



NetApp accounts

Set up and administration

NetApp

June 16, 2022

Table of Contents

- NetApp accounts 1
 - Managing your NetApp account..... 1
 - Monitoring operations in your account 10
- Roles 13

NetApp accounts

Managing your NetApp account

After you perform initial setup, you can administer your account settings later by managing users, service accounts, workspaces, Connectors, and subscriptions.

[Learn more about how NetApp accounts work.](#)

Managing your account with the Tenancy API

If you want to manage your account settings by sending API requests, then you'll need to use the *Tenancy* API. This API is different than the Cloud Manager API, which you use to create and manage Cloud Volumes ONTAP working environments.

[View endpoints for the Tenancy API](#)

Creating and managing users

The user's in your account can access the manage the resources in your account's workspaces.

Adding users

Associate Cloud Central users with the NetApp account so those users can create and manage working environments in Cloud Manager.

Steps

1. If the user hasn't already done so, ask the user to go to [NetApp Cloud Central](#) and sign up.
2. From the top of Cloud Manager, click the **Account** drop-down.



3. Click **Manage Account** next to the currently selected account.



4. From the Members tab, click **Associate User**.
5. Enter the user's email address and select a role for the user:
 - **Account Admin**: Can perform any action in Cloud Manager.
 - **Workspace Admin**: Can create and manage resources in assigned workspaces.
 - **Compliance Viewer**: Can only view Cloud Data Sense compliance information and generate reports for workspaces that they have permission to access.
 - **SnapCenter Admin**: Can use the SnapCenter Service to create application consistent backups and restore data using those backups. *This service is currently in Beta.*
6. If you selected Workspace Admin or Compliance Viewer, select one or more workspaces to associate with that user.



The image shows a dialog box titled "Associate User" with a user icon at the top. Below the title is a light blue instruction bar stating: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." Below this are three input fields: "User's Email" containing "test@netapp.com", "Role" with a dropdown menu showing "Workspace Admin", and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close icon. At the bottom are two buttons: a grey "Cancel" button and a blue "Associate User" button.



Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1

Cancel Associate User

7. Click **Associate**.

Result

The user should receive an email from NetApp Cloud Central titled "Account Association." The email includes the information needed to access Cloud Manager.

Removing users

Disassociating a user makes it so they can no longer access the resources in a NetApp account.

Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.



- From the Members tab, click the action menu in the row that corresponds to the user.

5 Members

Type	Name	Email	Role	Workspace	
	Ben	[REDACTED]	Account Admin	All Workspaces	...
	Tom	[REDACTED]	Account Admin	All Workspaces	...
	Ben	[REDACTED]	Workspace Admin	None	...

- Click **Disassociate User** and click **Disassociate** to confirm.

Result

The user can no longer access the resources in this NetApp account.

Managing a Workspace Admin's workspaces

You can associate and disassociate Workspace Admins with workspaces at any time. Associating the user enables them to create and view the working environments in that workspace.






Steps


- From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.



- From the Members tab, click the action menu in the row that corresponds to the user.

5 Members

Type	Name	Email	Role	Workspace
	Ben		 Account Admin	All Workspaces
	Tom		 Account Admin	All Workspaces
	Ben		Workspace Admin	Newone



3. Click **Manage Workspaces**.

4. Select the workspaces to associate with the user and click **Apply**.

Result

The user can now access those workspaces from Cloud Manager, as long as the Connector was also associated with the workspaces.

Creating and managing service accounts

A service account acts as a "user" that can make authorized API calls to Cloud Manager for automation purposes. This makes it easier to manage automation because you don't need to build automation scripts based on a real person's user account who can leave the company at any time. And if you're using federation, you can create a token without generating a refresh token from the cloud.

You give permissions to a service account by assigning it a role, just like any other Cloud Manager user. You can also associate the service account with specific workspaces in order to control the working environments (resources) that the service can access.

