IBM DS8880 Integrated Copy Services Manager and LDAP Client on the HMC

Bert Dufrasne
Jean Iyabi
Integrated Copy Services Manager and LDAP support

IBM® Copy Services Manager (CSM) is a replication management solution that is based on the IBM Tivoli® Productivity Center for Replication technology. CSM inherits all the Tivoli Productivity Center for Replication capabilities and continues to provide Copy Services solutions for most IBM storage offerings.

The IBM DS8880, starting with firmware Release 8.1, Licensed Machine Code (LMC) 8.8.10.xx.xx, includes CSM for the IBM System Storage® DS8000®, which is pre-installed on the Hardware Management Console (HMC). If you ordered the CSM feature code as part of your IBM DS8000 system configuration, you only need to activate CSM.

CSM as installed on the HMC, or acquired separately, includes a lightweight build of the IBM WebSphere® Liberty server code, to use to authenticate CSM users through a Lightweight Directory Access Protocol (LDAP). The same integrated LDAP support can be used for remote authentication of DS8000 users. Furthermore, if you simply want to take advantage of the CSM LDAP client for DS8000 LDAP authentication, the CSM license and CSM activation are not required.

This IBM Redpaper™ publication describes the requirements for setup and usage of CSM on the DS8000 HMC, for both Copy Services management and LDAP authentication.

IBM Copy Services Manager introduction

This section provides a brief general introduction to the Copy Services Manager.

By using CSM, you can coordinate copy services on various IBM Storage Systems, including DS8000, IBM SAN Volume Controller (SVC), IBM Storwize® V7000, and IBM XIV®. CSM can control data replication within a storage system but also between different storage systems after they are actively connected.

Copy Services Manager simplifies and automates replication solutions, such as failover/failback, the reestablishment of mirroring, and data recoverability management, at a remote site by using Metro Global Mirror and Metro Global Mirror with Hyperswap (three-site management). CSM offers more advanced Copy Services solutions for migration and disaster recovery needs.
CSM helps to reduce the downtime of critical applications by providing the following data replication tasks:

- Plan for replication when you are provisioning storage
- Monitor and track replication operations
- Automate the mapping of source volumes to target volumes
- Keep data that is on multiple related volumes consistent across storage systems if a planned or unplanned outage occurs

In addition to the common Copy Services functions, such as IBM FlashCopy®, Metro Mirror (MM), Global Mirror (GM), and Metro Global Mirror (MGM) data replication, CSM now supports Hyperswap for multi-target (MT) MM/GM sessions, Multiple Incremental FlashCopy, MT MM/GM, and MT MM/GM with Practice (where the last two functions include the MGM configuration).

When IBM HyperSwap® for multi-target MM/GM or MM/GM with Practice is enabled, the IBM z™ automatically swaps I/O from the source to the target if a primary read/write I/O error occurs.

Storage system migration from a target system by using the multi-target sessions is possible without the feature code to a new target system with the feature code.

### Accessing the Copy Services Manager GUI

You can access Copy Services Manager functions through a graphical user interface (GUI) or a command-line interface (CLI). This paper describes the CSM GUI when CSM is on the DS8000 HMC.

You can launch the CSM for DS8000 GUI from any workstation that can connect to the DS8000 HMC over the network. The CSM GUI can be accessed from any supported internet browser, by pointing to the following URL, where `HMC-IP` is the Internet Protocol (IP) address of your HMC:

```
https://<HMC-IP>/CSM/
```

**Important:** A port number must *not* be specified, unlike the case for the CSM standalone product.

The panel that is shown in Figure 1 opens.

![Figure 1   CSM GUI main page](image)
The default user administrator is `csmadmin` and the default password is `passw0rd`. Replace the letter O with a zero.

After you log on successfully, the CSM Overview window opens, as shown in Figure 2.

The Copy Services Manager GUI reports the state of the administration components and information for the established copy operations, in real time. It also reports the state of the CSM standby server if a CSM standby server is set up for the high availability configuration.

![Figure 2   CSM GUI Session Overview](image)

The following actions and selections are available from the taskbar:

- **Overview**
  This page shows a status summary for all sessions, storage systems, host systems, and management servers that Copy Services Manager is managing.

- **Sessions**
  The Sessions option provides information about all sessions, including statistics. From this option, you can complete all actions for the sessions that you defined, or you can create a session. The actions depend on the type of session.

- **Storage**
  The Storage option provides information about storage systems, host connections, and volumes:
  - **Storage Systems**
    Use this page to create and manage storage system connections and to configure the use of the IBM DS8000 Easy Tier® heat map transfer function.
  - **Host Connections**
    You can connect to two types of host systems: IBM AIX® or IBM z/OS®. Host Systems connections are used when you want to use the Open HyperSwap feature for AIX or z/OS HyperSwap.
- Volumes
  The Volumes option under the Storage drop-down menu shows details about the volumes that are associated with a storage system, for example, the type and capacity of the volumes and connection to host.

- Paths - ESS/DS Paths
  The Enterprise Storage System/Data Storage (ESS/DS) Paths option shows the defined paths between source and target storage systems. You can view and manage the paths. By selecting this option, you start the Path Management wizard to add a path between a source and target storage system.

- Console
  The Console option provides detailed information about actions that were taken by the Copy Services Manager users, errors that occurred during normal operation, and hardware error indications. Clicking each message in the Console panel provides more information about the message.

