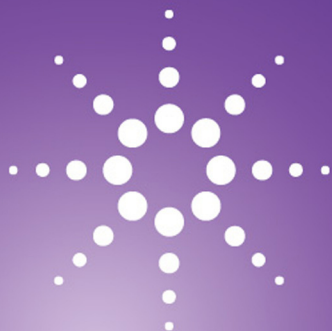
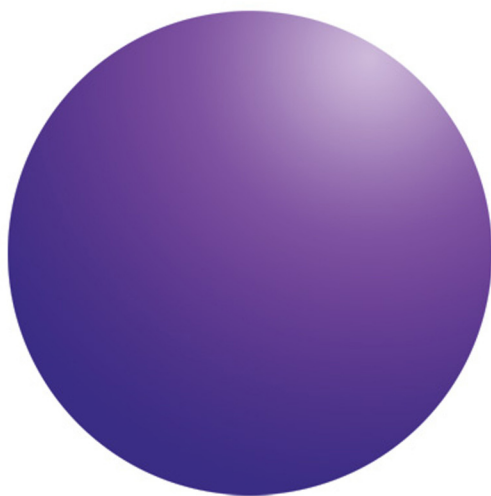




Agilent OpenLAB Data Store Administration



Guide for Administrators



Agilent Technologies

Notices

© Agilent Technologies, Inc. 2013

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Agilent Technologies, Inc. as governed by United States and international copyright laws.

Manual Part Number

M8623-90002

Edition

July 2013

Printed in USA

Agilent Technologies, Inc.
3501 Stevens Creek Blvd.
Santa Clara, CA 95051 USA

Microsoft[®] is a U.S. registered trademark of Microsoft Corporation.

Warranty

The material contained in this document is provided “as is,” and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Agilent disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Agilent shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Agilent and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Restricted Rights Legend

U.S. Government Restricted Rights. Software and technical data rights granted to the federal government include only those rights customarily provided to end user customers. Agilent provides this customary commercial license in Software and technical data pursuant to FAR 12.211 (Technical Data) and 12.212 (Computer Software) and, for the Department of Defense, DFARS 252.227-7015 (Technical Data - Commercial Items) and DFARS 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation).

Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a **CAUTION** notice until the indicated conditions are fully understood and met.

WARNING

A **WARNING** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a **WARNING** notice until the indicated conditions are fully understood and met.

Contents

- OpenLAB Data Store System Architecture 5
- OpenLAB Data Store Licensing 6
 - Licenses 6
 - Flexera License Manager 6
- Security and Data Integrity 7
 - Security Aspects 7
 - Data Integrity 7
- OpenLAB Control Panel 8
 - License Management 8
 - System Activity Log 9
 - Diagnostics 10
 - Administrative Reports 10
 - Authentication Provider 11
 - Security Policy 12
 - User Management 13

OpenLAB Data Store System Architecture

OpenLAB Data Store and OpenLAB Shared Services (OLSS) are installed together on a Windows 2008 R2 SP1 server.

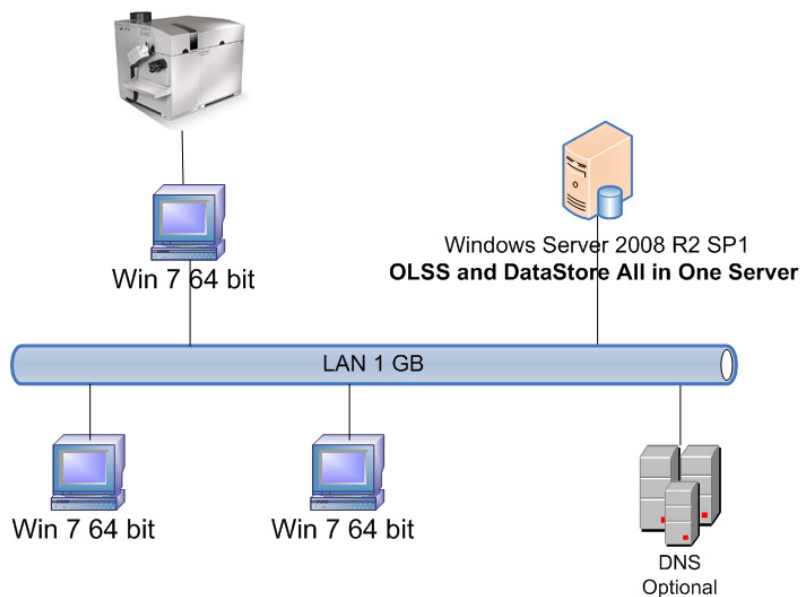


Figure 1 OpenLAB Data Store architecture

Client machines that access the Data Store server make use of the following components:

- OpenLAB Data Store web interface

OpenLAB Data Store provides a thin client web based user interface that can be accessed using Microsoft Internet Explorer. The web interface provides access to the Data Store folders and files.

- OpenLAB Control Panel

The OpenLAB Control Panel is the user interface that provides access to administrative functions used for managing OpenLAB Data Store and OpenLAB Shared Services.

