



OpenLab EZChrom

Guide for Administrators

Notices

© Agilent Technologies, Inc. 2010-2020

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

M8201-90088

Edition

Rev. C

09/2020

Printed in Germany

Agilent Technologies
Hewlett-Packard-Strasse 8
76337 Waldbronn

Software Revision

This guide is valid for revision A.04.10 of Agilent OpenLab EZChrom.

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

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as “Commercial computer software” as defined in DFAR 252.227-7014 (June 1995), or as a “commercial item” as defined in FAR 2.101(a) or as “Restricted computer software” as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Agilent Technologies’ standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will

receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

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.

In this Guide ...

This manual describes the concepts of OpenLab EZChrom (system architecture, licensing strategy, data integrity) and its administration with the OpenLab Control Panel. In addition, it contains specific information on the administration of OpenLab EZChrom .

Table 1 Terms and abbreviations used in this document

Term	Description
CDS	Chromatography Data System
EZChrom	OpenLab EZChrom
Data Store	OpenLab Data Store; as of rev. 2.3, the product name is OpenLab Server 2.5
OpenLab Server	New product name, formerly known as OpenLab Data Store.
Content Management	Data storage component provided as part of OpenLab Server
ECM	OpenLab Enterprise Content Manager
AIC	Agilent Instrument Controller
Control Panel	OpenLab Control Panel
Microsoft Control Panel	Part of the Microsoft Windows operating system
Shared Services	Set of components and services for licensing, users and roles, instrument configuration, security policy and more. Installed on all computers; accessed via the OpenLab Control Panel.
OpenLab CDS Shared Services Server	Server running the Shared Services. Formerly known as OpenLab Shared Services Server.

1 Architectural Concepts

This chapter gives you an overview of the general concepts of Agilent OpenLab EZChrom architecture. In the following, the term EZChrom refers to OpenLab EZChrom.

2 OpenLab Control Panel

Using the OpenLab Control Panel, you can access OpenLab CDS Shared Services control features such as security policy, central configuration, or lab status at a glance. These features are described in more detail in this chapter.

3 OpenLab CDS Shared Services Server

This chapter describes the OpenLab Server Maintenance Tool.

4 EZChrom-Specific Administration

This chapter describes fail over procedures and tools for AIC administration.

5 Appendix

This chapter contains information on privileges used in EZChrom, and on driver license features for instruments of other vendors than Agilent.

Contents

1	Architectural Concepts	7
	Overview	8
	OpenLab CDS System Architecture	9
	Workstation	9
	Networked Workstation	10
	Distributed Systems	11
	Backward Compatibility During Upgrade	15
	OpenLab CDS Licensing	21
	General Product Structure	21
	License Types	23
	Licensing Scheme	23
	Flexera License Manager	25
	License Upgrade	25
	Security and Data Integrity	27
	Security	27
	Data Integrity	27
2	OpenLab Control Panel	29
	Project Management	30
	Instrument Management/Lab Status at a Glance	30
	License Management	32
	System Activity Log	33
	Diagnostics	34
	Administrative Reports	35
	Authentication Provider	36
	Setting the Authentication Provider and Storage Location	37
	Security Policy	39

User Management	41
Users	41
Groups	42
Roles and Privileges	43
Specific Roles for Individual Instruments or Projects	44
3 OpenLab CDS Shared Services Server	45
Shared Services Maintenance	46
Using Backup and Restore Functions	47
Configuring Access to Windows Domain	49
Managing Server Settings	50
Maintenance Procedures	51
Update Database Statistics	51
Procedures for PostgreSQL Database	51
Procedures for SQL Server	52
Monitor Resource Usage on OpenLab CDS Shared Services Server	53
Additional Best Practices	53
4 EZChrom-Specific Administration	54
Fail Over Procedures for OpenLab EZChrom	55
AIC Driver and Install Tool	62
Use the AIC Driver and Install Tool	62
Change the Password of the Instrument Service Account	64
Change the Password of the AFS Administrator	65
5 Appendix	68
Privileges in OpenLab Control Panel	69
Administrative Privileges	75



1

Architectural Concepts

This chapter gives you an overview of the general concepts of Agilent OpenLab EZChrom architecture. In the following, the term EZChrom refers to OpenLab EZChrom.



Overview

OpenLab EZChrom contains the following software and interface modules:

- Control Panel
The Control Panel is the user interface that provides access to OpenLab CDS components, as well as administrative functions used for managing Shared Services features.
- Shared Services
- These services offer central access, central configuration, lab status at a glance, and remote control of instruments. The central functions can be used by all OpenLab modules.
- Reporting
- Instrument control, data acquisition and data analysis module
- File System or Central Data Storage (Content Management provided by OpenLab Server)

OpenLab CDS System Architecture

Workstation

In a workstation, all components (shared services, CDS, control panel) are installed on the same computer.

The following figure shows the configuration of an OpenLab CDS Workstation. You can have multiple instruments on one workstation (see *OpenLab EZChrom Requirements* guide).

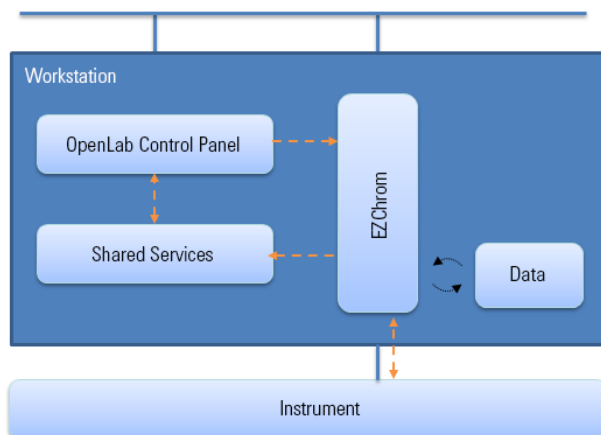
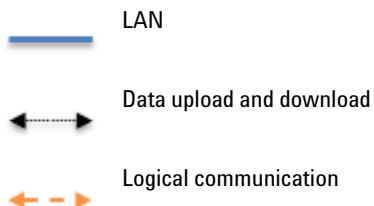


Figure 1 OpenLab CDS Workstation



Networked Workstation

In larger laboratories with many instruments in a network, you can install Shared Services on a either a dedicated *OpenLab CDS Shared Services server* or an *OpenLab Server 2.5*. Networked Workstations offer central administration of users, roles, and licensing.

The instrument status can be viewed from any Networked Workstation. However, you can launch and configure instruments only from the specific PC on which you configured the instrument.

The following figure shows an OpenLab CDS Networked Workstation configuration. There can be multiple workstations that are part of the Networked Workstation system. The figure shows only one EZChrom instance, but you can configure multiple instances and associated instruments on the same machine.

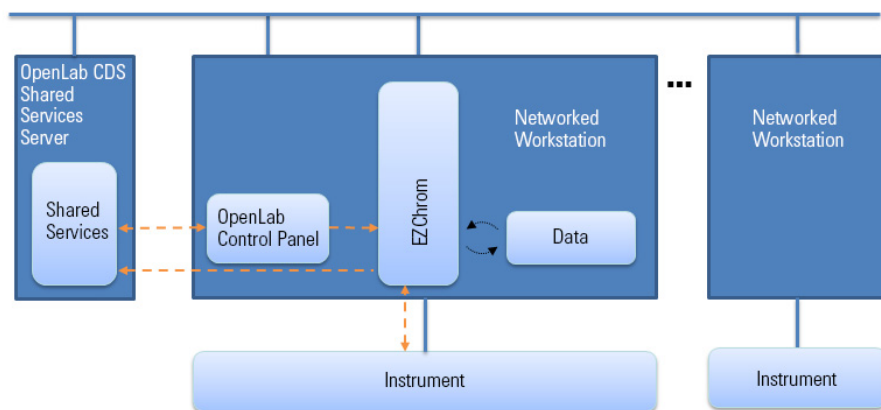
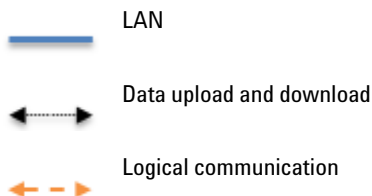


Figure 2 OpenLab CDS Networked Workstation



You can use the OpenLab EZChrom Networked Workstation configuration with or without central data storage. If you are connected to a central data repository, the data stored on the workstation is synchronized with the central repository.

If you use the Content Management provided by OpenLab Server, Content Management and Shared Services are installed on one server. In case of OpenLab ECM systems, separate Shared Services servers are required per ECM server.

With EZChrom, you can also use a network file share (the Enterprise Path) for storing your data.

Distributed Systems

With EZChrom installed as a Distributed System, you are able to access and run instruments from any EZChrom client PC in the system.

As in the Networked Workstation installation, the OpenLab Control Panel provides an overview of all instruments in the system. You can access all information provided by Shared Services from any EZChrom Client. For example, you can see which instruments are available in which location and which status (Online, Offline, Error, In Run, Not Ready, etc.) the instruments currently have.

In contrast to the Networked Workstation installation, in a Distributed System you can configure, launch and control any instrument from any EZChrom Client PC.

The Distributed System configuration enables you to work more flexibly with instrument sessions. You can, for example, launch an online instrument, start a sequence, and then disconnect only the CDS Client while the instrument continues to run on the Agilent Instrument Controller machine (AIC). You or another user can later connect to this instrument again from a different EZChrom Client to finish work on the online instrument or to analyze the data.

EZChrom Architecture

NOTE

The Distributed System configuration is supported with Network File Share, OpenLab Server, or OpenLab ECM.

In an EZChrom Distributed System, the instruments are configured and controlled from the Client PC through the instrument connection on the AIC. The AIC is a regular PC and can control up to four EZChrom Clients. You can access the EZChrom server instance on the AIC machine from any EZChrom Client with EZChrom installed. When you close the EZChrom application on the CDS client, you disconnect from the EZChrom Server instance running on the AIC. The EZChrom server instance continues to run on the AIC until the connection is closed in the OpenLab Control Panel.

The data is written on a file share. If you use central data storage, the data is synchronized with the central data repository. The following figure shows the system architecture of EZChrom with OpenLab ECM.

If you use the Content Management provided by OpenLab Server, Content Management and Shared Services are installed on one server. In case of OpenLab ECM systems, separate Shared Services servers are required per ECM server.

With EZChrom, you can also use a central file-based data storage.