- Settings
  The Settings option includes the Advanced Tools option, Management Servers option, and Administration option:
  - Advanced Tools
    The Advanced Tools option provides the following features:
    - Create a Package Log Files for analysis purpose if a problem with Copy Services Manager occurs.
    - Create a backup of the Copy Services Management server configuration.
    - Change the automatic browser refresh rate (in seconds) to refresh the content in the GUI.
    - Enable or disable the Metro Mirror heartbeat, which is used to ensure data consistency across multiple storage systems if the Copy Services Management server cannot communicate with one or more storage systems.
    - Export the file of the Copy Services Management license.
  - Management Servers
    Use this page to manage the active and standby management servers in a high-availability relationship. Also, you can view the status of the management servers. If you are logged in to the active server, you can select Action to Reconnect or Remove standby to set it as the standby. If you are logged in to the standby server, you can select the Action drop-down option Reconnect or initiate a takeover.
  - Administration
    The Administration option is used to view a list of Copy Services Management users and groups and their access privileges. You can also give users and groups different access privileges.
Enabling Copy Services Manager

With DS8880 and DS8000 Release 8.1 microcode, you can use the Copy Services Manager code that is integrated on the Hardware Management Console (HMC).

For the Copy Services Manager (CSM) on HMC entitlement, an order of IBM Copy Services Manager V6 (5725-Z54) is required before you can configure CSM on the HMC. Table 1 shows the feature code that corresponds to the capacity that you need to license. Ensure that the number of years of software support and maintenance that is purchased is tied to the length of the warranty on the DS8880.

**Table 1  CSM on HMC**

<table>
<thead>
<tr>
<th>Feature code</th>
<th>CSM on HMC licensed capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>8450</td>
<td>Inactive</td>
</tr>
<tr>
<td>8451</td>
<td>1 - 100 TB</td>
</tr>
<tr>
<td>8452</td>
<td>101 - 250 TB</td>
</tr>
<tr>
<td>8453</td>
<td>251 - 500 TB</td>
</tr>
<tr>
<td>8454</td>
<td>501 - 1250 TB</td>
</tr>
<tr>
<td>8455</td>
<td>1251 - 3000 TB</td>
</tr>
<tr>
<td>8456</td>
<td>3001 - 6000 TB</td>
</tr>
<tr>
<td>8457</td>
<td>6001 - 10000 TB</td>
</tr>
</tbody>
</table>

The CSM functionality must be enabled by applying a license key. Download your key from the IBM Disk Storage Feature Activation (DSFA) website:

http://www.ibm.com/storage/dsfa

When you apply the license key, enablement files are activated on the CSM instance at the HMC. Then, you can export the csm-license.zip file from that CSM GUI to use on a stand-alone server, if you want. Otherwise, for stand-alone servers, you can purchase the CSM Distributed license from IBM Passport Advantage® and you can purchase the z/OS license from shopZSeries.
Follow these steps to apply the license files:

1. Log in to the Copy Services Manager GUI as a user with administration privileges. The default user is csmadmin and the password is passw0rd (replace the letter O with a zero).

2. In the top menu bar, on the far right, click **Update Licenses** (Figure 3). (Or, you can apply the license files by clicking **Settings → Administration** to access the Update Licenses option.)

3. Enter a Try-and-Buy key that is provided by your IBM marketing representative or IBM Business Partner. (Or, click **Choose File** to browse for the correct license enablement compressed (.zip) file to upload.)

4. If no file is chosen, click **CLEAR**. You are presented with a license file that you must accept to proceed.

5. Click **Apply** to submit, or click **Cancel** to exit without applying any licenses.

   **Note:** The menu option “Update Licenses” in both cases appears only when either a Try-and-Buy Key or a full license is applied. If either of those items is applied, this menu option disappears.

   ![Figure 3 Applying a license key](image)

The DS8000 HMC is not a general-purpose server. The DS8000 HMC is a closed environment management server where Copy Services Manager must operate within the restriction of that environment and it is the central point of control for data replication management.

   **Note:** When you use CSM on HMC, the number of managed storage systems must be limited to four. This limitation is inherent to the HMC server performance characteristics.

**Installing the CSM command-line interface**

Copy Services Manager provides both a graphical user interface and a command-line interface to configure and manage the DS8000 Copy Services. The CSM CLI can be installed to run on a remote system. Various operating systems are supported.
You can download the correct compressed files for the operating system of your choice and extract them from the ordering system. Download the CSM Distributed License from IBM Passport Advantage and download the z/OS license from shopZSeries.

Table 2 lists the available package types and associated file names.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Copy Services Manager CLI installation package file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows</td>
<td>csm-CLI-6.1.1-win.zip</td>
</tr>
<tr>
<td>AIX</td>
<td>csm-CLI-6.1.1-aix.tar.gz</td>
</tr>
<tr>
<td>Linux 64-bit IBM PowerPC® and IBM Power Architecture®</td>
<td>csm-CLI-6.1.1-linux-ppc.tar.gz</td>
</tr>
<tr>
<td>Linux on IBM z Systems™</td>
<td>csm-CLI-6.1.1-linux-s390x.tar.gz</td>
</tr>
<tr>
<td>RedHat or SUSE Linux Enterprise</td>
<td>csm-CLI-6.1.1-linux-x86_64.tar.gz</td>
</tr>
<tr>
<td>z/OS</td>
<td>csm-CLI-6.1.1-zos.pax</td>
</tr>
</tbody>
</table>

