Insight Security (SecurityAdmin Tool)

OnCommand Insight

NetApp
September 19, 2024

Table of Contents

SecurityAdmin Tool

OnCommand Insight provides features that allow Insight environments to operate with enhanced security. These features include encryption, password hashing, and the ability to change internal user passwords and key pairs that encrypt and decrypt passwords. You can manage these features on all servers in the Insight environment using the **SecurityAdmin Tool**.

What is the SecurityAdmin Tool?

The security admin tool supports making changes to the contents of the vaults as well as making coordinated changes to the OnCommand Insight installation.

The primary uses for the SecurityAdmin tool are for **Backup** and **Restore** of security configuration (i.e. vault) and passwords. For example, you can back up the vault on a Local Acquisition Unit and restore that on a Remote Acquisition Unit, ensuring password coordination throughout your environment. Or if you have multiple OnCommand Insight Servers in your environment, you may want to take a backup of the Server vault and restore that to other Servers to keep passwords the same. These are just two examples of the ways SecurityAdmin can be used to ensure cohesion in your environments.

It is strongly recommended to **back up the vault** whenever you backup an OnCommand Insight database. Failure to do so may result in loss of access.

The tool provides both **interactive** and **command line** modes.

Many SecurityAdmin Tool operations change the contents of the vault and also make changes to the installation, ensuring that the vault and the installation remain in sync.

For example,

- when you change an Insight user password, the user's entry in the sanscreen.users table will be updated with the new hash.
- when you change a mySQL user's password, the appropriate SQL statement will be executed to update the user's password in the mySQL instance.

In some situations, there will be multiple changes made to the installation:

- when you modify the dwh mySQL user, in addition to updating the password in the mySQL database, multiple registry entries for ODBC will be updated as well.

In the following sections the term "coordinated changes" is used to describe these changes.

Execution Modes

- Normal/Default Operation - SANscreen Server Service must be running

  For the default execution mode, the SecurityAdmin Tool requires that the **SANscreen Server service** is running. The server is used for authentication, and many coordinated changes to the installation are made by making calls to the server.

- Direct Operation - SANscreen Server Service may be running or stopped.

When run on an OCI Server or DWH installation, the tool may also be run in "direct" mode. In this mode authentication and coordinated changes are performed using the database. The Server service is not used.

Operation is the same as normal mode with the following exceptions:

- Authentication is supported only for non-domain admin users. (Users whose password and roles are in the database, not LDAP).
- The "replace keys" operation is not supported.
- The re-encryption step of vault restore is skipped.
- Recovery Mode The tool may also be run even when access to both the server and the database is not possible (for example because the root password in the vault is incorrect).

  When run in this mode, authentication is not possible and, hence, no operation with a coordinated change to the installation may be performed.

  Recovery mode may be used to:

- determine which vault entries are wrong (using the verify operation)
- replace the incorrect root password with the correct value. (This does not change the password. The user must enter the current password.)

> If the root password in the vault is incorrect and the password is not known and there is no backup of the vault with the correct root password, the installation cannot be recovered using the SecurityAdmin Tool. The only way to recover the installation is to reset the mySQL instance's password following the procedure documented at https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html. After performing the reset procedure, use the correct-stored-password operation to enter the new password into the vault.

Commands

Unrestricted Commands

Unrestricted commands make any coordinated changes to the installation (except trust stores). Unrestricted commands may be performed without user authentication.

Command	Description
backup-vault	Create a zip file containing the vault. The relative path to the vault files will match the vaults path relative to the installation root. • wildfly/standalone/configuration/vault/* • acq/conf/vault/* Note that it is strongly recommended to backup the vault whenever you back up an OnCommand Insight database.
check-for-default-keys	Check to see if the vault's keys match those of the default vault used in pre-7.3.16 instances.

correct-stored-password	Replace an (incorrect) password stored in the vault with the correct password known to the user. This may be used when the vault and installation are not consistent. **Note that it does not change the actual password in the installation.**
	change-trust-store-password Change the password used for a trust-store and store the new password in the vault. The trust-store's current password must be "known".
verify-keystore	check whether the values in the vault are correct: • for OCI users, does the hash of the password match the value in the database • for mySQL users, can a database connection be made • for keystores, can the keystore be loaded and its keys (if any) read
list-keys	list the entries in the vault (without showing the stored value)

