

### Request structure

Not applicable.

### Response structure

Not applicable.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/certificates/refresh
```

## Set serial number

The method `serial_number/set` sets the serial number of the HCP for cloud scale system. You must provide a valid serial number for the system to function.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/serial_number/set
```

### Request structure

The request body is:

```
{
  "value": "serial_number"
}
```

Parameter	Required	Type	Description
value	Yes	String	The serial number of your HCP for cloud scale system.

### Response structure

The response returns the same parameter as the request.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials were noit valid.
405	Method Not Allowed	The specified HTTP method is not allowed for administrative data. Resend using POST.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/serial_number/set
```

JSON request:

```
{  
  "value": "SerialNumber48692"  
}
```

JSON response:

```
{  
  "value": "SerialNumber48692"  
}
```

---

## Chapter 5: User management methods

The management API includes user management methods.

Before issuing a MAPI call, request and submit a CSRF token.

For information on CSRF tokens refer to [Requesting and submitting a CSRF token \(on page 12\)](#).

### Generate S3 user credentials

You can generate new S3 user credentials for access to the bucket. The method `user/generate_credentials` returns a new `secretKey`-`accessKey` pair corresponding to the user associated with the OAuth token that was submitted. The creation of a new key pair invalidates any previous key pairs for the user. A user account cannot generate S3 credentials associated with a different user account.

#### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/s3/user/generate_credentials
```

#### Request structure

Not applicable.

#### Response structure

The response body is:

```
{
  "id": {
    "id": "uuid"
  },
  "secretKey": "key",
  "accessKey": "key"
}
```

Parameter	Type	Description
id	UUID	The ID of the user.

Parameter	Type	Description
secretKey	String	The secret key of the S3 credentials to access the bucket.
accessKey	String	The access key of the S3 credentials to access the bucket.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for user data. Resend using POST.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/s3/user/generate_credentials
```

JSON response:

```
{
  "id": {
    "id": "edded8d-99f1-43f4-88fa-0cd9032ef7bd"
  },
  "secretKey": "bff...",
  "accessKey": "TSP18Pop..."
}
```

## List users

You can retrieve a list of all users of the HCP for cloud scale system by user ID, display name, and realm. You can also filter the list to retrieve a subset.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/user/list
```

**Request structure**

The request body is:

```
{
  "count": [nnnn],
  "startingFrom": ["uuid"],
  "nameFilter": ["match_string"]
}
```

Parameter	Required	Type	Description
count	No	Integer	The number of users to return. Up to 1000 users; default: 1000.
startingFrom	No	UUID	The UUID to start from. Leave blank to start from the beginning of the list.
nameFilter	No	String	A string used to filter the list to return only names that start with this string.

**Response structure**

The response body structure is:

```
[
  {
    "displayName": "",
    "id": "",
    "realmId": ""
  }
  .
  .
  .
]
```

Parameter	Type	Description
displayName	String	The display name of the user.
id	UUID	The ID of the user.
realmId	String	The realm of the user.

**Return codes**

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for user data. Resend using POST.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/user/list
```

JSON request:

```
{
  "count": 1,
  "startingFrom": "3fa85f64-0810-1954-b3fc-2c963f66afa6",
  "nameFilter": ""
}
```

JSON response:

```
[
  {
    "displayName": "Zhang.Guo-Ming@company.com",
    "id": "3fa85f64-0810-1954-b3fc-2c963f66afa6"
    "realmId": "2d64d267-a23b-54c8-9be5-a3832faad4b2"
  }
]
```

## List user buckets

You can retrieve a list of buckets owned by users of the HCP for cloud scale system by user ID and bucket name. You can also filter the list to retrieve a subset.

**HTTP request syntax (URI)**

```
POST https://host_ip:9099/mapi/v1/user/list_buckets
```



## Request structure

The request body is:

```
{
  "id": "uuid",
  "count": [nnnn],
  "startingAfter": ["string"]
}
```

Parameter	Required	Type	Description
id	Yes	UUID	The ID of the user.
count	No	Integer	The number of buckets to return. Up to 1000 buckets; default: 1000.
startingAfter	No	String	The bucket name to start after alphabetically. Leave blank to start from the beginning of the list. Use this parameter to retrieve bucket lists in groups.

## Response structure



**Note:** If the user ID provided does not exist, the response is an empty list.

The response body structure is:

```
[
  {
    "bucketId": "",
    "bucketName": ""
  },
  .
  .
  .
]
```

Parameter	Type	Description
bucketId	UUID	The UUID of the bucket.
bucketName	String	The display name of the bucket.

**Return codes**

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	The request is missing a valid parameter.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for user data. Resend using POST.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/user/list_buckets
```