After you download the correct csm-CLI file package, follow these steps:

1. Extract the file package to a directory on the remote system. Name it the CSM_CLI_DIR directory. Follow these steps based on the operating system:
   - For Windows, extract the files by right-clicking and selecting **Extract All**.
   - For AIX or Linux, use **gunzip** and then **tar** commands to extract the files.
   - For z/OS, extract the files by using the **pax** command.
   For z/OS only, after you extract the files by using the **pax** command, you must perform an additional step to set the file attributes on the Java libraries that the CLI uses. Run the following commands:
   ```bash
   extattr +a CSM_CLI_DIR/csm/Java/lib/s390x/compressedrefs/libj9ifa27.so
   extattr +a CSM_CLI_DIR/csm/Java/lib/s390x/default/libj9ifa27.so
   ```

2. Open the CSM_CLI_DIR/csm/CLI directory.

3. Edit the repcli.properties file. You can open the repcli.properties file with any text editor program and edit it by typing the server name and port of your CSM server.
   The default setting of the repcli.properties file is shown:
   - The port=9560. Leave the default unchanged.

   **Note:** Port 9560 is the default port that is used during the CSM installation. If you used a custom port, you must change the port setting to use your custom port.

4. Start the Copy Services Manager CLI by entering the **csmcli.bat** command for Windows or the **csmcli.sh** command on AIX, Linux, or z/OS systems.
5. You are prompted to enter the associated Copy Services Manager user name and password. The default user name is csmadmin and the default user password is passw0rd (replace the letter O with a zero).

6. The csmcli> prompt appears. You can now run the Copy Services Manager CLI on your remote system, as illustrated in Example 1.

Example 1 Starting CSMCLI from Windows

C:\CSM_CLI\csm\CLI>csmcli.bat
Please enter a username for logging onto the server
    csmadmin
Please enter a password for logging onto the server
> xxxxxxx
IBM Copy Services Manager Command Line Interface (CLI)
Copyright 2007, 2015 IBM Corporation
CLI Client Version: 6.1.1.2, Build: a20160512-1407
Authentication file: csmcli-auth.properties

Connected to:
    Server: xxx.xxxxxxx.ibm.com     Port: 9560   UseREST: false
    Server Version: 6.1.1.2, Build: a20160512-1407

    csmcli>

CSM standby server

For high availability and resiliency in your environment, an active Copy Services Manager server can be paired with a standby CSM server that runs on a different physical system and preferably at a remote site. This standby or backup CSM can reside on a secondary DS8000 HMC (assuming that it is at Release 8.1) or on a stand-alone server.

Although CSM can be installed on both HMCs, when you use dual HMCs, CSM is not part of the high availability support that is provided by the dual HMC setup. Each CSM instance that is enabled on an HMC is considered separate and not automatically backed up by the secondary HMC. High availability for CSM is handled through the CSM Active/Standby support. The CSM code must be at the same level on the standby and active servers.

After the active and the standby CSM servers are connected (paired), a synchronization process is initiated. The active server controls and manages the data replication and the standby server records the changes to the active server. Both servers are identical in configuration and data contents. If the active server fails, you can issue a takeover on the standby.

The active management server and the standby management server need to be connected. This connection creates the management server relationship that initiates the synchronization process. Each management server can be in one management server relationship only.

If a connectivity issue or an issue with the alternative server occurs, the management server relationship is disconnected, which stops synchronization. If a problem occurs during synchronization, the alternative server database is restored to its original state before the synchronization began. A reconnect command is necessary to restore synchronization.
Setting up a standby server

You can set up either a remote server or a local server as a standby.

**Setting up a remote server as the standby server**
To set up the remote server as the standby server, follow these steps (Figure 4):
1. Connect to the local server with the administration privileges.
2. Click **Settings → Management Servers**.
3. On the Management Servers page, click **Select Action**, then select **Define Standby**.

![Figure 4: Define the standby server or set the server as a standby](image)

4. Enter the domain name or IP address of the server that you want to use as the standby server. Log in to the standby (remote) server by entering the user name and password. Refer to Figure 5.

![Figure 5: Domain name or IP address of the server to set as standby](image)

5. Click **OK** to connect to the standby server.
6. From the remote server GUI, select **Settings → Management Servers**.
7. Click **Select Action** and click **Set this Server as Standby** from the drop-down menu.
8. Enter the domain name or the IP address of the active server (Figure 6). Click **OK**.

![Set this Server as the Standby for Active Server](image)

*Figure 6  Add the domain name or IP address of the active server*

The Management Servers page of both the local server GUI and the remote server GUI now shows a list with the local server as *Active* and the remote server as *Standby*. The status is *Synchronized*.

A Synchronized status indicates that the standby server contains the same data as the active server. Any update to the active server database is replicated to the standby server database.

**Setting the local server as the standby server**

To set up the local server on which you are logged in as the standby server, follow these steps:

1. Select **Settings → Management Servers**.
2. On the Management Servers page, click **Select Action** and select **Set this Server as Standby**.
3. Enter the domain name or IP address of the server that you want to use as the active server.
4. Click **OK** to connect to the active server. The server on which you are logged in is now the standby server.

**Important:** When you set a management server as the standby server, all of the information on that management server is cleared. The operation cannot be undone.