Restricted Commands

Authentication is required for any non-hidden command which makes coordinated changes to the installation:

Command	Description
restore-vault-backup	Replaces the current vault with the vault contained in the specified vault backup file. Performs all the coordinated actions to update the installation to match the passwords in the restored vault: • update the OCI communication user passwords • update the mySQL user passwords, including root • for each keystore, if the keystore password is "known", update the keystore using the passwords from the restored vault. When run in normal mode, also reads each encrypted value from the instance, decrypts it using the current vault's encryption service, re-encrypts it using the restored vault's encryption service, and stores the re-encrypted value.
synchronize-with-vault	Performs all the coordinated actions to update the installation to match the user passwords in the restored vault: • updates the OCI communication user passwords • updates the mySQL user passwords, including root
change-password	Changes the password in the vault and performs the coordinated actions.

replace-keys	Create a new empty vault (which will have different keys than the existing vault). Then copy the entries from the current vault to the new vault. Then reads each encrypted value from the instance, decrypt it using the current vault's encryption service, re-encrypt it using the restored vault's encryption service, and store the re-encrypted value.

Coordinated Actions

Server Vault

_internal	update password hash for user in database
acquisition	update password hash for user in database if acquisition vault is present, also update the entry in the acquisition vault
dwh_internal	update password hash for user in database
cognos_admin	update password hash for user in database if DWH and windows, update SANscreen/cognos/analytics/configuration/SANscreenAP.properties to set the cognos.admin property to the password.
root	execute SQL to update the user password in mySQL instance
inventory	execute SQL to update the user password in mySQL instance

dwh	execute SQL to update the user password in mySQL instance if DWH and windows, update the windows registry to set the following ODBC related entries to the new password: • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_capacity\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_capacity_efficiency\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_fs_util\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_inventory\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_performance\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_ports\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_cloud_cost\PWD
dwhuser	execute SQL to update the user password in mySQL instance
hosts	execute SQL to update the user password in mySQL instance
keystore_password	rewrite the keystore with the new password - wildfly/standalone/configuration/server.keystore
truststore_password	rewrite the keystore with the new password - wildfly/standalone/configuration/server.trustore
key_password	rewrite the keystore with the new password - wildfly/standalone/configuration/sso.jks
cognos_archive	none

Acquisition Vault

acquisition	none
truststore_password	rewrite the keystore with the new password (if it exists) - acq/conf/cert/client.keystore

Running the Security Admin Tool - Command Line

The syntax to run the SA tool in command line mode is:

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-
options>

where

-s                      selects server vault
-au                     selects acquisition vault

-db                     selects direct operation mode

-lu <user>              user for authentication
-lp <password>          password for authentication
<addition-options>      specifies command and command arguments as
described below
```

Notes:

- The "-i" option may not be present on the command line (as this selects interactive mode).
- for the "-s" and "-au" options:
  - "-s" is not allowed on an RAU
  - "-au" is not allowed on DWH
  - if neither is present, then
    - the server vault is selected on Server, DWH, and Dual
    - the acquisition vault is selected on RAU
- The -lu and -lp options are used for user authentication.
  - If <user> is specified and <password> is not, then user will be prompted for the password.
  - If <user> is not supplied and authentication is required, then the user will be prompted for both <user> and <password>.

Commands:

Command	Usage

correct-stored-password	`securityadmin [-s | -au] [-db] -pt <key> [<value>]`
	
	`where`
	
	`-pt specifies the command ("put")`
	`<key> is the key`
	`<value> is the value. If not present, user will be prompted for value`

backup-vault	`securityadmin [-s | -au] [-db] -b [<backup-dir>]`
	
	`where`
	
	`-b specified command`
	`<backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used`
	`The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip`

backup-vault	`securityadmin [-s | -au] [-db] -ub <backup-file>`
	
	`where`
	
	`-ub specified command ("upgrade-backup")`
	`<backup-file> The location to write the backup file`

list-keys	`securityadmin [-s | -au] [-db] -l`
	
	`where`
	
	`-l specified command`

check-keys	`securityadmin [-s | -au] [-db] -ck`
	
	`where`
	
	`-ck specified command`
	
	`exit code:`
	`1 error`
	`2 default key(s)`
	`3 unique keys`

verify-keystore (server)	`securityadmin [-s] [-db] -v`
	
	`where`
	
	`-v specified command`

upgrade	`securityadmin [-s | -au] [-db] [-lu <user>] [-lp <password>] -u`
	
	`where`
	
	`-u specified command`
	
	`For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal's password from vault.`
	`For acquisition vault, if -lu is not present, then no authentication will be attempted`

replace-keys	`securityadmin [-s | -au] [-db] [-lu <user>] [-lp <password>] -rk`
	
	`where`
	
	`-rk specified command`

restore-vault-backup	`securityadmin [-s | -au] [-db] [-lu <user>] [-lp <password>] -r <backup-file>`
	
	`where`
	
	`-r specified command`
	`<backup-file> the backup file location`

change-password (server)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-un <user> entry ("user") name to update`
	`-p <password> new password. If <password not supplied, user will be prompted.`
	`-sh for mySQL user, use strong hash`

change-password for acquisition user (acquisition)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

change-password for truststore-_password (acquisition)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]`
	
	`where`
	
	`-utp specified command ("update-truststore-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

synchronize-with-vault (server)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>`
	
	`where`
	
	`-sv specified command`

Running the Security Admin Tool - Interactive Mode

Interactive - Main Menu

To run the SA tool in interactive mode, enter the following command:

