OpenLab ChemStation with
Content Management Systems

Administration Guide

Notices

Document Information

Copyright

Software Revision

This guide is valid for OpenLab ChemStation LTS 01.11.

Warranty

Technology Licenses

Restricted Rights Legend

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 guide details on administration and maintenance for distributed systems of OpenLab ChemStation with a content management system (OpenLab ECM, OpenLab Server, or OpenLab ECM XT). It also describes the settings required by 21 CFR Part 11, and it provides information on the workflows for ChemStation using a central data storage.

Table 1   **Terms and abbreviations used in this document**

Term	Description
AIC	Agilent's Analytical Instrument Controller
CDS	Chromatography Data System
ChemStation	OpenLab ChemStation
Control Panel	OpenLab Control Panel
Microsoft Control Panel	Part of the Microsoft Windows operating system
ECM	OpenLab ECM, rev. 3.x
ECM XT	OpenLab ECM XT

1   Introduction

This chapter introduces the integration of ChemStation with a content management system (OpenLab ECM, OpenLab Server, or OpenLab ECM XT) and describes how to ensure compliance with 21 CFR Part 11.

2   Basic Concepts

This chapter describes how to log in to ChemStation, explains the user interface items and toolbars related to the central data storage, and describes the main preference settings.

3   Working with ChemStation and Central Data Storage

This chapter describes the basic workflows for ChemStation with a central data storage system.

Contents

1 Introduction

This chapter introduces the integration of ChemStation with a content management system (OpenLab ECM, OpenLab Server, or OpenLab ECM XT) and describes how to ensure compliance with 21 CFR Part 11.

What is a Central Data Storage?

Agilent provides two systems for central data storage:

- *OpenLab Server* is available as a single server solution providing the Content Management component for small to medium laboratories with up to 100 instrument points. It provides the necessary security in support of regulatory compliance.

- *OpenLab ECM* is available as a single server or multi-server, distributed solution for comprehensive data management needs for laboratories with a few instruments to hundreds of instruments. It also provides the necessary security in support of regulatory compliance.

Both systems are web-based and allow you to securely store, archive, and catalog your chromatographic files such as data, reports, methods, and any electronic file type such as Microsoft Office documents, Adobe PDF documents, images, and molecular drawings,

The content management system allows you to easily collect, organize, search, and review all of your ChemStation data. They automatically extract searchable metadata from files, and provide powerful search capabilities. ECM additionally provides embedded viewers for many file types.

In this document, the terms *central data storage* or *central repository* refer to instances of either OpenLab ECM or OpenLab Server. As the interface and workflows for both systems are very similar, the specific product names are only used in places where there is a difference in associated concepts or procedures.

NOTE	This manual describes several features of OpenLab ECM and OpenLab Server. For further information on those products, see also the product-specific manuals.

Using ChemStation with Central Data Storage

ChemStation provides an interface to the central data storage, which enable you to store analytical data and reports in a secure location. From ChemStation, you can log in to the central data storage and store ChemStation files in the central data repository:

- Methods (*.m)
- Sequence templates (*.s)
- Data files (*.d)
- Report templates for Intelligent Reporting (*.rdl)
- Reports (*.pdf, *.xlsx, *.docx, or *.txt)
- Library files (*.uvl)
- Column databases (*.mdb)
- Easy Sequence templates (*.est)
- Classic report templates (*.frp)

The storage of ChemStation data can be either automatic (that is, at the end of a single run or sequence) or manual. A manual storage is possible only when you already have a version in the system. The data can be downloaded later to ChemStation for review or reprocessing at any time.

Furthermore, ChemStation in combination with central data storage offers features that enable users to comply with 21 CFR Part 11 and similar regulations for electronic records and electronic signatures:

- Mandatory login/connection to the central data storage system
- Configurable session locking
- Configurable ChemStation user roles and privileges
- Full data traceability through audit trails for methods and results
- Full data versioning

You can use *OpenLab ECM* in the following installation scenarios:

- Workstation
- Networked Workstation
- Distributed System

You can use *OpenLab Server* in the following installation scenarios:

- Networked Workstation
- Distributed System

The main workflows for the transfer of raw data and methods/sequence templates/report templates are listed below. These workflows indicate the system activities in relation to the work processes.

Naming Conventions

Make sure you only use the following characters for ChemStation items such as file or directory names, names of sequence templates, or names of ChemStation methods:

A-Z, a-z, 0-9, _ (underscore), - (hyphen)

Check your names for leading or trailing blanks. They are not allowed, but are easily overlooked.

NOTE   If you use tokens, file names or directory names are automatically created based on information such as instrument names, operator names, or sample names. Make sure that these names follow the same naming convention.

NOTE   Automatically created file names may include specific characters for Front and Back injector location. These characters may be localized. They are valid even if they are not part of the characters listed above.

The following reserved device names cannot be used as the name of a file. Also avoid these names followed by an extension (e.g. Nul.txt):

- CON, PRN, AUX, NUL
- COMx (where x is a number from 1 to 9)
- LPT1x (where x is a number from 1 to 9)

NOTE   English, Japanese, and Chinese operating systems are used to test naming conventions. Agilent cannot give a support statement for non-English operating systems and their special characters.

Overview of data-related workflows
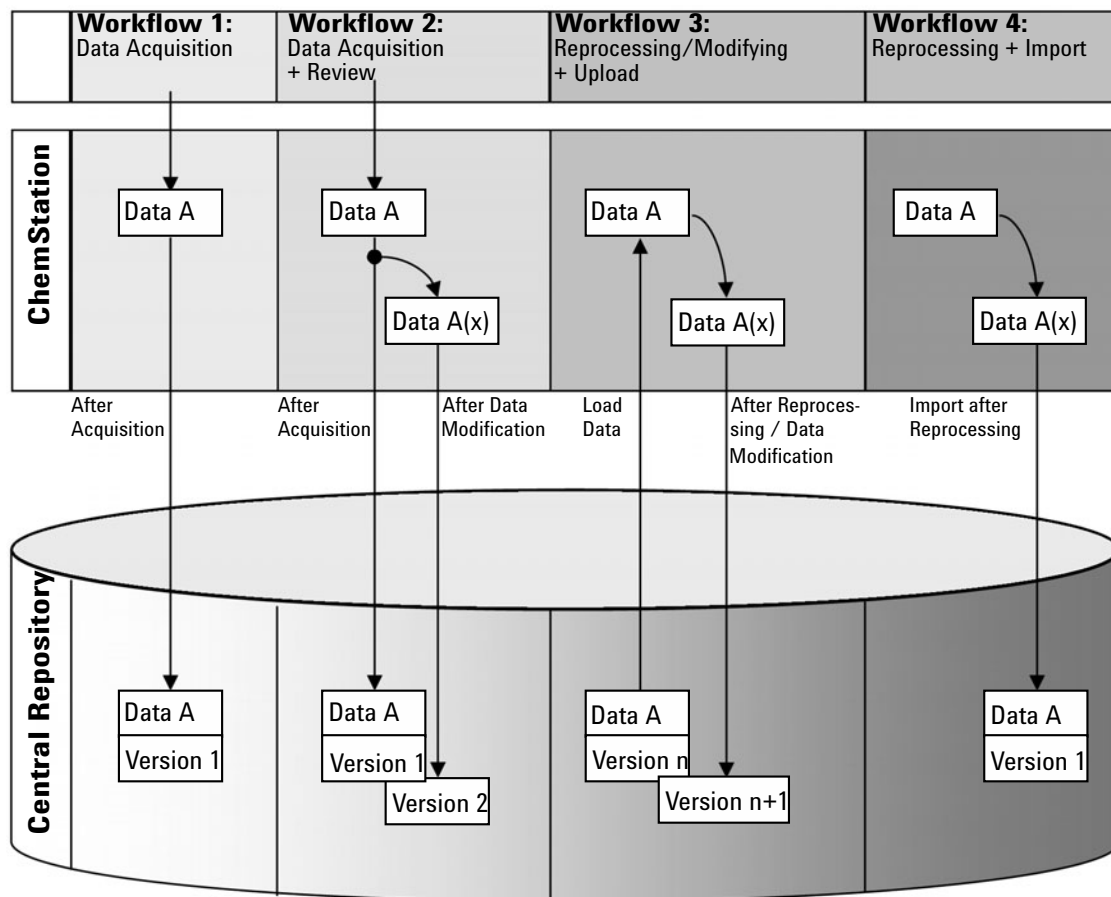
Figure 1   Overview of data-related workflows

Workflow 1: Raw data acquisition and automatic transfer to the central repository

1 Analytical raw data is acquired using ChemStation.

2 The raw data is automatically uploaded to the central repository using the configured path definitions immediately after the single run/sequence is finished.

3 The data is added to the defined storage location.

Workflow 2: Offline revision during acquisition

1   Analytical raw data is acquired using ChemStation.

2   While the acquisition is still running, part of the data is changed using an offline ChemStation.

3   The raw data is automatically uploaded to the central repository using the configured path definitions immediately after the single run/sequence is finished.

    The initial version of the data is added to the defined storage location.

4   After work in the offline ChemStation is finished, the changed data is also automatically uploaded to the central repository.

    The second version of the data is added to the central repository.

Workflow 3: Reprocessing data and automatic upload to the central repository

1   Existing analytical data is loaded from the central repository into ChemStation.

2   The data is reprocessed in ChemStation.

3   The data is automatically uploaded to the central repository. The storage location in the repository is defined by the original path definitions of the downloaded data.

4   A new version of the data is added to the central repository.

Workflow 4: Import after reprocessing

1   Existing analytical data is opened locally.

2   The data is reprocessed in ChemStation.

3   After reprocessing, the data is automatically uploaded to the central repository. The storage location in the repository is defined by the current preferences in ChemStation.

4   The initial version of the data is added to the central repository.

Overview of workflows for methods/sequence templates/report templates

	Workflow 1: Save new method	Workflow 2: Save changed method
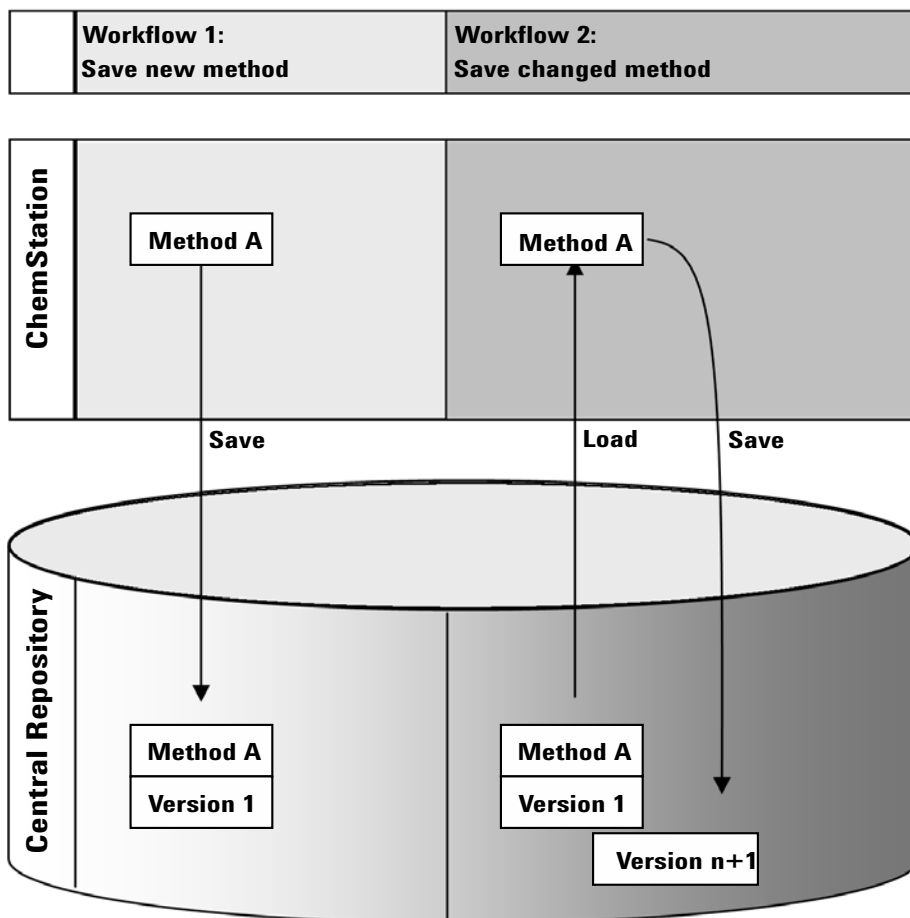
Figure 2   Overview of workflows for methods, sequence templates, or report templates

Workflow 1: Uploading a new method, sequence template or report template

1 A new method, sequence template, or report template is created.

2 The method, sequence template, or report template is uploaded to the central repository using the path selected by the user.

3 The version 1 of the method, sequence template, or report template is automatically created in the central repository.

Workflow 2: Saving a changed method, sequence template or report template

1 An existing method, sequence template, or report template is loaded from the central repository.

2 The method, sequence template, or report template is modified in ChemStation.

3 The changed method, sequence template, or report template is saved to the central repository.

4 A new version of the method, sequence template, or report template is automatically created in the central repository.

Storage Model in OpenLab ECM and OpenLab Server

File Management in OpenLab ECM

ECM provides a four-level data storage model with the structure of Location, Cabinet, Drawer, Folder. The Location, Cabinet, Drawer and Folder names comprise the path name (called either LCDF path or Remote Data Path) of the storage location. Data is stored at Folder level only.

The ECM program's content structure is similar to rooms filled with file cabinets. Each cabinet has multiple drawers, which contain hanging folders. Finally, paper files are stored in the folders. The LCDF structure can be created using the ECM Web Client. In addition, it is possible to create additional Locations, Cabinets, Drawers, and Folders using the ChemStation Remote Data Path. In ChemStation, it is also possible to set predefined tokens for the Drawers and Folders.

In the ECM tree view, locations are denoted by a house icon. Inside each Location, Cabinets are denoted by the file cabinet icon. Inside each Cabinet, Drawers are denoted by the drawer icon. Finally, inside each Drawer, Folders are denoted by the folder icon. The entire content structure appears in the Content book.
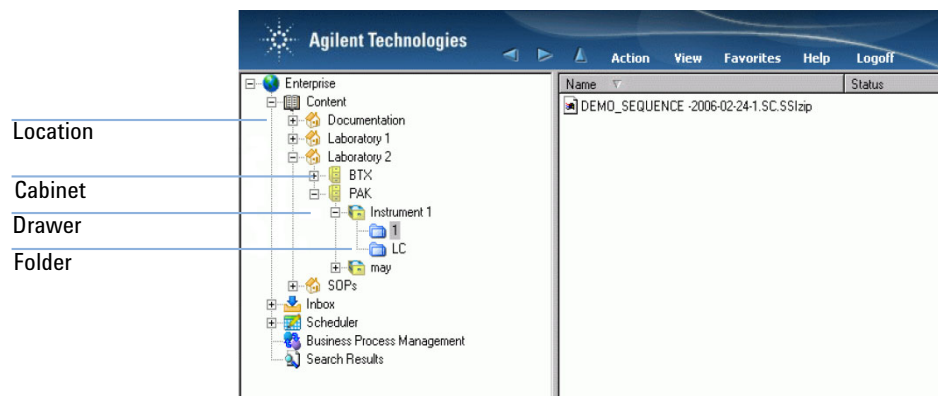
Figure 3   LCDF structure in OpenLab ECM

Uploaded objects can be stored in the lowest (i.e. Folder) level only. It is not possible to upload data to other levels of the hierarchy.

For convenience, you can use tokens for the Location, Cabinet, Drawer, and Folder. The system then automatically creates the corresponding path elements. The following tokens are available: instrument name, operator name, instrument number, or computer name.

File Management in OpenLab Server

For details on the file management in OpenLab Server, please refer to the OpenLab Server documentation.

The Content Management component of OpenLab Server provides a multi-level storage model. The number of levels is not limited, and you can store your data at any folder level.
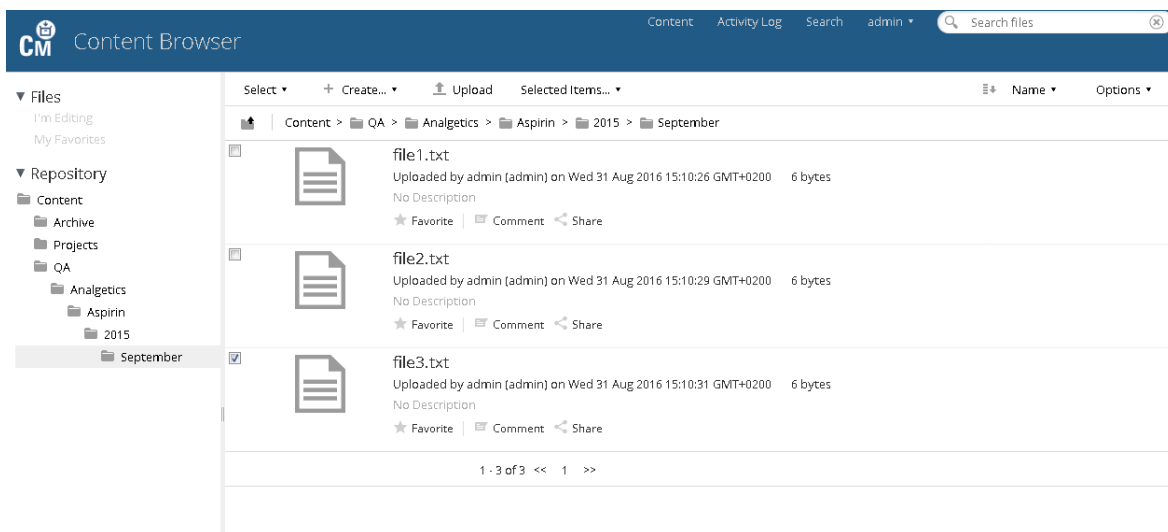
Figure 4   Folder structure in the CM Content Browser

For convenience, you can use tokens for all elements of the Remote Data Path. The system then automatically creates the corresponding path elements. The following tokens are available: instrument name, operator name, instrument number, or computer name.

21 CFR Part 11 Compliance

Effective August 20, 1997, the U.S. Food and Drug Administration (FDA) released and published a new rule to enable pharmaceutical companies to approve their results with electronic signatures and to transfer paper-based documentation into electronic records. This rule is known as 21 Code of Federal Regulations Part 11 (referred to as 21 CFR Part 11) and applies to all industry segments regulated by the FDA.

21 CFR Part 11 includes the US Federal guidelines for storing and protecting electronic records and applying electronic signatures. The intent of these guidelines is to ensure that electronic records subject to these guidelines are reliable, authentic, and maintained with high integrity.

ChemStation in combination with OpenLab ECM or OpenLab Server provides the necessary controls for managing system access, audit trail functions, versioning of ChemStation data, and electronic signature functions. These systems ensure secure record keeping and data archival.

2 Basic Concepts

This chapter describes how to log in to ChemStation, explains the user interface items and toolbars related to the central data storage, and describes the main preference settings.

Login and Lock Options

User Permissions

You start ChemStation from the OpenLab Control Panel. To prevent unauthorized access, ChemStation with central data storage requires authentication with a user name and password. If you use ECM, the ECM server is used as the authentication provider. With OpenLab Server, users can be created locally or imported from the Windows Domain. You log in with your user credentials of the corresponding system.

You need specific user privileges for working with ChemStation as well as for working with the central data storage system. You specify the user privileges as follows:

*   OpenLab ChemStation privileges are set in the OpenLab Control Panel.

*   ECM privileges are set directly in OpenLab ECM.

*   OpenLab Server/Content Management privileges are set in the OpenLab Control Panel.

For more information on roles and user privileges, see "Users, Roles, and Privileges Concept with OpenLab ECM" on page 90 and "Users, roles, and privileges concept with OpenLab Server" on page 93.

User Credentials

The **Login** dialog requires you to enter a set of valid authorization credentials in order to log in to OpenLab Control Panel.

You need to enter the following login details:

*   **Login:** the user name defined in the OpenLab Control Panel.

    With ECM, this is the ECM user, which can be a Windows domain user or an ECM built-in user. With OpenLab Server/Content Management, this is the OpenLab Control Panel user, which can be a Windows domain user or an internally created user.

