Security and credential management

SnapManager Oracle

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/us-en/snapmanager-oracle/windows/concept_what_user_authentication_is.html on November 04, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Security and credential management . . . 1
- What user authentication is . . . 1
- Storing encrypted passwords for custom scripts . . . 2
- Authorizing access to the repository . . . 2
- Authorizing access to profiles . . . 3
- Viewing user credentials . . . 3
  - Example of viewing user credentials . . . 3
- Clearing user credentials for all hosts, repositories, and profiles . . . 4
  - Setting credentials after clearing the credential cache . . . 4
- Deleting credentials for individual resources . . . 5
  - Deleting user credentials for repositories . . . 5
  - Deleting user credentials for hosts . . . 5
  - Deleting user credentials for profiles . . . 5

Security and credential management

You can manage security in SnapManager by applying user authentication. The user authentication method allows you to access resources such as repositories, hosts, and profiles.

When you perform an operation using either the command-line interface (CLI) or graphical user interface (GUI), SnapManager retrieves the credentials set for repositories and profiles. SnapManager saves credentials from previous installations.

The repository and profiles can be secured with a password. A credential is the password configured for the user for an object, and the password is not configured on the object itself.

You can manage authentication and credentials by performing the following tasks:

- Manage user authentication either through password prompts on operations or by using the smo credential set command.

  Set credentials for a repository, host, or profile.

- View the credentials that govern the resources to which you have access.
- Clear a user's credentials for all resources (hosts, repositories, and profiles).
- Delete a user's credentials for individual resources (hosts, repositories, and profiles).

If the repository database is on a Windows host, then both local or administrator user and the domain user must have the same credentials.

What user authentication is

SnapManager authenticates the user by using an operating system (OS) login on the host where the SnapManager server is running. You can enable user authentication either through password prompts on operations or by using the smo credential You can enable user authentication either through password prompts on operations or by using the smo credential set command.

User authentication requirements depend on where the operation is performed.

- If the SnapManager client is on the same server as the SnapManager host, you are authenticated by the OS credentials.

  You are not prompted for a password because you are already logged in to the host where the SnapManager server is running.

- If the SnapManager client and the SnapManager server are on different hosts, SnapManager needs to authenticate you with both OS credentials.

  SnapManager prompts you for passwords for any operation, if you have not saved your OS credentials in your SnapManager user credential cache. If you enter the smo credential set -host command, you save the OS credentials in your SnapManager credential cache file and so SnapManager does not prompt for the password for any operation.

If you are authenticated with the SnapManager server, you are considered the effective user. The effective user for any operation must be a valid user account on the host on which the operation is executed. For example, if you execute a clone operation, you should be able to log in to the destination host for the clone.

SnapManager for Oracle might fail in authorizing users created in Central Active Directory Services, such as LDAP and ADS. To ensure the authentication does not fail, you must set configurable auth.disableServerAuthorization to true.

As an effective user you can manage credentials in the following ways:

- Optionally, you can configure SnapManager to store user credentials in the SnapManager user credentials file.

  By default, SnapManager does not store host credentials. You might want to change this, for example, if you have custom scripts that require access on a remote host. The remote clone operation is an example of a SnapManager operation that needs the login credentials of a user for a remote host. To have SnapManager remember user host login credentials in the SnapManager user credentials cache, set the host.credentials.persist property to true in the smo.config file.

- You can authorize user access to the repository.
- You can authorize user access to profiles.
- You can view all user credentials.
- You can clear a user's credentials for all resources (hosts, repositories, and profiles).
- You can delete credentials for individual resources (hosts, repositories, and profiles).

Storing encrypted passwords for custom scripts

By default, SnapManager does not store host credentials in the user credentials cache. However, you can change this. You can edit the smo.config file to allow storing of host credentials.

The smo.config file is located at <default installation location>\properties\smo.config

1. Edit the smo.config file.
2. Set host.credentials.persist to true.

Authorizing access to the repository

SnapManager enables you to set credentials for database users to access the repository. Using credentials, you can restrict or prevent access to the SnapManager hosts, repositories, profiles, and databases.

If you set credentials by using the credential set command, SnapManager does not prompt you for a password.

You can set user credentials when you install SnapManager or later.