```
securityadmin -i
```

On a server or dual install, SecurityAdmin will prompt the user to select either the server or local acquisition unit.

Server and Acquisition Unit nodes Detected! Select the node whose security needs to be re-configured:

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

On DWH, "Server" is automatically selected. On a remote AU, "Acquisition Unit" will automatically be selected.

Interactive - Server: Root password recovery

In Server mode, the SecurityAdmin Tool will first check that the stored root password is correct. If not, the tool will display the root password recovery screen.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

If option 1 is selected, the user will be prompted for the correct password.

```
Enter password (blank = don't change)
```

```
Enter correct password for 'root':
```

If the correct password is entered, the following will be displayed.

```
Password verified.  Vault updated
```

Pressing enter will display the server unrestricted menu.

If the wrong password is entered, the following will be displayed

```
Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```

Pressing enter will return to the recovery menu.

If option 2 is selected, the user will be prompted to provide the name of a backup file from which to read the correct password:

```
Enter Backup File Location:
```

If the password from the backup is correct, the following will be displayed.

```
Password verified.  Vault updated
```

Pressing enter will display the server unrestricted menu.

If the password in the backup is incorrect, the following will be displayed

```
Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```

Pressing enter will return to the recovery menu.

Interactive - Server: Correct Password

The "Correct Password" action is used to change the password stored in the vault so that it matches the actual password required by the installation. This command is useful in situations where a change to the installation has been made by something other than the securityadmin tool. Examples include:

- The password for a SQL user was modified by direct access to mySQL.
- A keystore is replaced or a keystore’s password is changed using keytool.
- An OCI database has been restored and that database has different passwords for the internal users

"Correct Password" will first prompt the user to select which password to store the correct value.

```
Replace incorrect stored password with correct password.  (Does not change
the required password)
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

After selecting which entry to correct, the user is prompted for how they wish to provide the value.

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

If option 1 is selected, the user will be prompted for the correct password.

```
Enter password (blank = don't change)
```

```
Enter correct password for '{user}':
```

If the correct password is entered, the following will be displayed.

```
Password verified.  Vault updated
```

Pressing enter will return to the server unrestricted menu.

If the wrong password is entered, the following will be displayed

```
Password verification failed - {additional information}
Vault entry not updated.
```

Pressing enter will return to the server unrestricted menu.

If option 2 is selected, the user will be prompted to provide the name of a backup file from which to read the correct password:

```
Enter Backup File Location:
```

If the password from the backup is correct, the following will be displayed.

```
Password verified.  Vault updated
```

Pressing enter will display the server unrestricted menu.

If the password in the backup is incorrect, the following will be displayed

```
Password verification failed - {additional information}
Vault entry not updated.
```

Pressing enter will display the server unrestricted menu.

Interactive - Server: Verify Vault Contents

Verify Vault Contents will check whether the vault has keys which match the default vault distributed with earlier OCI versions and will check whether each value in the vault matches the installation.