JSON request:

```
{
  "id": "3fa85f64-0810-1954-b3fc-2c963f66afa6",
  "count": 1,
  "startingAfter": "September"
}
```

JSON response:

```
[
  {
    "bucketId": "9b805cee-56aa-42a7-b89e-9087d6ade984",
    "bucketName": "October"
  }
]
```

## Revoke OAuth user tokens

The method `user/revoke_tokens` revokes OAuth tokens belonging to a specific user. You can use the method `/user/list` to look up the ID of the user whose tokens you want to revoke.

**HTTP request syntax (URI)**

```
POST https://host_ip:9099/mapi/v1/user/revoke_tokens
```

**Request structure**

The request body is:

```
{
  "id": "uuid"
}
```

Parameter	Required	Type	Description
id	Yes	UUID	The UUID of the user whose OAuth credentials you are revoking.

**Response structure**

Not applicable.

**Return codes**

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	User ID not valid.
401	Unauthorized	Access was denied because credentials are not valid.
404	Not Found	The user ID was not found.
405	Method Not Allowed	The specified HTTP method is not allowed for user data. Resend using POST.

**Example**

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/user/revoke_tokens
```

JSON request:

```
{
  "id": "3fa85f64-1024-1954-b3fc-2c963f66afa6"
}
```

## Revoke S3 user credentials

The method `user/revoke_credentials` revokes all S3 credentials belonging to a specific user. Users can revoke their own S3 credentials. Users with appropriate permissions can revoke other users' S3 credentials. You can use the method `/user/list` to look up the ID of the user whose credentials you want to revoke.

### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/user/revoke_credentials
```

### Request structure

The request body is:

```
{
  "id": "uuid"
}
```

Parameter	Required	Type	Description
id	Yes	UUID	The UUID of the user whose S3 credentials you are revoking.

### Response structure

The response body is:

```
{
  "id": {
    "id": "uuid"
  },
  "secretKey": "key",
  "accessKey": "key"
}
```

Parameter	Type	Description
id	UUID	The ID of the user.
secretKey	String	The secret key of the S3 credentials.
accessKey	String	The access key of the S3 credentials.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
400	Bad Request	User ID is not valid.
401	Unauthorized	Access was denied because credentials are not valid.
404	Not Found	The user ID was not found.
405	Method Not Allowed	The specified HTTP method is not allowed for user data. Resend using POST.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/user/revoke_credentials
```

JSON request:

```
{
  "id": "3fa85f64-1024-1954-b3fc-2c963f66afa6"
}
```

JSON response:

```
{
  "id": {
    "id": "3fa85f64-1024-1954-b3fc-2c963f66afa6"
  },
  "secretKey": "bff...",
  "accessKey": "TSP18Pop..."
}
```

---

## Chapter 6: Public methods

The management API includes public methods.

### Get service port

The method `public/discovery/get_service_port` retrieves the external port used by an HCP for cloud scale service. You don't need an OAuth token to use this method.

#### HTTP request syntax (URI)

```
POST https://host_ip:9099/mapi/v1/public/discovery/get_service_port
```

#### Request structure

The request body is:

```
{
  "portType": "type"
}
```

Parameter	Required	Type	Description
portType	Yes	String	The type of service: <ul style="list-style-type: none"><li>ADMIN_APP: System Management application.</li><li>JAEGER_QUERY: Tracing service.</li><li>MAPI: Management API.</li><li>PROMETHEUS: Metrics service.</li></ul>

#### Response structure

The response body is:

```
{
  "portType": "type",
  "portNumber": nnnnn
}
```

Parameter	Type	Description
portNumber	Integer	The HTTP port of service.

### Return codes

Status code	HTTP name	Description
200	OK	The request was executed successfully.
401	Unauthorized	Access was denied because credentials are not valid.
405	Method Not Allowed	The specified HTTP method is not allowed for public data. Resend using POST.

### Example

Request example:

```
POST https://10.10.24.195:9099/mapi/v1/discovery/get_service_port
```

JSON request:

```
{
  "portType": "ADMIN_APP"
}
```

JSON response:

```
{
  "portType": "ADMIN_APP",
  "portNumber": 8000
}
```

**Hitachi Vantara**

Corporate Headquarters  
2535 Augustine Drive  
Santa Clara, CA 95054 USA



[HitachiVantara.com/contact](https://HitachiVantara.com/contact)