- **Password**: the password provided by your administrator, which can be changed on request (for 'built-in' users), or the password of your Windows domain account, if you are logging in using your Windows domain user name.
- **Domain**: the domain administrating the users

ChemStation Operator Name

ChemStation stores the operator name in the sample info (when running single samples) or in the sequence parameters (when running a sequence). This ChemStation operator name is your full user name as configured in the authentication system (e.g. OpenLab Control Panel with internal authentication, ECM with built-in users, or Windows Domain). The operator name cannot be overwritten.

Session lock

If you leave the ChemStation computer for a period of time, you can lock ChemStation.This is a safety feature to ensure that there is no unauthorized access to ChemStation. To unlock the session, a user must first provide a valid login before continuing to work with ChemStation.

In ChemStation, there are the following options to activate the session lock:

- *Privately* (**User >Lock Session >privately**): Only the user who activated the session lock, or a user with the **Break Session Lock** privilege, can log in.
- *Non-privately* (**User >Lock Session >non privately**): Any valid user can log in. This is useful, for example, if there is a shift change, and the leaving personnel locks the ChemStation until the personnel of the new shift starts working.
- *Toolbar lock button*: The toolbar lock button can be configured to lock the ChemStation session privately or non-privately.
- *Time-based*: ChemStation will automatically lock after a given period of time when there is no user interaction (**Inactivity Timeout** setting in the Security Policy area of OpenLab Control Panel).
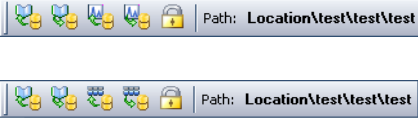
   The time-based session lock can be configured to lock the ChemStation session either privately or non-privately (see "ChemStation Administration Tool" on page 38).

User Interface in ChemStation Related to the Central Data Repository

Overview of the interface elements

When connected to a central data storage system, additional menus and interface elements are available in ChemStation. Depending on the external system, they are automatically labeled either with **ECM** or with **CM**.

Menu	Element type	Description
Method	**Enable Audit Trail** Command	See "Method Audit Trail" on page 73. The Method Audit Trail can also be enabled on a system without central data storage.
Sequence >Sequence Parameters	**Sequence Parameters** Tab	See "Remote Data Path as Sequence Parameter" on page 25
Report	**Report History** Command	See "Report History" on page 76
View >Preferences	Tabs In the **Preferences** dialog: • **Transfer Settings** • **Audit Trail**	See "Preferences" on page 28 and "Audit Trails and Logbooks" on page 73. The Method Audit Trail and Results Audit Trail can also be enabled on a system without central data storage. Therefore the **Audit Trail** tab is visible in the Preferences also in a system without central data storage.
ECM or **CM**	**ECM** or **CM** Menu	See "The ECM or CM Menu" on page 22
User	**User** Menu	See "The User menu" on page 24. If authentication has been set up, the **User** menu is also visible on a system without central data storage.

Menu	Element type	Description
Toolbar (depending on the current view)	• Shortcuts to several commands of the **ECM** or **CM** and **User** menus • **LCDF** info	• Path info in the **Data Analysis** view: shows the remote path of a file that has been stored to the central repository. • Path info in the **Method and Run Control** view: shows the remote path for automatic upload after acquisition. • With ECM, the path is shown with backslashes; with Content Management, it uses forward slashes (for example, Location/test/test/test).
Several details related to the central repository in the **System Diagram** in **Method and Run Control** view (classic ChemStation only).	Details view	The following details are available: • **Path** • **Operator** • **Automatic transfer after acquisition** • **Automatic transfer after reprocessing** • **Automatic transfer after any data modification** • **Automatic import after reprocessing**

The ECM or CM Menu

All commands related to the central repository are available in a separate menu. Depending on the central data storage system, the menu is named either **ECM** or **CM**. The menu and its commands depend on the view that is currently active. See the following table for details.

NOTE   There is no **ECM** or **CM** menu in the **Verification (OQ/PV)** or **Diagnosis** view.

Command	Description	Available in ChemStation views
Update Methods ... **Update Sequences Templates ...**	Update all methods/sequence templates that are stored in the local file system with the current version from the central repository (if it exists there). Local changes are overwritten.	• **Method and Run Control**
Update Report Templates ...	Update all report templates that are stored in the local file system with the current version from the central repository (if it exists there). Local changes are overwritten.	• **Report Layout** (Intelligent Reporting)

Command	Description	Available in ChemStation views
Cleanup Data	The **Cleanup Data** command deletes data or result sets from the local file system that exist in the central repository as well. You can delete all data or selected data. Make sure you uploaded the latest version to the central repository before you confirm this command. See "Cleanup Data on Shutdown" on page 33.	• **Data Analysis**
Manage Queue	With the **Manage Queue** command you can continue any interrupted data upload to the central repository. See "Manage Queue on Connect" on page 33.	• **Method and Run Control** • **Data Analysis**
Preferences	See "Preferences" on page 28 for more details on the **Preferences** dialog.	• **Method and Run Control** • **Data Analysis** • **Report Layout** (Intelligent Reporting)
Method-related commands: **Load Method ...** **Save Method**	See "Workflows for Methods and Templates" on page 60	• **Method and Run Control** • **Data Analysis**
Data-related commands: **Load Data ...** **Save Data** **Save Data As ...**	See "Data-related workflows" on page 50	• **Data Analysis**
Commands related to the sequence template: **Load Sequence Template ...** **Save Sequence Template**	See "Workflows for Methods and Templates" on page 60	• **Method and Run Control**
Commands related to report templates: **Load Report Template** **Save Report Template**	See "Workflows for Methods and Templates" on page 60	• **Report Layout** (Intelligent Reporting)

Command	Description	Available in ChemStation views
Commands related to reports: ![icon] Load Report Template ![icon] Save as PDF ![icon] Save as XLSX ![icon] Save as DOCX ![icon] Save as TXT	• You can load a specific report template from the central repository. • You save the report generated with this template as a PDF, XLSX, DOCX, or TXT file to the central repository. TXT files do not contain any graphical information.	• **Review** (only available with Intelligent Reporting)
Download Files ...	Download library files (*.uvl), column databases (*.mdb), Easy Sequence templates (*.est), and classic report templates (*.frp) from the central repository.	• **Method and Run Control** • **Data Analysis**
Upload Files ...	Upload library files (*.uvl), column databases (*.mdb), Easy Sequence templates (*.est), and classic report templates (*.frp) to the central repository.	• **Method and Run Control** • **Data Analysis**

The User menu

Command	Description	Available in ChemStation views
Change User ...	Log in as a different user (only affects the ChemStation login, not the OpenLab Control Panel login).	• **Method and Run Control** • **Data Analysis** • **Review** • **Report Layout**
Lock Session	• **privately** • **non privately** See "Session lock" on page 20.	• **Method and Run Control** • **Data Analysis** • **Review** • **Report Layout**

Remote Data Path as Sequence Parameter

Instead of specifying the remote data path in the **Preferences** for all acquisition sequences to be run (see "Remote Data Path" on page 29), the remote data path can also be set directly in the sequence template. This allows you to set up different remote paths for each sequence without having to modify the Preferences. The **Path** for a sequence template is set up in the **Sequence Parameters** tab.
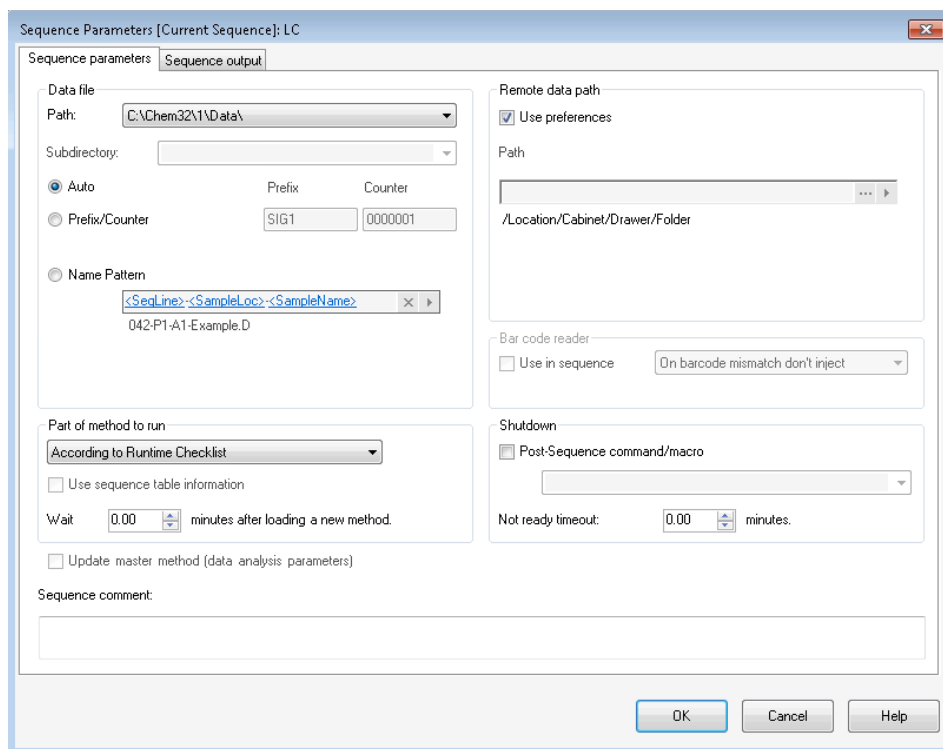
Figure 5   Sequence Parameters tab of the Sequence Parameters dialog

Use Preferences: When this check box is selected, the remote data path as specified in the **Preferences** will be used. Any path specified in the **Sequence Parameters** will be ignored for this sequence. When this check box is cleared, the remote data path will be used as specified when the sequence template is used for data acquisition.

Path: To specify the remote data path, you can select a folder path available in the central data storage system. Click the button with the three dots [...] to select the required path. Alternatively, you can click the arrow [▸] to select one of the predefined tokens for automatic path creation. With these tokens, the system automatically creates the items if they do not already exist in the central data storage system.

NOTE	In ECM, there are separate privileges to create content and create folders. If you use tokens, make sure you have the required privileges in ECM to create folders! Alternatively, another user who has the required privileges can create the necessary folders in advance.

Compressed ChemStation File Formats

When ChemStation data is uploaded to the central repository, the data is automatically packaged into an SSIzip file. Depending on the type of data, different packaging formats are used.

ChemStation data	Packaging format	Icon in ChemStation
Single Runs (containing *.d file, *.rdl files, and DA.M)	*.D.SSIZIP	
Result set The result set contains recursively the whole sequence data stored in the sequence subdirectory: • all *.d files along with DA.M • all methods *.m used during acquisition • batch file *.b • sequence logbook file *.log • all *.rdl files used for sequence summary reports and single injection reports	*.SC.SSIZIP	
Methods	*.M.SSIZIP	
Sequence templates	*.S	

The packaging of ChemStation data is part of ChemStation and cannot be changed manually.

The packaging is automatically carried out when the data is uploaded to the central repository. When the SSIZIP files are downloaded from the central repository to ChemStation, they are automatically unpacked into the corresponding directory in the ChemStation Explorer.

Preferences

The **Preferences** dialog contains two tabs that are relevant to the central data storage system: the **Transfer Settings** tab and the **Audit Trail** tab.

On the **Transfer Settings** tab, you must specify the following preferences in order to automatically store ChemStation data to a central repository:

- Path
- Automatic Data Transfer Settings
- Transfer Management Settings
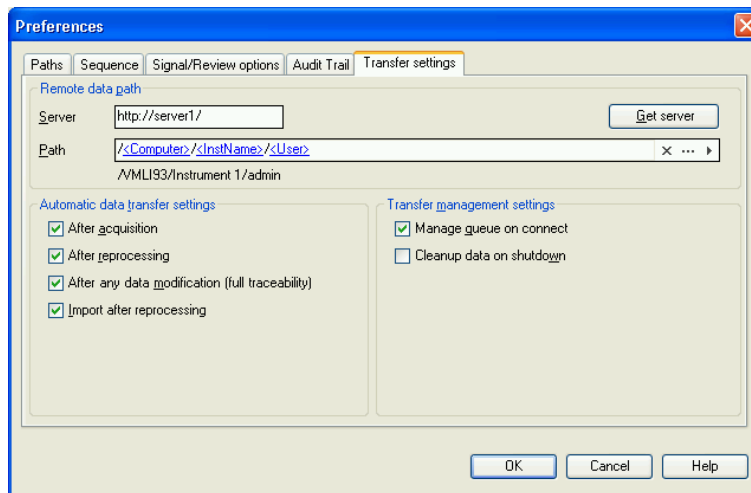
Figure 6   Transfer Settings tab in the Preferences dialog

Each of these items can be specified independently for each instrument. Offline and online sessions are automatically synchronized.

On the **Audit Trail** tab, you can enable the Method Audit Trail and Results Audit Trail. The Sequence Audit Trail is automatically enabled together with the Results Audit Trail. For details on audit trails see "Audit Trails and Logbooks" on page 73.
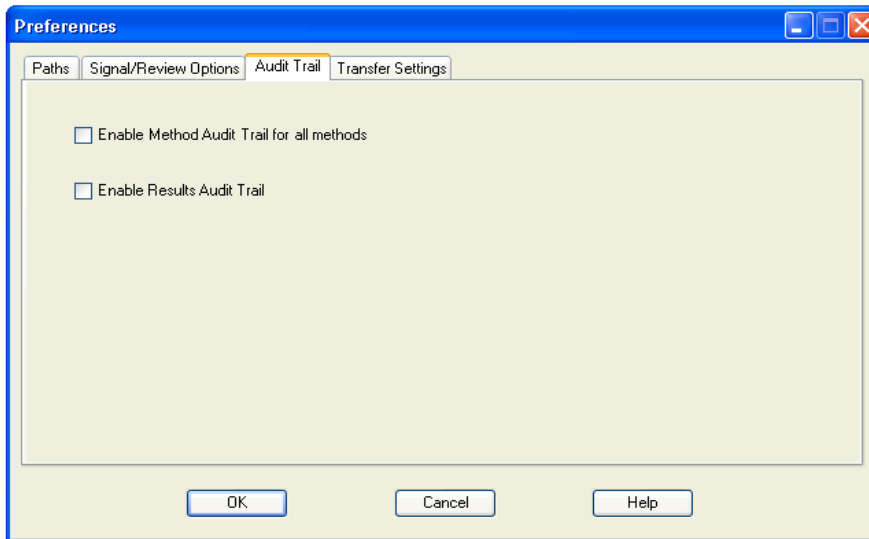
Figure 7   Audit Trail tab in the Preferences dialog

Remote Data Path

The remote data path needs to be specified in order to save the data to the correct location in central repository.

In the **Preferences** dialog, the **Transfer Settings** tab (see Figure 6 on page 28) allows you to define the **Path** setting. This path reflects the LCDF structure in ECM, shown with backslashes, or the folder path in Content Management, shown with forward slashes.

ChemStation Rev. B and OpenLab ChemStation Data in one ECM

In ECM, you may have stored data from different ChemStation revisions, for example, from rev. B and OpenLab CDS ChemStation Edition (rev. C). If you work with ChemStation rev. C, you can load and process data from ChemStation rev. B. However, if you work with ChemStation rev. B, you can only process data from this revision (or older), you cannot process data from rev. C.

CAUTION   **Wrong results or incompatible data**

If you reprocess ChemStation rev. C data in ChemStation rev. B, you may obtain wrong or incomplete results.

If you reprocess ChemStation rev. B data in ChemStation rev. C, it may no longer be possible to reprocess these data in ChemStation rev. B.

- ✓ **Clearly separate the files from ChemStation rev. B and ChemStation rev. C in ECM.**

- ✓ **With OpenLab ECM Enterprise, we recommend using different ECM Accounts for ChemStation rev. B data and ChemStation rev. C data.**

- ✓ **With OpenLab ECM Workgroup, use clearly separated LCDF locations.**

Server/Account

Under **Server** (see Figure 6 on page 28), you specify the server on which the central data storage system is installed. For ECM, you must also specify the ECM Account.

ChemStation obtains the server and account information automatically from OpenLab Control Panel. If the fields are empty or do not match the current configuration, you can click **Get Server** to reset the fields. ChemStation then keeps the information for future sessions.

NOTE   One OpenLab Shared Services Server is required per ECM Account.

NOTE   Do not manually change the server name or ECM Account name in ChemStation. If you do, and the information does not match the configuration used in OpenLab Control Panel, data upload will fail due to a host mismatch.

Path

To specify the storage location in the central repository, you can either browse to a an existing storage location in the central repository using the button with the three dots [⋯], or click the arrow [▸] to select predefined tokens for automatic path creation. With these tokens, the system automatically creates the required items if they do not already exist in the central repository. Tokens are available for the instrument name, the user name, the instrument number, or the computer name.

Alternatively, the path can be specified as **Sequence Parameter** (see "Remote Data Path as Sequence Parameter" on page 25).

With ECM, uploaded files can be stored only at the Folder level. With Content Management, uploaded files can be stored at any level of the folder hierarchy.

NOTE   If no path is specified, a warning message will be shown at ChemStation startup.

NOTE   In ECM, there are separate privileges to create content and create folders. If you use tokens, make sure you have the required privileges in ECM to create folders! Alternatively, another user who has the required privileges can create the necessary folders in advance.

Automatic Data Transfer Settings

In the **Preferences** dialog (**View >Preferences**), the **Transfer Settings** tab allows you to specify the automatic settings for the transfer of raw data. The transfer settings, as well as the Remote Data Path, are used to automatically upload data to the central data storage.

NOTE   If the connection to the central data storage is lost for any reason, the data cannot be automatically uploaded as specified in the transfer settings. The data is then queued in the Queue Management (see "Queue Management" on page 35).

NOTE   If you perform data acquisition from the **Diagnosis** view or **OQ/PV** view, the transfer settings are ignored. The analytical raw data is written to the local ChemStation data file system as predefined in the diagnosis or verification methods.

After Acquisition

If you select this check box the data is automatically uploaded to the central repository after an acquisition. The raw data files are written to the local ChemStation file system while the sequence is still running. When the complete sequence is finished, the raw data files are packed in an SSIZip file which is then uploaded to the central repository.

For more information, please refer to "Workflow 1: Acquisition and automatic upload" on page 50.

After Any Data Modification

If you select this check box, the result set is automatically uploaded to the central repository after you changed the data analysis parameters for a sample and generated a report. The data is uploaded even if you do not reprocess the sequence. Note that data is considered modified if one of the following applies:

- You change the data analysis parameters or the method. Note that you can also change the method via the navigation table, for example, by adding or deleting an instrument curve. Undoing the change does not erase the "modified" status of the method.

- You switch to another result set, and a dialog asks you to save a changed method. If you do not save the changed method, the result set is marked as potentially modified. When you load the result set again and print a report preview, the result set is marked as modified.

- If you shut down the software and you changed the method, a dialog will ask you to save the changed method. If you do not save the method, the result set is considered modified anyway (and may be uploaded depending on your data transfer settings).

For more information, please refer to "Workflow 2: Offline review during acquisition" on page 52.

After Reprocessing

If you select this check box, the result set is automatically uploaded to the central repository each time after you reprocessed the sequence.

For more information, please refer to "Workflow 3: Reprocessing data and automatic upload" on page 55.

Import after Reprocessing

If you select this check box, a sequence that is only stored locally is automatically uploaded to the central repository after reprocessing. This setting is useful, for example, if you reprocess data from an older version of ChemStation.

For more information, please refer to "Workflow 4: Import after reprocessing" on page 58.

Transfer Management Settings

Manage Queue on Connect

If the connection to the central data storage is lost for any reason, a running data upload might be interrupted. In this case, the remaining data is written to an internal queue.

If you select the check box **Manage Queue on Connect**,the queue is shown allowing the user with sufficient privileges to resume the data upload.

Alternatively, you can open the **Queue Management** dialog (see Figure 8 on page 35) at any time with the **ECM >Manage Queue** or **CM >Manage Queue** command in the **Data Analysis** view. **The Queue Management** dialog box allows you to manage the export of residual ChemStation data to central data storage after, for example, a network failure. You can process the queue, save selected items to the local computer, or delete items from the queue. If you delete an item from the queue, it will not be transferred to central data storage. If the system activity log has been activated, an entry will be made in the system activity log.