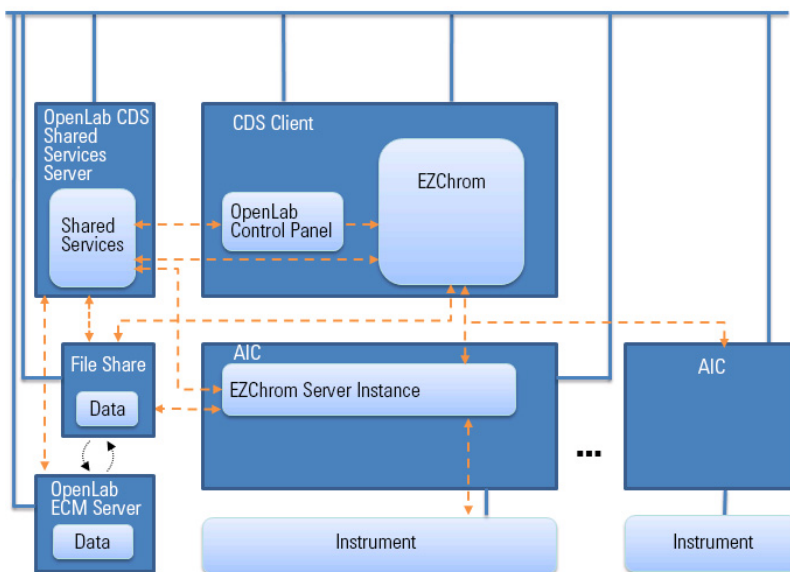
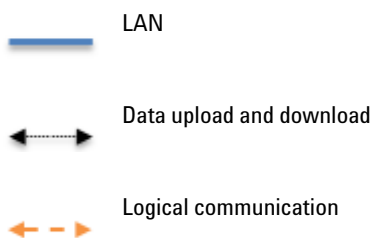


Figure 3 EZChrom with Distributed System with ECM



Networked Workstations in Distributed Systems

When an instrument cannot be controlled by an AIC or needs to be isolated and controlled by a single computer, you can add one or multiple Networked Workstations to a Distributed environment.

The following figure shows a mixed topology with one Networked Workstation, one CDS Client, one AIC, and central data storage. You can have multiple Networked Workstations, multiple CDS Clients, and multiple AICs in this topology.

In a mixed environment, you can use the Networked Workstation to access all instruments configured on this workstation, and you can also use it as a CDS Client for all instruments configured on AICs. Instruments configured on a Networked Workstation cannot be controlled from a CDS Client.

Systems with both ChemStation Edition and EZChrom being controlled by the same OpenLab CDS Shared Services Server are not supported.

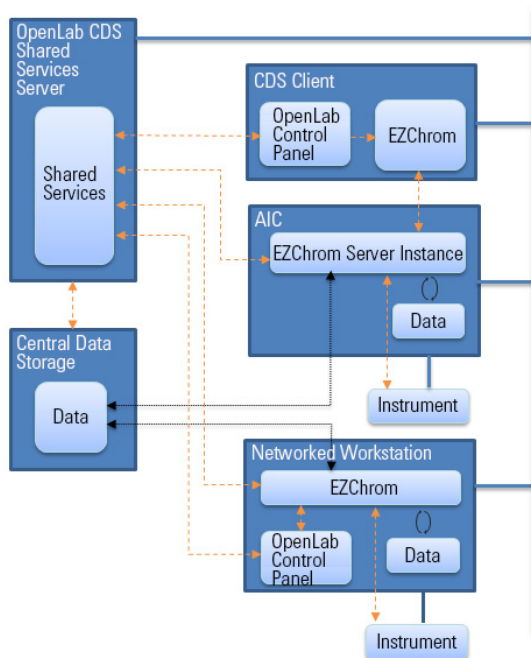
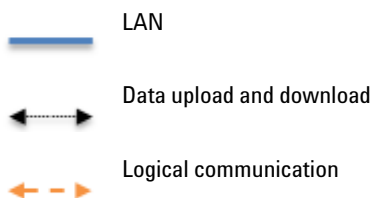


Figure 4 Mixed topology



Backward Compatibility During Upgrade

Backward compatibility was introduced in OpenLab Shared Services A.02.01 and OpenLab Data Store A.02.01 (bundled with EZChrom rev. A.04.06). It allows lab operation and minimizes lab downtime during an upgrade by having

the existing and the newer version of the data system on the same Networked or Distributed environment. The environment with different versions is to be used only during the upgrade phase. Procedures must be in place so older clients or workstations are not used to access and reprocess data created by newer clients or workstations.

During the upgrade phase, the **Instruments** and **Projects** tabs will be fully functional in the existing revision of the Control Panel. You can start and operate an instrument that was configured and running prior to the upgrade. Administrative tasks such as adding users or changing passwords must be done on the newer revision of the software. No other functionality is supported until the system upgrade is completed.

The following table shows the compatibility between the EZChrom edition with OpenLab Shared Services Server during an upgrade:

	OpenLab Shared Services A.02.01	OpenLab Shared Services A.02.02	OpenLab CDS Shared Services 2.1	OpenLab CDS Shared Services 2.3	OpenLab CDS Shared Services 3.4
EZChrom A.04.04	Yes with Hotfix OLSSA010405 ¹	No	No	No	No
EZChrom A.04.05	Yes with Hotfix OLSSA010501	Yes with Hotfix OLSSA010501	No	No	No
EZChrom A.04.06	Yes	Yes	No	No	No
EZChrom A.04.07	No	Yes	Yes	No	No
EZChrom A.04.08	No	Yes	Yes	No	No
EZChrom A.04.09	No	No	No	Yes	No
EZChrom A.04.10	No	No	No	No	Yes

¹ get latest Hotfixes/Updates from SubscribeNet

The following table shows compatibility between the EZChrom edition with OpenLab Data Store and OpenLab Server during an upgrade:

	Data Store A.02.01	Data Store A.02.02	Data Store 2.0	OpenLab Server 2.1	OpenLab Server 2.3	OpenLab Server 2.4	OpenLab Server 2.5
EZChrom A.04.04	Yes with Hotfix (OLSSA010405)	No	No	No	No	No	No
EZChrom A.04.05	Yes with Hotfix 01 (OLSSA010501)	Yes with Hotfix 01 (OLSSA010501)	No	No	No	No	No
EZChrom A.04.06	Yes	Yes	No	No	No	No	No
EZChrom A.04.07	No	Yes	No	Yes	No	No	No
EZChrom A.04.08	No	Yes	No	Yes	No	No	No
EZChrom A.04.09	No	No	No	Yes	Yes	Yes	No
EZChrom A.04.10	No	No	No	No	No	No	Yes

NOTE

Different revisions can be used during the upgrade phase. Agilent recommends that installations are on the same software version. Acquisition and data analysis are supported on the same version of software last used for reprocessing, or on a newer version of the software.

Mixed Configuration with EZChrom and OpenLab CDS 2.5

An environment with an OpenLab Server 2.5 supports using both OpenLab CDS 2.5 and EZChrom A.04.10 clients and AICs.

All instruments are visible on any client or Networked Workstation.

Routine work During routine work, use the EZChrom clients to access instruments that are controlled by a EZChrom AIC, and use OpenLab CDS 2.5 clients to access instruments controlled by an OpenLab CDS 2.5 AIC. The data storage is provided by OpenLab Server 2.5. Both environments share the same storage.

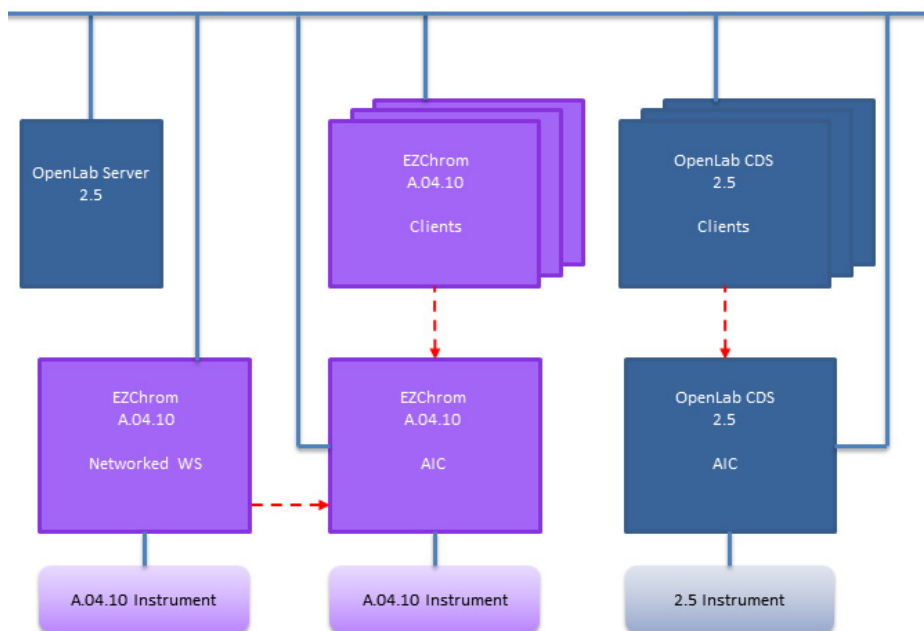


Figure 5 Routine work with EZChrom A.04.10 and OpenLab CDS 2.5

Use an instrument structure in the Control Panel that helps you differentiating the instruments.

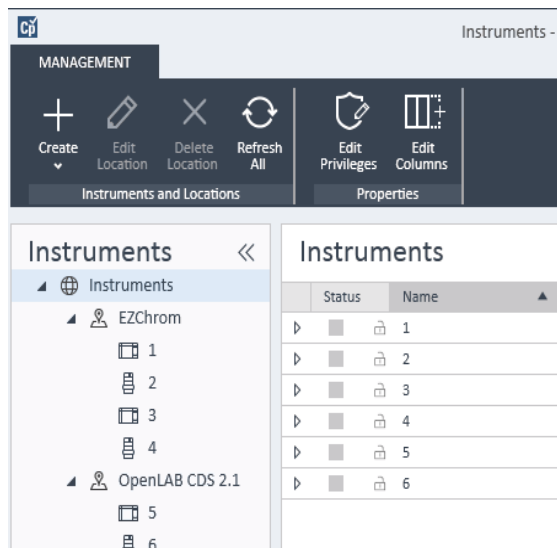


Figure 6 Instrument structure example

Migration The mixed configuration allows to transfer your acquisition method setpoints from EZChrom systems to OpenLab CDS 2.5.