*Always avoid a situation where two management servers are active.* If a condition occurs on the storage systems, both management servers respond to the same condition, which might lead to unexpected behavior. After a takeover, shut down the active server to prevent the two servers from managing the same set of pairs.

**Removing a server from the standby state**

To remove a server from the standby state, follow these steps:

1. Connect to the local server if the remote server is the standby server.
2. Select **Settings → Management Servers** and then click **Select Action**.
3. From the drop-down menu, select **Remove Standby**.

   A warning message (Figure 7) states that “This command will remove the standby management server. Both management servers will be active with identical configurations. Do you want to continue?”

   ![Figure 7](image1.png)

   **Figure 7** A warning message appears when you remove the standby

4. Click **Yes** to the prompt, and the standby server is removed.

5. Connect to the remote server.

6. Click **Settings → Management Servers**.

   The Management Servers page still displays the local server as Active and the remote server as Standby.

7. Click **Select Action** and the drop-down menu shows Reconnect and Takeover as possible choices (Figure 8).

   If you want to reconnect the active server to the standby server, select **Reconnect**. Otherwise, select **Takeover**.

   ![Figure 8](image2.png)

   **Figure 8** Select Action menu with Reconnect and Takeover options
If you selected Takeover, a warning message appears, as shown in Figure 9. The message states “This command will make this standby management server an active management server. Both management servers will be active with identical configurations. Do you want to continue?”

![Figure 9](image)

8. Click Yes and the remote server role changes to Active and the status is No Standby.

**Important:** Using two management servers that are active at the same time is inadvisable. If two management servers are active and a condition occurs on the storage systems, both management servers respond to the same conditions, which might lead to unexpected behavior.

You must shut down the active server after a takeover to prevent both servers from managing the same set of pairs.

**HMC recovery**

In a problem situation, you can use the Recovery feature of the HMC to rebuild the HMC. If the recovery is invoked, you can issue the CSMCLI `mkbackup` command to create a compressed file that is a backup of the CSM data store. This backup is in the `/extra/csm` directory of the server to which the `mkbackup` command was issued. You can use the compressed file on the silent installer to re-enable CSM with the same session configuration that it used before the HMC recovery.

As an alternative to the CSM `mkbackup` command, if the recovery is due to a corruption on the HMC that requires that the HMC is rebuilt, you can repopulate an instance of CSM by making the old active CSM server the new standby server. You can use the active/standby CSM support to repopulate a CSM instance.

**Upgrading or uninstalling Copy Services Manager on the HMC**

Copy Services Manager can also be upgraded and uninstalled from a DS8000 HMC by using the DS8000 codeload process.

**Tip:** Uninstalling CSM does not remove CSM from the HMC. It is retained to ensure that the embedded Lightweight Directory Access Protocol (LDAP) functionality can be used independently of CSM. See “Enabling remote LDAP authentication for CSM and DS8000” on page 14.

Microcode Release 8.1 or later needs to be running on the DS8000. A DS8000 microcode upgrade to the newest version basically upgrades CSM to a newer level if anyone is provided with the DS8000 microcode build.
During a microcode upgrade, the Copy Services Manager server is not available.

To ensure continuity, you need a high-availability environment that includes an active CSM and a standby CSM, as described in “Setting up a standby server” on page 9. The Copy Services management sessions continue from the standby during the upgrade process.

**Tip:** With DS8000 Release 8.1.1 or later, you can now update the CSM code with new releases, independently of a DS8000 code load that is performed by an IBM service support representative (SSR).

### Preparing for a CSM code upgrade on the HMC

Perform these steps before you begin the upgrade for a CSM server that runs on the HMC:

1. Ensure that the synchronization of the standby server is complete. The Copy Services Manager sessions are not in the Preparing, Suspending, or Recovering state.
2. Move the management of the Copy Services Manager to the standby server by issuing the `takeover` command.
3. On the standby server, remove the original server from the standby relationship.
4. Upgrade the original server to the latest version of Copy Services Manager.
5. When the sessions are not in a transitory state, start Copy Services Manager on the original server.
6. Start the code upgrade as explained below in “Upgrading the CSM code on the HMC”.

### Upgrading the CSM code on the HMC

**Important:** Starting with DS8000 Release 8.1.1, you can update the CSM code on the HMC.

The IBM System Storage DS® Command-Line Interface (DSCLI) command `lssoftware` is now available to display the current software level:

`lssoftware [-s | -l ] -type csm -hmc [1 | 2 | all]`

Before you upgrade the code, use the `lssoftware` command to check the installed CSM level (Example 2).

#### Example 2   Checking the current CSM level on the HMC

dscli> lssoftware -l
Date/Time: June 13, 2016 7:25:02 PM PDT IBM DSCLI Version: 0.0.0.0 DS: IBM.2107-75DMC41
Type Version                 Status  HMC
=======================================
CSM V6.1.1.2-a20160521-0703 Running 1
CSM V6.1.1.2-a20160521-0703 Running 2

The DSCLI command `installsoftware` is now available to upgrade the code:

`installsoftware [-dev storage_image_ID] -type csm -loc Software_package -hmc [1 | 2 | all]`

You can download the new CSM code that you want to install from IBM Fix Central to a system that is logged in to the HMC. Use the `installsoftware` command and point to the location of the update code, as shown in Example 3.
Example 3   Installing the updated CSM code on both HMCs

dscl> installsoftware -loc /home/hscroot/wht/csm-setup-6.1.1.2-linux-x86_64.bin
   -certloc /home/hscroot/wht/csm-setup-6.1.1.2-linux-x86_64.bin.crt -type CSM -hmc ALL

Date/Time: June 13, 2016 7:25:45 PM PDT IBM DSCLI Version: 0.0.0.0 DS: IBM.2107-75DMC41
CMUC00294I installsoftware: Upload file successfully.
CMUC00294I installsoftware: Software CSM is successfully installed on HMC 1.
CMUC00294I installsoftware: Software CSM is successfully installed on HMC 2.

