Scalar i2000 Addendum

Purpose of This Document

This addendum provides documentation not included in the i6.1 and i6.5 releases of the Scalar i2000 product guides. This addendum documents the updated procedures for setting up and using LDAP functionality included in the i6.5 release. This addendum also includes previously published information describing the Quantum Encryption Key Manager application that was supported with the Scalar i2000 i6.1 release.

Scalar i2000 Enhancements

New in i6.5 Release

The Scalar i2000 i6.5 release provides enhancements to the Lightweight Directory Access Protocol (LDAP) features. LDAP is the industry standard Internet protocol that provides centralized user account management. For the current procedures for configuring LDAP, see Setting Up LDAP on page 2.

New in i6.1 Release

The Scalar i2000 i6.1 release supports the licensable Quantum Encryption Key Manager (Q-EKM) application in conjunction with supporting LTO-4 tape media encryption using the IBM LTO-4 Fibre Channel drives. The Scalar i2000 user documentation was not updated for the i6.1 release. For a description of the Q-EKM menu options on Scalar i2000 library, see Supporting Encryption on page 6.

For more information about installing and configuring the Q-EKM server and Q-EKM best practices, see the *Quantum Encryption Key Manager User's Guide* (6-01847-xx).

Setting Up LDAP

You can configure the Lightweight Directory Access Protocol (LDAP) settings any time after the initial library configuration. Once you enable and configure LDAP, you can view your current LDAP settings using the LDAP menu.

Note: Active Directory no longer requires Windows Services for Unix 2.5.

CAUTION	Any LDAP configurations from i6.3.1 and earlier will not import into the i6.5 LDAP configuration. You must reconfigure LDAP for the i6.5 update.

LDAP Server Guidelines

LDAP is the industry standard Internet protocol that provides centralized user account management subsystem. User account information is centralized and shared by different applications, simplifying user account management tasks. Administrative users can add, delete, and modify only local user account information. For more information concerning setting up user accounts, see the *Scalar i2000 User's Guide.*

User and Group Access

For LDAP users with library user privileges, access to library partitions is determined by group assignment on the LDAP server. Groups must be created on the LDAP server with names that correspond to the library partition names. Users with user privileges must be assigned to these groups on the LDAP server to have access to the corresponding partitions on the library. LDAP users with administrative privileges have access to all partitions and administrative functions and do not need to be assigned to partition-related groups on the LDAP server.

Note: Usernames and group objects must be in LDAP Distinguished Names formats.

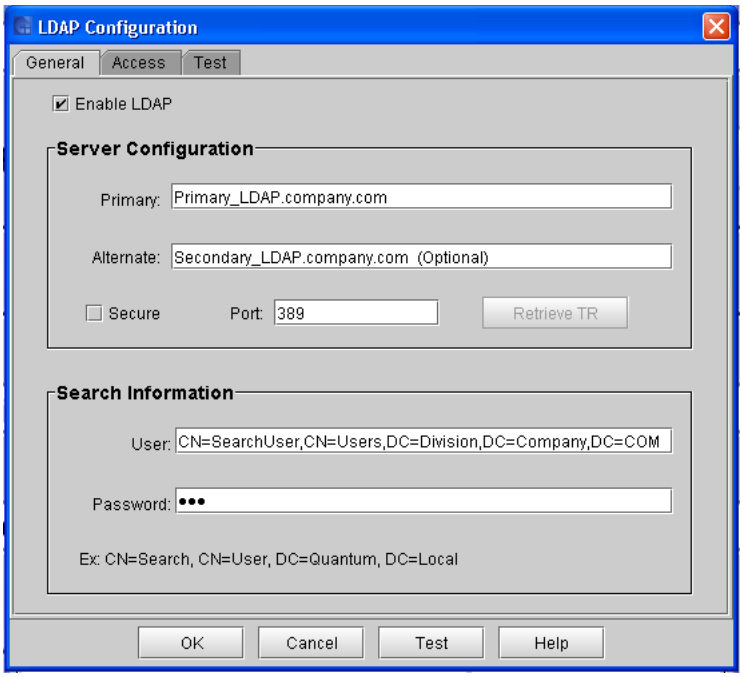
OpenLDAP 2.4

You must install and run OpenLDAP 2.4 or above. The supported Objects in OpenLDAP 2.4 and above are of type "Person" or derived objects, and the group Objects must be of type "GroupOfNames".