Cleanup Data on Shutdown

If you select this check box, upon shutdown ChemStation checks the local file system for files that will be or have already been stored in the central repository. It deletes all local data and sequence files that are stored in the central repository or are queued for an upload. Methods and sequence templates remain on the local file system.

> **CAUTION**
>
> **Inadequate check box selection**
>
> **Loss of data**
>
> ✓ **If you select the Cleanup Data on Shutdown check box, you should also select the Automatic Data Transfer Settings After Acquisition, After Reprocessing, and After Any Data Modification. Otherwise, if the users forget to upload the data to the central data storage before closing ChemStation, data might be lost.**

CAUTION   Unintentional deletion of data

Loss of data

✓ **If you select the Cleanup Data on Shutdown check box and shut down the ChemStation, the item in the Queue may be the only remaining copy of the data. If you want to delete data from the queue while using the Cleanup Data on Shutdown setting, consider saving the item locally first.**

NOTE   Consider selecting the **Cleanup Data on Shutdown** check box when the system shall be compliant to 21 CFR Part 11.

Alternatively, you can open the **Data Cleanup** dialog at any time with the **Cleanup Data** command in the **ECM** or **CM** menu. This dialog box lists all data sets that are also kept in the central data storage system apart from the currently loaded data. The following columns are available:

- **Directory**: Location of the local file

- **ECM Information** or **CM Information**: Server of the central data storage system and path for the file in the central repository. For ECM, also the ECM Account is shown.

- **Last Modified**: Date/Time when the file in the central repository was last changed

- **Locally Modified**: Information whether the local copy has been modified

- **Local Version**: ECM or CM version that was downloaded to the local directory

You can now manually select the data sets to be deleted from the local disk.

Alternatively, via a drop down list you can deselect all data sets, select all data sets, select only single runs, select only result sets, select items older than one day, or items older than a week.

After pressing **OK**, the local copies of the selected data sets are deleted.

Both automatic cleanup on shutdown and manual cleanup are only possible if the following conditions are fulfilled:

- the ChemStation user is logged on to the central data storage system

- no other instance of the ChemStation instrument is open

- the queue in the Queue Management is empty

- the navigation table is empty (no data loaded)

If one of these conditions is not fulfilled, automatic cleanup will not be performed and it is not possible to open the **Data Cleanup** dialog.

Queue Management

The **Queue Management** dialog is opened via **ECM >Manage Queue ...** or
CM >Manage Queue ... respectively. If you selected the check box **Manage Queue
on Connect**, and there are interrupted transfers, the dialog is also opened when
you start ChemStation.

With this dialog, you can manage the data transfers from ChemStation to the
central data storage that were interrupted or could not be started. Each failed
transfer job is listed in a separate line[1].
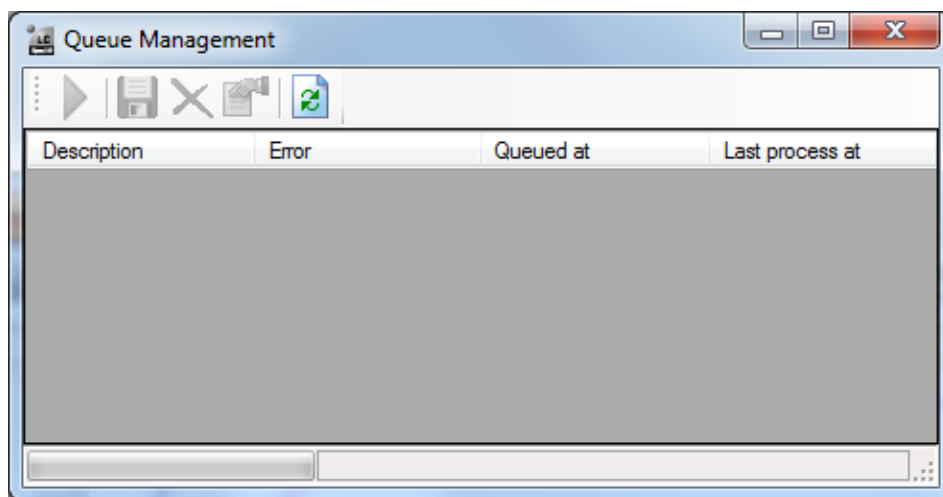
Figure 8   Queue Management

The following information is provided for each line:

- **Description**: Information on the version of the data that will be transferred.
  Two values are possible:

  - **Import**: Generates the first version. No older version of the data exists in
    the central data storage system at this time. The data has been newly
    created and will be uploaded as Version 1.

  - **Commit**: There is already at least one version of the data in the central data
    storage system. The version number of the uploaded data will be
    increased by one. Reprocessing a sequence for example will create a
    commit entry (version n + 1).

[1] When the connection to the database is lost, the status line of the ChemStation will show a
   "lightning bolt" icon. A number is indicating items in the queue waiting to be uploaded to the
   backend.

- **Error**: Error that disrupted the data transfer. For details on the possible errors, see the *Troubleshooting* section in this document.
- **Queued at**: Date when the unsuccessful transfer was queued.
- **Last process at**: Date when the transfer was last attempted.

The toolbar offers you the following commands to manage the queue:

Table 2   Queue management toolbar

Icon	Tooltip	Description
▶	Process queue	Continue processing the transfer jobs. As long as there is no error, all pending transfer jobs will be processed in the order as they are shown in the list. This function is only active if you select the first line in the list.
💾	Save selected item locally	Save the data of the corresponding item to the file system.
✕	Delete selected item	Delete the data of the corresponding item from the queue. *Note*: If you use the **Cleanup Data on Shutdown** option in the Transfer Management Settings, this may be the only remaining copy of the data. Consider saving the item locally first.
🖼	Properties	Display the **Queue Management** dialog box, which shows details of the items in the queue in either summary or detailed form.
🔄	Refresh view	Update the display of the items in the list.

When items are selected from the queue or saved to the local disk, an audit trail entry will be added to the Audit Trail of the central data storage system.

NOTE   When items are deleted from the queue or information on a failed transfer is saved to the local disk, the items have not yet been uploaded to the central data storage system.

Queue Management Details Dialog Box

The **Queue Management Details** dialog box is displayed when you click the tool in the toolbar of the **Queue Management** dialog box. It shows the command-specific details of the commands in the **Queue Management** dialog box. The **Queue Management Details** tabs offer two views of the command details:

- Summary tab
- Details tab

In either tab, the tools in the toolbar allow you to navigate through the command details:

	Displays the details of the first command in the list.
	Displays the details of previous command in the list.
	Displays the details of next command in the list.
	Displays the details of last command in the list.

Summary tab

The **Summary** tab gives the following summary information about the selected item:

Command Description	The description of the item.
Created	The date and time when the item was added to the queue.
Changed	The date and time when the item was last processed.
Last Error	A description of the error that caused the item to be added to the queue.

Details tab

The **Details** tab gives detailed information about the selected item. You cannot edit the information in this list. The toolbar provides the following tools:

	Sorts the properties by category.
	Sorts the properties alphanumerically.

ChemStation Administration Tool

The ChemStation Administration Tool offers a number of functions related to the ChemStation configuration. One of these functions is to configure the data handling and audit trail settings per ChemStation instance (that is, per instrument and per online or offline instance). Alternatively, this function allows using the same settings for all instances running on a workstation, networked workstation, or Agilent Instrument Controller (AIC). Access to the ChemStation Administration Tool is therefore strictly limited:

- The ChemStation Administration Tool can only be opened directly on the ChemStation PC. In Distributed System installations, you must open the tool directly on the relevant AIC, not on a client.

- The ChemStation Administration Tool can only be started by users who are member of the local user group **CSAdministrators** (see "Enabling users to start the ChemStation Administration Tool" on page 39).

To start the ChemStation Administration Tool:

1 From the Start menu in the Task Bar, select
Start >Agilent Technologies >ChemStation Administration Tool.
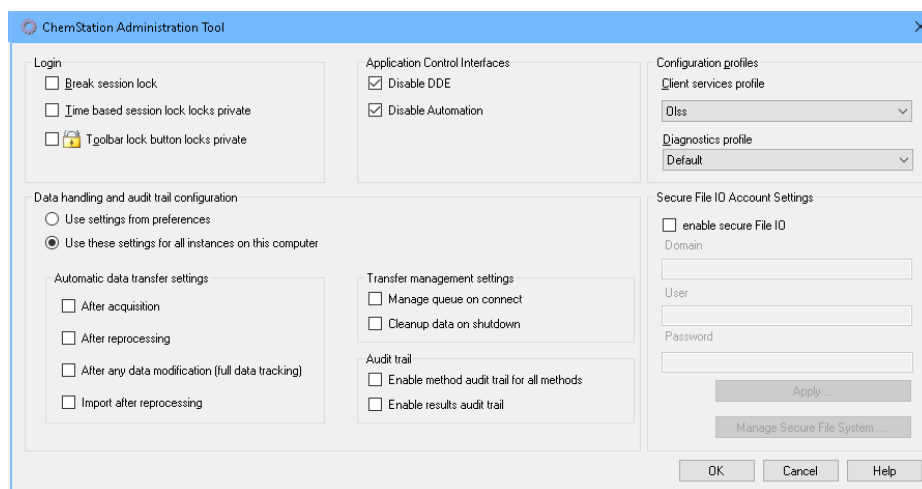
Figure 9   ChemStation Administration Tool

Enabling users to start the ChemStation Administration Tool

During the installation of OpenLab ChemStation, the local user group **CSAdministrators** is automatically created. Only members of this group are allowed to run the ChemStation Administration Tool. The user who installs ChemStation is automatically added to the **CSAdministrators** group.

To add a Windows user to the **CSAdministrators** group:

1   Go to **Start >Control Panel >Administrative Tools**[1].

2   Select **Computer Management**
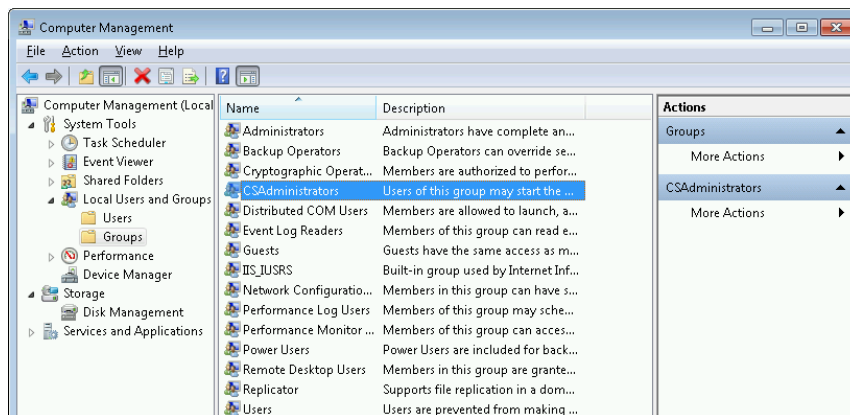
Figure 10   Computer Management window

---

[1]   View the items by icon to see a list of all items

3 Under **Groups**, right-click the group **CSAdministrator** and select **Add to Group...** from the context menu.

The **Properties** dialog shows the users who are currently members of the group.
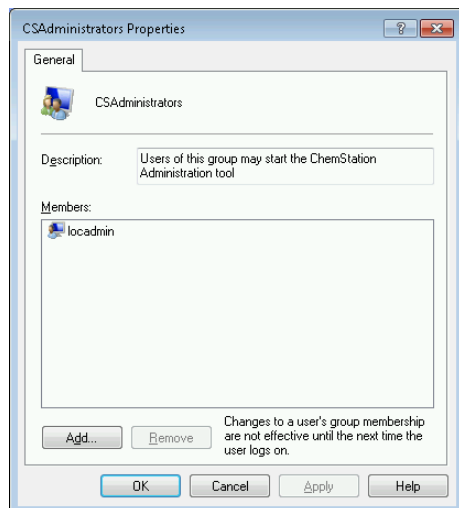
4 Use the **Add** button to add the required users.

After confirming with **OK**, the **Properties** dialog also contains the newly added users.

Session Lock Settings

In the ChemStation Administration Tool, you can set the following options for creating and breaking session locks:
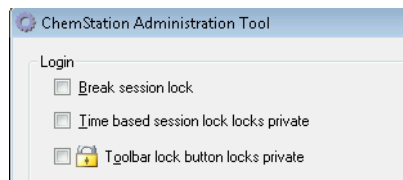
Figure 11   ChemStation Administration Tool

Break Session Lock

If a ChemStation is currently locked and the authentication provider is unavailable, selecting this check box is the only way to regain access to the current ChemStation session.

Select the **Break session lock** check box during a fail over scenario. A locked ChemStation can then be accessed by any user just by clicking **OK** in the **Login** dialog. Login credentials are ignored. Users do *not* need the **Break session lock** privilege.

CAUTION	**Unlimited access**

Be aware that, as a consequence, the user who regained access to ChemStation now has unlimited access to all ChemStation functions.

✓ **Do only use this option in emergency cases (for example, you use a Networked System, your Shared Services server is down, and authentication is no longer possible).**

✓ **Note down when and by whom this option got activated.**

✓ **Deactivate it immediately after use to avoid security issues.**

For details in fail over scenarios, see "Fail Over Procedures" on page 113.

Time Based or Private Locks

- **Time based session lock locks private**: If ChemStation has been locked by a session time out, only the current user or a user with the required privileges can unlock this session.
- **Toolbar lock button locks private**: If ChemStation has been locked using the Lock button on the ChemStation toolbar, only the current user or a user with the required privileges can unlock this session.

Data Handling and Audit Trail Configuration

The ChemStation Administration Tool offers to conveniently configure all ChemStation instances on a client at the same time with the same settings. By default, the option **Use these settings for all instances on this computer** is already selected.

To force the settings for all ChemStation instances

1 Select the option **Use these settings for all instances on this computer**.

2 Select the required check boxes. The settings are the same as in the **Preferences** dialog (see "Preferences" on page 28).

3 Click **OK**.

Configuration Profiles

By providing specific client services profiles, you activate specific functions and behaviors in ChemStation.

- **Olss**

  ChemStation communicates with the Shared Services; it sends status information to the Shared Services, and uses the settings defined in the Shared Services (for example, user authentication, roles and privileges, configuration settings, audit trail settings). Use this profile for ChemStation instances that are connected to the Shared Services, but have no connection to a central data storage system. The upload and download to the content management (CM) system is disabled.

- **OlssEcm**

  In addition to communication with Shared Services, ChemStation allows transferring data files to and from OpenLab ECM 3.x. Use this profile for ChemStation instances that are connected to OpenLab Shared Services together with ECM 3.x. Do not use in combination with OpenLab ECM XT.

  In a fail over scenario, where the connection between the workstation and OpenLab ECM is interrupted, you can set the authentication provider in OpenLab Shared Service to **None**. This allows you to log on to ChemStation in the absence of OpenLab ECM.

  In this case, using the **OlssEcm** profile allows ChemStation to send the data files to the queue. Once the authentication provider in the Shared Services is set back to ECM, the upload can be resumed.

- **OlssDataStore**

  In addition to communication with Shared Services, ChemStation allows transferring data files to and from OpenLab Server or OpenLab ECM XT. Use this profile for ChemStation instances that are connected to OpenLab Server or ECM XT.

Folder Protection with Secure File I/O

ChemStation metadata such as validated master methods or sequences templates must be stored in secured locations in your content management system. For usage with your instruments these methods or sequence templates are also stored in various local folders. By default, the content of these folders is not protected against modification or deletion from local file browsers or from file dialogs within ChemStation.

To ensure data integrity, enable the Secure File I/O function for ChemStation. All relevant local paths will then be protected. The relevant paths are set by default, but can also be configured. The content of protected paths can no longer be modified by Windows file operations because access is denied for members of the Windows user group **Interactive**[1]. The protected folders can only be used inside ChemStation. If user authentication is enabled, only users with sufficient privileges can delete the locally stored data for housekeeping purposes. If those methods or sequences have been actively used with your instrument, copies are also stored along with results and their associated audit trails.

Prepare Secure File I/O in Windows

1 Ensure that all relevant ChemStation folders are on an NTFS file system.

2 Do not use ChemStation folders on removable storage devices (for example, external disks or USB media).

3 Create a standard user account (local or domain) with the same or fewer privileges than a normal ChemStation user. Do not grant administration or power user privileges. Make sure that this user is *not* a member of any group, especially not the **Interactive** group.

This account will be used by the ChemStation for internal file operations. As the user is not supposed to log on interactively, do not use the option **Change password at next logon**.

NOTE   Consider using a password that never expires. If this is not possible due to your security policy, plan a downtime for ChemStation while updating the password.

As long as the password for this user account is expired, do not use the ChemStation. ChemStation will not work properly until you have updated the password in the ChemStation Administration Tool.

---

[1] In Windows, all users who log on interactively are automatically assigned to the *Interactive* group. The membership persists for the time the users remain logged in.

Enable Secure File I/O in ChemStation

1 Click **Start >All Programs >Agilent Technologies >ChemStation Administration Tool** to open the ChemStation Administration Tool.

2 In the ChemStation Administration Tool, select the **enable secure file IO** check box.

3 Provide the credentials of the special user account that you have prepared.

4 Click **Apply.**

5 A dialog lists all directories that are going to be protected. Click **OK** to confirm.

For all paths that are protected, a ProtectionInfo.xml file is stored in the root folder. This protection information file contains the time stamp and the Windows user who enabled protection - that is either the user who enabled the path from the ChemStation Administration tool, or the user who configured a new instrument.

The Protection Information file provides proof for a given folder when the last activation was performed. Any period of time before that date is unspecified. The file can be used to demonstrate the uninterrupted protection status of a folder since it contains the date, time and user who last enabled protection.

Enabling or disabling secure file I/O is not logged to the OpenLab Control Panel Activity Log or the Windows Event Logs (application or Security).

When the folder is unprotected, the ProtectionInfo.xml file is deleted. Note, deleting this file will not unprotect the folder.

6 For administrative tasks, you can temporarily disable the protection of specific folders:

   a Shut down all ChemStation sessions.

   b In the ChemStation Administration Tool, click **Manage Secure File System**.

   c In the list of directories, find the relevant path and click **Unprotect**.

      The protection information file is deleted to document the interruption of the protection state.

   d After finishing your tasks, click **Protect All** to restore protection for all relevant folders.

      New protection information files are created.

   e Start ChemStation again.

      ChemStation will only start if all folders are protected.

Check privileges for Chemstation users

In the OpenLab Control Panel, specific privileges can be configured. Several privileges are relevant for Secure File I/O. They handle occasions when data, methods, or sequences need to be loaded from unprotected locations (which are outside of the secure folders). These privileges are enabled in the default ChemStation Roles to maintain the current workflows.

To ensure data integrity, it is recommended to uncheck these privileges when Secure File I/O is enabled.

The relevant privileges are:

- **ChemStation: Data >Load data from not configured path**

  Required for loading data from unprotected paths, or adding data paths that are not empty to the ChemStation.

- **ChemStation: Method >Load method from not configured path**

  Required for loading a method from an unprotected path, saving a method to an unprotected path, or adding method paths to the ChemStation (Preferences dialog).

- **ChemStation: Sequence >Load sequence template from not configured path**

  Required for loading sequence templates from unprotected paths, saving sequence templates to unprotected paths, or adding paths that are to the ChemStation (Preferences dialog).

Important Notes for Working with Secure File I/O

When using Secure File I/O to protect your ChemStation folders:

- Do not share protected folders. Sharing a folder will break the protection.

  If your data resides within the public documents folder (default setting), do not turn on public sharing.

- Do not log in interactively with the user account provided in the ChemStation Administration Tool.

  If this user logs in interactively, you will not be able to save any changed data in ChemStation until the user logs out again.

- If the password for this user account has expired, do not use the ChemStation until you updated the password in the ChemStation Administration Tool. ChemStation will not work properly as long as the password is outdated.

