



# Work with the management node REST API

HCI

NetApp  
June 25, 2020

This PDF was generated from [https://docs.netapp.com/us-en/hci/docs/task\\_mnode\\_work\\_overview\\_API.html](https://docs.netapp.com/us-en/hci/docs/task_mnode_work_overview_API.html) on June 25, 2020. Always check docs.netapp.com for the latest.

# Table of Contents

- Work with the management node REST API ..... 1
  - Management node REST API UI overview ..... 1
  - Get authorization to use REST APIs ..... 1
  - Configure a proxy server ..... 2
  - Get logs from management services ..... 4

# Work with the management node REST API

## Management node REST API UI overview

By using the built-in REST API UI ([https://\[mNode IP\]/mnode](https://[mNode IP]/mnode)), you can run or understand APIs relating to the management node services, including proxy server configuration, service level updates, or asset management.

Tasks you can perform with REST APIs:

- [Get authorization to use REST APIs](#)
- [Enable Active IQ and NetApp HCI monitoring](#)
- [Add compute and controller assets to the management node](#)
- [Change the storage cluster administrator password](#)
- [Configure a proxy server for the management node](#)
- [Get logs from management services](#)

### Find more information

- [Access the management node](#)
- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Get authorization to use REST APIs

You must authorize before you can use APIs for management services in the REST API UI. You do this by obtaining an access token.

To obtain a token, you provide cluster admin credentials and a client ID. Each token lasts approximately ten minutes. After a token expires, you can authorize again for a new access token.

Authorization functionality is set up for you during management node installation and deployment. The token service is based on the storage cluster you defined during setup.

### *Before you begin*

- Your cluster version should be running NetApp Element software 11.3 or later.
- You should have deployed a management node running version 11.3 or later.

### *Steps*

1. Open the REST API UI on the management node:

```
https://[management node IP address]/mnode
```

2. Click **Authorize**.



Alternately, you can click on a lock icon next to any service API.

3. Complete the following:

- a. Enter the cluster user name and password.
- b. Select **Request body** from the Type drop-down list.
- c. Enter the client ID as **mnode-client**.
- d. Do not enter a value for the client secret.
- e. Click **Authorize** to begin a session.



If the error message **Auth Error TypeError: Failed to fetch** is returned after you attempt to authorize, you might need to accept the SSL certificate for the MVIP of your cluster. Copy the IP in the Token URL, paste the IP into another browser tab, and authorize again.

The Available authorizations screen indicates **Authorized**.

4. Close the Available authorizations dialog box.



If you try to run a command after the token expires, a **401 Error: UNAUTHORIZED** message appears. If you see this, authorize again.

## Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Configure a proxy server

If your cluster is behind a proxy server, you must configure the proxy settings so that you can reach a public network.

A proxy server is used for telemetry collectors and reverse tunnel connections. You can enable and configure a proxy server using the REST API UI if you did not already configure a proxy server during installation or upgrade. You can also modify existing proxy server settings or disable a proxy server.

The command to configure a proxy server updates and then returns the current proxy settings for the

management node. The proxy settings are used by Active IQ, the NetApp HCI monitoring service that is deployed by the NetApp Deployment Engine, and other Element software utilities that are installed on the management node, including the reverse support tunnel for NetApp Support.

#### *Before you begin*

- You should know host and credential information for the proxy server you are configuring.
- Ensure that your cluster version is running NetApp Element software 11.3 or later.
- Ensure that you have deployed a management node running version 11.3 or later.

#### *Steps*

1. Access the REST API UI on the management node by entering the management node IP address followed by `/mnode`:

```
https://[management node IP]/mnode
```

2. Click **Authorize** or any lock icon and complete the following:
  - a. Enter the cluster user name and password.
  - b. Enter the client ID as `mnode-client`.
  - c. Click **Authorize** to begin a session.
  - d. Close the window.
3. Click **PUT /settings**.
4. Click **Try it out**.
5. To enable a proxy server, you must set `use_proxy` to true. Enter the IP or host name and proxy port destinations.

The proxy user name, proxy password, and SSH port are optional and should be omitted if not used.

```
{
  "proxy_ip_or_hostname": "[IP or name]",
  "use_proxy": [true/false],
  "proxy_username": "[username]",
  "proxy_password": "[password]",
  "proxy_port": [port value],
  "proxy_ssh_port": [port value: default is 443]
}
```

6. Click **Execute**.

## **Find more information**

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Get logs from management services

You can retrieve logs from the services running on the management node by using the REST API.

You can pull logs from all public services or specify specific services and use query parameters to better define the return results.

### *Before you begin*

- Ensure that your cluster version is running NetApp Element software 11.3 or later.
- Ensure that you have deployed a management node running version 11.3 or later.

### *Steps*

1. Access the REST API UI on the management node by entering the management node IP address followed by /mnode:

```
https://[IP address]/mnode
```

2. Click **Authorize** or any lock icon and complete the following:
  - a. Enter the cluster user name and password.
  - b. Enter the client ID as `mnode-client`.
  - c. Click **Authorize** to begin a session.
3. Click **GET /logs**.
4. Click **Try it out**.
5. Specify the following parameters:
  - **Lines:** Enter the number of lines you want the log to return. This parameter is an integer that defaults to 1000.



Avoid requesting the entire history of log content by setting Lines to 0.

- **service-name:** Enter a service name.



Use the GET /services command to list services on the management node.

- **type:** Select the specific log type to pull:
  - **service:** Pulls regular public running services. This is the default and most common option.

- **syslog:** Pulls all syslog from the host machine.
- **all:** Pulls from all public services and syslogs.
- **since:** Adds an ISO-8601 timestamp for the service logs starting point.



Use a reasonable **since** parameter when gathering logs of wider timespans.

- **archived:** Adds archived files to the log request.

6. Click **Execute**.

## Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

## Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.