OpenLDAP must be compiled with Overlay Support and requires the installation of "memberOf" overlay. More information can be found in the man pages of OpenLDAP with the "man slapo-memberof" command.

Configuring LDAP

1 From the Setup menu, click **LDAP**.
The **LDAP Configuration** dialog box displays with the **General** tab displayed.



2 In the **General** tab, you can enable or disable LDAP functionality:

- To enable LDAP, select **Enable LDAP**.
- To disable LDAP, clear the **Enable LDAP** check box.

Note: If you disable LDAP, single sign-on functionality will not be available on the library.

3 To configure or modify LDAP, use the appropriate tabs and set the following configurations:

General tab

- **Server Configuration**
  Primary: You must provide a primary IP address or DNS name.
  Alternate: An alternate IP address or DNS name is optional.
- **Secure**
  Use this check box to enable the setup options to access a secure LDAP server, which can be done using any port except 389. The default secure port is 636. If you enable this option, you must retrieve the Trusted Root Certificate from the server by clicking **Retrieve TR**.
  Port: Enter the appropriate port in this field. The default port for non secure connection is 389 – and 636 for secure (SSL) based LDAP connections. The port setting can be changed.
  Retrieve TR: Use this function to retrieve the Trusted Root Certificate from the LDAP server. A dialog box displays basic Trust Root certificate

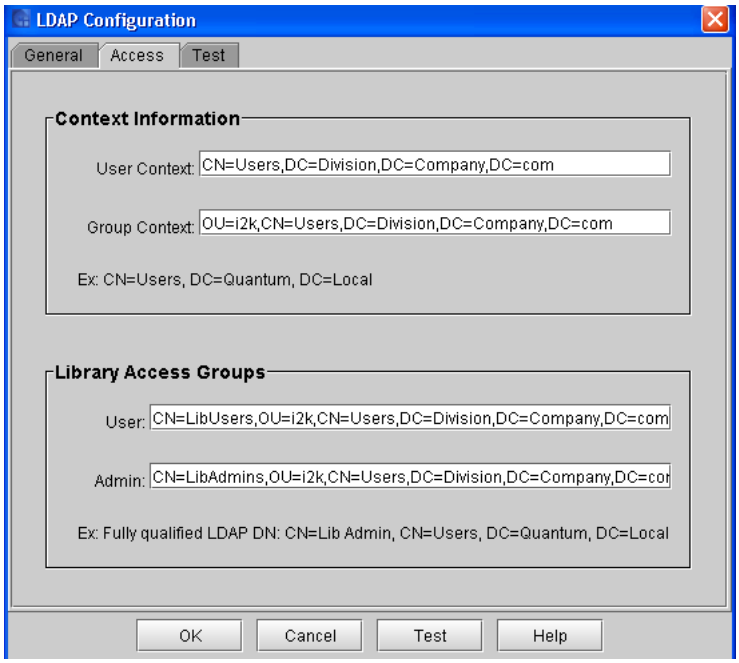
information, for example, subject name, MD5, and SHA 1 hashes. It is recommended that you verify this information independently on the LDAP server.

Caution:	The first time you use **Retrieve TR**, the process can take 5 to 10 minutes. To connect to a secure LDAP server, you must complete the retrieval process.

- **Search Information**
  To use this feature administrative user rights are not required, but you must have the right to search usernames in the LDAP directory.

To validate your configuration, click **OK** or **Test**.

Access tab
Use this tab to configure LDAP authentication.