- 1 Configure the same instrument on both EZChrom AIC and OpenLab CDS 2.5 AIC.
- 2 Start the instrument from an EZChrom client, and upload the acquisition method setpoints to the instrument. Close EZChrom (a simple disconnect is not sufficient).
- 3 Start the same instrument from the OpenLab CDS 2.5 client, and download the acquisition method setpoints from the instrument. Save with a new method name.

Close the instrument connection before starting it again from an EZChrom client.

CAUTION

Instrument access from different systems

The instrument may become inaccessible

Always launch and close instruments from the same system. Do not launch an instrument from EZChrom and close it from OpenLab CDS 2.5, or vice versa.

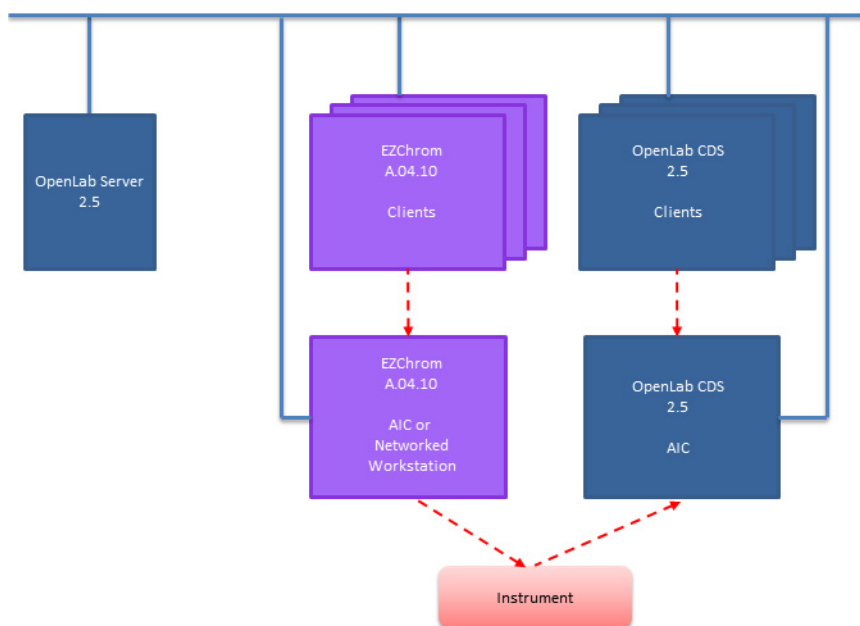


Figure 7 Transfer of method setpoints from EZChrom to OpenLab CDS 2.5

The transfer is one-way only. After transferring, you can use the EZChrom method on the OpenLab CDS 2.5 system. You cannot transfer acquisition methods from OpenLab CDS 2.5 to EZChrom, or process OpenLab CDS 2.5 data in EZChrom.

OpenLab CDS Licensing

This chapter summarizes the main components and features of Agilent OpenLab EZChrom, and outlines the licensing strategy for these components and features.

For procedures on how to obtain and install licenses, please refer to the *Licensing* chapter in the respective installation guide.

General Product Structure

OpenLab EZChrom has been designed as a combination of software modules for instrument control, data acquisition and data analysis (integration, quantification and reporting), automation and customization. Technique-specific single instrument products provide control capabilities for a given separation technique, e.g. for a Gas Chromatograph or Liquid Chromatograph. A single instrument configuration may be expanded by additional software modules (Add-ons).

The sections below describe the product modules. For more information on the product licenses, see “[Licensing Scheme](#)” on page 23.

Core module

The core module provides data analysis, automation and customization functions (no instrument control) for the following separation techniques:

- Gas chromatography (GC)
- Liquid chromatography (LC)
- Analog data acquisition with external event protocol (A/D)

Instrument drivers

Technique-specific single instrument drivers provide control capabilities for the separation techniques listed above. By installing multiple instrument drivers, Agilent OpenLab EZChrom is capable of controlling more than one analytical system, for example, two LCs, two GCs, or an LC and a GC.

The instrument control capability of OpenLab EZChrom may be expanded by purchasing additional modules to allow mixed technique configurations.

Add-ons

The acquired data is typically two-dimensional ("2D"), that is, by measuring detector response over time. Spectroscopic detectors can deliver three-dimensional ("3D") data, by additionally measuring detector response over a third axis (for example, wavelength or mass range).

For 3D data, the OpenLab CDS 3D UV Add-on module permits analysis and reporting:

License Types

The licensing strategy introduced with OpenLab EZChrom helps you use your licenses more effectively. In contrast to A.03.xx EZChrom revisions, licenses for instrument control, drivers and add-ons are *floating licenses*. Any instrument that starts up requests the necessary licenses from license management, and when the instrument is closed, it returns the licenses. Therefore, you only need licenses to cover the maximum number of concurrently running instruments rather than one for each installed instrument. License management is accessed via the OpenLab Control Panel.

Licenses are of two types:

- *Counted licenses* are consumed once for each associated software or instrument module.
- *Shared licenses* can be shared per PC or instrument. For example, the core license is a shared license, which means you need only one license per PC, no matter how many EZChrom instances you run on it.

There is a 60-day Startup License for the entire OpenLab EZChrom installation. The expiration period starts with the installation.

Licensing Scheme

Figure 8 on page 24 shows the licenses for EZChrom in the different installation scenarios:

- Workstation
 - One OpenLab EZChrom core license
 - Instrument and Add-on licenses as needed; you can run up to four 2D LC or GC instruments on the same workstation.
- Networked Workstation
 - One OpenLab CDS Shared Services server license
 - One OpenLab EZChrom core license for each Networked Workstation; you can connect multiple Networked Workstations to the OpenLab CDS Shared Services server.
 - Instrument and Add-on licenses as needed; you can run up to four 2D LC or GC instruments on the same Networked Workstation.

- Distributed System
 - One OpenLab CDS Shared Services server license
 - One OpenLab EZChrom core license and AIC-Add-on license for each Agilent Instrument Controller (AIC) machine. You need one AIC license for each AIC connected to the server.
 - Instrument and Add-on licenses as needed; you can run up to ten 2D LC or GC instruments on the same AIC.

To control instruments from vendors other than Agilent, an Agilent Instrument Control License is required in addition to the driver license for the other vendor's instrument. A list of driver licenses that are available for instruments from other vendors can be found in the *Supported Instruments and Firmware Guide*.

For Agilent instruments, Agilent Instrument Control licenses and Agilent Driver licenses are always bundled together. They are shown as one product license in the License Management. You can see these items as separate lines in the license file itself only.

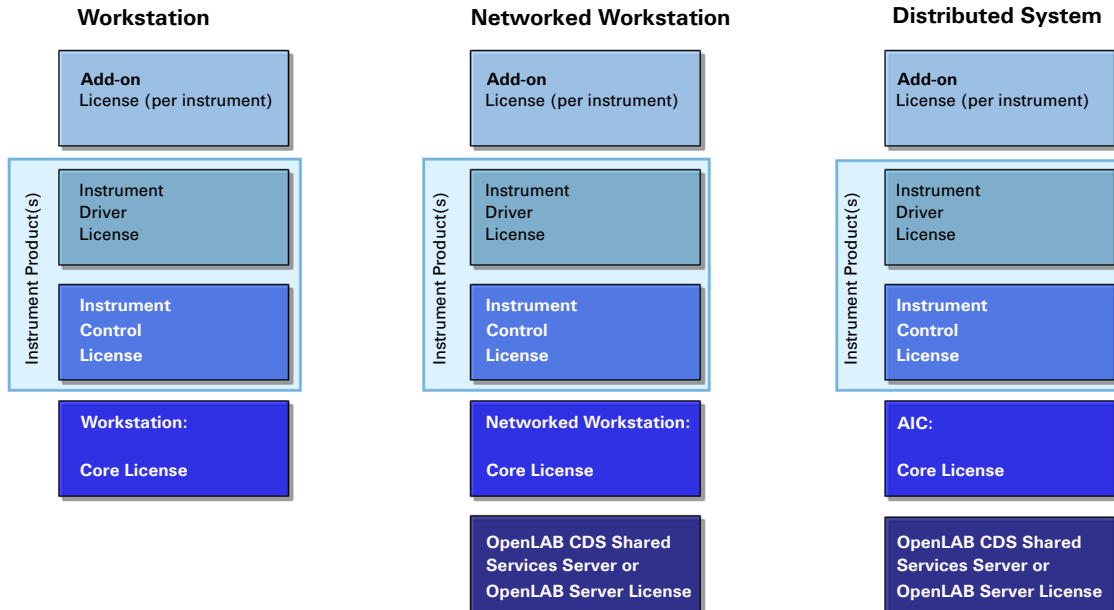


Figure 8 Licensing schema

Flexera License Manager

The Shared Services use a 3rd party tool called *FlexNet Producer Suite* from Flexera to manage the licenses. The required components are installed by default together with OpenLab CDS Shared Services. The license server can be the local PC, or a remote OpenLab CDS Shared Services server.

License Management in 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. Each time you start an instrument, the instrument requests licenses from the License Server service; therefore, you can only start an instrument if this service is running.

License Upgrade

If you are upgrading from an older version, you will need to upgrade your licenses in SubscribeNet prior to upgrading to the next version of OpenLab EZChrom. We strongly recommend upgrading your licenses *before* upgrading the core software. Standalone workstations which are upgraded to the new core software version, without a new workstation license, will not work until the new workstation licenses are added to the OpenLab Control Panel.

If you are under SMA subscription, proceed as follows to upgrade your licenses:

- 1 Log into the Agilent Electronic Software and License Delivery (<https://agilent.subscribenet.com/>).
- 2 Navigate to **Manage Licenses by Host**, and search for the machine hosting your workstation. Alternatively, select the machine from the drop-down list.
If the relevant host name does not appear, you may be managing your licenses in multiple SubscribeNet accounts. You will need to log into those accounts to upgrade those workstation licenses.
- 3 Click **Upgrade All** to upgrade all licenses on this host to the most recent version. Confirm the upgrade on the next screen.

This upgrades the license file to the most current version. SubscribeNet will send you an email with a new license file.

4 Put the new license file on your system.

If you have multiple standalone Workstations, repeat this step for each individual workstation.

In systems that include a server, you only need to provide the license file once, as licenses are managed on the central OpenLab CDS Shared Services server.

Security and Data Integrity

This chapter explains the built-in security and how it complies with the FDA 21 CFR Part 11. It also explains the system security features provided by OpenLab CDS Shared Services.