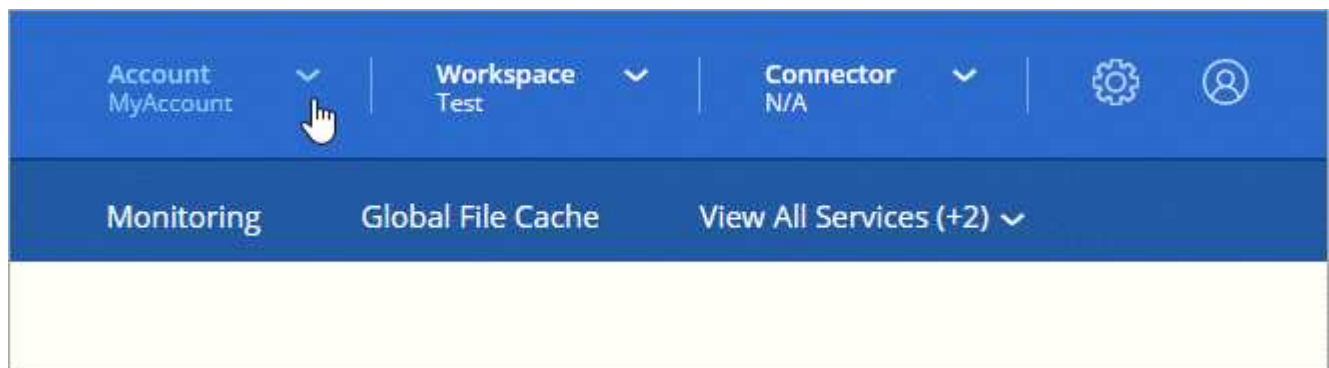
When you create the service account, Cloud Manager enables you to copy or download a client ID and client secret for the service account. This key pair is used for authentication with Cloud Manager.

Creating a service account

Create as many service accounts as you need to manage the resources in your working environments.

Steps

1. From the top of Cloud Manager, click the **Account** drop-down.



2. Click **Manage Account** next to the currently selected account.



3. From the Members tab, click **Create Service Account**.
4. Enter a name and select a role. If you chose a role other than Account Admin, choose the workspace to associate with this service account.
5. Click **Create**.
6. Copy or download the client ID and client secret.

The client secret is visible only once and is not stored anywhere by Cloud Manager. Copy or download the secret and store it safely.
7. Click **Close**.

Obtaining a bearer token for a service account

In order to make API calls to the [Tenancy API](#), you'll need to obtain a bearer token for a service account.

```
curl --location --request POST 'https://netapp-cloud-account.auth0.com/oauth/token' \
--header 'Content-Type: application/json' \
--data-raw '{
  "grant_type": "client_credentials",
  "client_secret": "<client secret>",
  "audience": "https://api.cloud.netapp.com",
  "client_id": "<client id>"
}'
```

Copying the client ID

You can copy a service account's client ID at any time.

Steps

1. From the Members tab, click the action menu in the row that corresponds to the service account.



2. Click **Client ID**.
3. The ID is copied to your clipboard.

Recreating keys

Recreating the key will delete the existing key for this service account and then create a new key. You won't be able to use the previous key.

Steps

1. From the Members tab, click the action menu in the row that corresponds to the service account.



2. Click **Recreate Key**.
3. Click **Recreate** to confirm.
4. Copy or download the client ID and client secret.

The client secret is visible only once and is not stored anywhere by Cloud Manager. Copy or download the secret and store it safely.

5. Click **Close**.

Deleting a service account

Delete a service account if you no longer need to use it.

Steps

1. From the Members tab, click the action menu in the row that corresponds to the service account.



2. Click **Delete**.
3. Click **Delete** again to confirm.

Managing workspaces

Manage your workspaces by creating, renaming, and deleting them. Note that you can't delete a workspace if it contains any resources. It must be empty.

Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. Click **Workspaces**.
3. Choose one of the following options:
 - Click **Add New Workspace** to create a new workspace.
 - Click **Rename** to rename the workspace.
 - Click **Delete** to delete the workspace.

Managing a Connector's workspaces

You need to associate the Connector with workspaces so Workspace Admins can access those workspaces from Cloud Manager.

If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in Cloud Manager by default.

[Learn more about users, workspaces, and Connectors.](#)

Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. Click **Connector**.
3. Click **Manage Workspaces** for the Connector that you want to associate.
4. Select the workspaces to associate with the Connector and click **Apply**.

Managing subscriptions

After you subscribe from a cloud provider's marketplace, each subscription is available from the Account Settings widget. You have the option to rename a subscription and to disassociate the subscription from one or more accounts.

For example, let's say that you have two accounts and each is billed through separate subscriptions. You might

disassociate a subscription from one of the accounts so the users in that account don't accidentally choose the wrong subscription when creating a Cloud Volume ONTAP working environment.

[Learn more about subscriptions.](#)

Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. Click **Subscriptions**.

You'll only see the subscriptions that are associated with the account that you're currently viewing.