Limitations

The following features are not supported when Secure File I/O is enabled:

- Import/Export eMethods
- Migration of non-container data to new result sets
- Download files (method, sequence, data) using the content management web interface, and storing them to a protected folder

  These files must be downloaded from within the ChemStation application.
- GC Backflush Wizard
- G2887BA SIMDIS
- M8350AA MatchCompare
- M8370AA OpenLab Data Analysis Add-on
- Easy SamplePrep
- G7818A Cirrus GPC Software
- A2Prep software
- Method Scouting Wizard
- G4218A Evaporative Light Scattering Detector
- 2D-LC Add-on

Since Secure File I/O protects the folders/directories containing methods, sequences, data for OpenLab ChemStation, this prevents access from outside applications as Explorer or Notepad from making edits to ChemStation produced data, methods, etc. This also includes some of Agilent's Add-on programs such as A2Prep as these programs need to access ChemStation folders/directories. Any application that needs to access or write to a protected ChemStation folder/directory will not be allowed and therefore cannot be used when Secure File I/O is enabled.

3 Working with ChemStation and Central Data Storage

This chapter describes the basic workflows for ChemStation with a central data storage system.

Transferring Data to or from the Central Repository

You can open and save different ChemStation items into their ChemStation contexts:

- Methods
- Sequence templates and Easy Sequence templates
- Report templates for Classic or Intelligent Reporting
- Single run data
- Sequence data
- Library files
- Column databases

Methods, single run data and sequence data are stored in the central repository as SSIZIP file (see "Compressed ChemStation File Formats" on page 27).

When the data is uploaded to the central data storage, local copies of the files still remain in the ChemStation file system. If a file is loaded from the central data storage back into ChemStation, changes made to this file will automatically be saved into its original location in the repository as a new revision.

While Master Methods, Sequence Templates and Report Templates can only be saved manually to the repository, Single runs and sequence data will automatically be uploaded to the repository, see "Data-related workflows" on page 50 for details on the different automatic upload options.

For downloading data from the central data storage, several **load** commands are available in the **ECM** or **CM** menu. Depending on the current view, you can load different files.

- In the **Data Analysis** view, you can load single run data or sequence data.
- In the **Method and Run Control** view, you can load methods and sequence templates.
- If you use Intelligent Reporting, you can also download report templates from the central data storage in the **Report Layout** view.

The following workflows are examples that represent typical tasks done with ChemStation and central data storage.

Data-related workflows

Workflow 1: Acquisition and automatic upload

The workflow *Acquisition and automatic upload* illustrates how raw data is uploaded to the central repository directly after the acquisition is finished. The raw data is initially stored locally. After completing the acquisition, the data is automatically uploaded to the central repository.
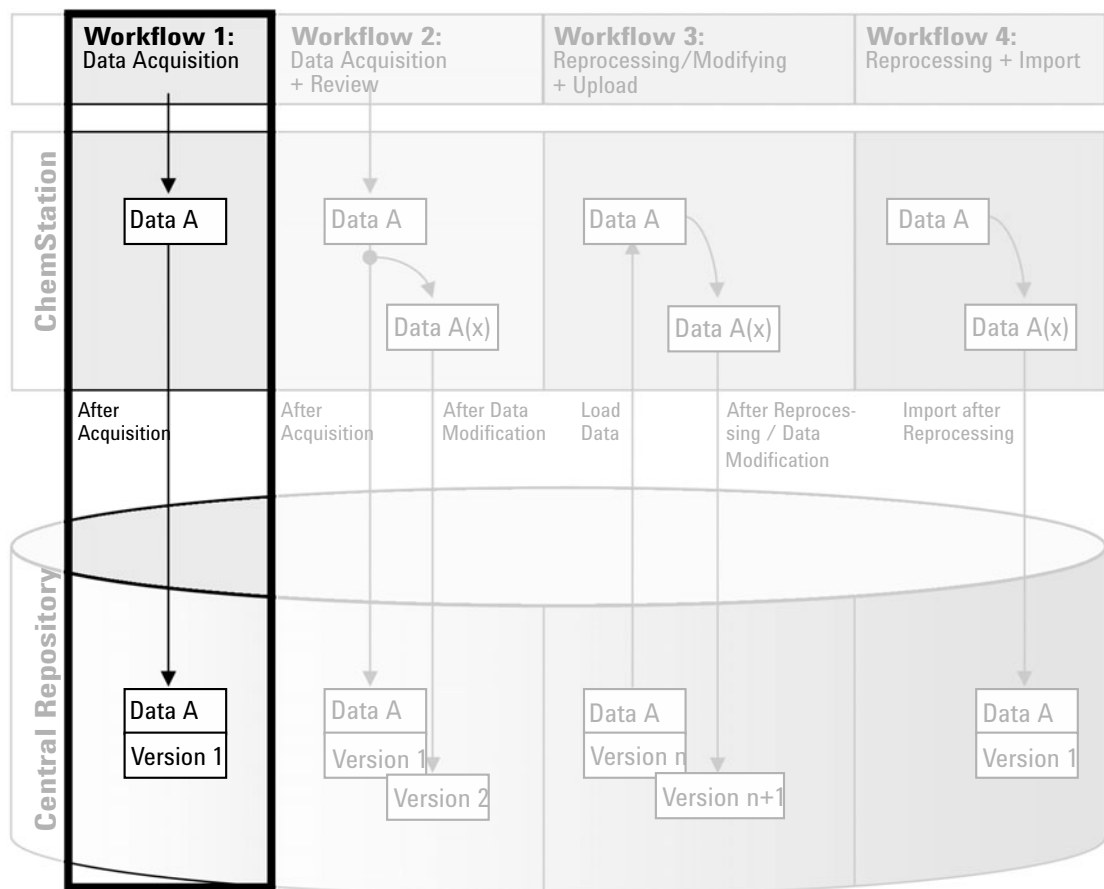
Figure 12   Acquisition and automatic upload

To save data to the central repository automatically after completion of a single run or sequence:

1 Log in to the OpenLab Control Panel and launch an online ChemStation.

2 Load a sequence template.

Your user name for the central data storage system is automatically inserted as operator name into the sequence template.

3 Click **View >Preferences**.

4 On the **Transfer Settings** tab, configure the following settings:

- **Path**: Select the location in the central repository that you want to use for the sequence data upload.

- Select the **After Acquisition** check box.

5 Configure the sequence parameters and the sequence table.

6 Start the acquisition.

While the acquisition is running, the raw data, method definition, and a copy of the sequence template are locally stored on the ChemStation computer.

After the sequence is finished, all data is automatically uploaded as an *.SC.SSIZIP* file to the central repository to the previously defined remote path. The local copy of the data remains on the ChemStation computer. The file name of the result set is determined by the settings in the sequence template (for more details on the sequence template settings, refer to the manual *Agilent OpenLab ChemStation Concepts and Workflows*). The sequence icon in the ChemStation Navigation Pane changes to . After finishing the upload, the icon changes to . The remote path of the result set is shown in the ChemStation toolbar.

NOTE The color of the **Sequence Data** icon in the Navigation Pane allows you to track the modification status of the data (the asterisk indicates a pending upload):

, : The result set is queued for an upload, or has been uploaded to the central repository and has not been modified locally

, : The result set is queued for an upload, or has been uploaded to the central repository and has been modified locally

---

NOTE The upload process may take some time when large amounts of data are uploaded. During this time ChemStation is busy and the user cannot perform tasks in ChemStation. Please wait until the upload is completed.

Workflow 2: Offline review during acquisition

The workflow *Offline revision during acquisition* illustrates how raw data is reviewed while the acquisition is still running. Directly after the acquisition is finished, the original raw data is automatically uploaded to the central repository. After the review, the changed data is again uploaded to the central repository. When the data is uploaded the second time, a new version is created.
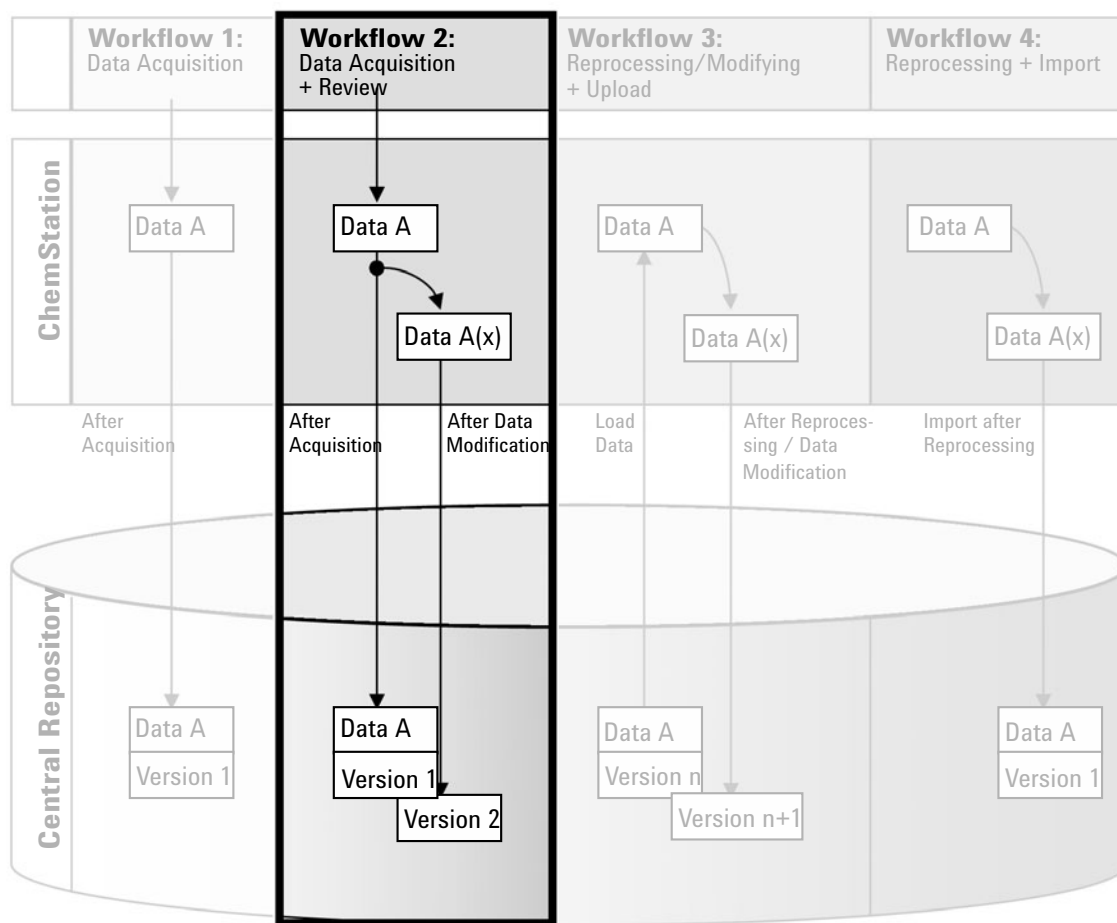
Figure 13   Offline review during acquisition

To save data to the central repository automatically after modification:

1 Log in to the OpenLab Control Panel and launch an online ChemStation.

2 Load a sequence template.

Your user name for the central data storage system is automatically inserted as operator name into the sequence template.

3 Click **View >Preferences**.

4 On the **Transfer Settings** tab, configure the following settings:

- **Path**: Select the storage location that you want to use for the sequence data upload.

- Select the **After Acquisition** check box.

- Select the **After Any Data Modification** check box.

5 Start the acquisition.

While the acquisition is running, the raw data, method definition, and a copy of the sequence template are stored locally on the ChemStation computer.

6 Open an offline ChemStation and change some data analysis parameters for one of the already finished samples. Save your changes locally.

If you only want to review data without modifying them, use the **Review** view. This prevents you from modifying the data unintentionally (see "After Any Data Modification" on page 32).

7 After finishing the acquisition and the work in the offline instance, the following versioning will be done, depending on which occurred first:

a If the acquisition finished before you have completed your offline changes:

- The original raw data is automatically uploaded as an *.SC.SSIZIP* file, *Version 1*, to the central repository using the previously defined remote data path. The path of the new sequence is shown in the toolbar in the online ChemStation.

  The file name of the result set is determined by the settings in the sequence template (for more details on the sequence template settings refer to the manual *Agilent OpenLab ChemStation Concepts and Workflows*).

  The sequence icon in the ChemStation Navigation Pane changes from

   to . After finishing the upload, the icon changes to .

- An Upload dialog opens in the online ChemStation. Click **OK** to confirm that you finished all work in the offline instance. As soon as you

confirm this dialog, the changed data is uploaded as *Version 2* to the central repository.

A local copy of the changed data remains on the ChemStation computer.

b If you saved your offline changes before the acquisition has finished:

- Upon confirming that you finished your work in the offline instance, the changed data is uploaded as *Version 1* to the central repository.
- The original raw data is automatically uploaded as an *.SC.SSIZIP* file, *Version 2*, to the central repository.

NOTE	For both versions (the one after acquisition and the one from the parallel offline review) the ChemStation operator is the user who has run the acquisition, even if another user has performed the review in the Offline ChemStation.

Workflow 3: Reprocessing data and automatic upload

The workflow *Reprocessing data and automatic upload* illustrates how data is reprocessed and then automatically uploaded. This workflow applies to data that has been previously stored in the central repository. A new version of the data is created in the central repository for the reprocessed or changed data.

Please note that the analysis and reprocessing of data is supported only on software versions same as or higher than the one used for the acquisition or last reprocessing.
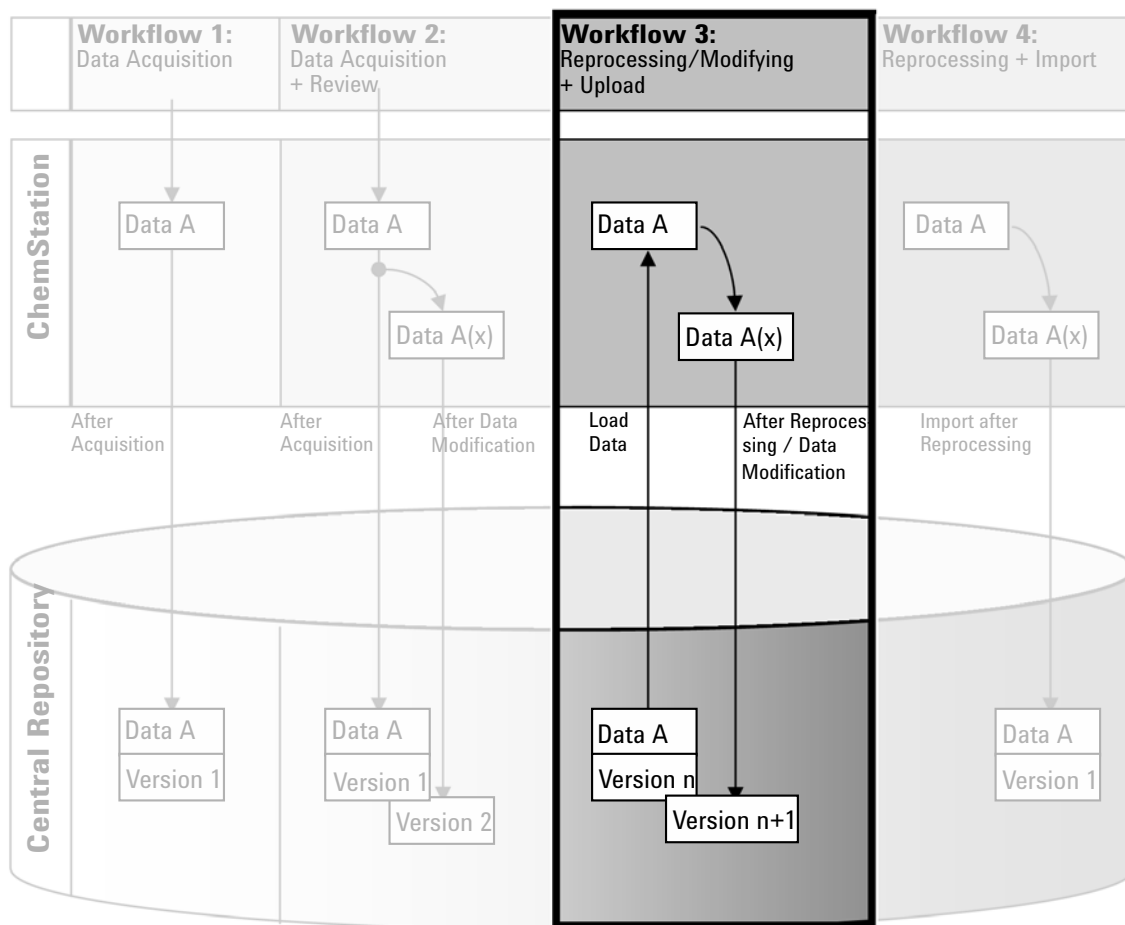
Figure 14   Reprocessing data and automatic upload

To save data to the central repository automatically after reprocessing:

1 Log in to OpenLab Control Panel and launch an online or offline ChemStation.

2 Select **ECM >Load Data** or **CM >Load Data** to download a sequence from the central repository.

A dialog opens where you can select the required data. Navigate to the folder that contains your data and select one of the following packaged files:

- Single run data: **.D.SSIZIP* files

- sequence data: **.SC.SSIZIP* files
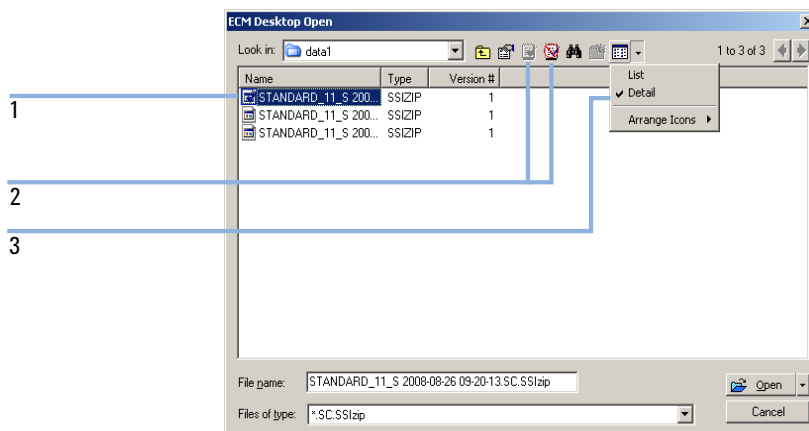
Figure 15   ECM Desktop Open dialog

If the item is checked out, it is marked with a blue or red icon (see marker 1):

(blue icon): the item has been checked out by you (current user)

(red icon): the item has been checked out by another user

You can load any checked out item. However, if an item has been checked out by another user, the other user must check in the item before you can save it back to the central repository.

To check out or check in an item, you can use the respective icons available in the dialog (see Figure 15 on page 56, marker 2). You can only check out the latest version of an item.

In order to see more details regarding the type and version of the available items, select the **Detail** view (see Figure 15 on page 56, marker 3). To open an older version of an item, select the **Open Revisions** command from the **Open** menu (see Figure 16 on page 57). This opens the **File Versions** dialog, where all available versions of the item are listed (see Figure 17 on page 57).

Figure 16   Open Revisions command
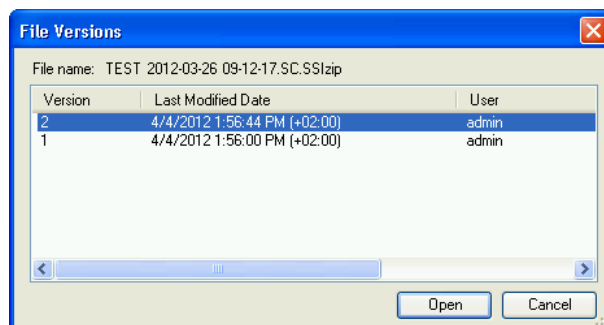
Figure 17   File versions dialog

3 Select **Open** in either dialog to download the item to ChemStation.

OR

Select **Open As Checked Out** in order to modify an item. With this option you make sure that you are working on the latest version.

The remote data path is shown in the ChemStation toolbar.

4 In the **Data Analysis** view, click **View >Preferences**.

5 On the **Transfer Settings** tab, configure the following settings:

- Select the **After Reprocessing** check box.
- Select the **After Any Data Modification** check box.

6 Modify or reprocess the sequence data.

After the reprocessing is finished, the sequence data is uploaded with its original name to its original remote data path. The version number is increased by one.

The local copy of the reprocessed data remains on the local file system of the ChemStation computer.