Security

The OpenLab Control Panel functionality related to security includes the following (see [“OpenLab Control Panel”](#) on page 29 for details):

- System Activity Log
- Selection of authentication provider
- User Management
- Security Policy

Data Integrity

The result data is stored either locally or in a central data repository, depending on the installed EZChrom configuration. If you store the data in the local file system, you must manually back up the data. With EZChrom, you can reach full compliance with 21 CFR Part 11 together with OpenLab ECM, OpenLab Data Store, or OpenLab Server. These systems store data in compliance with FDA 21 CFR Part 11. They provide secure data storage with access control and an audit trail. Data files are versioned to ensure data integrity and traceability. In addition, OpenLab ECM and OpenLab Server provide electronic signatures allowing users to sign off on data. The systems can be configured to automatically back-up and archive data on a regular basis.

In addition, with OpenLab CDS networked systems you can also use a network file share for storing your data. In this case, you must configure Advanced File Security (AFS) to be compliant with 21 CFR Part 11. AFS provides enhanced security on the enterprise path in order to prevent any unauthorized access to project data outside of the data system. This configuration sets the appropriate Windows sharing and security settings to allow only a defined group to access the enterprise data from Windows Explorer. This may only be configured if your system uses Windows Domain as the Shared Services authentication provider.

For more information on configuring AFS, refer to the *Networked and Distributed System Installation and Configuration* guide.



2 OpenLab Control Panel

Using the OpenLab Control Panel, you can access OpenLab CDS Shared Services control features such as security policy, central configuration, or lab status at a glance. These features are described in more detail in this chapter.



Project Management

A project is the set of directories that store related methods, data, sequences, and templates. Individual access rights can be applied to each project.

Project Groups can be used to arrange projects to match your organization.

The Projects pane is automatically available when the Control Panel is used with EZChrom.

Instrument Management/Lab Status at a Glance

The **Instruments** view in OpenLab Control Panel offers an overview of all instruments in the network or on the workstation. You can see the following information for all instruments, summarized on one page:

- Status of the instrument (including color-coded state, current run, and run status)

The status is stored and constantly updated in the Shared Services database in which the instrument is stored. It can be monitored by every OpenLab Control Panel connected the corresponding server.

- Instrument Name
- Instrument location
- Instrument type
- Last change of configuration

Depending on the configuration, this information may be accessed only from a single PC or from multiple workstations in a network.

You can create a tree of different locations in the OpenLab Control Panel, and add instruments to these locations. Using locations, you can organize your instruments for example by department, by laboratory, or by lab bench. For each instrument, you can provide basic information such as the name, description, and instrument type.

NOTE

Mixed scenarios with ChemStation and EZChrom instruments are not supported.

Depending on your privileges in OpenLab EZChrom, you can perform several operations on the instruments:

- View instrument information (instrument status, instrument details, activity log)
- View the locations and instruments tree
- Edit the instrument information
- Configure the instrument

The instrument configuration is stored on the local PC or AIC, but you access the configuration tool from the OpenLab Control Panel.

- Launch the instrument online or offline.

Workstation and Networked Workstation: As the instrument configuration is stored on the local PC, you only launch instruments that are configured on this PC.

Distributed System: As the instrument configuration is stored on an AIC, you can launch all instruments remotely from any EZChrom client in the network.

Your privileges can differ for the different locations and instruments (see [“Specific Roles for Individual Instruments or Projects”](#) on page 44).

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 *Licensing* chapter in the respective installation guide.

License Management in the 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 obtain a license.

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 EZChrom licensing strategy, a license is only in use as long as a software instance is running (see “[License Types](#)” on page 23).
- **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 Shared Services or with specific instruments. You can filter the list in order to view events of a specific type, in a specific time range, created by a specific user, or containing a specific description only.

The following types of events are recorded:

- System (e.g. Control Panel specific events)
- Instrument Management (e.g. Adding instruments)
- Instrument (e.g. instrument specific error messages)
- Instrument Controller (e.g. adding a new Networked Workstation or AIC)
- User (e.g. adding a new user or changing user privileges)
- Group (e.g. adding a new user group or changing group privileges)
- Security (e.g. successful and unsuccessful login events)
- License (e.g. adding a new license)

The messages can come from other components, such as the user management, or from an instrument module. Instrument messages include error messages, system messages or event messages. EZChrom records these events in its own environment but also sends the events to the System Activity Log. The System Activity Log records these events irrespective of whether you have been alerted to them or not. 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 server.
- Create a report, either for the local system or for the 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:

Instrument Controllers Report

Detailed information of all Instrument Controllers. When this report is generated on a Workstation, the information presented relates to the local system. When this report is generated on a client-server system, all Instrument Controllers are included.

Instruments Report

Provides detailed information about configuration and access privileges for all instruments on the system. On client-server systems, this report includes all instruments on all Instrument Controllers.

Projects Report

Provides detailed information about configuration and access privileges for all projects on the system.

Roles and Privileges Report

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

System Report

This report provides a consolidated view of the system, which includes all information about instrument controllers, instruments, projects, roles, users, and groups.

User's and Group's Role Assignment Report

This report provides an overview of all users and groups with their assigned roles.

Authentication Provider

Authentication providers are used to prove the identity of users that log in to the system. OpenLab CDS Shared Services support the following Authentication providers:

- **None**

In this mode, no login screen is shown when you access the OpenLab Control Panel. The user is automatically logged in to the application with security disabled. All log entries record the user as "Anonymous". With the authentication provider **None**, the Security Policy and User Management nodes are unavailable in OpenLab Control Panel.

NOTE

With the authentication provider **None**, any activity logs will display a generic **System** operator with no additional identification. This is not recommended for regulated environments.

- **Internal**

In this mode, the user's credentials are created and stored in the OpenLab CDS Shared Services database. You are asked to create an administrator account for OpenLab CDS Shared Services before setting up other users. This is the only mode in which you can create new users within the system.

- **Windows Domain**

You import existing Windows users into OpenLab CDS Shared Services. The authentication is done either by a Windows Active Directory domain or NT 4.0 Domain within the Enterprise. Shared Services only use the identity and password of the mapped users; roles and privileges for OpenLab CDS are still configured with the Shared Services.

- **ECM**

In this mode, an OpenLab ECM system is responsible for authentication. When you start the OpenLab Control Panel, the application will prompt for ECM credentials to validate a user. You must choose an existing ECM user as an administrator for the Shared Services. The Search function helps you to find specific ECM users. The Shared Services only use the identity and password of the mapped users; roles and privileges for OpenLab CDS are still configured with the Shared Services.

Setting the Authentication Provider and Storage Location

- 1 Open OpenLab Control Panel from the OpenLab Control Panel shortcut on the desktop, or go to **Start > All Programs > Agilent Technologies > OpenLab Shared Services > Control Panel**.
- 2 From the navigation pane, select **Administration > System Configuration**.
- 3 In the **System Configuration** toolbar, select **Edit System Settings**.

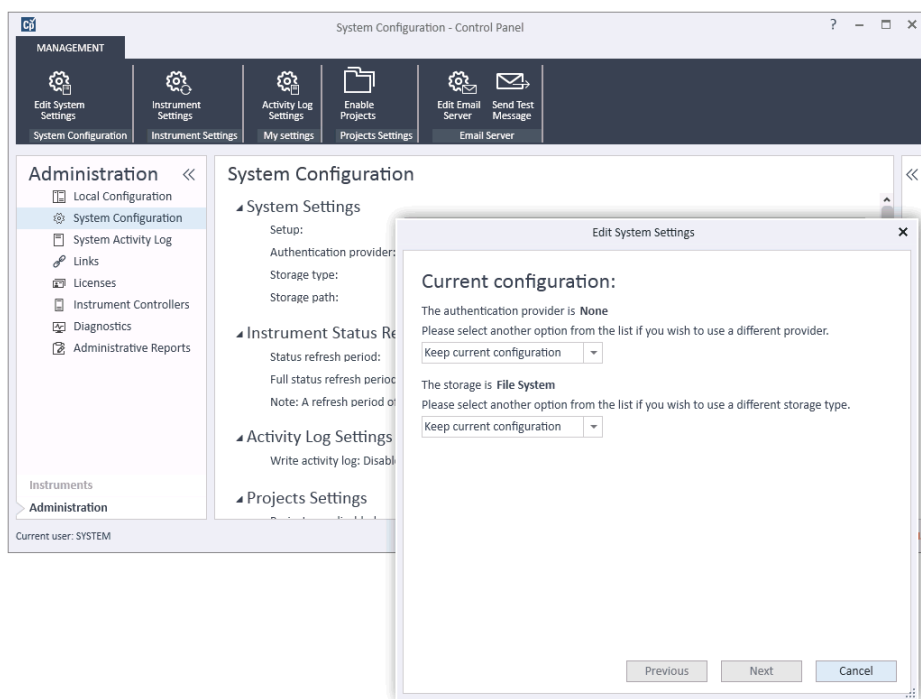


Figure 9 Edit System Settings dialog in the OpenLab Control Panel

- 4 In the **Edit System Settings** window, select your authentication provider from the drop-down list.

If you installed a server, the **Internal** authentication provider is automatically configured during the installation. If required, you can change the authentication provider to **Windows domain**.

- 5 Select your storage provider from the drop-down list.
The storage type **Content Management** is available only if OpenLab Server has been deployed.
- 6 Select **Next**.
- 7 Select a user to administrate the system.
 - a If you selected **Internal** as an authentication provider:
 - Select **Create Account**.
 - In the **Create Administrator Account** dialog box, enter a **Name** and a **Password**.
 - b If you selected **Windows Domain** as an authentication provider:
 - Select the check box to activate the input fields.
 - Enter a **Domain**, **User**, and **Password**.
 - Select **Select Account**.
 - Enter a search string.
 - In the **Search Users** dialog box, select **Search** to view a list of users.
 - Select a user.
 - c If you selected **ECM** as an authentication provider:
 - Provide the **ECM Server URL** and enter the ECM user credentials.
 - Select **Select Account**.
 - Enter a search string.
 - In the **Search Users** dialog box, select **Search** to view a list of users.
 - Select a user.
- 8 Select **OK**.
- 9 Select **Next**.
- 10 Review your settings and select **Apply**.

Security Policy

Once an authentication provider is configured, security policy is enabled and allows you to configure, for example, an inactivity timeout or password policies.

