



# Managing user access

## Snap Creator Framework

Zachary Wambold  
January 19, 2021

# Table of Contents

- Managing user access ..... 1
  - Users ..... 1
  - Roles ..... 1
  - Permissions ..... 1
  - Operations ..... 2
  - Profiles ..... 2
- Managing user access for storage controllers ..... 3

# Managing user access

Snap Creator provides security features such as role-based access control (RBAC), which enables you to manage user access within Snap Creator.

RBAC involves users, roles, permissions, operations, and profiles. The users, roles, and permissions can be defined by Snap Creator users.

## Users

- Users are uniquely identified by a user name and password.
- A user can be assigned and unassigned to one or more roles and profiles.
- The `SNAPCREATOR_USER` in the `snapcreator.properties` file is added as a user when the Snap Creator Server is started.
- The `SNAPCREATOR_USER` in the `snapcreator.properties` file is assigned the Default Administrator role when the user is created during startup.

## Roles

Roles have one or more permissions. The assigned permissions determine the actions a user can perform and also which GUI elements the user can access. There are three built-in roles:

- **ADMINISTRATOR**

Has full access to all the APIs. This is the only role which can create, edit, and delete users.

- **OPERATOR**

This role is configured to be a super user and has access to all the APIs except RBAC.

- **VIEWER**

Has very limited access. This role has access to read-only Snap Creator API calls.

These built-in roles cannot be added, removed, or modified.

## Permissions

Permissions are a set of operations the user is authorized to perform. The following are built-in permissions:

- **BACKUP**

Required to perform a backup or clone operation.

- **CONFIGURATION**

Required to create, read, update, and delete configuration files.

- **CUSTOM**

Required to start a custom plug-in operation.

- **EXTENDED\_REPOSITORY**

Required to perform catalog (also known as extended repository) operations.

- **GLOBAL**

Required to create, edit, and delete global configuration files.

- **POLICY\_ADMIN**

Required to call policy operations (for example, addPolicy, updatePolicy, removePolicy).

- **POLICY\_VIEWER**

Required for read-only policy operations.

- **RBAC\_ADMIN**

Required to manage users (for example, create, update, delete users, and roles; also to assign and unassign roles, permissions).

- **RBAC\_VIEW**

Required to view user accounts, assigned roles, and assigned permissions.

- **RESTORE**

Required to perform restore operations.

- **SCHEDULER**

Required to perform scheduler operations.

- **VIEWER**

Provides authorization for read-only operations.

## Operations

Operations are the base values that Snap Creator checks for authorization. Some examples of operations are getTask, fileCloneCreate, createTask, dirCreate, and so on.



Operations cannot be added, removed, or modified.

## Profiles

- Profiles are assigned to users.
- Profiles in RBAC are created in the profile directory on the file system.
- Certain Snap Creator APIs check if a user is assigned to a profile and also check the permissions for operations.

For example, if a user wants a job status, RBAC verifies if the user has authorization to call SchedulerGetJob and then checks if the profile associated with the job is assigned to the user.

- If a user, who is assigned the Operator role, creates a profile, then that profile is automatically assigned to the user.

## Managing user access for storage controllers

If you are not using the Active IQ Unified Manager proxy, you need a user name and password to communicate with the storage controllers. Passwords can be encrypted for security.



You should not use the root user or the admin/vsadmin user. Best practice is to create a backup user with the necessary API permissions.

Network communications are through HTTP (80) or HTTPS (443), so you must have one or both of these ports open between the host where Snap Creator runs and the storage controllers. A user must be created on the storage controllers for authentication. For HTTPS, you must ensure that the user is enabled and configured on the storage controllers.

## Copyright Information

Copyright © 2021 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.