1. Enter the following command:

   smo credential set -repository -dbname repo_service_name -host repo_host -login -username

repo_username [-password repo_password] -port repo_port

Authorizing access to profiles

SnapManager enables you to set a password for a profile to prevent unauthorized access.

1. Enter the following command: smo credential set -profile -name profile_name [-password password]

Related information

The smo credential set command

Viewing user credentials

You can list the hosts, profiles, and repositories to which you have access.

1. To list the resources to which you have access, enter this command:smo credential list

Example of viewing user credentials

This example displays the resources to which you have access.

```
smo credential list
```

```
Credential cache for OS user "user1":
Repositories:
Host1_test_user@SMOREPO/hotspur:1521
Host2_test_user@SMOREPO/hotspur:1521
user1_1@SMOREPO/hotspur:1521
Profiles:
HSDBR (Repository: user1_2_1@SMOREPO/hotspur:1521)
PBCASM (Repository: user1_2_1@SMOREPO/hotspur:1521)
HSDB (Repository: Host1_test_user@SMOREPO/hotspur:1521) [PASSWORD NOT SET]
Hosts:
Host2
Host5
```

Related information

The smo credential list command

Clearing user credentials for all hosts, repositories, and profiles

You can clear the cache of your credentials for resources (hosts, repositories, and profiles). This deletes all of the resource credentials for the user running the command. After clearing the cache, you must authenticate your credentials again to gain access to these secured resources.

1. To clear your credentials, enter the smo credential clear command from the SnapManager CLI or select **Admin** > **Credentials** > **Clear Cache** from the SnapManager GUI.
2. Exit the SnapManager GUI.

   NOTE:

   - If you have cleared the credential cache from the SnapManager GUI, you do not need to exit the SnapManager GUI.
   - If you have cleared the credential cache from the SnapManager CLI, you must restart SnapManager GUI.
   - If you have deleted the encrypted credential file manually, you must restart the SnapManager GUI again.
3. To set the credentials again, repeat the process to set credentials for the repository, profile host, and profile. For additional information on setting the user credentials again, refer to "Setting credentials after clearing credential cache."

Related information

The smo credential clear command

Setting credentials after clearing the credential cache

After clearing the cache to remove the stored user credentials, you can set the credentials for the hosts, repositories, and profiles.

You must ensure that you set the same user credentials for the repository, profile host, and profile that you had given earlier. An encrypted credentials file is created while setting the user credentials.

The credentials file is located at C:\Documents and Settings\Administrator\Application Data\NetApp\smo\3.3.0.

From the SnapManager graphical user interface (GUI), if there is no repository under Repositories, perform the following steps:

1. Click **Tasks** > **Add Existing Repository** to add an existing repository.
2. Perform the following steps to set the credentials for repository:
   a. Right-click the repository and select **Open**.
   b. In the Repository Credentials Authentication window, enter the user credentials.
3. Perform the following steps to set the credentials for host:
   a. Right-click the host under the repository and select **Open**.
   b. In the Host Credentials Authentication window, enter the user credentials.

4. Perform the following steps to set the credentials for profile:
    a. Right-click the profile under the host and select **Open**.
    b. In the Profile Credentials Authentication window, enter the user credentials.

Deleting credentials for individual resources

You can delete the credentials for any one of the secured resources, such as a profile, repository, or host. This enables you to remove the credentials for just one resource, rather than clearing the user's credentials for all resources.

Related information

The smo credential delete command

Deleting user credentials for repositories

You can delete the credentials so a user can no longer access a particular repository. This command enables you to remove the credentials for just one resource, rather than clearing the user's credentials for all resources.

1. To delete repository credentials for a user, enter this command:smo credential delete -repository -dbnamerepo_service_name-hostrepo_host-login -usernamerepo_username-portrepo_port

Deleting user credentials for hosts

You can delete the credentials for a host so a user can no longer access it. This command enables you to remove the credentials for just one resource, rather than clearing all the user's credentials for all resources.

1. To delete host credentials for a user, enter this command:smo credential delete -host-namehost_name -username-username

Deleting user credentials for profiles

You can delete the user credentials for a profile so a user can no longer access it.

1. To delete profile credentials for a user, enter this command:smo credential delete -profile -nameprofile_name

Copyright information

Copyright © 2025 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.