Workflow 4: Import after reprocessing
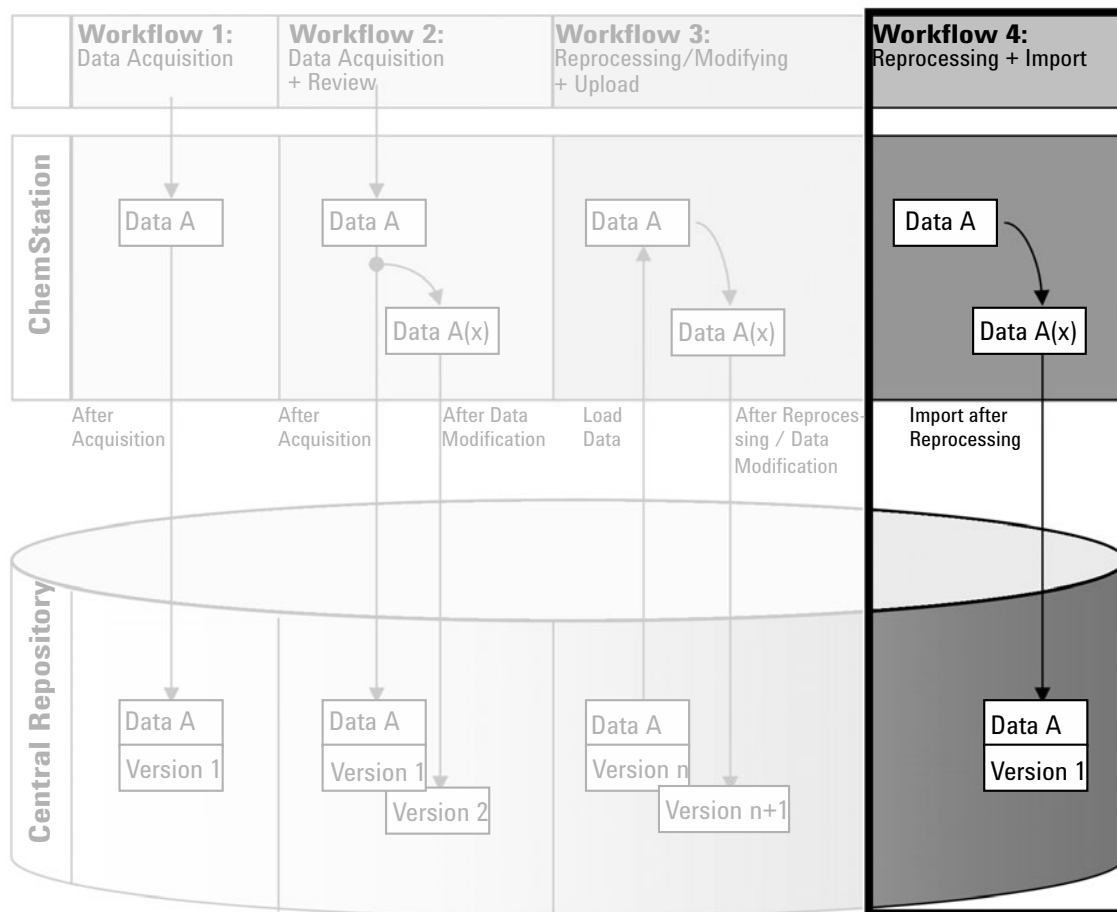
Figure 18   Import after reprocessing

The workflow *Import after reprocessing* illustrates how locally saved data is reprocessed and then automatically imported into the central repository.

To save data to the central repository automatically after reprocessing:

1 Log in to OpenLab Control Panel and launch an offline ChemStation.

2 From the local file system, open a sequence that has never been saved to the central repository before.

3 In the **Data Analysis** view, click **View >Preferences**.

4 On the **Transfer Settings** tab, configure the following settings:

   • **Path**: Select the storage location that you want to use for the sequence data upload.

   • Select the **Import after Reprocessing** check box.

5 Reprocess the sequence data.

NOTE   The data will not be uploaded if you only modify it. You need to reprocess the sequence data.

The sequence data is uploaded as a new *.SC.SSIZIP* file, version 1, to the previously defined remote data path in the central repository. The file name of the result set is determined by the settings in the sequence template (for more details about the sequence template settings refer to the manual *Agilent OpenLab ChemStation Concepts and Workflows*).

The sequence icon in the ChemStation Navigation Pane changes from 🗂 to 🗂.

After finishing the upload, the icon changes to 🗂.

The local copy of the reprocessed data remains on the local file system of the ChemStation computer.

Workflows for Methods and Templates

The following workflows are applicable to methods and sequence templates. If you enabled Intelligent Reporting in Instrument Configuration in the OpenLab Control Panel, these workflows also apply to report templates. The diagrams show the workflows using methods as an example.

Workflow 1: Save new method

The workflow *Save new method* illustrates how newly created or locally stored methods or sequence template can be manually uploaded to the central repository.
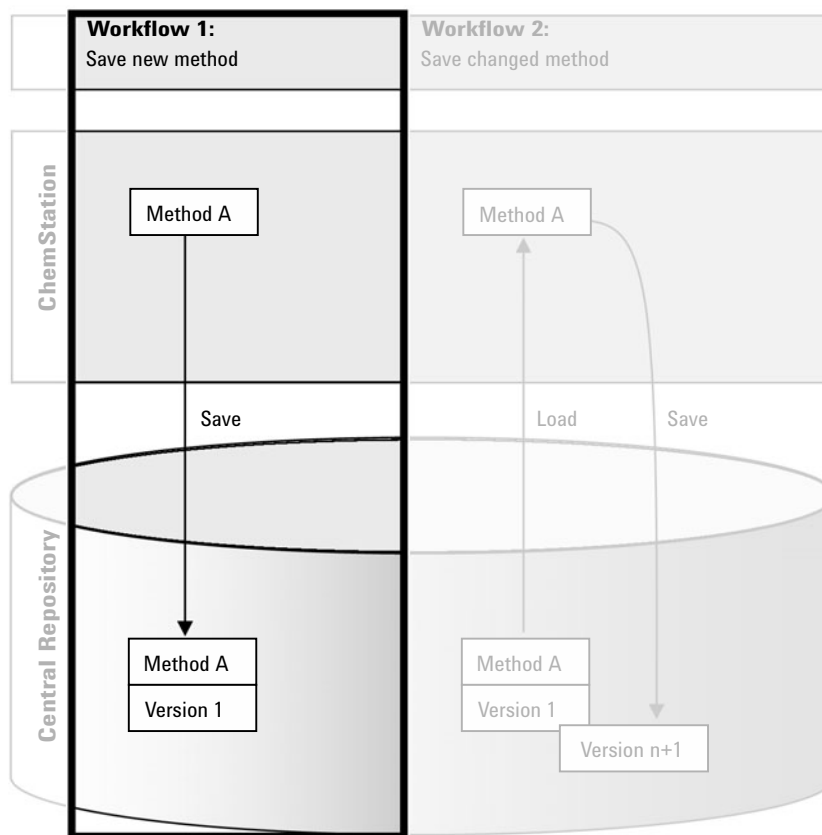
Figure 19   Save new method, sequence template, or report template

To upload a new method, sequence template, or report template:

1 Log in to OpenLab Control Panel and launch an offline ChemStation.

2 In ChemStation, load the method/sequence template/report template or create a new one.

3 Select the appropriate Save command from the **ECM** or **CM** menu.

In the **Method and Run Control** view:

- **Save Method**
- **Save Sequence Template**

In the **Report Layout** view (only with Intelligent Reporting):

- **Save Report Template**

4 In the **Save** dialog, navigate to the remote data path of your choice to upload the method/sequence template/report template.

In ECM, you can only upload items into a Folder, not into a Location, Cabinet, or Drawer. In Content Management, you can select any path.

5 If necessary, save the item using a different name. The original name is used by default, but you can modify the name.

6 Click **Save**.

The **Add File** dialog opens.

7 Enter a reason for the upload and click **OK**. The reason is then shown in the Audit Trail of the central data storage system (see "Audit Trail of the Central Data Storage" on page 76).

The progress of the upload is displayed in a window until the item is uploaded.

After finishing the upload, the SSIZIP file is available in the central repository as version 1. The file is saved to the remote data path defined in the Preferences (see "Remote Data Path" on page 29).

The method icon in the ChemStation Navigation Pane changes from to .

The icon for a sequence template changes from to .

The icon for report templates changes from to

Workflow 2: Save changed method
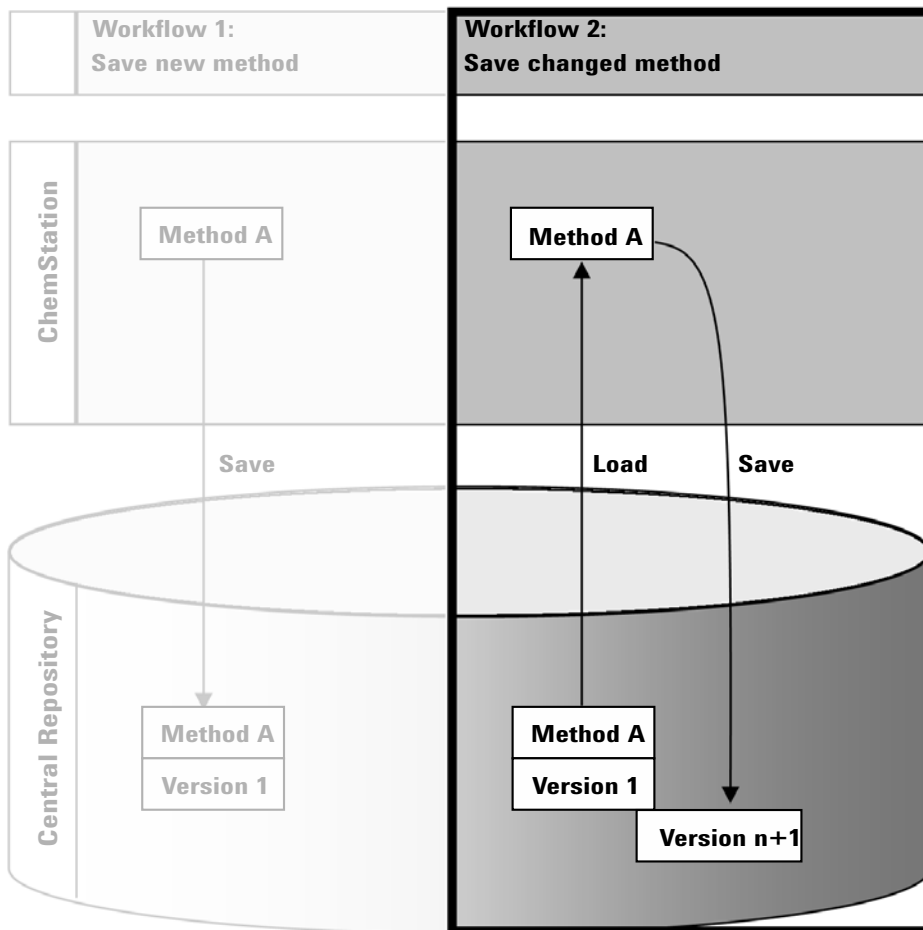
Figure 20   Save changed method

The workflow *Save changed method* illustrates how methods, sequence templates, or report templates that are already stored in the central repository are edited and saved under the same name as a new version.

1 Log in to OpenLab Control Panel and launch an online or offline ChemStation.

2 Load a method, sequence template, or report template.

- Open a method/sequence template/report template from your local PC. Choose an item that has been uploaded to the central repository before.

  Methods are indicated by 🔲, sequence templates by 🔲, and report templates by 🔲 in the ChemStation Navigation Pane.

– or –

- Select the **Load Method**, **Load Sequence Template**, or **Load Report Template** commands in the **ECM** or **CM** menu to download an item from the central repository.

If you use one of the Load commands, a dialog will open where you can select the required data. Navigate to the folder to load the method (**.M.SSIZIP*), sequence template (**.S* or **.S.SSIZIP*), or report template (**.RDL*) of your choice.
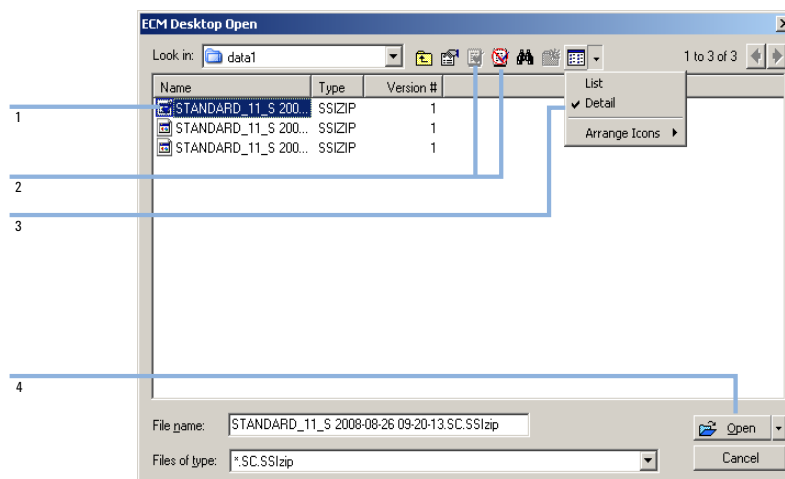
Figure 21   ECM Desktop Open dialog

If the item is checked out, it is marked with a blue or red icon (see Figure 21 on page 63, marker 1):

- 🔲 (blue icon): the item has been checked out by you (current user)

- 🔲 (red icon): the item has been checked out by another user

You can load any checked out item. However, if an item has been checked out by another user, the other user must check in the item before you can save it back to the central repository.

To check out or check in an item, you can use the respective icons available in the Open dialog (see Figure 21 on page 63, marker 2). Using these icons, you can only check out the latest version of an item.

In order to see more details regarding the type and version of the available items, select the **Detail** view (see Figure 21 on page 63, marker 3). To open an older version of an item, select the **Open Revisions** command from the **Open** menu (see Figure 22 on page 64, marker 1). This opens the **File Versions** dialog, where all available versions of the item are listed (see Figure 23 on page 64).
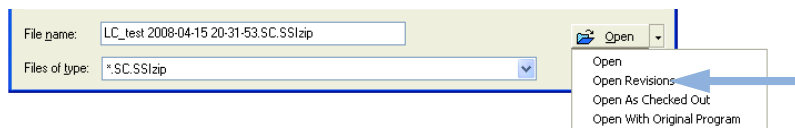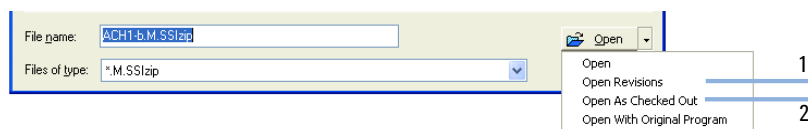

Figure 22   Open Revisions command
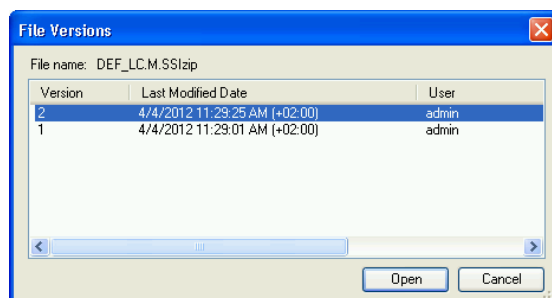
Figure 23   File versions dialog

3 Select **Open** in either dialog to download the item to ChemStation. To prevent other users from modifying the item, select the **Open As Checked Out** command. The item is then marked as checked out in the central data storage system (see Figure 22 on page 64, marker 2).

NOTE

ChemStation files (data, methods, sequence templates, and report templates) are not automatically checked out of the central data storage system! In order to modify those items in ChemStation, check them out manually. Otherwise, there is no guarantee that you are working on the latest version.

If the file already exists on the ChemStation computer in the specified location, you must choose a different download location.

The remote path of methods and templates is shown in the ChemStation toolbar.

4 Make the required changes to the loaded item.

A modified method is indicated by in the navigation pane.

A modified sequence template is indicated by .

A modified report template is indicated by .

5 Select the appropriate Save command in the **ECM** or **CM** menu to save the changed item.:

- **Save Method**
- **Save Sequence Template**
- **Save Report Template**

<table>
<tr><td>

NOTE

</td><td>

If you have not checked out the item before loading it from the central data storage, and another user has checked out the item in the meantime, you cannot proceed with the upload back to the central data storage. A warning message is displayed, and it is not possible to save the item until the other user has released the checked out item.

</td></tr>
</table>

6 When the **Add File** dialog opens, enter a reason for the upload and click **OK**. The reason is then shown in the Audit Trail of the central data storage system (see "Audit Trail of the Central Data Storage" on page 76).

The progress of the upload is displayed in a window until the item is uploaded to the central repository.

The *.M.SSIZIP/.S/.RDL* file is uploaded with its original name to its original remote data path (the path is shown as a tooltip of the method/sequence template/report template in ChemStation). The version number is automatically increased by one.

Updating the Local Master Method, Sequence Template, or Report Template

A copy of files (Master Method, Sequence Template, or Report Template) uploaded to the central repository is kept locally and may not be the latest version. The update command will allow you to download the latest version from ECM or Content Management and update the local copy.

1 Make sure the master method, sequence template, or report template to be updated is currently not loaded. A currently loaded item is not available for update.

2 Select the appropriate Update command from the **ECM** or **CM** menu:

   • **Update Methods ...**

   • **Update Sequence Templates ...**

   • **Update Report Templates ...**
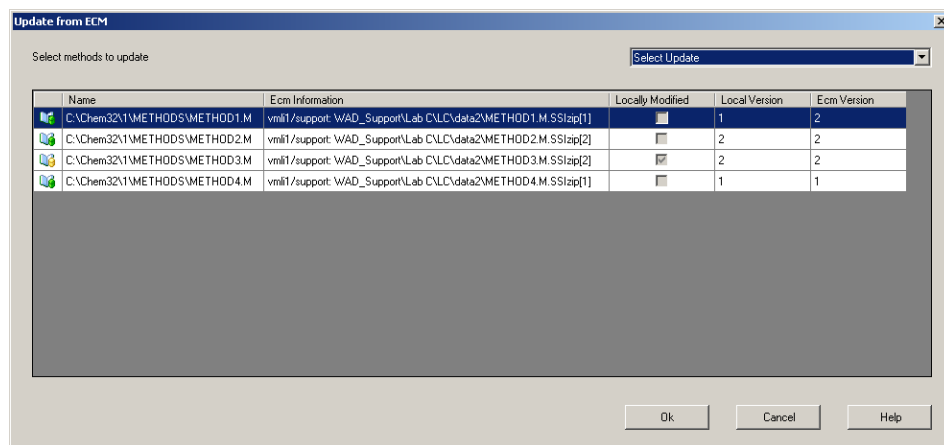
Figure 24   Update Methods dialog box

A dialog box is displayed where you can select the items to be updated.

The dialog box lists all items that have previously been uploaded to the central data storage. The following columns are available:

- **Name**: Path and Name of the local copy of the method, sequence template, or report template.

- **ECM Information**/**CM Information**: Server of the central data storage system and path of the file in the central repository; for ECM, also the ECM Account is shown.

- **Locally Modified**: A check box indicating whether the local copy was modified.

- **Local Version**: Version number of the local copy of the method, sequence template, or report template.

- **ECM Version**/**CM Version**: Version number of the file in the central repository.

3 You can now manually select the items that are to be updated. Alternatively you can use the drop down list to deselect all items, select those items with a higher version number in the central repository, or select all items that have been modified locally.

After clicking **OK**, the selected local items are updated with the version from the central data storage.

4 Administration Regarding 21 CFR Part 11 Compliance

This chapter explains the purpose of 21 CFR Part 11 and how the integration of ChemStation with a central data storage system and addresses the requirements of 21 CFR Part 11.

Introduction to 21 CFR Part 11

Effective August 20, 1997, the U.S. Food and Drug Administration (FDA) released and published a new rule to enable pharmaceutical companies to approve their results with electronic signatures and to transfer paper-trail documentation into electronic records. This rule is known as 21 Code of Federal Regulations Part 11 (referred to as 21 CFR Part 11) and applies to all industry segments regulated by the FDA.

The impact of this rule on current work practices and data handling in the pharmaceutical industry has been much higher than expected. *"The industry wanted to have a rule on electronic signatures, but what they got was a rule on electronic records."* (Martin Browning, former FDA inspector, during a validation seminar in Washington D.C.)