The possible results for each key are:

OK	The vault value is correct
Not Checked	The value cannot be checked against the installation
BAD	The value does not match the installation
Missing	An expected entry is missing.

```
Encryption keys secure: unique, non-default encryption keys detected

             cognos_admin: OK
                    hosts: OK
             dwh_internal: OK
                inventory: OK
                  dwhuser: OK
        keystore_password: OK
                      dwh: OK
      truststore_password: OK
                     root: OK
                _internal: OK
          cognos_internal: Not Checked
             key_password: OK
              acquisition: OK
           cognos_archive: Not Checked
 cognos_keystore_password: Missing


Press enter to continue
```

Interactive - Server: Backup

Backup will prompt for the directory into which the backup zip file should be stored. The directory must already exist, and the file name will be ServerSecurityBackup-yyyy-mm-dd-hh-mm.zip.

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:

Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

Interactive - Server: Login

The login action is used to authenticate a user and gain access to operations which modify the installation. The user must have admin privileges. When running with the server, any admin user may be used; when running in direct mode, the user must be a local user rather than an LDAP user.

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

or

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

If the password is correct and the user is an admin user, the restricted menu will be displayed.

If the password is incorrect, the following will be displayed:

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

If the user is not an admin, the following will be displayed:

```
Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!
```

Interactive - Server: Restricted Menu

Once the user logs in, the tool displays the Restricted Menu.

```
Logged in as: admin
Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:
```

Interactive - Server: Change Password

The "Change Password" action is used to change an installation password to a new value.

"Change Password" will first prompt the user to select which password to change.

```
Change Password
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

After selecting which entry to correct, if the user is a mySQL user, the user will be asked whether to strong hashing for the password

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections

Use strong password hash? (Y/n): y
```

Next, the user is prompted for the new password.

```
New Password for '{user}':
If the password is empty, the operation is cancelled.

Password is empty - cancelling operation
```

If a non-empty password is entered, the user is prompted to confirm the password.

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

If the change is unsuccessful, the error or exception will be displayed.

Interactive - Server: Restore

Interactive - Server: Change Encryption Keys

The Change Encryption Keys action will replace the encryption key used to encrypt the vault entries and replace the encryption key used for the vault's encryption service. Because the encryption service's key is changed, encrypted values in the database will be re-encrypted; they will be read, decrypted with the current key, encrypted with the new key, and saved back to the database.

This action is not supported in direct mode as the server provides the re-encryption operation for some database content.

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

Interactive - Server: Fix Installation

The Fix Installation action will update the installation. All installation passwords that are changeable via the securityadmin tool, except root, will be set to the passwords in the vault.