With the authentication provider **Internal**, you can set all of the parameters described below in the OpenLab Control Panel. With an external authentication provider (e.g. Windows Domain), you can only set the inactivity time in the OpenLab Control Panel; all other parameters are defined by the external system.

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 0 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 .	

Table 2 Security Policy settings

Setting	Description	21 CFR Part 11 Requirements
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 EZChrom. The default setting is <i>10 min</i> . 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

Once an authentication provider is set, you can configure Groups and Roles.

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 CDS.

Users

The following information is required if you create a new internal user:

Table 3 User Credentials

Value	Description	Mandatory
Name	Username to log in to the system. The following characters are not allowed as part of a username: < > : " / \ % * ? ' °	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
Password never expires	The password will never expire, even if a password expiration period is set in the security policy.	No

Table 3 User Credentials

Value	Description	Mandatory
Account is disabled	Select the check box to disable an account. Users with disabled accounts cannot log in any more. Accounts may be automatically disabled after too many failed login attempts. If an account 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 account 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.	

When using an external authentication provider (Windows Domain or ECM), the OpenLab Control Panel allows you to search and import the user into the application. 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 delete 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.

Assign users to groups either in the external system or in the Control Panel. If you need additional user assignments that are relevant only for OpenLab EZChrom, create them in the 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 or for a specific instrument or location. The system contains a list of predefined roles which are installed as part of the system installation (for example, **Instrument Administrator**, **Instrument User**, or **Everything**). Each role has certain privileges assigned.

Privileges are grouped according to the three main role types (Project role, Instrument role, and Administrative role). 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. For example, a user with the role *Chemist* may need another role such as *Instrument User* with the privilege to run an instrument.

You can create a tree of different locations in the Control Panel, and add instruments to the relevant locations. For each instrument or instrument group, you can assign different Instrument roles (see also [“Specific Roles for Individual Instruments or Projects”](#) on page 44). For example, a user can have the role **Instrument Administrator** for one instrument, and **Instrument User** for another instrument.

You can also create a tree of different projects or project groups in the Control Panel, and assign different Project roles for different projects (see also [“Specific Roles for Individual Instruments or Projects”](#) on page 44). For example, a user can have the role **Project Administrator** in one project, so that he can manage the settings in the Control Panel. In a second project, he may have a role that allows him to edit the content of a project, but not to change the project settings.

Table 4 Description of role types

Role Type	Description
Administrative privileges	These privileges are globally assigned to a user or group and cannot be changed on the instrument/location level. They are the typical administration privileges such as Backup and restore , Manage security , Manage printers etc.
Instrument privileges	These privileges can be assigned globally or on the instrument/location level. Privileges for instruments are, for example, View instrument or location and Run instrument . Users need the View instrument or location privilege on the global level to see the locations and instruments tree in the OpenLab Control Panel.
Project privileges	Privileges for accessing or modifying different levels of data. You can assign these privileges globally or on project level.

Specific Roles for Individual Instruments or Projects

By default, the roles of users or groups are globally set for all locations or instruments. The role settings are inherited from the root node **Instruments**. In order to assign a different role to a user or group for one specific node, you can deselect the **Inherit privileges from parent** check box in the **Edit Privileges** dialog for the required node. Afterwards, you can assign a different role that will be valid only for the specific node.

You can assign **Instrument** roles to individual locations or instruments.

Administrative roles are always set globally.



3 OpenLab CDS Shared Services Server

This chapter describes the OpenLab Server Utility Tool.



Shared Services Maintenance

The Shared Services Maintenance tool helps managing the system. It is automatically installed with your OpenLab software.

NOTE

The Shared Services Maintenance tool can only be started by administrators.

- 1 To start the application, go to **Start > All Programs > Agilent Technologies > OpenLab SharedServices > Shared Services Maintenance**.

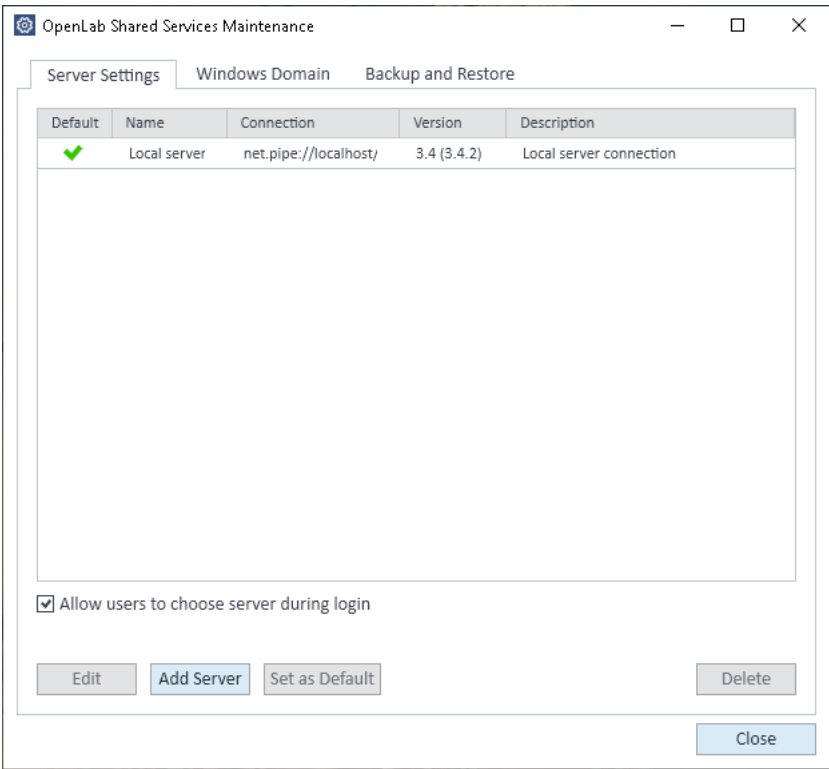


Figure 10 OpenLab Shared Services Maintenance (for example with **Server Settings** tab selected)

Using Backup and Restore Functions

In order to simplify backup and restore tasks for the Shared Services database, the **Backup and Restore** tab of the **Shared Services Maintenance** provides a simple interface for performing these tasks.

These functions are supported by the following database types:

- SQL Server Express or Compact
- PostgreSQL

For details on the maintenance of OpenLab Server and supported database types, refer to the OpenLab Server documentation on the OpenLab Server installation media.

Backup

Backup options offered by the utility depend on the SQL server edition installed on the system.

When using SQL Server Compact (installed on workstations), only a *full* database backup is allowed. This is a direct file copy of the existing database files used for the workstation.

When using SQL Server Express (installed with a Distributed System), you have the option to perform both full and incremental (transaction log) backups.

To perform a backup:

- 1 Specify the backup directory and retention time.

When a new backup is performed, the currently set retention time is used to delete any files older than specified.

- 2 Click **Backup**.

The backup is placed in the specified backup directory. Backups older than the retention time are deleted.

NOTE

The tool automatically generates filenames for the backup files. Never change these filenames, as the tool relies on a specific naming convention.

- 3 Select the type of backup.

NOTE

For an SQL Server, backups are grouped into related sets, where each set contains a single full backup and all the incremental backups based on it.

For an SQL Server, a new backup file is created for each month regardless of the method selected.

Retention time applies on a per transaction basis so that no month's backup file is deleted unless every transaction in that backup is younger than the set time. This includes the full and incremental log transactions.

Restore

Restore operations behave slightly differently depending on what version of SQL Server you are using.

- 1 Specify the backup directory and click **Restore**.

NOTE

The database is taken offline while this process executes a restore.

The restore function operates on backup sets, which include a full backup and all related incremental backups.

When restoring SQL Server Express, or compact database backups for client or server systems, you will restore to the selected backup in the list.

- 2 Verify that all connections to the system are shut down before performing a restore.
- 3 If you have selected the most recent backup, and if additional transactions have been executed against that database, the tool will also ask if you would like to save those changes prior to restoring the database. Click **Yes** to effectively perform a transaction log backup prior to the restore.

This message will not display for restore operations with an SQL Server Compact (installed on workstations).

Configuring Access to Windows Domain

If you use Windows domain authentication to identify your OpenLab users, OpenLab must be given access to the server where these credentials are stored.

Normally, if a machine has been joined to the domain, the trust relationship between this machine and the domain server is sufficient to grant this access. If a problem occurs while selecting an account: Use the **Windows Domain** tab in the **Shared Services Maintenance** program to specify or change the credentials that OpenLab will use to access your Windows domain server. The user specified here must have the privilege to obtain user and group information from the domain.

This feature can only access credentials that are stored on the computer where you opened the Shared Services Maintenance program.

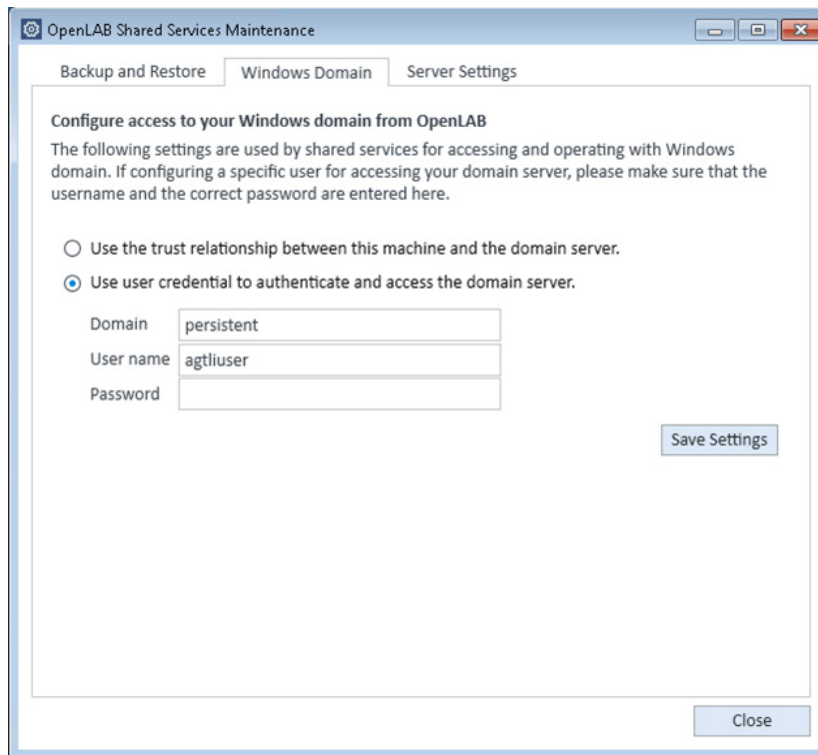


Figure 11 Windows Domain tab with specific user credentials

- 1 Choose the **Windows Domain** tab.
- 2 Enter the user credentials and click **Save Settings**.

