



Managing user access

OnCommand Unified Manager 9.5

NetApp
October 23, 2024

Table of Contents

Managing user access	1
Adding users	1
Editing the user settings	1
Testing a remote user or remote group	2
Viewing users	2
Deleting users or groups	3
Changing the local user password	3
What the maintenance user does	4
What RBAC is	4
What role-based access control does	4
Definitions of user types	4
Definitions of user roles	5
Unified Manager user roles and capabilities	6
Description of user access windows and dialog boxes	8

Managing user access

You can create roles and assign capabilities to control user access to selected cluster objects. You can identify users who have the required capabilities to access selected objects within a cluster. Only these users are provided access to manage the cluster objects.

Adding users

You can add local users or database users by using the Management/Users page. You can also add remote users or groups that belong to an authentication server. You can assign roles to these users and, based on the privileges of the roles, users can manage the storage objects and data with Unified Manager, or view the data in a database.

Before you begin

- You must have the OnCommand Administrator role.
- To add a remote user or group, you must have enabled remote authentication and configured your authentication server.
- If you plan to configure SAML authentication so that an identity provider (IdP) authenticates users accessing the graphical interface, make sure these users are defined as “remote” users.

Access to the UI is not allowed for users of type “local” or “maintenance” when SAML authentication is enabled.

About this task

If you add a group from Windows Active Directory, then all direct members and nested subgroups can authenticate to Unified Manager, unless nested subgroups are disabled. If you add a group from OpenLDAP or other authentication services, then only the direct members of that group can authenticate to Unified Manager.

Steps

1. In the toolbar, click  , and then click **Users** in the left Management menu.
2. On the **Management/Users** page, click **Add**.
3. In the **Add User** dialog box, select the type of user that you want to add, and enter the required information.

When entering the required user information, you must specify an email address that is unique to that user. You must avoid specifying email addresses that are shared by multiple users.

4. Click **Add**.

Editing the user settings

You can edit user settings—such as the email address and role—that are specified each user. For example, you might want to change the role of a user who is a storage operator,

and assign storage administrator privileges to the user.

Before you begin

You must have the OnCommand Administrator role.

About this task

When you modify the role that is assigned to a user, the changes are applied when either of the following actions occur:

- The user logs out and logs back in to Unified Manager.
- Session timeout of 24 hours is reached.

Steps

1. In the toolbar, click , and then click **Users** in the left Management menu.
2. In the **Management/Users** page, select the user for which you want to edit settings, and click **Edit**.
3. In the **Edit User** dialog box, edit the appropriate settings that are specified for the user.
4. Click **Save**.

Testing a remote user or remote group

You can validate that a remote user or remote group can access the Unified Manager server by using the authentication settings that are specified for your authentication servers.

Before you begin

- You must have enabled remote authentication, and configured your authentication settings so that the Unified Manager server can validate the remote user or remote group.
- You must have the OnCommand Administrator role.

Steps

1. In the toolbar, click , and then click **Users** in the left Management menu.
2. In the **Management/Users** page, select a remote user or remote group that you want to validate, and then click **Test**.

Viewing users

You can use the Management/Users page to view the list of users who manage storage objects and data using Unified Manager. You can view details about the users, such as the user name, type of user, email address, and the role that is assigned to the users.

Before you begin

You must have the OnCommand Administrator role.

Steps

1. In the toolbar, click , and then click **Users** in the left Management menu.

The list of users is displayed in the Management/Users page.

Deleting users or groups

You can delete one or more users from the management server database to prevent specific users from accessing Unified Manager. You can also delete groups so that all the users in the group can no longer access the management server.

Before you begin

- When you are deleting remote groups, you must have reassigned the events that are assigned to the users of the remote groups.
If you are deleting local users or remote users, the events that are assigned to these users are automatically unassigned.
- You must have the OnCommand Administrator role.

Steps

1. In the toolbar, click , and then click **Users** in the left Management menu.
2. In the **Management/Users** page, select the users or groups that you want to delete, and then click **Delete**.
3. Click **Yes** to confirm the deletion.

Changing the local user password

You can change your local user login password to prevent potential security risks.

Before you begin

You must be logged in as a local user.