For verification, use the lssoftware command again, as shown in Example 4, to verify that
the new level of the CSM code is installed.

Example 4   Verify the new level of the CSM code

dscl> lssoftware -l

Date/Time: June 13, 2016 7:29:45 PM PDT IBM DSCLI Version: 0.0.0.0 DS: IBM.2107-75DMC41

<table>
<thead>
<tr>
<th>Type</th>
<th>Version</th>
<th>Status</th>
<th>HMC</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSM</td>
<td>V6.1.1.2-a20160526-0718</td>
<td>Running</td>
<td>1</td>
</tr>
<tr>
<td>CSM</td>
<td>V6.1.1.2-a20160526-0718</td>
<td>Running</td>
<td>2</td>
</tr>
</tbody>
</table>

Enabling remote LDAP authentication for CSM and DS8000

Copy Services Manager (CSM) supports both basic authentication and Lightweight Directory
Access Protocol (LDAP) authentication. You can configure the server so that both basic and
LDAP authentication methods can be used concurrently. The repositories (user registry) for
basic users and LDAP users are different.

The CSM GUI and CSM CLI support the ability to add, remove, or modify the basic user
registry and to configure communication to an LDAP server. The LDAP client, which is
included with CSM on HMC, is enabled, by default.

You configure LDAP authentication for CSM through IBM WebSphere Liberty, which is
integrated in CSM. After you configure LDAP for CSM, you can use the CSM GUI or the CSM
CLI to also enable LDAP authentication for DS8000 users. Later, you need to configure the
DS8000 HMC to point to the CSM authentication server on that same HMC. (See
“Configuring the DS8000 for LDAP remote authentication” on page 20.)

Important: After you configure the LDAP authentication, users from the basic user registry
are still able to authenticate. We suggest that at least one user from the basic user registry
retains the administrator role. This user serves as a backup if a loss in communication to
the LDAP servers occurs.

Note: LDAP must be enabled in both HMCs if dual HMCs are installed in the DS8000.

The CSM users and roles are entirely separate from the DS8880 users and roles. Passwords
are managed separately and independently between CSM and the DS8000.
You can use the CSM GUI to configure LDAP authentication in your Copy Services Manager environment by following these steps:

1. Log in to the Copy Services Manager GUI as a user with administrator privileges. The default user is `csmadmin` and the password is `passw0rd` (replace the letter O with a zero).
2. In the menu bar, select **Settings → Administration** (Figure 10).

**Note:** The Administration page shows a status indicator for the LDAP server. If you are configuring LDAP for the first time, the status is shown as *Not configured* with a link to Modify, as shown in Figure 10.

Tip: A CSM license or enablement is *not* required to use the CSM LDAP for DS8000 authentication.
3. Click **Modify**. The LDAP Configuration panel is displayed, as shown in Figure 11.

4. Select the authentication method. Select either Active Directory, which is the Microsoft implementation of directory services that support LDAP, or another directory that is supported by LDAP (Figure 11).

The Active Directory method is selected, by default.
Configuring for an Active Directory server

If you selected Active Directory from the drop-down menu for the authentication method, follow these steps and refer to Figure 12 to configure LDAP by using an Active Directory server:

1. Click **Add Server** if you are configuring LDAP for the first time.
2. Type the correct Active Directory server host name and click **Add**. The server name is displayed in the Server list.

**Note:** You can specify one or more Active Directory servers.

3. Type the user ID in the User ID field.
4. Type the associated password for the user ID in the Password field.
5. Type the domain name in the Domain field.
6. Click **Test** to test the connection. If the system cannot connect, an error message appears.

**Note:** If you get a message that no users or groups were found, you can modify your inputs and click **Test** again. Or, you can save the configuration without any more changes.

7. Click **Save** to complete the Active Directory configuration, or click **Cancel** to exit.

![LDAP Configuration](image)

*Figure 12  Active Directory parameters*

When you correctly complete all of the fields and the test connection is successful, one or more Active Directory servers are configured for LDAP authentication.
**Configuring LDAP by using an LDAP server**

Follow these steps to configure LDAP by using an LDAP server:

1. Click **Add Server** if you are configuring LDAP for the first time.

2. Type the correct LDAP server name and associated port. Then, click **Add**. The LDAP server and port are displayed in the LDAP Server list (Figure 13).

3. Type a string value for the filter to search on in the “Search base for users and groups” field.

4. Type the name of the user to bind the LDAP server to in the Bind Distinguished Name (DN) field.

5. Type the password for the bind name in the Bind Password field.

6. Click **Test** to test the connection. If the system cannot connect, an error message appears.

7. Click **Save** to complete the LDAP configuration, or click **Cancel** to exit.

**Note:** You can specify one or more LDAP servers.

8. Optional: You can select the **Enable SSL** check box to upload a Secure Sockets Layer (SSL) key file from the LDAP server that you are connecting to. Then, click **Load Certificate** and select the file name.