OpenLAB Data Store Licensing

Licenses

Table 1 lists the License Features in OpenLAB Data Store.

Table 1 Licenses

Decription	License Feature(s) in OpenLAB Data Store
OpenLAB CDS Shared Services Server Software	1 x AgilentOpenLABSharedServices
OpenLAB Data Store Server	1 x AgilentOpenLABDataStoreServer
OpenLAB Data Store MS Instrument	2 x OpenLABDataStoreMSInst

Flexera License Manager

OpenLAB Data Store uses a 3rd party tool called *FlexNet Producer Suite* from Flexera to manage the licenses. The required Licensing server components are installed by default on the Data Store server.

License Management in OpenLAB Shared Services requires an additional Windows service to be running. This Windows service is called *Agilent OpenLAB License Server*. This service must be running on the server where you manage your licenses.

Security and Data Integrity

This section explains the built-in security and how it supports the FDA 21 CFR Part 11. It also explains the system security features provided by OpenLAB Shared Services.

Security Aspects

In OpenLAB Data Store, security aspects are covered by OpenLAB Shared Services.

The OpenLAB Shared Services functionality related to security includes the following (see [“OpenLAB Control Panel”](#) on page 8 for details):

- System Activity Log
- Selection of authentication provider
- Users, Groups and Roles Management
- Security Policy

Data Integrity

OpenLAB Data Store stores data in a manner that supports compliance with 21 CFR Part 11. It provides secure data storage with access control and an audit trail. Data files are versioned to ensure data integrity and traceability. In addition, OpenLAB Data Store provides electronic signatures allowing users to sign off on data.

OpenLAB Control Panel

Using the OpenLAB Control Panel, you can access OpenLAB Shared Services control features such as security policy, central configuration. These features are described in more detail in this chapter.

License Management

This service includes the administration of all licenses that are required for your system.

Before adding a license file, you must first purchase the license and generate the license file using SubscribeNet. For more information on generating new license files, refer to the *Agilent OpenLAB Data Store for MS Installation Guide*.

License Management in OpenLAB Control Panel provides the following functions:

- You can add license files to the license server.
- You can navigate to the license monitor and view the properties of all licenses installed on a given license server.
- You can remove license files from the license server. This may be useful if an invalid license file has been added.
- You can view or change the license server.
- You can view, copy, or save the MAC Address of the license server.
- You can navigate to the Agilent Electronic Software and License Delivery web page to get a license.

For more information on adding license files and viewing the license properties, refer to the OpenLAB Control Panel online help.

The following properties are shown for installed licenses:

- **Feature:** This indicates the type of license used.
- **Version:** If a license is versioned, you can see the version number. For licenses that are not versioned, the version is always shown as 1.0.

- **In Use (Available):** This indicates the number of licenses that are currently in use and, in brackets, the total number of licenses. With the OpenLAB Data Store licensing strategy, a license is only in use as long as a software instance is running (see “[OpenLAB Data Store Licensing](#)” on page 6).
- **Expiration:** If the license is only valid for a certain period of time, the expiration date is displayed.
- In the **Alerts** pane, you are informed if the number of available licenses has gone down to zero for a specific feature, or if you have started a software instance which requires a license that is unavailable.

System Activity Log

The System Activity Log allows you to centrally access all system activities. It contains information on the various events associated with OpenLAB Shared Services. You can filter the list in order to view only events of a specific type, in a specific time range, created by a specific user, or containing a specific description.

The following types of events are recorded:

- System
- User
- Group
- Security
- Printer
- License

To get more information on an event, expand the line of interest in the activity logbook viewer.

NOTE

By default, activity logging is disabled. To enable it in OpenLAB Control Panel, you must have the **Edit activity log properties** privilege. Once enabled, activity logging cannot be disabled again.

Diagnostics

The Diagnostics view allows you to access several reports and tools for diagnostic purposes:

- Ping the OpenLAB Shared Services server.
- Create a report, for the OpenLAB Shared Services server, with information on the operation system, processors, disk drives, processes, network and connections.
- Centrally access and download all the log files, trace files, etc. that are created by the registered modules.

Administrative Reports

In the Administrative Reports view, you can additionally create and export various XML or PDF reports related to the system configuration:

- **Roles and Privileges Report**

Describes all roles defined on the system, including details of all privileges included in each role.

- **Users and Groups Report**

This report provides an overview of all users and groups access rights to instruments and projects on the system. Note that users and groups that have not been granted access to instruments or projects are not included in this report.

Authentication Provider

Authentication providers are used to prove the identity of users that log in to the system. OpenLAB Data Store supports the following Authentication providers:

- **Internal**

In this mode, the user's credentials are stored in the OpenLAB Shared Services database. You are asked to create an administrator account for OpenLAB Shared Services before setting up other users. This is the only mode in which you can create new users within the system; in all other modes you can only map to users that exist in a different system.

- **Windows Domain**

You import existing Windows users into OpenLAB Shared Services. The authentication is done by a NT 4.0 Domain within the Enterprise. OpenLAB Shared Services only use the identity and password of the mapped users; roles and privileges for OpenLAB Data Store are still configured with OpenLAB Shared Services.