Managing Server Settings

In a client/server configuration, use **Server Settings** to manage server connections for your local system. The list of servers here determines which servers users may choose to connect to when they log into OpenLab. Administrators can limit users from switching to a non-default server from this tab.

This feature manages server connections for the computer where you are using the **Shared Services Maintenance** program.

The server connections for each client in a client/server system are managed through each client, therefore to change the server connections for a client, access the **Shared Services Maintenance** program installed on that client.

In a workstation configuration, there is typically one server connection so this feature is not used.

- 1 Select the **Server Settings** tab.

A table shows all server entries and the default server connection.

For workstation installations, by default there is one entry for the local OpenLab CDS Shared Services server. For distributed or networked workstation installations, there is a second entry for the central OpenLab CDS Shared Services server (default).

- 2 You can add more servers by clicking **Add Server**.

You can switch the default server by selecting a server and clicking **Set as default**.

- 3 By default, the **Allow users to choose server during login** check box is selected. To forbid users to connect to non-default servers, clear this check box.

Users will need to contact their administrator in order to connect to another server.

All connections provided here will be listed under **Local Configuration** in the OpenLab Control Panel.

Maintenance Procedures

Update Database Statistics

To maintain optimal database performance, periodically update the Shared Services server database statistics. These statistics are used by the database engine to determine the most optimal way to execute queries.

You need to update statistics for the OLSharedServices database. If a custom database name was chosen during installation, use the correct name from your installation notes.

Procedures for PostgreSQL Database

For PostgreSQL database, these procedures must be performed on a regular basis. The frequency depends on the usage of the system. As a guideline, you should at least do this every time a full backup is taken.

Updating Statistics Using the Maintenance Wizard

- 1 Start PostgreSQL pgAdmin, connect as the database administrator, and select the database you want to update the statistics. The default database administrator user name is 'postgres' and the default password is an empty string (no characters).
- 2 Right-click the database and select **Maintenance....** The following form is displayed.

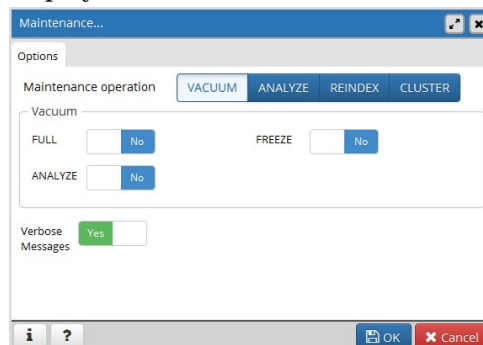


Figure 12 Maintain Database

- 3 Choose **ANALYZE**, and click **OK** to analyze the database.

Additional Maintenance for PostgreSQL Database

PostgreSQL supports some additional maintenance commands that can be beneficial to helping keep your database system running smoothly. These include VACUUM and REINDEX. See the PostgreSQL documentation for additional details about these commands.

CAUTION

PostgreSQL Service packs or Hotfixes

Only apply Agilent provided service packs or Hotfixes retrieved from SubscribeNet to your OpenLab PostgreSQL server.

Procedures for SQL Server

For MS SQL Server database the procedure to update statistics can be easily automated using the SQL Server Management Studio.

Updating Statistics Using Maintenance Plan Wizard

- 1 Start SQL Server Management Studio and connect as the database administrator.
- 2 Expand the server.
- 3 Expand the Management folder.
- 4 Right-click **Maintenance Plans** and select **Maintenance Plan Wizard**. Use the wizard to create a plan customized to meet your maintenance requirements.
 - a Select a **Weekly Schedule** to be executed at a time when there may be minimal activity (for example, Sunday, 12:00 noon).
 - b Select Update Statistics as the maintenance task.
 - c Choose the Shared Services database (OLSharedServices) as the database against which the task will be executed.

Monitor Resource Usage on OpenLab CDS Shared Services Server

Administrators of the system must regularly monitor disk space usage on all disks where data is stored. When the used disk space is close to 80 %, consider increasing disk space.

CPU, memory and network usage must be monitored to check for performance bottlenecks on the server.

Recommended Best Practices for Monitoring Resource Usage

- 1 Monitor the disk usage of OpenLab CDS Shared Services server at least weekly.
- 2 Optionally, implement automated disk space monitoring tools that send e-mail alerts when disk usage exceeds the thresholds. Examples of such tools are: Monit, Munin, Cacti, and Nagios.
- 3 Monitor system resource usage such as memory, CPU, and network throughput. Windows Performance Monitor can be used for this purpose.

Additional Best Practices

- 1 Apply 3rd party updates and patches on the OpenLab CDS Shared Services server.

Software patches and updates for OpenLab CDS and OpenLab Server are hosted on the <https://agilent.subscribenet.com> software distribution site. A separate login and an active Software Maintenance Agreement (SMA) are required for this site.

For further assistance, see
<http://www.agilent-labinformatics.com/ContactUs.htm>.

- 2 Apply Agilent software updates.

Apply software updates for Shared Services on your OpenLab CDS Shared Services server. When you receive notification of an update, please take note and read the information to determine if the update is applicable, and its urgency.



4 EZChrom-Specific Administration

This chapter describes fail over procedures and tools for AIC administration.



Fail Over Procedures for OpenLab EZChrom

OpenLab EZChrom has an option to connect to another instance of Shared Services. This gives you the ability to switch to local Shared Services on an AIC machine when the central OpenLab CDS Shared Services server in a Networked Workstation or Distributed System environment becomes unavailable. This will put you in a Workstation mode. You will then need to create projects, instruments, and users (if authentication is setup) on the local Shared Services, so you can connect to instruments and acquire data. When the central Shared Services server becomes available you can then reconnect your system to the central Shared Services server and move over your data.

If an AIC is acquiring data when the OpenLab CDS Shared Services server and Enterprise Path become unavailable, it will continue to acquire data until the sequence is finished. Once the sequence is finished the AIC will keep trying to put it on the Enterprise Path until it becomes available. When in fail over mode, follow a specific naming convention which distinguishes fail over file names from the file names on the distributed system. For instance, use this convention to prevent issues from copying files from the fail over workstation to the distributed system.

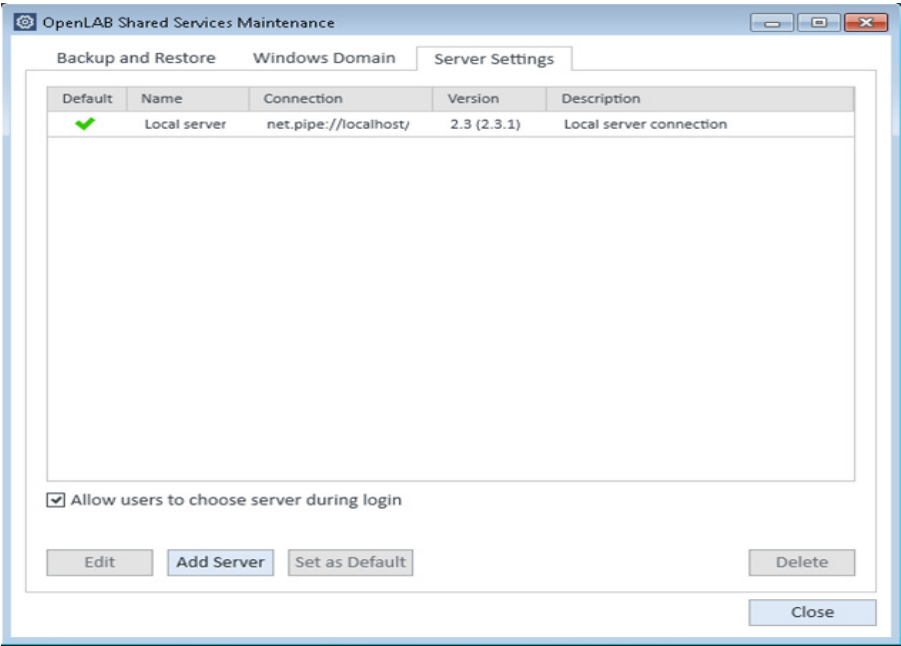
Do not apply electronic signatures while being connected to the local server. The signatures may become invalid after switching back to the central OpenLab CDS Shared Services server.

Connecting to the Local Server

Prerequisites You have installed an EZChrom AIC.

Convert an AIC to a local server

- 1 Log in as an administrator to the operating system of the machine that you want to convert.
- 2 If OpenLab Control Panel is open, close it.
- 3 Launch the **OpenLab Shared Services Maintenance** tool on the AIC, and select the **Server Settings** tab.
- 4 Select the local server, and click **Set as Default**.



- 5 Close the tool.

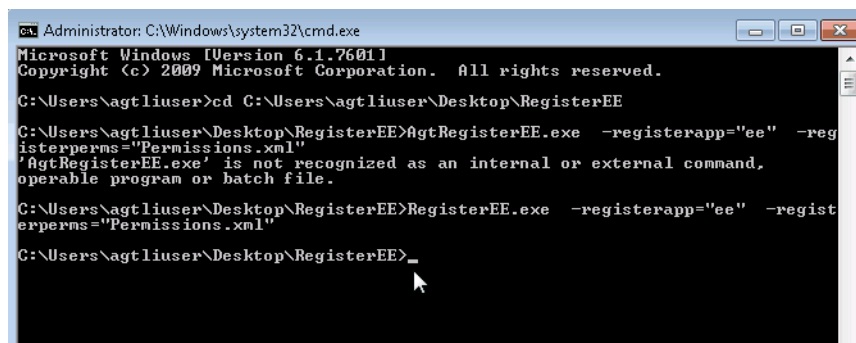
- 6 To confirm that the OpenLab Control Panel connects to the local server, launch the OpenLab Control Panel.

If it is connected to the local server, you will only see the **Administration** tab.

Under **Administration > Local Configuration**, verify that you are connected to the local server.