- The OCI internal users' passwords will be updated.
- mySQL users' passwords, except root, will be updated.
- The keystores' passwords will be updated.

```
Fix installation - update installation passwords to match values in vault

Confirm:  (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

The action will stop at the first unsuccessful update and display the error or exception.

Managing security on the Insight server

The `securityadmin` tool allows you to manage security options on the Insight server. Security management includes changing passwords, generating new keys, saving and restoring security configurations you create, or restoring configurations to the default settings.

About this task

You use the `securityadmin` tool to manage security:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

See the SecurityAdmin documentation for more information.

Managing security on the local acquisition unit

The `securityadmin` tool allows you to manage security options on the local acquisition user (LAU). Security management includes managing keys and passwords, saving and restoring security configurations you create or restoring configurations to the default settings.

Before you begin

You must have `admin` privileges to perform security configuration tasks.

About this task

You use the `securityadmin` tool to manage security:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

See the SecurityAdmin Tool instructions for more information.

Managing security on an RAU

The `securityadmin` tool allows you to manage security options on RAUs. You might need to backup or restore a vault configuration, change encryption keys, or update passwords for the acquisition units.

About this task

You use the `securityadmin` tool to manage security:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

One scenario for updating the security configuration for the LAU/RAU is to update the 'acquisition' user password when the password for that user has been changed on the server. The LAU and all of the RAUs use the same password as that of the server 'acquisition' user to communicate with the server.

The 'acquisition' user only exists on the Insight server. The RAU or LAU logs in as that user when they connect to the server.

See the SecurityAdmin Tool instructions for more information.

Managing security on the Data Warehouse

The `securityadmin` tool allows you to manage security options on the Data Warehouse server. Security management includes updating internal passwords for internal users on the DWH server, creating backups of the security configuration, or restoring configurations to the default settings.

About this task

You use the `securityadmin` tool to manage security:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

See the SecurityAdmin documentation for more information.

Changing OnCommand Insight internal user passwords

Security policies might require you to change the passwords in your OnCommand Insight environment. Some of the passwords on one server exist on a different server in the environment, requiring that you change the password on both servers. For example, when you change the “inventory” user password on the Insight Server you must match the “inventory” user password on the Data Warehouse server Connector configured for that Insight Server.