About this task

The passwords for the maintenance user and for remote users cannot be changed using these steps. To change a remote user password, contact your password administrator. To change the maintenance user password, see [Using the Maintenance Console](#).

Steps

1. Log in to Unified Manager.

2. From the top menu bar, click the user icon and then click **Change Password**.

The **Change Password** option is not displayed if you are a remote user.

3. In the **Change Password** dialog box, enter the current password and the new password.

4. Click **Save**.

After you finish

If Unified Manager is configured in a high-availability configuration, you must change the password on the second node of the setup. Both instances must have same password.

What the maintenance user does

The maintenance user is created during the installation of Unified Manager on a Red Hat Enterprise Linux or CentOS system. The maintenance user name is the “umadmin” user. The maintenance user has the OnCommand administrator role in the web UI, and that user can create subsequent users and assign them roles.

The maintenance user, or umadmin user, can also access the Unified Manager maintenance console.

What RBAC is

RBAC (role-based access control) provides the ability to control who has access to various features and resources in the OnCommand Unified Manager server.

What role-based access control does

Role-based access control (RBAC) enables administrators to manage groups of users by defining roles. If you need to restrict access for specific functionality to selected administrators, you must set up administrator accounts for them. If you want to restrict the information that administrators can view and the operations they can perform, you must apply roles to the administrator accounts you create.

The management server uses RBAC for user login and role permissions. If you have not changed the management server’s default settings for administrative user access, you do not need to log in to view them.

When you initiate an operation that requires specific privileges, the management server prompts you to log in. For example, to create administrator accounts, you must log in with Administrator account access.

Definitions of user types

A user type specifies the kind of account the user holds and includes remote users, remote groups, local users, database users, and maintenance users. Each of these types has its own role, which is assigned by a user with the role of OnCommand Administrator.

Unified Manager user types are as follows:

- **Maintenance user**

Created during the initial configuration of Unified Manager. The maintenance user then creates additional users and assigns roles. The maintenance user is also the only user with access to the maintenance console. When Unified Manager is installed on a Red Hat Enterprise Linux or CentOS system, the maintenance user is given the user name “umadmin.”

- **Local user**

Accesses the Unified Manager UI and performs functions based on the role given by the maintenance user or a user with the OnCommand Administrator role.

- **Remote group**

A group of users that access the Unified Manager UI using the credentials stored on the authentication server. The name of this account should match the name of a group stored on the authentication server. All users within the remote group are given access to the Unified Manager UI using their individual user credentials. Remote groups can perform functions according to their assigned roles.

- **Remote user**

Accesses the Unified Manager UI using the credentials stored on the authentication server. A remote user performs functions based on the role given by the maintenance user or a user with the OnCommand Administrator role.

- **Database user**

Has read-only access to data in the Unified Manager database, has no access to the Unified Manager web interface or the maintenance console, and cannot execute API calls.

Definitions of user roles

The maintenance user or OnCommand administrator assigns a role to every user. Each role contains certain privileges. The scope of activities that you can perform in Unified Manager depends on the role you are assigned and which privileges the role contains.

Unified Manager includes the following predefined user roles:

- **Operator**

Views storage system information and other data collected by Unified Manager, including histories and capacity trends. This role enables the storage operator to view, assign, acknowledge, resolve, and add notes for the events.

- **Storage Administrator**

Configures storage management operations within Unified Manager. This role enables the storage administrator to configure thresholds and to create alerts and other storage management-specific options and policies.

- **OnCommand Administrator**

Configures settings unrelated to storage management. This role enables the management of users, security certificates, database access, and administrative options, including authentication, SMTP,

networking, and AutoSupport.



When Unified Manager is installed on Linux systems, the initial user with the OnCommand Administrator role is automatically named “umadmin”.

- **Integration Schema**

This role enables read-only access to Unified Manager database views for integrating Unified Manager with OnCommand Workflow Automation (WFA).

- **Report Schema**

This role enables read-only access to reporting and other database views directly from the Unified Manager database. The databases that can be viewed include:

- netapp_model_view
- netapp_performance
- ocum
- ocum_report
- ocum_report_birt
- opm
- scalemonitor

Unified Manager user roles and capabilities

Based on your assigned user role, you can determine which operations you can perform in Unified Manager.