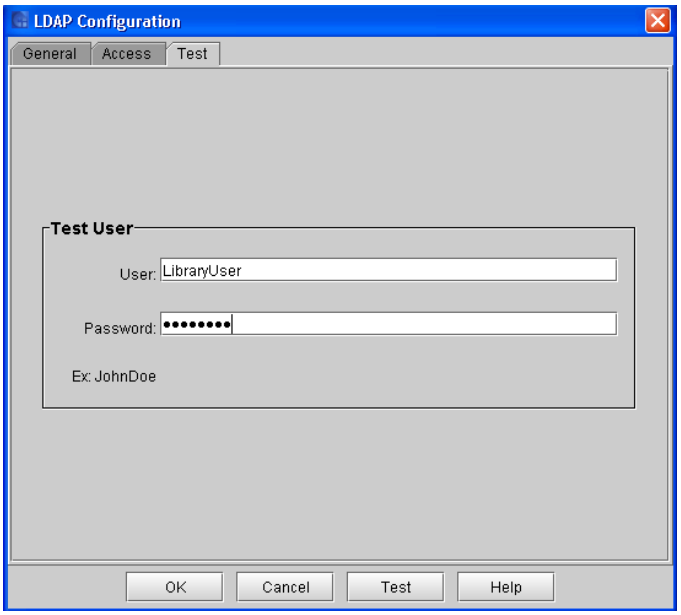


- **Context Information**
  User Context: This is a fully qualified LDAP DN and is used as the base to search for the login users. You can search for a user in the context specified and all contexts below it.
  Group Context: Use this to search and discover what groups a users is a member of. Only groups which are in the Group context or below are considered for library access.
- **Library Access Groups**
  User: The group associated with the library. User members that belong to the Library User Access Group have user rights to the library. To have full rights to a specific library partition, the users must also be members of a group with the actual name of the partition.

Admin: The group associated with the library administrator, equivalent to the local administrative user privilege level. Any member of this group has administrative privileges.

To validate your configuration, click **OK** or **Test**.

Test tab
If you have administrative rights, you can use the Test functionality to simulate an LDAP login for a specific user and quickly discover what access rights the user has and to what partitions the user has access.



Test User
User: Type the appropriate User name.
Password: Type the user password.

To initiate the library authentication process to the LDAP server, click **Test** after providing the user name and password.
A dialog box appears displaying what level of access the user is assigned, and to which library partition(s) the user has access.

4 After you have entered the LDAP configurations, click **Test** to verify the LDAP connection.
A connection with the LDAP server(s) is established and the library determines whether the LDAP Distinguished Names specified in the Access tab are valid.

A message box displays indicating that the success or failure of the LDAP connection.

- If the connection failed, the error message contains information that you can use to resolve the issue.
  Click **OK** to return to the LDAP Configuration dialog box.
- If the connection was successful, in the message box, click **OK** and continue.

5 To accept and save the library configuration, in the LDAP Configuration dialog box, click **OK**.

Supporting Encryption

The Scalar i2000 library supports encrypting LTO-4 tape media using IBM LTO-4 Fibre Channel drives only. All IBM LTO-4 FC drives are encryption-capable, but to use the Q-EKM software application, you must purchase a Q-EKM license and provide a server or servers on which to install Q-EKM. Q-EKM does not currently support encryption on other tape drive types or manufacturer brands, even if they are assigned to a partition selected for encryption.

Configuring the Encryption Settings

Encryption on the Scalar i2000 tape library is enabled by partition only. The default setting for encryption-capable drives permits external application-managed encryption support on all encryption-capable tape drives and media within a partition.

You cannot select individual drives for encryption; you must select an entire partition to be encrypted. If you encrypt a partition, all encryption-capable tape drives are enabled for encryption, and all data written to supported media is encrypted. Non encryption-capable tape drives will not be enabled for encryption, and non-supported media will not be encrypted.

You can only configure the encryption settings through the **Partitions > Modify** functionality.

> **Note:** In order for Q-EKM to work properly, you must upgrade both your library and tape drive firmware to the latest released versions. For instructions on performing the firmware upgrades, see the *Scalar i2000 User's Guide*.

Using Q-EKM to Manage Encryption

Q-EKM is an optional, licensed Java software program that generates, protects, stores, and manages the encryption keys. These keys are used by the LTO-4 tape drives to encrypt the information being written to tape media and read from tape media. Policy control and keys pass through the library-to-drive interface; therefore encryption is transparent. Q-EKM was designed to generate and communicate encryption keys for LTO-4 drives in Quantum libraries across the customer's environment.