- 7 Copy RegisterEE folder from Disk 4 to the machine.
- 8 Open a command prompt.
- 9 Run the following command, pointing to the path where the RegisterEE folder is copied on machine:

```
RegisterEE.exe -registerapp="ee" -registerperms="Permissions.xml"
```



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

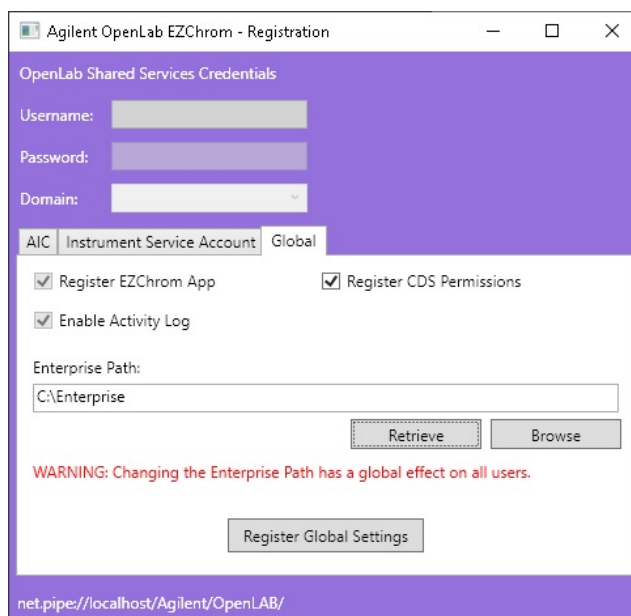
C:\Users\agtluser>cd C:\Users\agtluser\Desktop\RegisterEE
C:\Users\agtluser\Desktop\RegisterEE>AgtRegisterEE.exe -registerapp="ee" -registerperms="Permissions.xml"
'AgtRegisterEE.exe' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\agtluser\Desktop\RegisterEE>RegisterEE.exe -registerapp="ee" -registerperms="Permissions.xml"

