



Identity and authorization

Cloud Manager Automation

NetApp

February 21, 2022

This PDF was generated from https://docs.netapp.com/us-en/cloud-manager-automation/platform/get_nss_key.html on February 21, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- Identity and authorization 1
 - Generate an NSS user ID 1
 - Get the client and account identifiers 1
 - Create user token 3

Identity and authorization

Generate an NSS user ID

You can create a NetApp Support Site (NSS) user ID through the Cloud Manager web user interface. This ID is included when creating a Cloud Manager working environment.

About this task

Registering NSS credentials with Cloud Manager and creating an NSS user ID enables subscription to the Cloud Volumes ONTAP system, product support and analytics. For information about related NSS administrative tasks, see [Manage NSS credentials](#).

Before you begin

You must have a NetApp account (formerly Cloud Central account). You normally create this account when first signing in to Cloud Manager and it's displayed at the top of the web user interface. See [Learn about NetApp accounts](#) for more information.

Steps

1. Navigate to the Cloud Manager web site using a browser:

<https://cloudmanager.netapp.com>

2. Sign in using your NetApp account (formerly Cloud Central account) credentials.
3. Click on the **?** icon at the top right of the page and select **Support**.
4. Navigate to the **NSS Management** tab and click **Add NSS Account**.
5. When prompted, click **Continue** which redirects you to a Microsoft login page.

NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

6. Provide the NSS email address and password. After successful authentication, you will be redirected to the Cloud Manager page and an NSS user ID will be automatically generated.

After you finish

You can use the generated NSS user ID when creating a working environment with your preferred licensing model and cloud provider. The NSS user ID is required with BYOL licensing and optional for the PAYGO subscription.

Get the client and account identifiers

You can sign into the Cloud Manager web user interface to retrieve the client and account identifiers to use with the workflows. You can use these identifiers to access the metadata, authentication, and security related information.



This page includes two tasks describing how to use the Cloud Manager web user interface to retrieve the ID values. You can also use the Cloud Manager REST API to get the ID values. See [Get supported services](#) for more information.

Get the client identifier

You can retrieve the client ID and use it with the x-agent-id HTTP request header.

About this task

You need to access the client ID which is unique for each Cloud Manager Connector and then use it as the agent identifier.

Before you begin

You must have a NetApp account (formerly Cloud Central account). You created this account when you first logged in to Cloud Manager and it was displayed at the top of the Cloud Manager user interface. See [Learn more about NetApp accounts](#) for more information.

Steps

1. Navigate to the Cloud Manager web site using a browser:

<https://cloudmanager.netapp.com>

2. Sign in using your NetApp account (formerly Cloud Central account) credentials.
3. Click **Connector** at the top right of the page and select **Manage Connectors**.
4. On the **Manage Connectors** page, click the ellipses (...) icon.
5. Select the **Connector ID**. This value is based on the client ID.

You can use the Connector ID in the x-agent-id HTTP request header as shown in the workflow curl examples, `uzJbMFKEnuzi2ryLaENbCP52KBTXx0aIclients`.

Get the account identifier

You can also retrieve the account ID.

About this task

You can create multiple accounts and access the unique identifier for each account.

Before you begin

You must have a NetApp account (formerly Cloud Central account). You created this account when you first logged in to Cloud Manager and it's displayed at the top of the Cloud Manager user interface. [Learn more about NetApp accounts](#).

Steps

1. Navigate to the Cloud Manager web site using a browser:

<https://cloudmanager.netapp.com>

2. Sign in using your NetApp account (formerly Cloud Central account) credentials.
3. Click the **Account** drop-down and click **Manage Account** for the selected account.
4. In the **Overview** section copy the **Account ID** value.

Create user token

You must generate a bearer token to authenticate and access the Cloud Manager REST API. There are two workflows available depending on the type of authentication. You need to select the correct workflow:

- [Federated](#)
- [Nonfederated](#)

Create a user token with federated authentication

This workflow describes how to create an access token when using federated authentication.

Before you begin

Review the parameters in the **JSON input example** for the second workflow step. In particular, you must have the client identifier.

1. Generate a NetApp refresh token

Navigate to [Refresh Token Generator](#) and generate a long-lived token. You need to provide this in the `refresh_token` JSON input parameter in the next step.

2. Generate the user token

This API call uses the *Auth0* authentication service and not the NetApp Cloud Manager service. See the URL in the curl example below and adjust for your environment as needed.

HTTP method	Resource path
POST	/oauth/token

curl example

```
curl --location --request POST 'https://netapp-cloud-account.auth0.com/oauth/token' --header 'Content-Type: application/json' --d @JSONinput
```

Input parameters

The JSON input example includes the list of input parameters.

JSON input example

```
{
  "grant_type": "refresh_token",
  "refresh_token": "<REFRESH_TOKEN>",
  "client_id": "<CLIENT_ID>"
}
```

Output

The JSON output example includes the list of returned values. The `expires_in` value is expressed in seconds.

JSON output example

```
{
  "access_token": "<USER_TOKEN>",
  "id_token": "<ID_TOKEN>",
  "scope": "openid profile cc:update-password",
  "expires_in": 86400,
  "token_type": "Bearer"
}
```

Create a user token with nonfederated authentication

This workflow describes how to create an access token when using non-federated authentication.

Before you begin

Review the parameters in the **JSON input example** for the first workflow step. In particular, you must have the account credentials and the client identifier.

1. Generate the user token

This API call uses the *Auth0* authentication service and not the NetApp Cloud Manager service. See the URL in the curl example below and adjust for your environment as needed.

HTTP method	Resource path
POST	/oauth/token

curl example

```
curl --location --request POST 'https://netapp-cloud-account.auth0.com/oauth/token' --header 'Content-Type: application/json' --d @JSONinput
```

Input parameters

The JSON input example includes the list of input parameters.

JSON input example

```
{
  "username": "user@my-company-demo.com",
  "scope": "openid profile",
  "audience": "https://api.cloud.netapp.com",
  "client_id": "<CLIENT_ID>",
  "grant_type": "password",
  "password": "userpassword",
  "Realm": "Username-Password-Authentication"
}
```

Output

The JSON output example includes the list of returned values. The `expires_in` value is expressed in seconds.

JSON output example

```
{
  "access_token": "<USER_TOKEN>",
  "id_token": "<ID_TOKEN>",
  "scope": "openid profile cc:update-password",
  "expires_in": 86400,
  "token_type": "Bearer"
}
```

Copyright Information

Copyright © 2022 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.