The following table displays the functions that each user role can perform:

Function	Operator	Storage Administrator	OnCommand Administrator	Integration Schema	Report Schema
View storage system information	•	•	•	•	•
View other data, such as histories and capacity trends	•	•	•	•	•
View, assign, and resolve events	•	•	•		

Function	Operator	Storage Administrator	OnCommand Administrator	Integration Schema	Report Schema
View storage service objects, such as SVM associations and resource pools	•	•	•		
View threshold policies	•	•	•		
Manage storage service objects, such as SVM associations and resource pools		•	•		
Define alerts		•	•		
Manage storage management options		•	•		
Manage storage management policies		•	•		
Manage users			•		
Manage administrative options			•		
Define threshold policies			•		
Manage database access			•		
Manage integration with WFA and provide access to the database views				•	

Function	Operator	Storage Administrator	OnCommand Administrator	Integration Schema	Report Schema
Provide read-only access to reporting and other database views					•
Schedule and save reports	•	•	•		
Import and delete imported reports			•		

Description of user access windows and dialog boxes

Based on the RBAC settings, you can add users from the Management/Users page and assign appropriate roles to those users to access and monitor your clusters.

Management/Users page

The Management/Users page displays a list of your users and groups, and provides information such as the name, type of user, and email address. You can also use this page to perform tasks such as adding, editing, deleting, and testing users.

Command buttons

The command buttons enable you to perform the following tasks for selected users:

- **Add**

Displays the Add User dialog box, which enables you to add a local user, a remote user, a remote group, or a database user.

You can add remote users or groups only if your authentication server is enabled and configured.

- **Edit**

Displays the Edit User dialog box, which enables you to edit the settings for the selected user.

- **Delete**

Deletes the selected users from the management server database.

- **Test**

Enables you to validate whether a remote user or group is present in the authentication server.

You can perform this task only if your authentication server is enabled and configured.

List view

The List view displays, in tabular format, information about the users that are created. You can use the column filters to customize the data that is displayed.

- **Name**

Displays the name of the user or group.

- **Type**

Displays the type of user: Local User, Remote User, Remote Group, Database User, or Maintenance User.

- **Email**

Displays the email address of the user.

- **Role**

Displays the type of role that is assigned to the user: Operator, Storage Administrator, OnCommand Administrator, Integration Schema, or Report Schema.

Add User dialog box

You can create local users or database users, or add remote users or remote groups, and assign roles so that these users can manage storage objects and data using Unified Manager.

You can add a user by completing the following fields:

- **Type**

Enables you to specify the type of user you want to create.

- **Name**

Enables you to specify a user name that a user can use to log in to Unified Manager.

- **Password**

Enables you to specify a password for the specified user name. This field is displayed only when you are adding a local user or a database user.

- **Confirm Password**

Enables you to reenter your password to ensure the accuracy of what you entered in the Password field. This field is displayed only when you are adding a local user or a database user.

- **Email**

Enables you to specify an email address for the user; the email address specified must be unique to the user name. This field is displayed only when you are adding a remote user or a local user.

- **Role**

Enables you to assign a role to the user and defines the scope of activities that the user can perform. The role can be OnCommand Administrator, Storage Administrator, Operator, Integration Schema, or Report Schema.

Command buttons

The command buttons enable you to perform the following tasks:

- **Add**

Adds the user and closes the Add User dialog box.

- **Cancel**

Cancels the changes and closes the Add User dialog box.

Edit User dialog box

The Edit User dialog box enables you to edit only certain settings, depending on the selected user.

Details

The Details area enables you to edit the following information about a selected user:

- **Type**

This field cannot be edited.

- **Name**

This field cannot be edited.

- **Password**

Enables you to edit the password when the selected user is a database user.

- **Confirm Password**

Enables you to edit the confirmed password when the selected user is a database user.

- **Email**

Enables you to edit the email address of the selected user. This field can be edited when the selected user is a local user, LDAP user, or maintenance user.

- **Role**

Enables you to edit the role that is assigned to the user. This field can be edited when the selected user is a local user, remote user, or remote group.

Command buttons

The command buttons enable you to perform the following tasks:

- **Save**

Saves the changes and closes the Edit User dialog box.

- **Cancel**

Cancels the changes and closes the Edit User dialog box.

Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.