3. Click the action menu in the row that corresponds to the subscription that you want to manage.



The screenshot shows a table titled "2 Subscriptions" with a search icon in the top right corner. The table has four columns: Name, Service, Cloud Provider, and Status. There are two rows of data. The first row is "QA Subscription" with Service "test-service", Cloud Provider "aws", and Status "Unsubscribed". The second row is "metering service subscription QA !!!!!" with Service "cloud-volumes-ontap", Cloud Provider "aws", and Status "Subscribed". An action menu is open for the second row, showing two options: "Rename Subscription" and "Manage Accounts".

Name	Service	Cloud Provider	Status
QA Subscription	test-service	aws	Unsubscribed
metering service subscription QA !!!!!	cloud-volumes-ontap	aws	Subscribed

4. Choose to rename the subscription or to manage the accounts that are associated with the subscription.

Changing your account name

Change you account name at any time to change it to something meaningful for you.

Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. In the **Overview** tab, click the edit icon next to the account name.
3. Type a new account name and click **Save**.

Allowing private previews

Allow private previews in your account to get access to new NetApp cloud services that are made available as a preview in Cloud Manager.

Services in private preview are not guaranteed to behave as expected and might sustain outages and be missing functionality.

Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. In the **Overview** tab, enable the **Allow Private Preview** setting.

Allowing third-party services

Allow third-party services in your account to get access to third-party services that are available in Cloud Manager. Third-party services are cloud services similar to the services that NetApp offers, but they're

managed and supported by third-party companies.

Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. In the **Overview** tab, enable the **Allow Third Party Services** setting.

Disabling the SaaS platform

We don't recommend disabling the SaaS platform unless you need to in order to comply with your company's security policies. Disabling the SaaS platform limits your ability to use NetApp's integrated cloud services.

The following services aren't available from Cloud Manager if you disable the SaaS platform:

- Cloud Data Sense
- Kubernetes
- Cloud Tiering
- Global File Cache

If you do disable the SaaS platform, you'll need to perform all tasks from [the local user interface that is available on a Connector](#).



This is an irreversible action that will prevent you from using the Cloud Manager SaaS platform. You'll need to perform actions from the local Connector. You won't have the ability to use many of NetApp's integrated cloud services, and re-enabling the SaaS platform will require the help of NetApp support.

Steps

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. In the Overview tab, toggle the option to disable use of the SaaS platform.

Monitoring operations in your account

You can monitor the status of the operations that Cloud Manager is performing to see if there are any issues that you need to address. You can view the status in the Notification Center or in the Timeline.

This table provides a comparison of the Notification Center and the Timeline so you can understand what each has to offer.

Notification Center	Timeline
Shows high level status for events and actions	Provides details for each event or action for further investigation
Shows status for the current login session - the information won't appear in the Notification Center after you log off	Retains status for up to the last month
Shows only actions initiated in the user interface	Shows all actions from the UI or APIs

Notification Center	Timeline
Shows user-initiated actions	Shows all actions, whether user-initiated or system-initiated
Filter results by importance	Filter by service, action, user, status, and more

Monitoring operations status using the Notification Center

Notifications are like events where they track the progress of operations that you've initiated in Cloud Manager so you can verify whether the operation was successful, or if it failed. They enable you to view the status for Cloud Manager operations (and cloud services operations in the future) that you initiated during your current login session.

At this time, only notifications for creating and deleting the following Cloud Volumes ONTAP objects are supported:

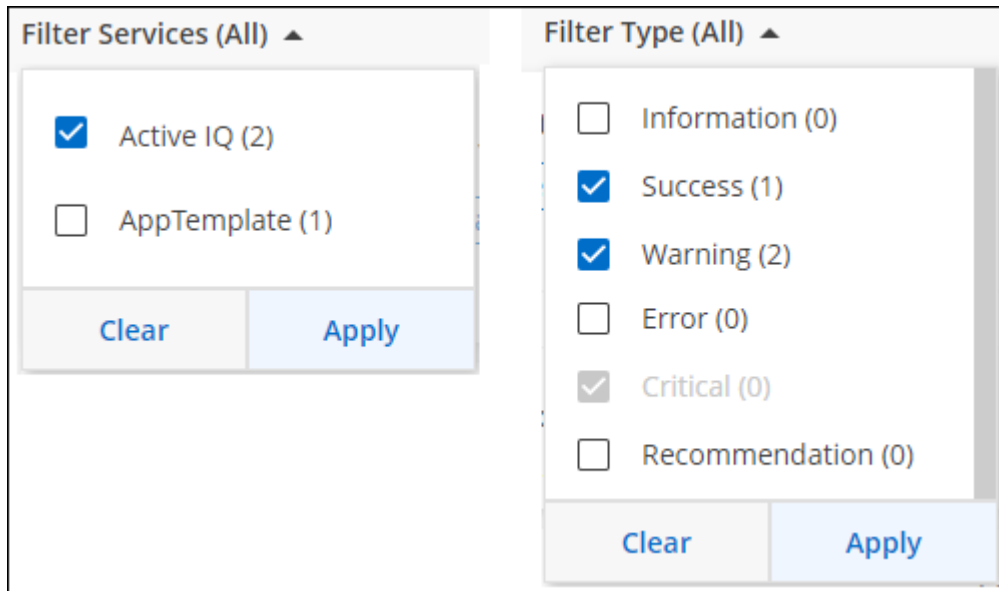
- working environments
- aggregates
- volumes