Before you begin

You should understand the dependencies of the user accounts before you change passwords. Failing to update passwords on all required servers will result in communication failures between the Insight components.

About this task

The following table lists the internal user passwords for the Insight Server and lists the Insight components that have dependent passwords that need to match the new password.

Insight Server Passwords	Required changes
_internal	
acquisition	LAU, RAU
dwh_internal	Data Warehouse
hosts	
inventory	Data Warehouse
root	

The following table lists the internal user passwords for the Data Warehouse and lists the Insight components that have dependent passwords that need to match the new password.

Data Warehouse Passwords	Required changes
cognos_admin	
dwh	
dwh_internal (Changed using the Server Connector configuration UI)	Insight server
dwhuser	
hosts	
inventory (Changed using the Server Connector configuration UI)	Insight server
root	

Changing passwords in the DWH Server Connection Configuration UI

The following table lists the user password for the LAU and lists the Insight components that have dependent passwords that need to match the new password.

LAU Passwords	Required changes
acquisition	Insight Server, RAU

Changing the “inventory” and “dwh_internal” passwords using the Server Connection Configuration UI

If you need to change the “inventory” or “dwh_internal” passwords to match those on the Insight server you use the Data Warehouse UI.

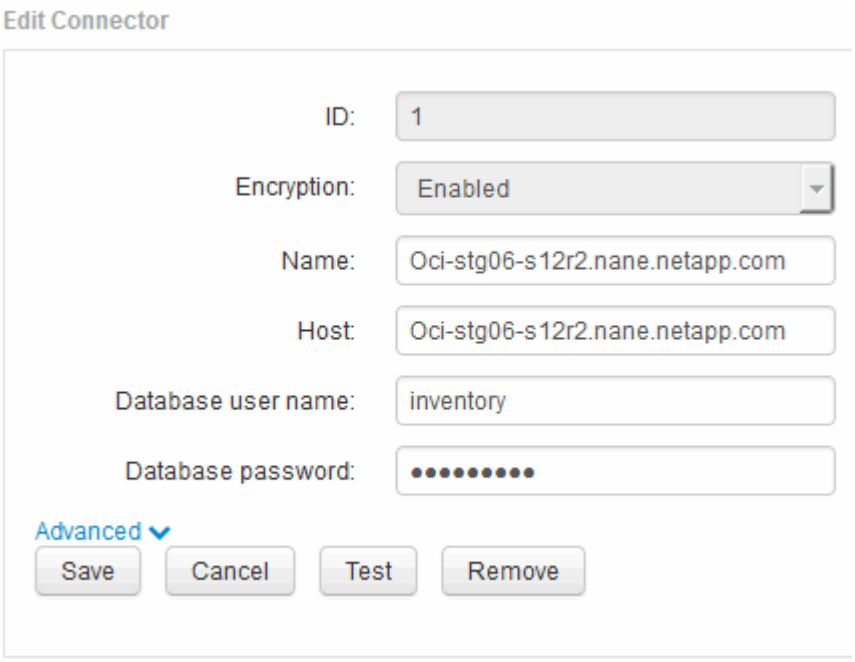
Before you begin

You must be logged in as administrator to perform this task.

Steps