C:\Users\agtluser\Desktop\RegisterEE>_
```

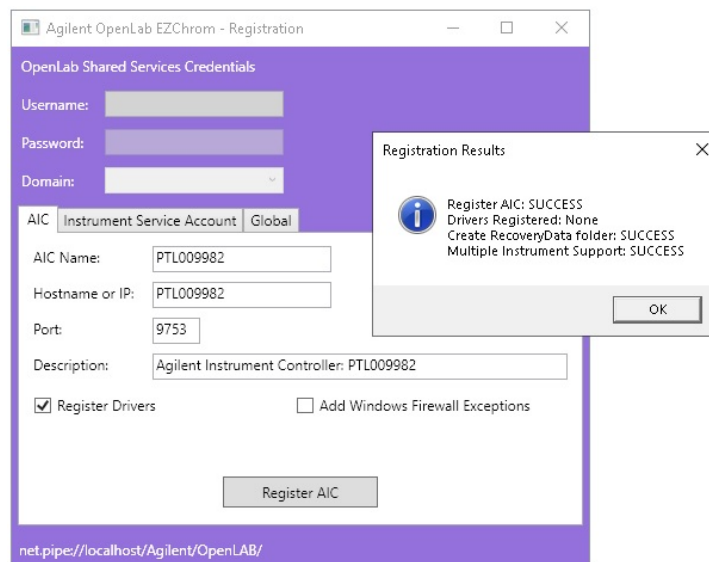
- 10 Launch the **AIC Driver and Install Tool**, and select the **Global** tab.

11 Under **Enterprise Path**, enter a local path, and click **Register Global Settings**.



The dialog box is titled "Agilent OpenLab EZChrom - Registration". It has a purple header bar. Below the header, there are three tabs: "AIC", "Instrument Service Account", and "Global". The "Global" tab is selected. Under the "Global" tab, there are four checkboxes: "Register EZChrom App" (checked), "Register CDS Permissions" (checked), "Enable Activity Log" (checked), and "Enterprise Path:" (unchecked). The "Enterprise Path:" field contains the text "C:\Enterprise". Below the field are two buttons: "Retrieve" and "Browse". Below the buttons is a red warning message: "WARNING: Changing the Enterprise Path has a global effect on all users." At the bottom of the dialog is a button labeled "Register Global Settings". The status bar at the bottom of the dialog shows the URL "net.pipe://localhost/Agilent/OpenLAB/".

12 Select the **AIC** tab, and click **Register AIC**.



The dialog box is titled "Agilent OpenLab EZChrom - Registration". It has a purple header bar. Below the header, there are three tabs: "AIC", "Instrument Service Account", and "Global". The "AIC" tab is selected. Under the "AIC" tab, there are four input fields: "AIC Name:" (containing "PTL009982"), "Hostname or IP:" (containing "PTL009982"), "Port:" (containing "9753"), and "Description:" (containing "Agilent Instrument Controller: PTL009982"). Below the fields are two checkboxes: "Register Drivers" (checked) and "Add Windows Firewall Exceptions" (unchecked). At the bottom of the dialog is a button labeled "Register AIC". The status bar at the bottom of the dialog shows the URL "net.pipe://localhost/Agilent/OpenLAB/".

A "Registration Results" dialog box is overlaid on the main dialog. It contains the following text: "Register AIC: SUCCESS", "Drivers Registered: None", "Create RecoveryData folder: SUCCESS", and "Multiple Instrument Support: SUCCESS". There is an "OK" button at the bottom right of the "Registration Results" dialog.

13 Reboot the machine.

14 Launch the OpenLab Control Panel.

The **Projects** and **Instruments** tabs appear.

Add failover license and configure instruments

- 1** In the OpenLab Control Panel, add a failover license.
- 2** Set the security as needed. The recommendation for fail over workstations is to use internal authentication.
- 3** Create new projects, instruments, and users (if authentication is set) in the local Shared Services instance.
- 4** Launch the instrument and create a new method. Save the newly created method.
- 5** Create a new sequence. Save the newly created sequence file.

Switching Back to Remote Server

- 1 Log on to the fail over workstation as a local administrator.
- 2 Launch the **OpenLab Shared Services Maintenance** tool, and select the **Server Settings** tab.
- 3 Select the Distributed System server, and click **Set as Default**.
- 4 Launch the **AIC Driver and Install Tool**.
- 5 On the **AIC** tab, re-register the AIC.
- 6 Reboot the machine.
- 7 Once the remote server is up and running, you need to copy data from the Enterprise folder on the local server to the remote server.
 - a *For a File System* - Manually copy all files from the local path to the storage path on the remote server.
 - b *For ECM and Content Management* - Use the procedure described below.

To copy data to the remote ECM or OpenLab server

- 1 Manually upload files from the Method, Sequence, Data, and Sample Prep folders from the fail over workstation to the Method, Sequence, Data, and Sample Prep folders on the ECM or OpenLab Server machine
- 2 The following changes to the method file on the ECM or OpenLab Server machine may be needed depending on how your methods were created.
 - **Method > Advanced > Files tab** – Make sure the baseline file path is changed to the ECM or Data Store path
 - **Method > Advanced > Advanced Report** – Make sure the report template name field is changed to the ECM or Data Store path.
- 3 The following changes to the sequence file on the ECM or OpenLab Server machine may be needed:
 - a Open your sequence and browse to **Sequence > Properties**. Verify the paths are changed to point to the ECM or Data Store path.
 - b In the Sequence Table:
 - Browse to the run type column. If the run type column has options selected which point to report template paths, these paths will need to be changed to the Data Store or ECM Path

- Look at the Sample Prep column. If this field is used, the path for the Sample Prep file will need to be changed to the Data Store or ECM path. This does not need to be changed if you are using the default path.
 - Look at filename column. Change this to the Data Store or ECM path if necessary. This does not need to be changed if you are using the default path.
 - Look at the Method column. Check the method path to see if it needs to be changed to the Data Store or ECM path. This does not need to be changed if you are using the default path.
- 4** Create a result set using the information from the files above:
- a** Open a sequence that was modified according to the procedures listed in the previous section.
 - b** Reprocess the sequence. After reprocessing a result set will be created in Content Management or ECM. When the result set is created in Content Management, a folder in the result folder will be created containing individual files. In ECM the result set will get zipped up in the Result folder. The result set package options selected in your project will determine which files are placed into the result set.

AIC Driver and Install Tool

The AIC Driver and Install Tool offers a number of functions related to the EZChrom configuration.

Use the AIC Driver and Install Tool

- 1 From the Start menu, select **Start > All Programs > Agilent Technologies > OpenLab EZChrom > AIC Driver and Install Tool**.

Agilent OpenLAB CDS EZChrom Edition - Registration

OpenLAB Shared Services Credentials

Username:

Password:

Domain:

AIC ☐ Instrument Service Account ☐ Global

AIC Name:

Hostname or IP:

Port:

Description:

☒ Register Drivers ☐ Add Windows Firewall Exceptions

net.pipe://localhost/Agilent/OpenLAB/

- 2 In the top area, enter the user name, password, and domain of the OpenLab Control Panel Administrator. This is required to change the settings on any of the tabs.
 - On the **AIC** tab, you can register a server as an AIC, for example, in case of a fail over. For details, see [“Fail Over Procedures for OpenLab EZChrom”](#) on page 55.
 - On the **Instrument Service Account** tab, you can retrieve or store the user who runs the instrument service. The user is recommended to be a domain user with a password that never expires. The user must be part of the local administrator group on the AIC. If you want to store your acquisition data on a network share, this user must have access to the shared folder.

After adding or changing the instrument service account, reboot all AICs.

NOTE

An instrument service account can only support up to 64 AICs due to a Microsoft limitation.

- On the **Global** tab, you can retrieve the current Enterprise Path or register a specific Enterprise Path. This is relevant, for example, in the case of a fail over. For details, see [“Fail Over Procedures for OpenLab EZChrom”](#) on page 55.

Change the Password of the Instrument Service Account

It is recommended to use a password that never expires. However, if you need to change the password, follow the procedure below.

- 1 Stop all acquisitions and close any OpenLab Control Panels.
- 2 Power off all Agilent Instrument Controllers (AICs) or Networked Workstations.
- 3 Change the password for the corresponding account in the customer domain.
- 4 From the Start menu, select **Start > All Programs > Agilent Technologies > OpenLab EZChrom > AIC Driver and Install Tool**.
- 5 In the top area, enter the user name, password, and domain of the OpenLab Control Panel Administrator. This is required to change the settings on any of the tabs.
- 6 Select the **Instrument Service Account** tab.
- 7 Enter the username, the new password, and the domain, then click **Store**.
- 8 Power on AICs or Networked Workstations.

Change the Password of the AFS Administrator

Advanced File Security (AFS) is an optional configuration for OpenLab EZChrom networked systems. It provides enhanced security on the Enterprise Path in order to prevent any unauthorized access to project data outside of the data system. This configuration sets the appropriate Windows sharing and security settings to allow only a defined group to access the enterprise data from Windows Explorer. This may only be configured if your system is configured to use Windows Domain as the Shared Services authentication provider.

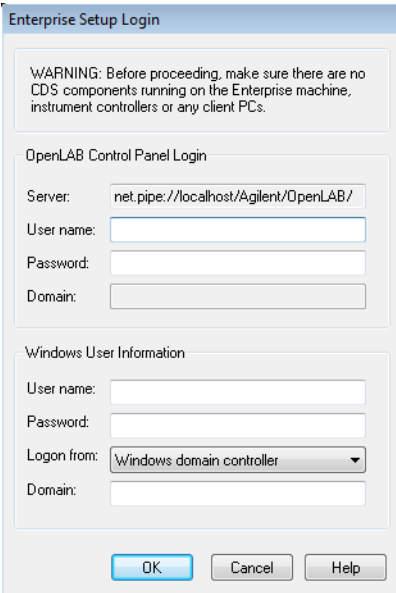
It is recommended to use a password that never expires. However, if you need to change the password, follow the procedure below.

- 1** Stop all acquisitions and close any OpenLab Control Panels.
- 2** Change the password for the corresponding account in the customer domain.
- 3** On any OpenLab EZChrom client, browse to the directory where the software was installed.
(by default: C:\Program Files\Agilent Technologies\EZChrom)

4 EZChrom-Specific Administration

Change the Password of the AFS Administrator

4 Launch EnterpriseConfig.exe.



The image shows a Windows-style dialog box titled "Enterprise Setup Login". It contains three main sections: a warning message, "OpenLAB Control Panel Login" fields, and "Windows User Information" fields. At the bottom are "OK", "Cancel", and "Help" buttons.

Enterprise Setup Login

WARNING: Before proceeding, make sure there are no CDS components running on the Enterprise machine, instrument controllers or any client PCs.

OpenLAB Control Panel Login

Server: net.pipe://localhost/Agilent/OpenLAB/
User name:
Password:
Domain:

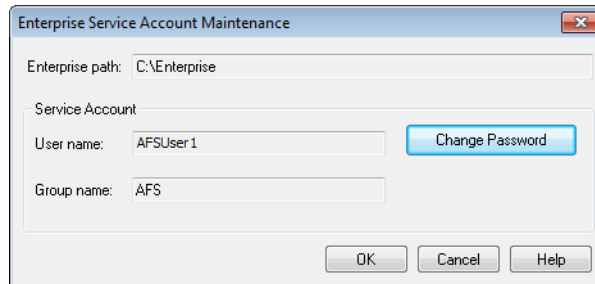
Windows User Information

User name:
Password:
Logon from: Windows domain controller
Domain:

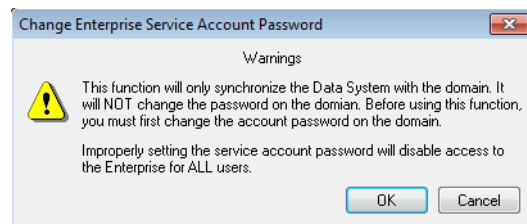
OK Cancel Help

- 5 In the **OpenLab Control Panel Login** section enter the user name, password, and domain of the OpenLab Control Panel Administrator.
- 6 In the **Windows User Information** section enter the user name and password of a user with edit permission to the enterprise path.
 - a If this is a domain user account, select **Logon from Windows Domain** and enter the domain name (recommended).
 - b If this is a local PC account, select **Windows Local PC**. This may only be an account local to the machine where the EnterpriseConfig.exe program is being run.
- 7 Click **OK**.

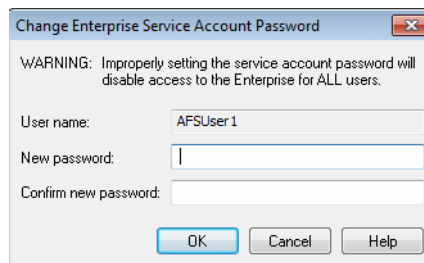
8 In the **Enterprise Service Account Maintenance** dialog, click **Change Password**.



9 Confirm the warning.



10 Enter the *new* password.



11 Click **OK**.



5 Appendix

This chapter contains information on privileges used in OpenLab EZChrom.



Privileges in OpenLab Control Panel

The privileges described in the following can be associated with different roles in OpenLab Control Panel. By default, the following roles are available:

- Everything
- System Administrator
- Instrument Administrator
- Project Administrator
- Instrument User

Additional default roles are available depending on the installed components. For example, with an OpenLab EZChrom installation, the additional default role **EZChrom Analyst** is available.

In OpenLab Control Panel under **Administration > Roles**, you can view or change the associated privileges, or create your own roles.

NOTE

Roles are only visible if user authentication is required.

Project Privileges

Table 5 Project Management

Name	Description	Relevant for ...
View project or project group	User can see a project and project details but cannot edit. With Content Management: User can view the content of the Content Management repository. <i>Note:</i> This privilege is required for all users.	EZChrom Content Management
Manage project or project group	User can create, edit, or move projects but cannot access settings.	EZChrom Content Management
Edit content of project	User can create new versions of documents in the Content Management system.	Content Management
Manage project or project group access	User can edit project access settings.	EZChrom Content Management
Access content using web client	User with this privilege is able to open the Content Browser interface.	Content Management

Table 6 E-Signature

Name	Description
E-Signature Sign Data Files	User can sign data files .
E-Signature Revoke	User can revoke the e-signature.

EZChrom-Specific Privileges

Table 7 EZChrom: Method

Privilege	Description
Save Method	Save a method file. Create a new method (requires one or more method privileges listed below.)
Edit Method Properties	View or change the method properties (Description, Options, Calibration, Audit Trail)
Open Method	Open a method file.
Instrument Setup	View or change the method instrument setup parameters.
Integration Events	View or change method integration events.
Peaks Groups	View or change the Peaks and Groups table
Advanced Parameters	View or change advanced method parameters (Export, Custom Parameters, Column/Performance, Files, Advanced Reports)
Custom Reports	Open, edit, save custom method reports
System Suitability	View or change system suitability parameters
Review Calibration	Allows access to the review calibration window
Calibrate	Run a calibration sample to update the method calibration. In order to create or modify the calibration parameters in a method, the user must also have the "Save Method" privilege assigned
Edit Running Method	Allows to edit a running method
Update Master Method	Allows update of the original master method when reviewing results in a container

Table 8 EZChrom: Data

Privilege	Description
Save Data	Allows to save a data file
Open Data	Allows to open a data file
Edit Properties	View or change the data properties description
Manual Integration Fixes	Allows to add or change manual integration fixes

Table 9 EZChrom: Sequence

Privilege	Description
Open Sequence	Allows to open a sequence
Sequence Save	Allows to save a sequence file
Process Sequence	Allows to process a sequence
Sequence Properties	Allows to view and edit sequence properties
Edit Any Running Sequence	Allows to edit any running sequence
Edit Own Running Sequence	Allows to edit own running sequence

Table 10 EZChrom: Sample Prep

Privilege	Description
Open Sample Prep	Allows to open an autosampler sample prep file
Save Sample Prep	Allows to save an autosampler sample prep file
Edit Sample Prep Properties	Allows to view or edit autosampler sample prep properties
Edit Running Sample Prep	Allows to edit a sample prep currently used (running)
Update Master Sample Prep	Allows update of the original master sample prep

Table 11 EZChrom: Control

Privilege	Description
Preview Run	Allows to preview a run
Single Run	Allows to perform single run acquisition
Sequence Run	Allows to perform sequence acquisition
Print Setup	Allows to set up a printer for the current instrument
Manual Control (idle only)	Allows to access manual control functions while the instrument is idle
Manual Control	Allows access to manual control functions whether or not instrument is idle
Monitor All Data	Allows to monitor real time plot from any running instrument
Abort Any Run	Allows to abort any running sequence or single run
Unlock instrument	Allows a user to unlock another user's lock when the instrument window is locked To be used in combination with the Unlock any locked UI privilege under System Administration . Both privileges are required to unlock another user's lock

Table 12 EZChrom: Standard Reports

Privilege	Description
Add Standard Report Template	Allows to add a standard report template

Table 13 EZChrom: Advanced/Intelligent Report

Privilege	Description
Open Advanced/Intelligent Report	Allows to open an advanced/intelligent report template
Save Advanced/Intelligent Report	Allows to save an advanced/intelligent report template
Lock/unlock report template items	Allows to lock and unlock report template items (tables, chromatograms, groups of items,...) to control who is allowed to modify those

Instrument Privileges

Table 14 Instrument Management

Name	Description
View instrument or location	User can view and access a location in the tree, but not edit access security, can view properties.
Manage Instrument or location	User can create and move locations and edit properties (name, description, etc).
Manage instrument or location access	User can view and edit the location access settings.
Run instrument	User can start an instrument session.
Service instrument	User can lock or unlock an instrument (to service it).

Administrative Privileges

Table 15 System Administration

Name	Description
Manage printers	Can add/remove printers and print server.
Edit activity log properties	Can change the Activity log Settings in OpenLab Control Panel (that is, can turn logging on for the System Activity Log).
Create administrative reports	Can create any of the system admin reports.
Manage system components	Can install/remove components (applications).
Manage Security	<p>Can change security settings. Can edit (add, change etc) users, groups and roles. <i>Note:</i> A user with this privilege can grant himself access to all settings in the OpenLab Control Panel. Be careful who you grant the Manage Security privilege.</p>
Manage instrument controllers	Can edit AIC configuration, manage the AICs in the Shared Services Maintenance tool.
Unlock any locked UI	<p>Can login into any locked portal or instrument session (will be a re-login), even if privately locked. To be used in combination with the Unlock instrument privilege under EZChrom: Control. Both privileges are required to unlock another user's lock</p>

Table 16 Content Management

Name	Description
Archive content	User can archive the content of the data repository.

In This Book

This manual contains information on the concepts of OpenLab EZChrom, and the administration with the OpenLab Control Panel.

General concepts:

- System Architecture
- Licensing Strategy
- Security and Data Integrity

OpenLab Control Panel

- Instrument Management
- License Management
- Log Files and Diagnostics
- Authentication Provider
- Security Policy
- User Management

© Agilent Technologies 2010-2020

Printed in Germany
09/2020



M8201-90088



Agilent Technologies