21 CFR Part 11 places high emphasis on the implementation of all measures to protect and secure electronic records. Notwithstanding the uncertainties and the changes that 21 CFR Part 11 requires in the behavior of both the pharmaceutical industry and the vendors of chemical analysis equipment, it is well worth implementing in today's laboratories because it can help the industry with one of the most important issues in pharmaceutical research-bringing new drugs on the market faster.

The major benefits of this shift towards electronic data management are in the potential productivity increase for the industry. The industry can decrease its data output on paper, speed up the data review and approval process, and benefit from new automation technology based on computerized system control, for example, in manufacturing or dissolution drug release testing.

In addition to this rule on electronic records, other general requirements for computerized systems are brought to the auditor's attention. These rules cover the basic requirements of validation which are limiting data access and ensuring data integrity and data traceability.

It is, of course, the industry that must ensure that its work practices support the FDA rules, but most of the requirements also affect the chemical analysis systems and suppliers of these systems.

21 CFR Part 11 Requirements

To fulfill the FDA rules and guidelines for compliant electronic records and computerized systems, it is important to understand the basic aspects of secure data handling.

- *Data security:* physical protection of data by limiting access to the system and preventing unauthorized access.

- *Data integrity:* protecting raw data and metadata and preventing these from unauthorized modification, and linking raw data and results to reproduce the original results at any time, for example, in an audit situation, and document each new result copy.

- *Audit traceability:* documenting who did what to the results and when, and tracing the user adding new reanalyzed versions to the original raw data.

General Aspects of Data Security in Computerized Networks - Open Versus Closed Systems

Before discussing details of data security in a chromatographic system, some general aspects of data security in a computerized network need to be considered.

It is generally known that data transfer over a public network can be accessed by unauthorized external persons, "hackers", who gain access either for personal amusement or intentional fraud.

If an electronic identification comprising user ID and a password is used to approve confidential or important data, users must be sure that their signatures are unbreakably linked to the data and that nobody can copy this signature or get access to the passwords. In a public system, this would require additional encryption technology, for example, a private/public key combination of data encryption. In contrast, if a computerized system is protected from unauthorized access, users can be sure that their signatures are private and are not accessible to unauthorized individuals.

The FDA also distinguishes between these two scenarios and defines them as *open* and *closed* systems. A *public* network system can therefore only be viewed as an open system and a protected network as a closed system, if it fulfills additional requirements.

In FDA terms, *"closed system means an environment in which access is controlled by persons who are responsible for the content of electronic records on the*

system" (11.3.5). The evidence of a system being a closed system is not a one-time check but an ongoing process of executing and documenting the system controls that make sure that the system is closed. In contrast, in an open system, *"those persons being responsible for the content of electronic records do not control the system access."*

As a result, open systems require additional encryption technology for all data transfer over the network.

OpenLab ChemStation is designed for and supported in closed systems.

Overview of Configuration Steps Required for Part 11

If you want to configure ChemStation with a central data storage system to be compliant with 21 CFR Part 11, you need to go through the following checklist:

*   Directory structure in the central data storage system prepared according to your needs

    See "Storage Model in OpenLab ECM and OpenLab Server" on page 15.

*   Roles/Users/Groups configured in the central data storage system and in OpenLab Control Panel

    See "Users/Groups/Roles Configuration" on page 86.

*   Configuration of the central data storage system with active audit trail and mandatory reason

    See "Audit Trail of the Central Data Storage" on page 76.

    See "Configuration of the Central Data Storage System" on page 81.

*   Password policy realized in OpenLab Control Panel

    See "User-Specific Settings" on page 84.

*   E-Signatures prepared (messages and privileges)

    See "Using electronic signatures" on page 95.

*   Automatic Data Transfer Settings and Transfer Management Settings activated

    See "Automatic Data Transfer Settings" on page 31.

*   Audit trail active for methods and results

    See "Method Audit Trail" on page 73 and "Results Audit Trail" on page 75.

*   Folders protected from external modification

    See "Folder Protection with Secure File I/O" on page 44

*   Emergency Plan available, based on options of the Administration Tool

    See "ChemStation Administration Tool" on page 38.

Audit Trails and Logbooks

In order to comply to 21 CRF Part 11, OpenLab ChemStation offers various audit trails and logbooks to document all activities associated with methods, results, reports, or any files stored in the repository. These audit trails and logbooks track all changes that are made to any file, including data acquisition, re-analysis, and long-term archiving.

Audit trails are stored in separate files, which are stored together with the sample or method data. The audit trail files are archived together with the other data in the respective SSIZIP files. Logbooks are available only in the Content Management system.

Method Audit Trail

Each method has a Method Audit Trail. By default, this Method Audit Trail contains the comments that you provide when you save a method. As there is no control on the provided text, there is no guarantee that the method changes are reproducible.

With regards to 21 CFR Part 11, OpenLab ChemStation allows you to generate a more detailed Method Audit Trail. If the function is activated, the Method Audit Trail contains not only the user comments, but also each individual activity related to the method:

- All changeable data analysis parameters are tracked. Each changed parameter is included with its old and new value. This means that you can reproduce exactly which value has been changed to what, when, and by whom.

  Depending on the instrument driver, the Method Audit Trail may also contain an entry for each changed instrument setting.

- In addition, the method audit trail also records activities that do not alter the method.

NOTE Reports that include a *Last changed* date may show an older date if the latest activity did not alter the method.

Examples for activities that do not alter the method:

- copy the method to the result set
- save the method interactively (with user comment)
- save method with a new name

NOTE   For instruments operated with classical drivers (single quad MSDs,) the instrument Method Audit Trail is not available.

To enable the Method Audit Trail only for the currently open method

You can also activate the Method Audit Trail only for one method. This might be useful, for example, when you have finished developing your method and want to track further changes.

1 Select **Method >Enable Audit Trail**.

2 In the **Audit Trail Status** dialog, select **Enable Method Audit Trail for this method**.

NOTE   Once a method is enabled for the detailed audit trail, you cannot disable it again.

You can save the method under a different method name. The Audit Trail of the new method will contain a comment about the method being based on the existing method.

To enable the Method Audit Trail for all methods

This is required if you want to comply to 21 CFR Part 11.

1 Select **View >Preferences**.

2 On the **Audit Trail** tab, select **Enable Audit Trail for all methods**, and click **OK**.

   Once enabled, the Method Audit Trail cannot be disabled.

NOTE   You can also use the ChemStation Administration Tool to enable the Method Audit Trail for all methods and all instruments (see "ChemStation Administration Tool" on page 38).

To view the Method Audit Trail for the currently open method in ChemStation

1 Select **Method >Method Audit Trail**.

Results Audit Trail

The Results Audit Trail contains information on manual integration events that are *not* saved to a method. Manual integration events that are saved to a method are listed in the corresponding Method Audit Trail.

If activated, this Results Audit Trail is added to the existing Data File Logbook (file name RUN.LOG). By default, the Data File Logbook only contains the acquisition parameters and reprocessing information for each sample. The Results Audit Trail additionally tracks the changes of all data analysis parameters for a sample.

To enable the Results Audit Trail

If you enable the Results Audit Trail, the relevant changes are tracked for *all* samples, independent of the sequence they belong to and independent of the user who carries out the change.

1 Select **View >Preferences**.

2 On the **Audit Trail** tab, select **Enable Results Audit Trail**.

To view the Results Audit Trail for the loaded sample in ChemStation

1 In the **Data Analysis** view, select **View >Current Data File Logbook**.

Sequence Audit Trail

The Sequence Audit Trail is automatically activated when the Results Audit Trail is enabled and will track changes made to the running sequence. The audit trail is saved along with the sequence, and tracks all changes to:

- the Sequence Table:
  - changes to any table cells
  - insertion and deletion of sequence lines
- the values in the **Sequence Parameters** dialog box
- values in sequence-related custom fields

For each change, the application logs:

- the date and time of creation of the audit trail entry
- the user who was logged on when the audit trail entry was generated
- a system-generated description of the change that resulted in the audit trail entry
- a user-generated comment

The latest Sequence Audit Trail entry is added to the top of the list. The list can be displayed and printed.

To view the Sequence Audit Trail for the currently loaded sequence

1   In either the **Method and Run Control** view or the **Data Analysis** view, select **Sequence >Sequence Audit Trail**.

Report History

If you create a ChemStation report, you can display the report on the screen, send it to a printer, or save the report as a specific file (*report.pdf*). These report outputs may easily be lost or overwritten, especially when you create several reports one after another.

ChemStation automatically tracks all reports that have been generated. If you have the results audit trail enabled you may see the Report History, that allows to reproduce an old or overwritten report. Select **Report >Report History** to see all reports created for the current data file. You can also export or print this history.

Audit Trail of the Central Data Storage

The Audit Trail of the central data storage system is a record showing who accessed the system and what operations a user performed during a given period of time. Since Data Store 2.0 (now "OpenLab Server") audit trail has been renamed to Activity Log.

You can view file-related, system administration, folder administration, and (for ECM) scheduler-related entries. For example, you can see when a file was added and who added it.

For each operation, the central data storage system asks the user for a reason. This reason is also shown in the Audit Trail/Activity Log. For automatic uploads default reasons are given by the system.

NOTE   In ECM, you must manually enable the Audit Trail. The entry of a reason for the audit trail can be set to be optional or mandatory. If the system shall be compliant to 21 CFR Part 11, the ECM Audit Trail must be enabled, and providing a reason must be mandatory (see "To configure the OpenLab ECM Account" on page 81). Using a reason must be regulated by a Standard Operating Procedure (SOP).

To Enable the OpenLab ECM Audit Trail

You can enable the ECM Audit Trail only for a complete ECM Account. To activate the ECM Audit Trail, select the check box **Enable audit trail for this account** when creating a new account.

It is not possible to activate the ECM Audit Trail afterwards for an existing account, or to deactivate the ECM Audit Trail if it has been activated during creation of the account.

To view the Audit Trail for a specific file in ChemStation

For both ECM and Content Management, you can view the Audit Trail for a specific file directly in ChemStation.

1 In the ChemStation Explorer, right-click the respective file.

2 Select **ECM Properties...** or **CM Properties...** from the context menu.

This command is only available if the file has been uploaded to central data storage.

3 In the **File Properties** dialog, select the **Audit Trail** tab.

This tab contains all Audit Trail entries associated with the file.

To view the Audit Trail for a specific file in OpenLab ECM

1 In ECM, right-click the respective file and select **Properties** from the context menu.

2 In the **File Properties** dialog, select the **Audit Trail** tab.

All actions related to this specific file are listed here, together with the date, ECM user name who performed the action, and a reason provided by the according user.

To view the Audit Trail/Activity Log for a specific file in Content Management

1 In the content browser, move the mouse over the file, then select **Activity Log** .

A file preview is shown, together with several document properties and a list of document actions.

To view the Audit Trail for all files in OpenLab ECM

1 In ECM, select the **Administration** page.

2 In the Navigation Pane, select the **Activity Log >Audit Trail** node.

All actions related to any ECM file are listed here, together with the file name, date, ECM user name who performed the action, and a reason provided by the respective user.

You can search the entries, for example, for a specific date or date range, or for entries related to specific categories (Files, Folders, System, Scheduler, or Instrument). Also you can print the entries or export them to a file.

To view the Audit Trail/Activity Log for all files in Content Management

1 In the content browser, click **Activity Log** in the top pane.

You can filter the list by date range and user name.

> **NOTE** The user name is case sensitive and needs to be an exact match.

System Log of the Central Data Storage

The System Log of the central data storage is a record that shows changes to the system, including configuration changes, e-mail notifications, and additions or changes to the directory structure.

You can view file-related, system administration, folder administration, or (for ECM) Scheduler-related entries. For example, you can see when a directory was added and by whom.

The System Log is always active; you do not need to enable it.

To View the OpenLab ECM Sytem Log

1 In ECM, select the **Administration** page.

2 In the navigation pane, select the **Activity Log >System Log** node.

All general actions related to ECM are listed here, together with the date, ECM user name who performed the action, and a reason provided by the respective user. Depending on the ECM Account administration, the reason may be optional or mandatory (see "To configure the OpenLab ECM Account" on page 81).

You can search the entries, for example, for a specific date or date range, or for entries related to specific categories (Files, Folders, System, Scheduler, or Instrument). Also you can print the entries or export them to a file.

To view the Content Management System Log

In Content Management, there is only one single activity log for the entire system. System activities are stored at the same place as file activities.

1 In the content browser, click **Activity Log** in the top pane.

You can filter the list by date range and user name.

NOTE   The user name is case sensitive and needs to be an exact match.

System Activity Log in OpenLab Control Panel

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. ChemStation 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.

All events have one of the following activity log severity levels:

- Info

  Used for all informational logs generated by the system. Most application and instrument activities fall into this severity level.

- Warning

  Used for entries describing activities or conditions that could lead to failure. Useful for instruments that shall record a consumable reaching a set limit.

- Error

  A failure has occurred. For example, the software did not behave as expected, an instrument has prematurely shut down, or a run was prematurely ended.

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.

To Enable the System Activity Log

1 In the OpenLab Control Panel, select the **Administration >System Configuration** page.
2 In the ribbon, click **Activity Log Settings**.
3 In the **Activity Log Settings** dialog, select the **Write activity log** check box, and confirm your settings.

Security Policy

21 CFR Part 11 requires that the company or laboratory have a security policy in place to ensure that only authorized users access the data.
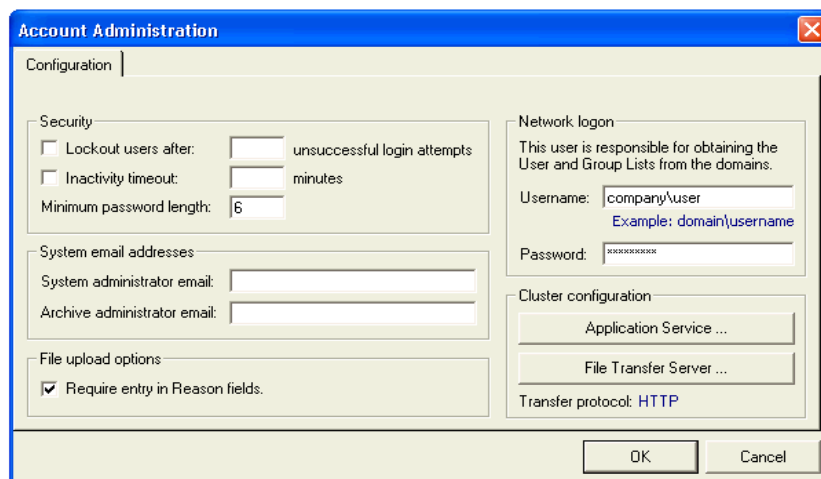
Configuration of the Central Data Storage System

The following sections describe how to configure the security policy with OpenLab ECM or OpenLab Server.

To configure the OpenLab ECM Account

1   In ECM, select the **Administration** page.

2   In the Navigation Pane, select the **Account Administration** node.

3   Double-click the **Configuration** item.

    The **Account Administration** dialog opens.

Table 3   Settings in ECM Account Administration

Setting	Description	21 CFR Part 11 Requirements
Lockout	If a user tries too often to log in with invalid user credentials, he is locked out of the system and cannot log in any more – not even with valid user credentials. You can define the number of allowed login attempts. This setting only applies to ECM built-in users, not to Windows domain users.	You should limit the number of allowed login attempts to three.
Inactivity Timeout	If a user does not perform any action for the given period of time, he is automatically logged out of the ECM Web Client. *Note*: The inactivity timeout of ChemStation is set in the Security Policy area of the OpenLab Control Panel.	You should specify a timeout.
System administrator email	The e-mail address you provide here will automatically be notified when a user was locked out after too many unsuccessful login attempts.	You should provide an e-mail address.
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*. This setting only applies to ECM built-in users, not to Windows domain users.	You should require a minimum password length of at least 5 characters.
Require entry in Reason fields	In each ECM Audit Trail or System Log entry the users can enter a specific reason for the action. If this check box is selected, the entry is mandatory.	The ECM Audit Trail and System Log reasons must be mandatory.

To configure OpenLab Server

1 In the OpenLab Control Panel, select **Administration >Security Policy** from the navigation pane.

Table 4   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 Control Panel is inactive for this amount of time, the user interface will be locked. This setting also applies to the other applications running with your Control Panel. The default setting is *10 min*. Set the value to zero to never lock.	

User-Specific Settings

21 CFR Part 11 does not define any specific rules for the password settings. However, your company must have defined a password policy.

To configure password settings in OpenLab ECM

1 In ECM, select the **Administration** page.

2 In the navigation pane, select the **Account Administration** node.

3 Double-click the **Users/Groups/Roles** item.

   You may consider the following settings for ECM built-in users:

   • User cannot change password

   • User must change password after next login

| NOTE | The minimum password length for ECM built-in users is defined in the ECM Account configuration (see "To configure the OpenLab ECM Account" on page 81). |

To configure password settings in OpenLab Server

1 In the OpenLab Control Panel, select **Administration >Users** from the navigation pane.

2 Select a user, and click **Edit** in the ribbon.

   With the authentication provider set to **Internal**, you can configure the following settings on the **General** tab:

Table 5   User Credentials

Value	Description	Mandatory
Name	Username to log in to the system. NOTE 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

Table 5 User Credentials

Value	Description	Mandatory
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
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.	

Users/Groups/Roles Configuration

Users with specific roles and privileges are needed in both the central data storage system and in ChemStation. First, you need to authenticate with a user name and password when you start ChemStation from the OpenLab Control Panel. Then, additional privileges are required for specific functions in ChemStation as well as in the central data storage system.

In ChemStation, user management is part of Shared Services, which you access via the OpenLab Control Panel. Each user can be member of specific groups. To each group, you can assign predefined roles that comprise specific privileges. If you use an external authentication provider, you can import users and groups from the external system.

Settings in OpenLab Control Panel

Users in OpenLab Control Panel

If you use the Content Management provided by OpenLab Server or OpenLab ECM XT, you create and manage users directly in the OpenLab Control Panel.

If you use ECM or Windows Domain 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.

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 ChemStation, 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 in OpenLab Control Panel

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 *ChemStation Operator* will always need another role such as *Instrument User* with the privilege to run an instrument.

You can create a tree of different locations in the OpenLab Control Panel, and add instruments to the relevant locations. For each instrument or instrument group, you can assign different Instrument roles (see also "Specific Privileges for Individual Nodes" on page 90). For example, a user can have the role **Instrument Administrator** for one instrument, and **Instrument User** for another instrument.

With OpenLab Server/Content Management, you can also create a tree of different projects or project groups in the OpenLab Control Panel, and assign different Project roles for different projects (see also "Specific Privileges for Individual Nodes" on page 90). For example, a user can have the role **Project Administrator** in one project, so that he can manage the settings in the OpenLab 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.

With OpenLab Server, you must first enable projects (see "Using Projects with Content Management" on page 89).

Table 6   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. • These privileges are globally assigned to ChemStation users. • Pprojects can be used to assign privileges to content areas in the Content Management system (see "Using Projects with Content Management" on page 89).

For a detailed list of privileges, see the Appendix.

Privileges Related to Central Data Storage

The following tables describe the privileges that are relevant for OpenLab Server.

Table 7   Administrative privileges

Privilege Name	Description
Archive content	The role **Archivist** includes this privilege by default. The user can archive and de-archive the content of the data repository.

Table 8   Project privileges

Privilege Name	Description
View project or project group	By default, this privilege is included in the **Project Administrator** role and in all **ChemStation** roles. The user can see a project and project details in OpenLab Control Panel, but cannot edit. Also, he can view the content of the OpenLab Server repository.
Manage project or project group	By default, this privilege is included in the **Project Administrator** role. User can create or edit project properties and can move the project but cannot access settings (only relevant for ChemStation with Content Management).
Edit content of project	By default, this privilege is included in the **Project Administrator**, **Content Management Approver**, and **Content Management Contributor** roles. The user can create new versions of documents in Content Management.
E-Signature Sign Data Files	By default, this privilege is included in the **Project Administrator** and **Content Management Approver** roles. The user can sign data files, view and edit project properties and create new versions of documents in Content Management.
Access content using web client	By default, this privilege is included in all **Content Management** roles. The user with this privilege is able to open the OpenLab Server Content Browser interface.