   When you modify an existing LDAP server configuration, the Enable SSL check box is selected. You can use the existing certificate file that is displayed or a new one. You can also clear the check mark from Enable SSL.

---

**Note:** If you get a message that no users or groups were found, you can modify your inputs and click **Test** again. Or, you can save the configuration without any more changes.

---

**Figure 13** LDAP parameters
When all of the fields are completed correctly, and the test connection is successful, one or more LDAP servers are configured for LDAP authentication. The LDAP server status indicator on the Administration page changes from Not Configured to the name of the LDAP server.

**Completing the CSM LDAP configuration**

After you configure LDAP authentication with CSM, the CSM authentication server, which is named csmAuth, creates its own truststore file with the certificate information at startup. The csmAuth server can have only one user registry, which in this case is the LDAP server. CSM does not use IBM WebSphere Integrated Console, but rather the lightweight Liberty server. The Storage Authentication Service (SAS) user for Copy Services Manager is any valid LDAP user.

After the initial configuration, the LDAP server status indicator on the Administration page changes from Not Configured (Figure 10 on page 15) to the name of the LDAP server.

For instructions about removing the LDAP server configuration, see “Removing LDAP for CSM by using CSM GUI” on page 26.

Otherwise, go to “Configuring the DS8000 for LDAP remote authentication” on page 20 to enable the DS8000 to use the same CSM LDAP server for DS8000 user authentication.

**LDAP authentication for the DS8000**

The IBM Storage System DS8000 allows directory services-based user authentication. This authentication capability is provided by the Copy Services Manager server, which is embedded into the DS8000 Hardware Management Console (HMC) with the Lightweight Directory Access Protocol (LDAP), which is built on Liberty WebSphere.

The DS8000 still supports local user management (basic user management). Maintaining local repositories of users and their permissions is simple and convenient when you work with only a few users and a few DS8000 servers or other systems. However, as the number of users and interconnected systems grows, authentication management quickly becomes difficult and time-consuming.

You can also take advantage of the LDAP integrated solution in CSM for LDAP authentication of DS8000 users. Support for DS8000 LDAP authentication no longer requires IBM Spectrum™ Control (formerly known as Tivoli Storage Productivity Center) and IBM Jazz™ for Service Management (JazzSM) services.
Figure 14 shows an overview of the DS8000 LDAP authentication architecture. The diagram on the left shows the earlier implementation that required Spectrum Control and the JazzSM authentication server. The diagram on the right shows the DS8000 Release 8.1 or later implementation.

Communication between the DS8000 HMC and the administrative clients (DS CLI or DS GUI) is unchanged, compared to basic user authentication. The communication model still uses a client/server connection with the DS8000 HMC IBM Enterprise Storage Server® Network Interface (ESSNI) server.

For example, when you use the DS CLI, the connection from a user standpoint is still established as it was without LDAP. The user establishes the connection by specifying the IP address of the HMC, and the user is prompted for a user ID and password.

Now, when the DS8000 is set to use Remote Authentication, the ESSNI server, instead of validating the user request against the local registry, passes the user’s credentials to the authentication client, which validates them against the LDAP server. If the user’s credentials are valid, an authentication OK token is returned to the ESSNI server, which executes the command against the DS8000.

**Configuring the DS8000 for LDAP remote authentication**

You can enable and configure the remote authentication through an LDAP repository from the DS8000 GUI to point to the CSM on the HMC for LDAP authentication. You perform this task after the LDAP is configured in the DS8000 management GUI or DSCLI.

To configure the DS8000 for LDAP, follow these steps:

1. Log in to the DS8000 Storage Management GUI as a user with administrator privileges.
2. Select **Settings → Security → Remote Authentication**.
3. Click **Enable Remote Authentication** (Figure 15).

![Remote Authentication](image1)

**Figure 15** Enable Remote Authentication

4. The Welcome page of the Remote Authentication wizard opens. When you click **Prerequisites**, the prerequisites are displayed (Figure 16).

![Remote authentication prerequisites](image2)

**Figure 16** Remote authentication prerequisites
5. Click **Next** to open the Authentication Servers tab to enter the Authentication Servers, as shown in Figure 17.

6. Use Copy Services Manager to communicate with an LDAP repository for remote authentication. (The use of IBM Spectrum Control™ as a stand-alone server is also possible.) The server host name is for whichever product you choose. Up to two authentication servers can be configured. The second authentication server functions as a backup.

**Note:** For Copy Services Manager, the server host name address format is https://<hostname>://<auth port>/CSMAuth/TokenService. Because CSM is preinstalled on the HMC, you can use a direct connection method and enter https://<HMC addr>:9562/CSMAuth/TokenService in the Server Host Name field.

7. Click the Folder icon next to the Truststore File field to browse to select the truststore file, which shows as test_trustStore.jks in our example in Figure 17.

For Copy Services Manager that is running on the HMC, log in as the administrator and download this file from https://<hostname>/CSM/security/key_itso.jks.

Otherwise, the location for this file is in this directory:

<install path>/liberty/wlp/usr/servers/csmAuth/resources/security/key_itso.jks

If you want to use more than one Copy Services Manager server for remote authentication, ensure that this file is the same between both csmAuth servers. Otherwise, the truststore file does not work for one of the csmAuth servers.