You display the notifications by clicking the notification bell (🔔) in the menu bar. The color of the little bubble in the bell indicates the highest level severity notification that is active. So if you see a red bubble, it means there's an important notification that you should look at.



Filtering notifications

By default you'll see all notifications. You can filter the notifications that you see in the Notification Center to show only those notifications that are important to you. You can filter by Cloud Manager "Service" and by notification "Type".

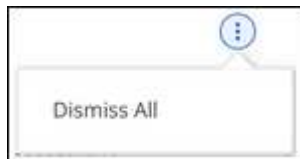


For example, if you want to see only "Error" and "Warning" notifications for Cloud Manager operations, select those entries and you'll see only those types of notifications.

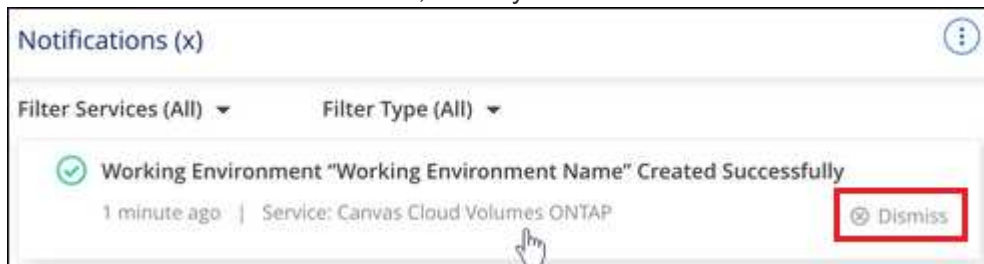
Dismissing notifications

You can remove notifications from the page if you no longer need to see them. You can dismiss all notifications at once, or you can dismiss individual notifications.

To dismiss all notifications, in the Notification Center, click  and select **Dismiss All**.



To dismiss individual notifications, hover your cursor over the notification and click **Dismiss**.



Auditing user activity in your account

The Timeline in Cloud Manager shows the actions that users completed to manage your account. This includes management actions such as associating users, creating workspaces, creating Connectors, and more.

Checking the Timeline can be helpful if you need to identify who performed a specific action, or if you need to

identify the status of an action.

Steps

1. Click **All Services > Timeline**.
2. Under the Filters, click **Service**, enable **Tenancy**, and click **Apply**.

Result

The Timeline updates to show you account management actions.

Roles

The Account Admin, Workspace Admin, Compliance Viewer, and SnapCenter Admin roles provide specific permissions to users.

The Compliance Viewer role is for read-only Cloud Data Sense access.

Task	Account Admin	Workspace Admin	Compliance Viewer	SnapCenter Admin
Manage working environments	Yes	Yes	No	No
Enable services on working environments	Yes	Yes	No	No
View data replication status	Yes	Yes	No	No
View the timeline	Yes	Yes	No	No
Switch between workspaces	Yes	Yes	Yes	No
View Data Sense scan results	Yes	Yes	Yes	No
Delete working environments	Yes	No	No	No
Connect Kubernetes clusters to working environments	Yes	No	No	No
Receive the Cloud Volumes ONTAP report	Yes	No	No	No
Create Connectors	Yes	No	No	No
Manage NetApp accounts	Yes	No	No	No
Manage credentials	Yes	No	No	No
Modify Cloud Manager settings	Yes	No	No	No
View and manage the Support Dashboard	Yes	No	No	No

Task	Account Admin	Workspace Admin	Compliance Viewer	SnapCenter Admin
Remove working environments from Cloud Manager	Yes	No	No	No
Install an HTTPS certificate	Yes	No	No	No
Use the SnapCenter Service	Yes	Yes	No	Yes

Related links

- [Setting up workspaces and users in the NetApp account](#)
- [Managing workspaces and users in the NetApp account](#)

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.