NOTE   Project roles apply globally for ChemStation.

Using Projects with Content Management

With OpenLab ChemStation, you can enable projects in the OpenLab Control Panel. Projects contain a path to a project folder in the Content Management system. For each project, you can assign specific content privileges to the users.

To Enable Projects

1 In the OpenLab Control Panel, navigate to **Administration >System Configuration**.

2 In the ribbon, click **Enable Projects**.

3 In the confirmation dialog box, click **OK**.

For details on assigning specific privileges to a project, see "Specific Privileges for Individual Nodes" on page 90.

Specific Privileges for Individual Nodes

By default, the roles of users or groups are globally set for all locations, instruments, project groups, or projects. The role settings are inherited from the root node **Instruments** or **Projects** respectively. 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.

If you use projects, you can assign **Project** roles to individual project groups or projects. For more information, see "Using Projects with Content Management" on page 89.

Administrative roles are always set globally.

Users, Roles, and Privileges Concept with OpenLab ECM

With ECM, you must select ECM as an external authentication provider in the OpenLab Control Panel. In ECM itself, you can either set up internal users or operate with the Windows users (see ECM documentation). Each user can be member of specific groups in ECM and in the OpenLab Control Panel. The groups available in ECM depend on the ECM configuration. The groups available in the OpenLab Control Panel can be imported from ECM and supplemented by new internal groups.

There are several default roles in both ECM and OpenLab ChemStation. In both systems, you must assign a specific role to each group. Roles and privileges must be configured separately for ECM and ChemStation:

- The privileges set in ECM define the accessible content and functions in ECM.
- The privileges set in the OpenLab Control Panel define which functions are available in ChemStation, and also which administrative tasks can be carried out in the OpenLab Control Panel.

NOTE Once you have created a new ECM user, group, or role, you cannot delete it again. You can only deactivate the unused item.

Default Roles and Privileges in OpenLab ECM

There are a number of default roles and privileges in ECM. The following tables show an overview of these roles and privileges.

Name	Description
Roles starting with ":"	Default ECM roles; can be restored by the Reset Roles function.
Privileges starting with "**Content:**"	Privilege related to creating, modifying or deleting content in ECM.
Privileges starting with "**System:**"	Privilege related to administrative tasks in ECM.

In addition, you can create your own roles in ECM, or grant further privileges to the default roles. For detailed information, refer to the ECM Administrator's Guide.

Assigning roles in OpenLab ECM

Users do not need any specific role in order to log in to ECM. However, in order for users to see a particular Location, Cabinet, Drawer, or Folder in the user interface, they must have the **:Reader** role as a minimum requirement. As a result, domain users with no global roles might not be able to view anything in the content unless they were granted the appropriate privileges.

You should grant the ChemStation users the **:Contributor** role. This can be done at the global level for the entire ECM Account, or individually for specific folders (see). The **:Contributor** role allows the ChemStation user to view and add content to ECM. The **:Contributor**

role should be enhanced with the **Content: Add Folder** privilege. This allows
ChemStation ECM users to add folders to the LCDF hierarchy.

NOTE	If the role does not include the **Add Folder** privilege, the users cannot add a new Remote Data Path (LCDF) in ChemStation.

In addition to the configuration of ECM roles, you must also configure
ChemStation roles and privileges for ChemStation users. The configuration of
ChemStation roles and privileges is done in the OpenLab Control Panel.

You find a complete list of all ECM and ChemStation privileges in the Appendix.

Roles and Folders in OpenLab ECM

ECM allows you to assign specific roles to users or user groups. This can be
done at the global level for the entire ECM Account, or individually for specific
folders. For example, a specific user group may have the **Contributor** role for
folder A, but at the same time have only the **Reader** role for folder B. The roles you
assign in ECM are only related to content storage in ECM; all roles related to
ChemStation and instrument settings are assigned in OpenLab Control Panel.

Preparations   If you want to assign roles at the folder level, you must first enable this feature in ECM. The setting is
valid for the complete ECM Account.

To enable roles for folders:

1 In ECM, select the **Administration** page.

2 In the navigation pane, select the **Account Administration** node.

3 Double-click the **Users/Groups/Roles** item.

   The **Account Administration** dialog opens.

4 On the **Roles** tab, select the required role and click **Edit**.

5 Select the **Available in folder access tab** check box.

Users, roles, and privileges concept with OpenLab Server

With OpenLab Server, all users, groups, roles, and privileges are configured in the OpenLab Control Panel. You can use Windows as an external authentication provider, but you set up all roles and privileges related to OpenLab in the OpenLab Control Panel. ChemStation and OpenLab Server refer to these settings.

Electronic Signature

Electronic signatures provide a means to sign documents as equally binding as a handwritten signature. In addition, electronic signatures are reproducible, because they are recorded in a secure, time stamped audit trail. Manipulation is prevented by enabling only users with specific privileges to sign electronically.

An electronic signature contains the user name (full name), date, and time when the signature was applied, the location where the signing occurred, and a user-configurable definition associated with the signature. The signature is always related to the complete result set, complete data file for a single run or to a report. The signature cannot be applied to a single file inside the SSIZIP file.

CFR 21 Part 11 requires that companies, especially ones that employ any type of approval process, use electronic signatures.

With OpenLab ECM, you can use the Agilent OpenLab Business Process Manager (BPM) module as an Add-on to create highly automated review or approval processes including e-mail notification.

Preparation

Privileges

Users must have a specific privilege in order to be able to sign electronically.

With ECM, a user must have the privilege **Content: File Signatures**. This privilege is, for example, assigned to the default role **:Approver** in ECM.

With OpenLab Server/Content Management, a user must have the privilege **E-Signature Sign Files**.

Reasons for the signature

With each signature, the users must either select a reason.

With OpenLab Server/ECM XT, the list of default reasons cannot be configured, and users are always allowed to provide their own reason.

With ECM, you can either restrict the users to the default reasons or allow them to provide their own reason. Also, you can configure the list of default reasons.

To allow specific signature reasons in OpenLab ECM:

1 In ECM, select the **Administration** page.

2 In the navigation pane, select the **Account Administration** node.

3 Double-click the **Electronic Signature** item.

   The **Account Administration** dialog opens.

4 To provide a new reason, enter the required text into the **Reasons** field and click ⬚.

5 To delete an existing reason, select the reason in the **Default reasons** list and click ✖.

6 If you want to allow users to provide their own reason with a signature, select the **User can specify reason** check box.

NOTE   If you clear this check box, the users can only select one of the default reasons.

7 If necessary, adjust the timeout settings:

- The **Signature screen timeout** defines, how long an e-signature dialog will stay open if no signature is submitted. The default setting is 5 minutes.
- The **Consecutive signature timeout** is relevant if an ECM user carries out several successive e-signatures. If the next e-signature takes place within the given timeout interval, the **location** and the **reason** provided in the first e-signature will be pre-filled in the next dialog. The default setting for the consecutive signature timeout is 5 minutes.

Using electronic signatures

To apply an electronic signature in OpenLab ECM

1 Right-click the required SSIZIP file and select **Electronically Sign >Electronic Signature** from the context menu.

The **Electronic Signature** dialog opens.

NOTE   The other command in the context menu, **Electronically Sign >Acrobat Plug-In Signature**, works only for PDF documents and only if you purchased the respective plugin. It enables you to add signatures directly inside PDF documents.

2 Enter your ECM user credentials (username, password, and domain).

3 Enter your current location. With this information, the location from where you provide the signature is reproducible.

4 Select a reason for the signature from the **Default reason** drop-down list.

- Or -

Select the **User specified** check box and enter a different reason into the text field. Note that this option is only available if the ECM Account is configured accordingly.

5 Click **Sign**.

The file is now signed electronically. The e-signature is shown in the file properties in the **eSig** tab. The e-signature is also included in the ECM Audit Trail.

To apply an electronic signature in OpenLab Server/ECM XT

1 In the content browser, move the mouse over the respective file, then select **Sign File** ✓.

A file preview is shown, together with several document properties and a list of document actions.

2 Under **Document Actions**, click **Sign File**.

The **Sign File** dialog opens.

3 Enter your login credentials.

4 Select a reason for the signature from the **Reason** drop-down list.

OR

Select the reason **Other**, and enter a different reason into the text field.

5 Click **OK**.

The file is now signed electronically. The e-signature is shown in the list of signatures under **Version History**.

To view electronic signatures in ChemStation

1 In the ChemStation Explorer, right-click the respective file.

2 Select **ECM Properties...** or **CM Properties...** from the context menu.

This command is only available if the file has been uploaded to central data storage.

3 In the **File Properties** dialog, select the **eSig** tab.

The electronic signature history for the file, including the date, signer's full name, and reason for each signature are listed.

To view electronic signatures in OpenLab ECM

The electronic signature itself is shown in the file properties in the **eSig** tab, and it is also part of the ECM Audit Trail.

The user preferences in ECM can be configured in such a way that the number of e-signatures applied to a file is shown by default in the ECM content display, together with the file name and status.

1   In ECM, select the **Administration** page.

2   In the navigation pane, select the **Account Administration** node.

3   Double-click the **User Preferences** item.

4   Click **Modify...** to modify the column settings.

5   Select **# of signatures** and click ➔ to add this property to the selected columns.

6   Click **OK**.

    The number of e-signatures is then shown on every content page in ECM.

To view electronic signatures in OpenLab Server/ECM XT

All e-signatures applied to a file are listed under **Version History** in the Properties page of the file.

5 Filter and Search Options

This chapter provides an overview of the filter and search options for ChemStation data in the central data storage system.

Attribute Extraction Services in OpenLab ECM

ECM Attribute Extraction Services (AES) provides the following AES for the extraction of metadata from ChemStation data files:

- The *ACAML* filter extracts all information contained in the .acaml files, which are part of the SSIZIP files uploaded by ChemStation revision B.03.02 and later.

- The *ChemStation XML* filter extracts peak, compound and result data from the result.xml file generated by the XML export routine in ChemStation revision A.10.02 and later.

- The *ChemStation* filter extracts basic sample and run data from the header of the channel files (*.ch), *.uv and *.txt files generated by all ChemStation revisions.

AES need to be installed by an ECM Administrator on the ECM Server; in addition, the filters need to be enabled for the system. The keys of an AES that are to be applied to a ChemStation file need to be selected for the respective LCDF structure. These are ECM administration tasks, and are described in the Enterprise Content Manager Administrator's Guide and the ECM online help.

The metadata can be queried using various search types in ECM. The ECM Search functionality is also available within ChemStation. When opening a file from ECM, the **ECM Open** dialog allows you to search for files of interest using the 'magnifying glass' icon, see Figure 25 on page 100.

Using the Quick Search, you can search through various alphanumeric fields by entering a search key, such as an operator name. On the upcoming search page, you select the **Advanced** tab where, depending on the enabled filter packages, various keys are enabled, see Figure 26 on page 100.
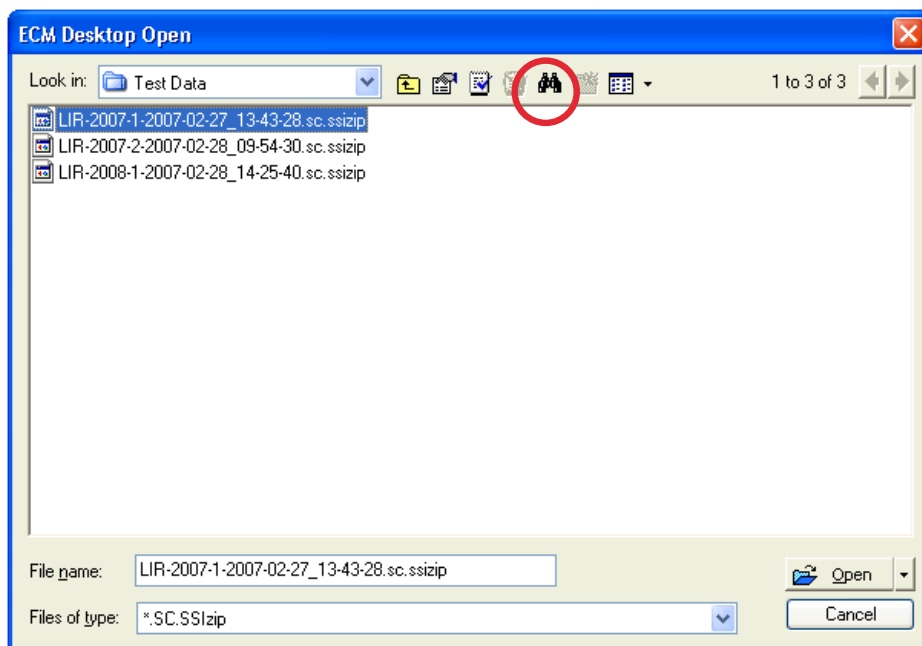
Figure 25   Search options
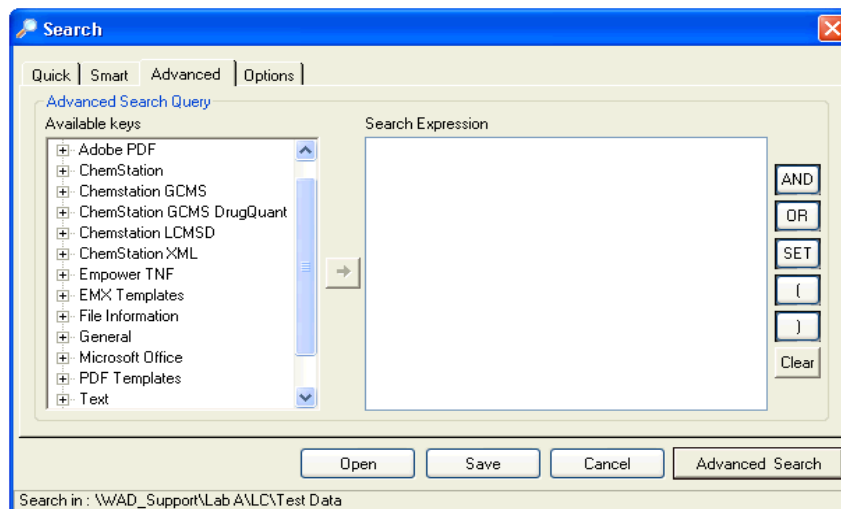
Figure 26   Filters available in search options

In the **Search** dialog, you can specify the available keys, and it is possible to define a search expression by combining two or more of the available keys using boolean operators. For detailed information regarding the use of the various search algorithms, refer to the online help of your ECM system or the Enterprise Content Manager Administrator's Guide, as well as the AES-related manuals.

ACAML Filter

ChemStation stores all result data in the ACAML format (ACAML = Agilent Common Analytical Markup Language), which results in .acaml files. There is one .acaml file for each sequence or single run. The .acaml files are always created when acquiring or reprocessing data.

When the data is uploaded to ECM, the .acaml file is part of the SSIZIP file. The ACAML filter extracts information from these files.

Please note that the ACAML filter is only available as of ECM 3.3.2 SP1.

ChemStation XML Attribute Extraction Service

The AES for ChemStation XML extracts key information from the following categories of the result.xml generated by ChemStation per data file. Note that ChemStation must be configured to generate the result.xml file, see the ChemStation XML Connectivity Guide.

- Acquisition (for example, instrument name, method information)
- Chromatogram (for example, derivative order, detector name)
- Custom
- Module
- Peaks (for example, peak name, amount, retention time, compound name)
- Sample (for example, calibration method, LIMS ID)
- Signal/noise

ChemStation Filter

The AES for ChemStation extracts attributes from *.ch, *.uv, and *.txt files created by the 16-Bit ChemStation (Rev A.x.x) or 32-Bit ChemStation (Rev B.x.x or later). It extracts key information from the header of ChemStation *.ch and *.uv data files (for example, sample name, method file, instrument model). From the report.txt file, it extracts key information (for example, sample name, acquisition method, analysis method). In addition, the service extracts information on support files from the category Content.

An ECM Scheduler Add-in for Agilent ChemStation enables the ECM Scheduler to automatically upload data generated by ChemStation to ECM.

Search Options in the OpenLab Server/ECM XT Web Interface

Using the Advanced Search

ChemStation stores all result data in the ACAML format (ACAML = Agilent Common Analytical Markup Language), which results in .acaml files. There is one .acaml file for each sequence or single run. The .acaml files are always created when acquiring or reprocessing data. When the data is uploaded to the central data storage, the .acaml file is part of the SSIZIP file.

When using the advanced search in the Content Browser of OpenLab Server/ECM XT, you can limit your search to specific metadata based on the values given in the .acaml file

1 In the top pane, click **Search**.

2 From the **Select field** drop-down list, select the field which you would like to use. You can use, for example, the following fields:

- Acquisition Operator
- Compound
- File name
- Method Name
- Sample Name
- Sequence Name

The corresponding search expression is entered in the search field.

3 In the search field, type your search criteria.

4 Click **Search**.

For more information, refer to the OpenLab Server/ECM XT documentation.

6 Maintenance Procedures

This chapter describes maintenance procedures for the Shared Services server database.

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 best 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.
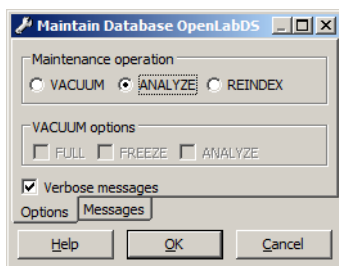
Figure 27   **Maintain Database**

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 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 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 Shared Services server.

   Software patches and updates for OpenLab ChemStation and OpenLab Shared Services 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 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.

Change Passwords for ChemStation Instrument Users

During installation of OpenLab ChemStation, the instrument users names and passwords are configured via an XML file. This XML file is stored under *<BaseInstallDirectory>\Logs\users.xml*.

By default, the installer creates the users.xml file automatically to generate local instrument users with passwords that never expire. The file has the following structure:

```
<?xml version="1.0" encoding="utf-8" ?>

<users>

<user UserName="AICHostName\CSIUser0" Password="xxxxxxxxxxxx" />

<user UserName="AICHostName\CSIUser1" Password="xxxxxxxxxxxx" />

<user UserName="AICHostName\CSIUser2" Password="xxxxxxxxxxxx" />

<user UserName="AICHostName\CSIUser3" Password="xxxxxxxxxxxx" />

[...]

<user UserName="AICHostName\CSIUser37" Password="xxxxxxxxxxxx" />

<user UserName="AICHostName\CSIUser38" Password="xxxxxxxxxxxx" />

<user UserName="AICHostName\CSIUser39" Password="xxxxxxxxxxxx" />

<user UserName="AICHostName\CSIUser40" Password="xxxxxxxxxxxx" />

</users>
```

The installer fills the structure with the auto-generated passwords and the machine-prefixed user names. After creating the accounts the passwords become encrypted and are only readable by the software.

Alternatively, you can specify instrument users names and passwords as required, and define domain users instead of local users. In this case, a security policy may require changing the passwords on a regular basis.

Change Passwords for ChemStation Instrument Users

Change Passwords for ChemStation Instrument Users

If you specified your own user names or passwords during the installation of an AIC, and you used *domain* users, it may become necessary to change their passwords on a regular basis.

1 Specify different user names or passwords in a *users.xml* file:

    a Provide domain users in the form: *UserName="<domain name>\<user name>".*

> **NOTE**
> Make sure that at least 41 different user names are provided. If you provide the same username twice, instrument access conflicts will arise.

    b Provide special passwords in the form: *Password="<user defined password>".* At this stage, write the passwords in clear text. Encryption will take place when registering the accounts with Shared Services.

       Make sure that the password complies with the domain policy for passwords. Special characters must be escaped as follows:

Character	Escaped Character
<	<
>	>
"	"
'	'
&	&

    c Enforce addition of users to the Local Administrators group by setting the users attribute:

```
<users unsafe="true">
```

2 In order to meet any requirement for an initial password change, change domain user passwords in Windows for each user in the users.xml.

3 Register the new passwords with Shared Services:

    a On the AIC, select **Start >Command Prompt**.

    b Type *cd <ChemStation installation directory>\Core* and press **Enter**.

    c Type *registerCSData.exe /remote /InstrumentUsers="<Path to users.xml file>" /URL="net.tcp://<OpenLab Shared Services server>:6577/Agilent/OpenLAB/" /User="<name of OpenLab Shared Services admin user>" /password="<password of OpenLab Shared Services admin user>"* and press **Enter**.