Enter the password in the Truststore Password field. The default password for the CSM truststore file is passw0rd (with a zero instead of the letter O).

For the WebSphere User Name and Password, when you use CSM, you can specify any valid LDAP user name and password.
8. Click **Next** to display the Create Authentication Mapping page (Figure 18). You need to assign DS8000 roles to the remote users or groups. These mappings grant the correct permissions to each user or group of users.

Click **Add Remote Mapping** (Figure 19 on page 24) to create authentication mapping and to select the DS8000 role that you want to map. Select whether to map the role to a user or group and enter the user or group name.

![Create Authentication Mapping](image)

**Figure 18  Create authentication mapping**

9. Click **Add** to finalize the mapping, or click **Cancel** to exit without applying any changes.
10. You can also modify or remove mappings by selecting a previously mapped role, user, or group. Click Actions (Figure 19), and click Modify or Remove:

- If you select **Modify**, you can change the role, user, or group name that is assigned to that mapping. Click **Modify** to save the changes, or click **Cancel** to exit without applying any changes.

- If you select **Remove**, the selected mapping is deleted and no longer appears in the column view. You can also select **Customize Columns** to add or remove columns, or to restore the default view.

![Figure 19 Remote authentication mapping](image)

11. Click **Next**.
12. On the Local Administrator page, you can define a local administrator role that is always active for recovery.

Select the **Allow** check box to assign a local administrator role. Then, select the user name of the administrator. Assign a password to the administrator, as shown in Figure 20.

![Figure 20 Define a local administrator](image)

13. Click **Next** to display the Administrator Verification page.

14. On the Administrator Verification page, choose a user name and password to assign to the administrator role, as shown in Figure 21.

![Figure 21 Administrator verification](image)
15. Assigning an administrator role helps to avoid a situation where you activate remote authentication to an LDAP server with no defined mapping for an administrator account. If you activated remote authentication without a defined mapped administrator and then log out, you cannot log back in to add new remote authentication mappings.

16. Review all of the selections on the Summary page, as shown in Figure 22, before you finalize the remote authentication setup.

![Remote authentication summary](image)

After you complete all of the steps of the wizard, the DS8000 is enabled and configured for remote authentication.

**Removing LDAP for CSM by using CSM GUI**

After you configure LDAP authentication in your Copy Services Manager environment, you can also remove the configuration by using the CSM GUI.

Follow these steps to remove the LDAP authentication support by using the CSM GUI:

1. Log in to the Copy Services Manager GUI as a user with administrator privileges. The default user is **csmadmin** and the password is **passw0rd** (replace the letter O with a zero).

2. Click **Settings → Administration**.

   **Note:** On the Administration page (Figure 10 on page 15), the options to modify or remove the LDAP configuration are available. The status indicator for the LDAP server shows if LDAP is configured.

3. Click **Remove**. A message is displayed. You are prompted to confirm that you want to remove the LDAP configuration.

4. Click **Yes** to confirm the removal or click **No** to cancel.

5. If you click **Yes**, another message is displayed that states that the LDAP configuration was removed successfully. Click **OK** to close the message.
Configuring LDAP for CSM by using the CSM CLI

The basic user registry is the default user-authentication method for Copy Services Manager. However, you can configure Copy Services Manager to use either an Active Directory server or another LDAP server type of authentication method. LDAP authentication does not prevent the basic user registry from being able to authenticate.

When you configure Copy Services Manager to connect to the correct server, all LDAP users are authenticated through that server.

It is a preferred practice for at least one user from the basic user registry to have an administrator role. This user serves as a backup if a loss in communication occurs to the LDAP servers.

You can use the Copy Services Manager command-line interface (CSM CLI) to configure LDAP authentication in your CSM environment by following these steps:

1. Log in to the Copy Services Manager CLI as a user with administrator privileges.
2. You can choose to establish either an Active Directory or LDAP server configuration:
   - Enter the `mkadcfg` command, as shown in Example 5, to configure CSM to use Active Directory server-based authentication. Type `mkadcfg -help` for more information about this command.
   
   **Example 5 Establishing an Active Directory server configuration**
   
   ```
csmcli> mkadcfg -server ADserver1.ibm.com:1234 -username admin -password passw0rd -domain ibm.com
   ```
   
   The following output is returned:
   
   
   - Enter the `mkldapcfg` command, as shown in Example 6, to configure CSM to use LDAP server-based authentication. Type `mkldapcfg -help` for more information about this command.
   
   **Example 6 Establishing an LDAP server configuration with security**
   
   ```
csmcli> mkldapcfg -server ldapserver.ibm.com:1234 -bindDN cn=root -baseDN ou=test,o=ibm,c=us -password passw0rd
   ```
   
   The following output is returned:
   

   **Important:** Only one authentication method can be used at a time. For example, if you enter the `mkadcfg` command first, and then enter the `mkldapcfg` command later, the last command overwrites the previous configuration.

Enabling DS8000 remote LDAP authentication through the DS CLI

You can enable and configure remote authentication through an LDAP repository. Use this scenario to enable remote authentication from the DS8000 command-line interface (CLI). If Copy Services Manager is used for remote authentication outside of DS8000, you can use the CSM CLI or CSM GUI.
The csmAuth server can have only one user registry, which, in this case, is the LDAP server. Therefore, no separate admin user, such as the JazzSM wsadmin user, exists. Copy Services Manager does not use WebSphere Integrated Console, but instead, CSM uses the lightweight WebSphere Liberty server. The Storage Authentication Service (SAS) user for Copy Services Manager is any valid LDAP user.