Security Policy

With the authentication provider **Internal**, you can set all of the parameters described below in the OpenLAB Control Panel. With Windows Domain authentication you can only set the inactivity time in the OpenLAB Control Panel; all other parameters are defined by the external system. [Table 2](#) describes the security policy settings.

Table 2 Security Policy settings

Setting	Description	21 CFR Part 11 Requirements
Minimum password length	If users change their passwords, they must choose a password with at least the given number of characters. The default setting is 5. Only available for authentication provider Internal .	You should require a minimum password length of at least 5 characters.
Password expiration period (days)	The default value is 30 days. When the user tries to log in after this period of time, the system will ask him to change the password. The expiration period starts with the last password change or with the creation of a user with a new default password. Only available for authentication provider Internal .	You should use an expiration period of 180 days or less.
Maximum unsuccessful login attempts before locking account	If a user tries to log in with invalid user credentials a number of times, the user is locked out of the system for a certain period of time (Account lock time , see below). Login is impossible, even with valid user credentials. You can define the number of allowed login attempts. The default setting is 3. Only available for authentication provider Internal .	You should limit the number of allowed login attempts to three.
Account lock time (minutes)	Once a user has exceeded the maximum number of allowed unsuccessful login attempts, this is the amount of time that must pass before he can try again. The default setting is 5 min. Only available for authentication provider Internal .	
Inactivity time before locking the application	If the OpenLAB Control Panel is inactive for this amount of time, the user interface will be locked. This setting is also used to set the time-based session lock in ChemStation. The default setting is 10 min. Set the value to zero to never lock.	
Single Sign-On	With Single Sign-On enabled, the user will not see the OpenLAB Control Panel login screen. Only available for authentication provider Windows Domain .	

User Management

OpenLAB Shared Services allow you to assign specific roles to users or user groups. If you manage your users within a Windows domain, you can map those existing users into OpenLAB Shared Services.

Each user can be member of multiple groups. You must assign a specific role to each group. You can also assign roles to single users; however, for the sake of clarity, it is strongly recommended to assign roles only on the group level.

The roles are equipped with numerous specific privileges which define what the users are allowed to view or do in OpenLAB Control Panel and in OpenLAB Data Store. [Table 3](#) describes the user credentials.

Users

Table 3 User Credentials

Value	Description	Mandatory
Name	Username to login to the system.	Yes
Description	Additional information about the user (e.g. department, function etc.)	No
Password	Password for the user; minimum password length is defined in the Security Policy.	Yes
Email address	Email address of the user.	No
Full name	The full (long) name of the user.	No
Contact Information	General contact information (e.g. telephone number, pager etc.)	No
User disabled	Select the check box to disable a user. Disabled users cannot log in any more. Users may be automatically disabled after too many failed login attempts. If a user is disabled, a corresponding message is displayed instead of the check box. After a given time (see Account lock time in the Security Policy settings), the user is automatically enabled again.	No
User cannot change password	Flag that indicates whether the user can change his own password. The flag is false by default (that is, users CAN change their passwords).	No
User must change password at next login	If set to true, the user has to change his password at the next login. The flag is automatically set to false after the user has changed the password successfully. The flag is true by default for new users.	No
Group Membership	Assign the user to the relevant groups.	
Role Membership	Assign roles directly to the user.	

If you use Windows domain as an external authentication provider you cannot create new users, but must import users that exist in the authentication systems. A search function helps you find specific users in the authentication system. In the OpenLAB Control Panel, you can manage the roles for those external users, but not the actual user credentials such as user name and password. If you want to remove an external user, you unmap the user in the OpenLAB Control Panel. The user continues to exist in the external authentication system.

Groups

If you use an external authentication provider, you can either import the names of groups that exist in the external system or create new internal groups. There is no limit on the number of groups that can be mapped or created.

You can assign users to groups in the external system or in OpenLAB Control Panel. If you need additional user assignments that are relevant only for OpenLAB CDS, you create them in OpenLAB Control Panel. Otherwise it is sufficient to only import the groups and assign the required roles to the groups.

If you delete or unmap a group, the users who were members in this group remain unchanged.

Roles and Privileges

Roles are used to assign privileges to a user or a user group globally. The system contains a list of predefined roles which are installed as part of the system installation (see [Table 4](#)). Each role has certain privileges assigned.

When you assign privileges to a role, you first select the required role type and then select the privileges related to this role type. Each role can only have privileges of one specific role type; the only exception is the predefined role **Everything**, which has all privileges of all role types. Users or groups may require multiple roles to perform system functions.

Table 4 Data Store Predefined roles

Privilege	Data Store Approver	Data Store Contributor	Data Store Reader	Archivist	System Administrator
Electronically sign files	X				X
Save or modify content	X	X			X
View content	X	X	X	X	X
View projects	X	X	X	X	X
Archive and de-archive content				X	X
Modify system settings					X
Manage security					X

www.agilent.com

© Agilent Technologies, Inc. 2013

Printed in USA 07/13



M8623-90002



Agilent Technologies