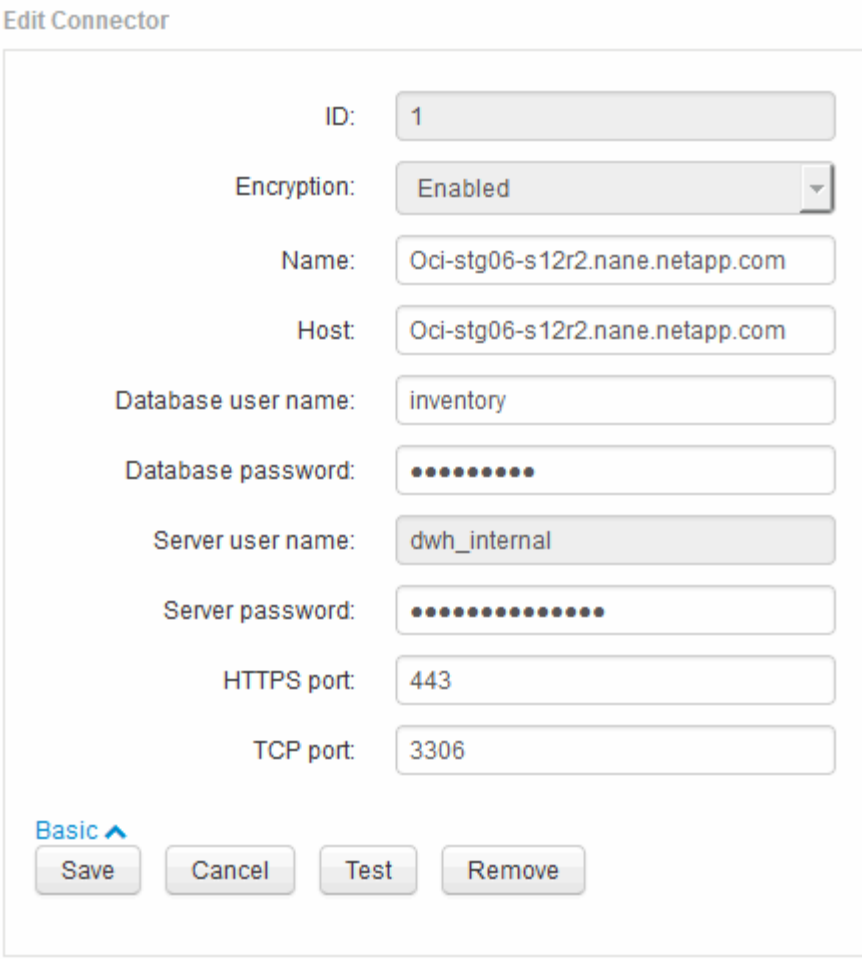
1. Log in to the Data Warehouse Portal at https://hostname/dwh, where hostname is the name of the system where OnCommand Insight Data Warehouse is installed.
2. From the navigation pane on the left, click **Connectors**.

   The **Edit Connector** screen is displayed.



3. Enter a new “inventory” password for the **Database password** field.
4. Click **Save**
5. To change the “dwh_internal” password, click **Advanced.**

   The Edit Connector Advanced screen is displayed.



6. Enter the new password in the **Server password** field:
7. Click save.

Changing the dwh password using the ODBC Administration tool

When you change the password on for the dwh user on the Insight server, the password must also be changed on the Data Warehouse server. You use the ODBC Data Source Administrator tool to change the password on the Data Warehouse.

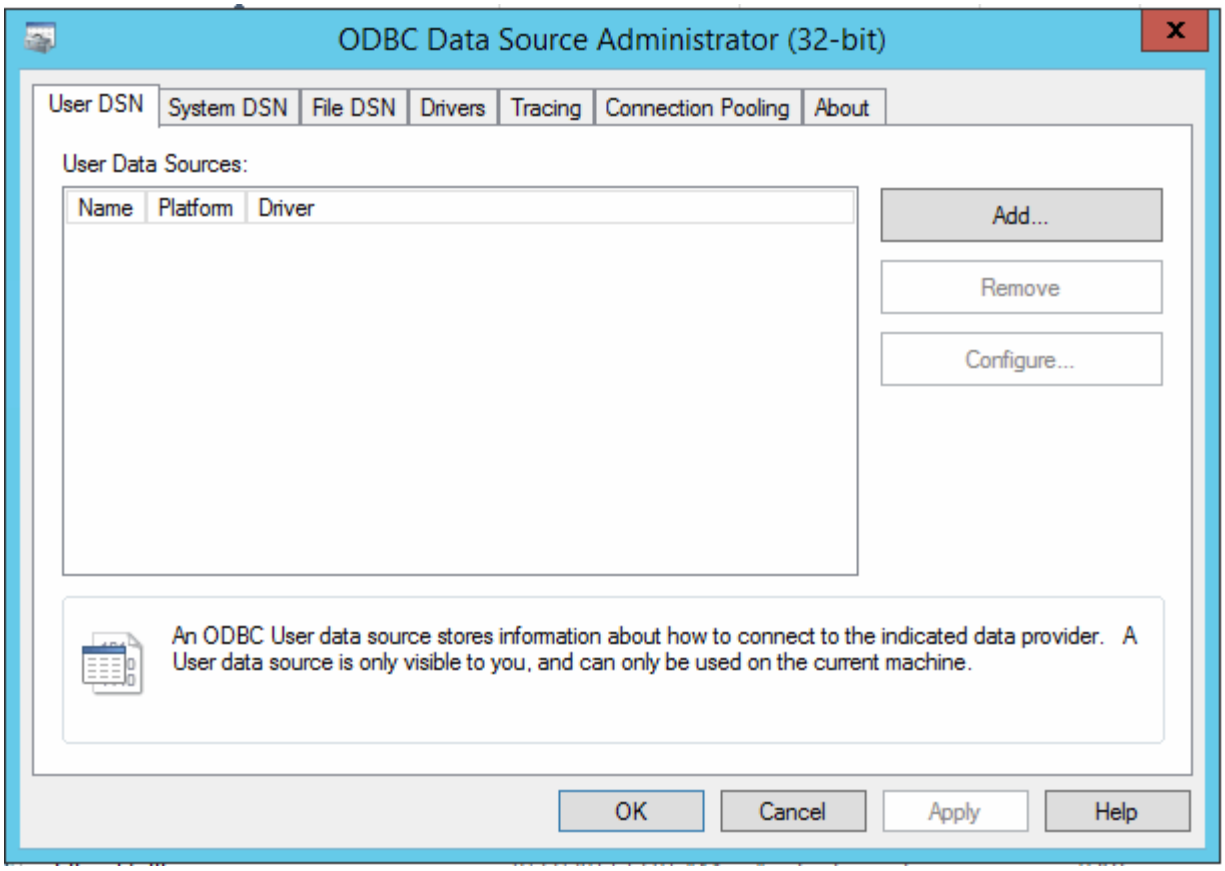
Before you begin

You must perform a remote login to the Data Warehouse server using an account with administrator privileges.

Steps

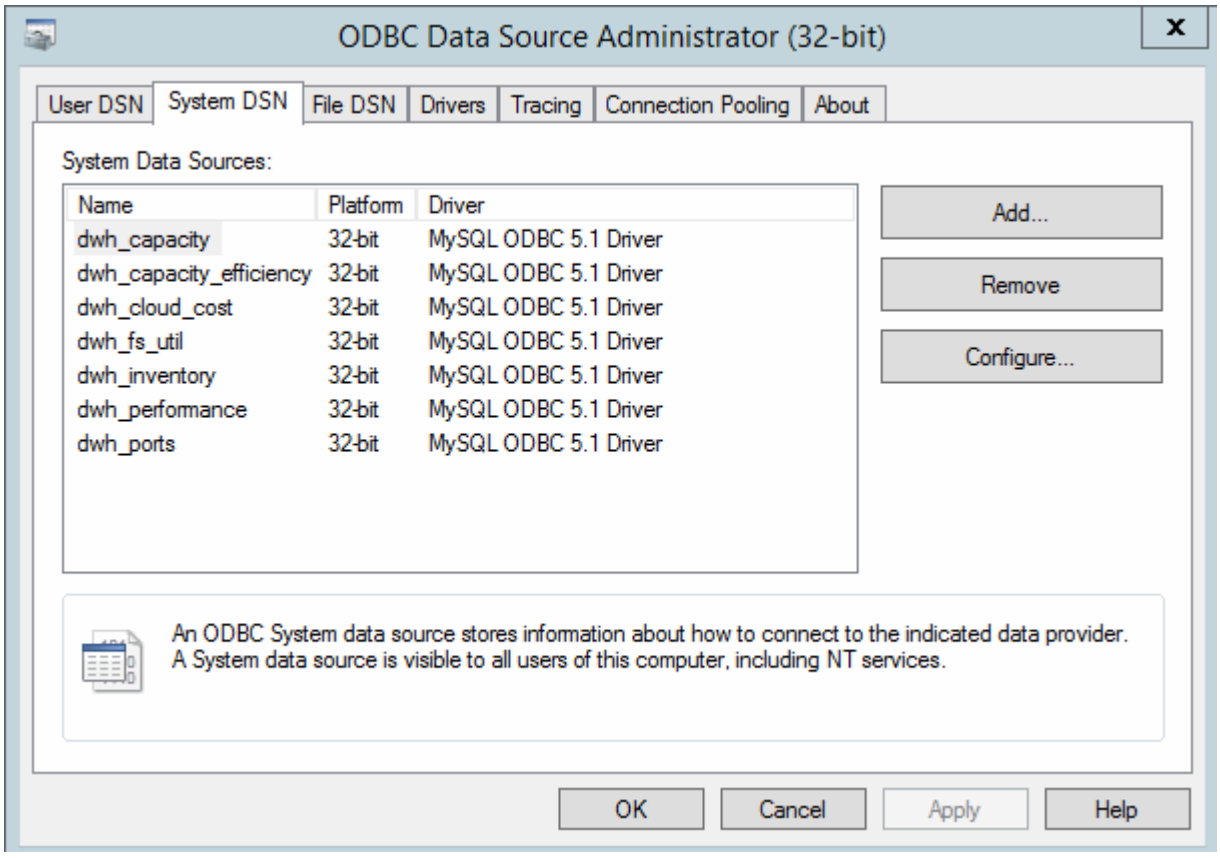
1. Perform a remote login to the server hosting that Data Warehouse.
2. Access the ODBC Administration tool at `C:\Windows\SysWOW64\odbcad32.exe`

   The system displays the ODBC Data Source Administrator screen.



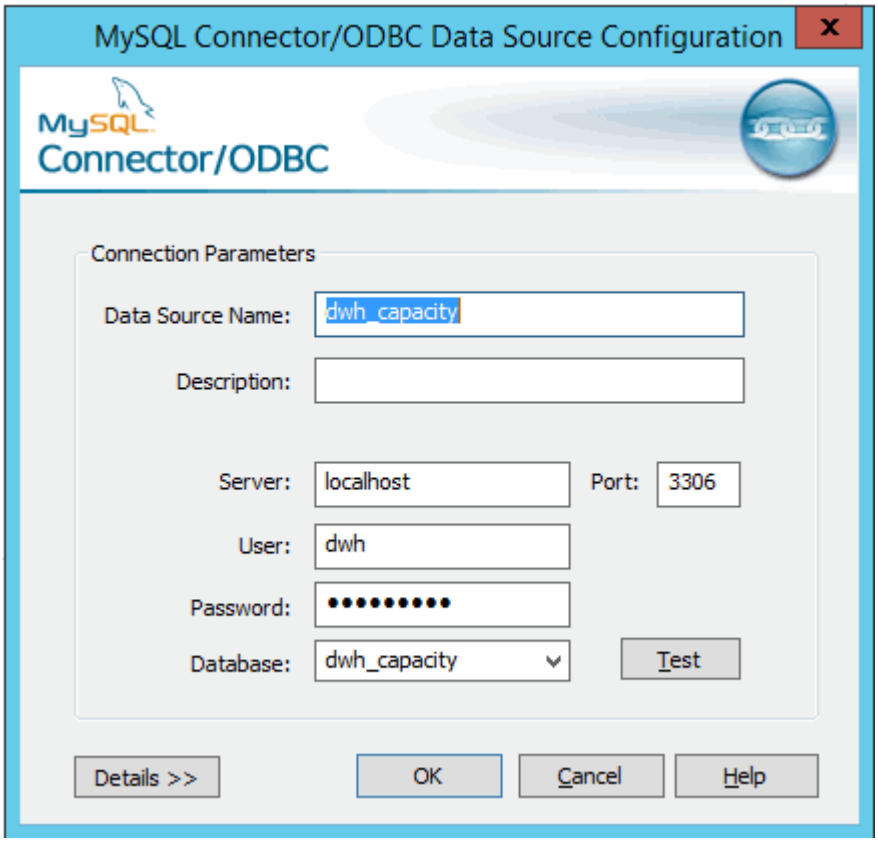
3. Click **System DSN**

   The system data sources are displayed.



4. Select an OnCommand Insight Data Source from the list.
5. Click **Configure**

   The Data Source Configuration screen is displayed.



6. Enter the new password in the **Password** field.

Copyright information

Trademark information