Follow these steps to enable remote authentication by using the DSCLI:

1. Open a DS CLI command line and log in to the DSCLI installation directory with the HMC IP address, user name, and password.

2. Check for existing authentication policies with the `lsauthpol` command.

   The default initial policy is set for basic (non-LDAP) authentication.

3. Create a new empty policy with the `mkauthpol -type sas itsopolicy` command.

   The `-type sas` specifies the authentication policy type. The `sas` (Storage Authentication Service) value is the only valid value for this parameter, and it is required. The `itsopolicy` is the name that we chose in our example for the new policy.

4. Add one or more policy servers to the policy by entering the `setauthpol` command with the `-action setauthserver` and `-loc` parameters.

   The `-loc` parameter is the URL to the Copy Services Manager server.

   Because Copy Services Manager is preinstalled on the HMC, use a direct connection method and enter `https://<HMC addr>:9562/CSMAuth/TokenService`.

5. Add the keystore file to the policy. Enter the `setauthpol` command with the `-action settruststore` and `-loc` parameters. The `-loc` parameter is the location of the truststore file. Use the `-pw` parameter for the truststore file password.

   You can download this file from `https://<hostname>/CSM/security/key_itso.jks` after you first log in to Copy Services Manager as an administrator.

   If you use more than one Copy Services Manager server for remote authentication, ensure that the `https://<hostname>/CSM/security/key.jks` file is the same between the two CSM servers. Otherwise, the truststore file does not work for one of the CSM servers. Restart the server with the file that you replaced.

6. Enter the `setauthpol` command with the `-action setsasuser` parameter to add the authentication user to the policy. Use the `-pw` parameter for the associated user password.

   The authentication user for this step must be a valid LDAP user. This user name is used for all authentication requests. You must update this setting when the password for this authentication user is updated.

7. Map existing users and user groups from the LDAP server to user groups on the DS8000 by entering the `setauthpol` command with the `-action setmap` parameter and `-groupmapUser:Group` values.

   Note: After you configure LDAP authentication with Copy Services Manager, you do not need to create your own truststore file with the certificate information. The Copy Services Manager csmAuth server creates a truststore file with the certificate information at startup. This file is created based on the same keystore that is used for the Secure Sockets Layer (SSL) settings. If that keystore is changed for any reason, a new keystore is created when the server is restarted. You can change the output information in the `csmauth.properties` file. The default values in this file are listed:

   ```
   ▶ itso.keystore.name=key_itso.jks
   ▶ itso.keystore.password=password
   ▶ itso.keystore.directory=resources/security
   ```
8. Now that the policy is set up, enter `lsauthpol itsopolicy` to check it. The policy is in the inactive state.
   Enter the `showauthpol` command to view the configuration parameters.
   Enter the `testauthpol` command to test the configuration.
9. If the test completed successfully, enter the `chauthpol` command with the `-activate` parameter to activate the policy.
10. Enter the `lsauthpol` command to check the state for the policy.

The DS8000 storage system is now enabled and configured for remote authentication.

Related information

The publications that are listed in this section are considered particularly suitable for a more detailed discussion of the topics that are covered in this paper.

IBM Redbooks

The following publications provide additional information about the topic in this document:

- *IBM DS8870 Copy Services for IBM z Systems*, SG24-6787
- *IBM DS8870 Copy Services for Open Systems*, SG24-6788
- *LDAP Authentication for IBM DS8000 Storage*, REDP-4505

Other publications

These publications are also relevant as further information sources:

- *IBM Copy Services Manager User’s Guide*, SC27-8542
- *IBM DS8880 Introduction and Planning Guide*, GC27-8525-06

Online resources

These websites are also relevant as further information sources:

- IBM Knowledge Center/IBM DS8880:
- IBM Knowledge Center/Copy Services Manager:
- DS8880 support:
Authors

This paper was produced by a team of specialists working at the International Technical Support Organization.

Bert Dufrasne
Jean Iyabi

Thanks to the following people for their contributions to this project:

Randy Blea, Christy Capps, Tony Ciaravella, Greg McBride, Pamela Schull, Heinz Blaschek.

Now you can become a published author, too!

Here’s an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at: ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- Find us on Facebook:
  http://www.facebook.com/IBMRedbooks
- Follow us on Twitter:
  http://twitter.com/ibmredbooks
- Look for us on LinkedIn:
  http://www.linkedin.com/groups?home=&gid=2130806
- Explore new IBM Redbooks® publications, residencies, and workshops with the IBM Redbooks weekly newsletter:
- Stay current on recent Redbooks publications with RSS Feeds:
  http://www.redbooks.ibm.com/rss.html
Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided “AS IS”, without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.
Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

AIX®
DS8000®
Easy Tier®
Enterprise Storage Server®
FlashCopy®
HyperSwap®
IBM®
IBM Spectrum™
IBM Spectrum Control™

IBM z™
IBM z Systems™
Jazz™
Passport Advantage®
Power Architecture®
PowerPC®
Redbooks®
Redpaper™
Redbooks (logo)®

Storwize®
System Storage®
System Storage DS®
Tivoli®
WebSphere®
XIV®
z Systems™
z/OS®

The following terms are trademarks of other companies:

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.