If you choose to purchase and use the licensed Q-EKM application, you must supply a server on which to install EKM. Professional Q-EKM integration must be performed by Quantum or Quantum authorized service personnel. For more information, contact the Quantum Technical Assistance Center at www.quantum.com/support.

> **Note:** Prior to configuring Q-EKM on the Scalar i2000 library, Quantum recommends installing and configuring the Q-EKM server or servers first.

Setting Up Q-EKM on the Scalar i2000

Setting up Q-EKM on the Scalar i2000 consists of the following steps:

Step 1: Enabling the Q-EKM License Key

6 From the menu bar, click **Setup > Licenses**.

The **Licenses** dialog box appears.
This dialog box lists the licensed features for your library, including their status, expiration date, and quantity.

7 To enable a license key, in the **Enter License Key** box, type the appropriate license key.

You do not need to highlight the feature before you enter a license key. License keys are not case sensitive and all inclusive. For example, J2BGL-22622-52C22 can be entered as j2bgl-22622-52c22.

8 Click **OK**.

Step 2: Configuring the Q-EKM Server

Server settings are only used when a partition's encryption method is set to "Enable Library Managed." For more information on partitions, see the *Scalar i2000 User's Guide* (6-00421-11).

> **Note:** In order to synchronize properly, the TCP/IP and SSL ports on the primary and secondary Q-EKM servers must be set to the same values. Synchronization causes the entire configuration properties files of the primary server to overwrite the configuration files on the secondary server. Because the TCP/IP and SSL ports are listed in the configuration properties files, the primary and secondary servers must use the same TCP/IP and SSL port settings. Make sure the libraries that access these servers have their Q-EKM port configuration settings set correctly.

1 From the menu bar, click **Setup > EKM Servers**.
The **EKM Servers** dialog box appears.

2 In the **Primary EKM Server** text box, type the host IP address.

3 In the **Primary port number** text box, type the port number for the primary EKM server. The default port is 3801.

4 Optionally, in the **Secondary EKM Server** text box, you can provide the IP address of a secondary EKM server.

> **Note:** If you do not plan to use a secondary server, you may type a zero IP address, 0.0.0.0, into the **Secondary EKM Server** text box, or you may leave this text box blank.

5 If you configured a secondary server, enter the port number for the secondary server into the **Secondary port number** text box.

6 Click **OK**.
An **Operation in progress** dialog box appears, indicating the settings are being modified. Upon successful completion, the system returns to the main console.

Step 3: Configuring the Partition Encryption Settings

You can only configure the Q-EKM settings through the **Modify Partitions** process**.** You must create the partition first, then go to **Modify Partitions** to view and change the Q-EKM options. For more information on creating and modifying partitions, see either the *Scalar i2000 online Help* or the *Scalar i2000 User's Guide*.

Encryption on the Scalar i2000 tape library is enabled by partition only. You cannot select individual drives for encryption; you must select an entire partition to be encrypted. If you encrypt a partition, all encryption-capable tape drives are enabled for encryption, and all data written to supported media is encrypted. Non encryption-capable tape drives will not be enabled for encryption, and non-supported media will not be encrypted.

1. In the **Partitions** dialog box, select the partition you want to modify.
   The **Partitions — Step 1:Choose Partition Properties** dialog box appears.
2. In the **EKM** drop-down list, select the appropriate encryption option.
   The encryption method that you select will apply to all encryption-capable tape drives and media in that partition.

Encryption Method	Description
Unsupported	Means that no tape drives in that partition support encryption. If "Unsupported" is shown, it is greyed out and you are unable to change the selection.
Allow Application Managed	This is the default setting if you have encryption-capable tape drives in the partition. This option should remain selected ***unless*** you are connecting the library to an external Q-EKM server. This option allows an external application to provide encryption support to all encryption-capable tape drives and media within the partition. The library will NOT communicate with the Q-EKM server on this partition. **Note:** If you want an application to manage encryption, you must specifically configure the application to do so.
Enable Library Managed	Enables encryption support via a connected Q- EKM server for all encryption-capable tape drives and media assigned to the partition.

3. If there are no other changes to your partition, click **Next.**
   For more information on partitions, see the online Help or the *Scalar i2000 User's Guide* (6-00421-11).