    After registration, the passwords in the users.xml file will appear encrypted and will be only readable by the software.

4 Restart OpenLab Control Panel before launching the reconfigured instruments.

Change Passwords for ChemStation Instrument Users

If you specified your own user names or passwords during the installation of an AIC, and you used *domain* users, it may become necessary to change their passwords on a regular basis.

1 Specify different user names or passwords in a *users.xml* file:

    a Provide local users in the form: *UserName="<AIC host name>\<user name>"*.

    OR

    Provide domain users in the form: *UserName="<domain name>\<user name>"*.

NOTE	Specify the same type of users (local or domain users) as during the AIC installation

Make sure that at least 41 different user names are provided. If you provide the same username twice, instrument access conflicts will arise.

    b Provide special passwords in the form: *Password="<user defined password>"*. At this stage, write the passwords in clear text. Encryption will take place when registering the accounts with Shared Services.

    Make sure that the password complies with the domain policy for passwords. Special characters must be escaped as follows:

Character	Escaped Character
<	<
>	>
"	"
'	'
&	&

   c Enforce addition of users to the Local Administrators group by setting the users attribute:

```
<users unsafe="true">
```

2 In order to meet any requirement for an initial password change, change domain user passwords in Windows for each user in the users.xml.

3 Register the new passwords with Shared Services:

   a On the AIC, select **Start >Command Prompt**.

   b Type *cd <ChemStation installation directory>\Core* and press **Enter**.

   c Type *registerCSData.exe /remote /InstrumentUsers="<Path to users.xml file>" /URL="net.tcp://<OpenLab Shared Services server>:6577/Agilent/OpenLAB/" /User="<name of OpenLab Shared Services admin user>" /password="<password of OpenLab Shared Services admin user>"* and press **Enter**.

    After registration, the passwords in the users.xml file will appear encrypted and will be only readable by the software.

4 Restart OpenLab Control Panel before launching the reconfigured instruments.

7 Fail Over Procedures

This chapter describes fail over procedures for Networked Workstations and Distributed Systems.

Introduction

OpenLab ChemStation is supported in a number of different configurations. All these configurations may require network communication beyond instrument connectivity. The networking infrastructure in different laboratories can have different levels of stability, reliability, and robustness.

OpenLab ChemStation provides a number of features to make it resilient against network or server outages. In case of a network or server outage, all running or queued sequences continue to run, and the data acquired is stored in the OpenLab ECM or OpenLab Server/ECM XT queue. The data can be uploaded to the central repository once the systems have been restored to normal operation. However, there will also be situations where users will want to start a ChemStation session during a network or server outage.

This chapter describes fail over and fail back concepts and procedures that ensure continued operation of ChemStation in case of network or instrument failures or server outages.

For a distributed system, this concept uses a workstation-based approach to remediate server unavailability. It requires dedicated failover workstation licenses that are commercially available.

Networking is involved in multiple areas:

- Instrument communication: Transfer of commands, methods and data
- Authentication: Startup of the OpenLab Control Panel and startup of ChemStation (from OpenLab Control Panel)
- Status reporting: ChemStation to OpenLab Shared Services server
- Data upload: ChemStation to central data storage
- Licensing: Licenses are retrieved from the License server (OpenLab Shared Services server by default)

Communication can be impacted if either the network or one of the following backend services is not available:

- Shared Services
- Central data repository (OpenLab ECM server or OpenLab Server)
- Windows Domain Controller, DNS server etc.
- License server

Depending on the system configuration, ChemStation has a number of connections to other systems.
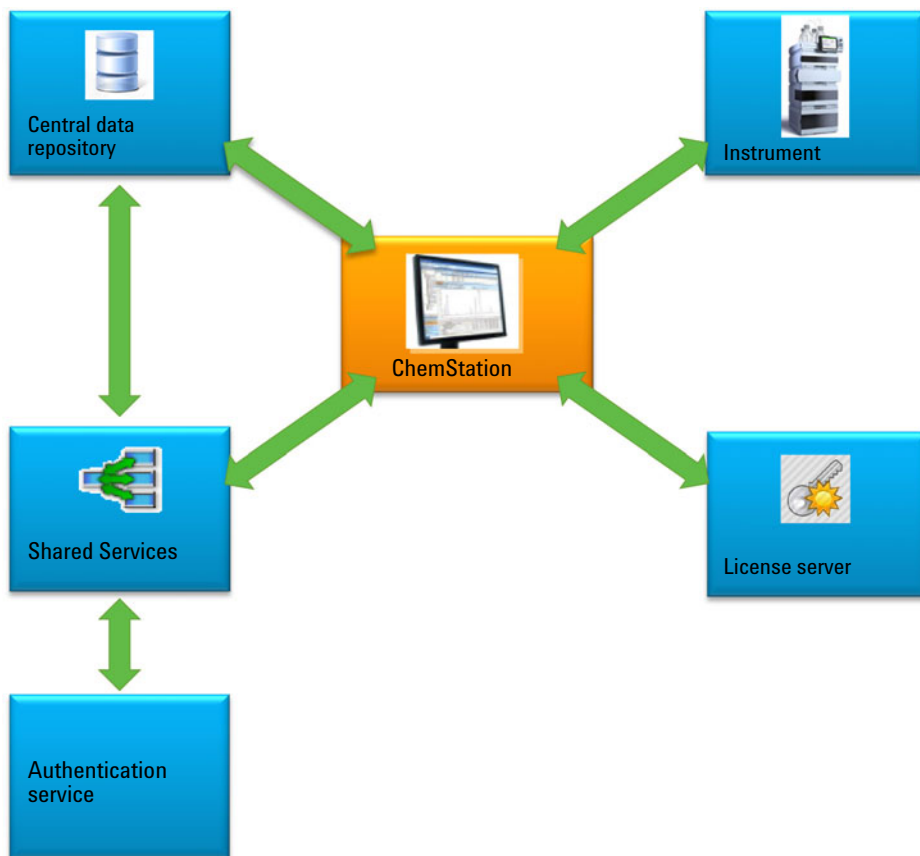
Figure 28   Connections to other systems depending on the system configuration

Table 9   Purpose of the various communication channels and backend systems

System	Purpose	Startup	Runtime	Comment
OpenLab Shared Services server	Always required. • Transfers authentication information. • Provides privileges for current user (authorization). • Provides information about license server location. • Receives and distributes instrument status. • Receives activity log.	Authentication/ authorization/ license server	Instrument status and activity log	Runtime communication is not mandatory - status information is discarded in case the server is not available. The activity log is buffered. Authentication may need a backend authentication service (e.g. Windows Domain Controller).
License server	Always required. Provides licenses for OpenLab ChemStation features.	Provides licenses	N/A	At runtime no further license checks are done. Licenses are mandatory. License server is installed on the OpenLab Shared Services server host machine.
OpenLab ECM server or OpenLab Server	Optional data storage backend.	Authentication (through OpenLab Control Panel and Shared Services)	Data upload and download	The server has two roles - authentication and backend storage. The runtime dependency for ChemStation is not mandatory, since ChemStation places uploads into a queue if the central repository is not available.

Scenarios

There are two main scenarios in case of a failure of a backend system or a network outage. In the first scenario the application (OpenLab Control Panel or ChemStation) is already running and continuous operation must be ensured. In the second scenario the application has not been started and has not yet established connections to one or more of the backend systems.

Scenario 1: ChemStation is Running

ChemStation acquires all of the required resources at startup:

- Licenses
- Privileges
- Connection token for central data storage (if applicable)

Once the ChemStation is started, the OpenLab Shared Services server and/or central data storage server may become unavailable:

- If the OpenLab Shared Services server is not available, then instrument status is no longer reported and activity logs are buffered for deferred upload. Data acquisition and upload to the central repository are still possible.
- If the central data storage is not available, then data upload to the central repository is no longer possible. Instead data is put into the queue and can be uploaded once the central data storage is available again.
- If the authentication provider is unavailable, re-authentication is not possible, i.e. it is not possible to switch to a different user or to log in in case of a session lock. You can break the session lock using the ChemStation Administration Tool (see "Session Lock Settings" on page 41).

NOTE   Data is automatically queued if the central data storage is unavailable. Once it is available again, queued data needs to be manually uploaded to the central repository (see "Troubleshooting" on page 134).

NOTE   In a distributed system, the existing ChemStation sessions on the AIC continue to run and acquire data. However, it is not possible to connect to these sessions from the remote client and to see their status in OpenLab Control Panel.

Scenario 2: ChemStation Startup

For ChemStation startup two main services are required:

- Licenses: Depending on the instrument configuration some licenses are mandatory in order to start up ChemStation. A core license is always required. This requires a connection to the license server.

- Authentication: When an authentication mode other than **None** is specified, the user must authenticate with his username and password. This requires a connection to the authentication backend (OpenLab Shared Services server, OpenLab ECM server, or Domain Controller).

Licensing   ChemStation needs to connect to a license server that holds valid licenses. If the license server is unavailable or ChemStation cannot connect to it, ChemStation cannot start up. If the central license server is not available it is possible to fall back onto a local licensing service. In this case failover licenses are required and must be configured on the fail over workstation. For details on populating the local licensing service with failover licenses, see "Prepare Local Failover Licenses (In Case the Central License Server Becomes Unavailable)" on page 124.

For a system with central data storage, ensure that you maintain a local copy on your workstation of all methods and sequences that are required if the central repository is unavailable. This may require periodic updates of the local methods and sequences from master methods and sequences kept in the central repository (for details, see "Prepare Local Methods and Sequences" on page 126).

Authentication Service   If any of the required authentication backends (OpenLab Shared Services server, OpenLab ECM server, or Domain Controller) is not available, users can connect to a local instance of Shared Services instead. This allows users to startup ChemStation. Instruments need to be set up in the local Shared Services database manually (for details, see "Prepare the Local Instrument Configuration" on page 123).

Since ChemStation workstations run a local copy of Shared Services and provide their own license server, traditional failover licenses would not apply. Instead, if the workstation failed, there could be a replacement workstation as part of a business continuity plan.

However, if the connection to OpenLab ECM is lost for a ChemStation using OpenLab ECM authentication, the workstation can not be started.

Networked Workstations

Preparations for Networked Workstations
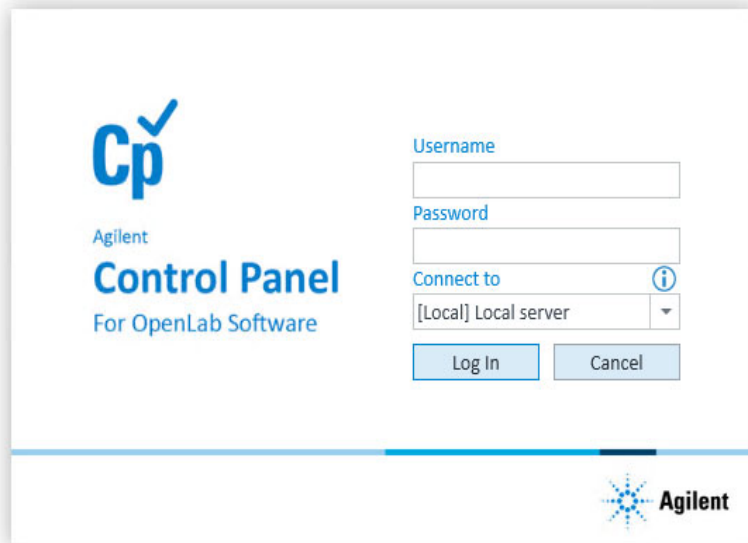
Connect to the Local Server

OpenLab ChemStation has an option to switch instances of Shared Services. This gives you the ability to use local Shared Services when the central OpenLab Shared Services server in a Networked Workstation or Distributed System becomes unavailable.

1 To connect to the local Shared Services instances, select **[Local] Local server** under **Connect to** when starting the OpenLab Control Panel.

NOTE   If you cannot select **[Local] Local server**, select the corresponding check box in the OpenLab Shared Services Maintenance tool (see "Manage Server Settings" on page 120).

OR

Alternatively, you can connect to the local Shared Services instance under **Administration >Local Configuration**. Select the local server, and click **Connect to Server**.
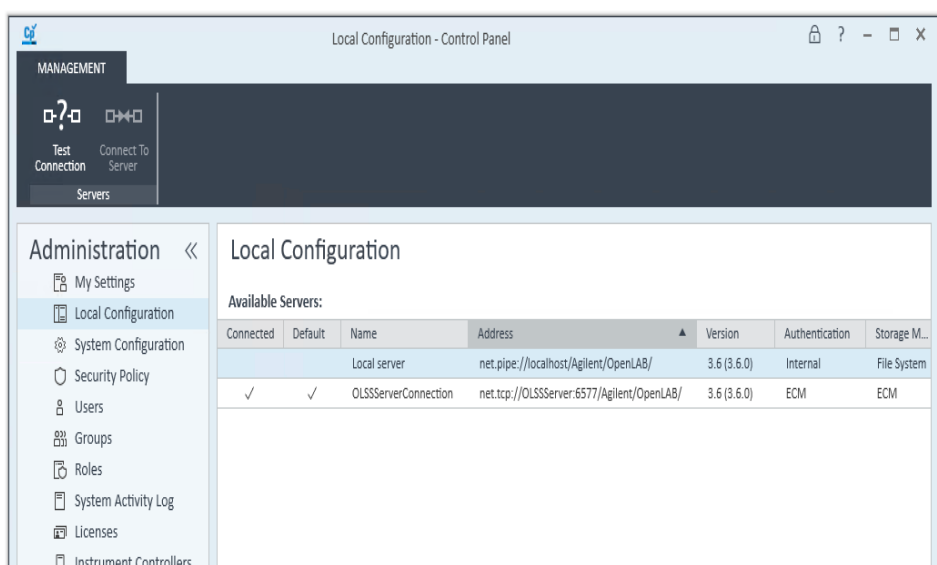
You can adjust the list of available servers from the OpenLab Shared Services Maintenance program (see "Manage Server Settings" on page 120).

Manage 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 in to the OpenLab Control Panel. 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 the client, therefore to change the server connections for a client, access the **Shared Services Maintenance** program installed on that client.

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

1 To start the application, go to **Start >All Programs >Agilent Technologies >Shared Services Maintenance**.
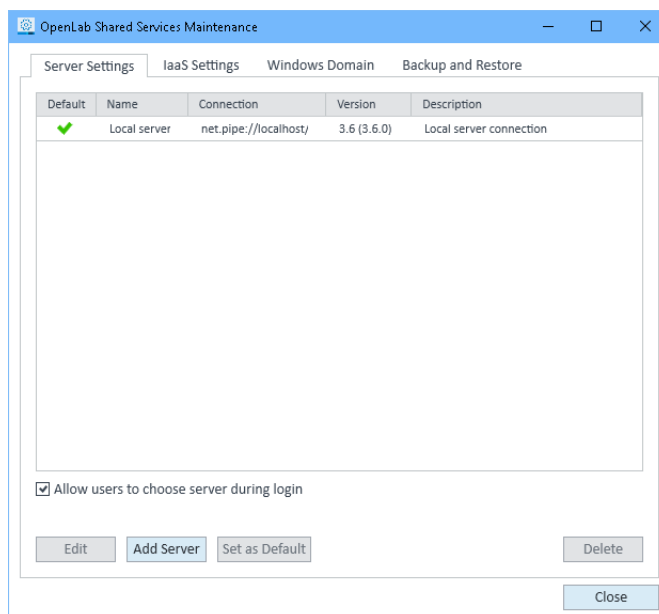
Figure 29   OpenLab Shared Services Maintenance (for example with Server Settings tab selected)

2 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 Shared Services server.

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

3 You can add more servers by clicking **Add Server**.

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

4 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.

Prepare Local Authentication Mode

If you are connecting to a local Shared Services instance, the default authentication mode is **None**. This allows users to work with the ChemStation without authentication. All users have all privileges. If user authentication is desired, use the authentication mode **Internal**. The other authentication modes (Windows Domain and OpenLab ECM) are not adequate for a fail over because they introduce dependencies to external systems.

The authentication mode **None** is the default and nothing needs to be done in preparation for the authentication mode **None**. If you wish to use the authentication mode **Internal** for a fail over configuration, you will need to switch to the local Shared Services instance, configure it to use the authentication mode **Internal**, and setup users and assign roles as required.

Prerequisites   On the central OpenLab Shared Services server, the **Allow users to choose server during login** check box must be selected in the OpenLab Shared Services Maintenance. See "Manage Server Settings" on page 120.

1   Connect to the local instance of OpenLab Shared Services (see "Connect to the Local Server" on page 119).
2   Set up the authentication mode **Internal**.
3   Set up users, and set up and assign roles as desired.
4   When finished, connect to the central OpenLab Shared Services server again.

Prepare the Local Instrument Configuration

In order to use the instruments that are configured on the central OpenLab Shared Services server and connected to a given workstation, they need to be made available in the local Shared Services instance on that workstation.

With ChemStation, you can use a batch file to make the instruments available on the workstation PC:

- Open a command prompt on the workstation and navigate to the ChemStation core directory in the ChemStation installation folder (e.g., C:\Program Files (x86)\Agilent Technologies\ChemStation\CORE).

- Run the OlssFailover.bat script file.

  This script copies instruments configured on the central OpenLab Shared Services to the local Shared Services database.

  If the local Shared Services instance has been configured to use an authentication other than **None**, provide the username and password of an administrative user as parameters in the syntax OlssFailover.bat [username] [password].

If you have made instruments available on the local Shared Services and then configured additional instruments, or removed instruments on the central OpenLab Shared Services server, repeat the above.

You can omit this preparation step and execute the batch file once the fail over has occurred. This has the advantage that all instrument configurations are current. However, we recommend executing the batch file ahead of time because a user in the laboratory may not able to execute a batch file and will not have the required user credentials available.

Preferably, put a procedure in place to ensure that the batch file is executed every time instruments are added or removed.

NOTE	All instruments that are part of a business continuity plan using the fail over licenses, must first be configured on the central OpenLab Shared Services server.

Prepare Local Failover Licenses (In Case the Central License Server Becomes Unavailable)

If the central license server becomes unavailable, the OpenLab application on a workstation PC can fall back to a local license service.

To prepare for this scenario, you can install failover licenses on the local license service. Failover licenses are additional workstation licenses that are installed on a workstation PC.

1 Obtain a failover license product.

For example, obtain product number M8205AA *Option 002: OpenLab ChemStation Failover Workstation License*. This failover license product includes a workstation core license, drivers, and add-ons for a workstation with up to four instruments.

2 Add the failover license product to the license pool in SubscribeNet.

NOTE	You can also use the licenses already available in your license pool. However, this is going to remove them from the pool of concurrent licenses.

3 In SubscribeNet, register the authorization codes, generate the failover licenses for the workstations, and configure the instruments for fail over mode.

Configure a license file with the required licenses, and enter the MAC Address of the workstation PC that the license file is to be put on. Store it locally on the workstation PC where you want to install it.

4 Connect to the local instance of Shared Services (see "Prepare Local Authentication Mode" on page 122).

5 In OpenLab Control Panel, go to the **Administration** page and click the **Licenses** node.

6 In the ribbon, click **Add**.

7   In the **Add Licenses** dialog browse to the location of the license file and add it.
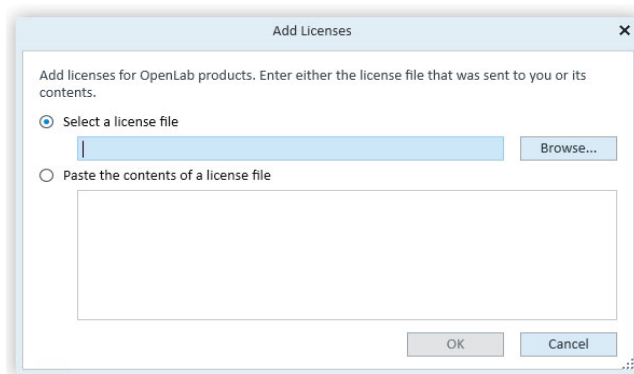
Figure 30   Entering the failover license for the local license service in the Add Licenses dialog

Prepare the Declaration of License Server (In Case the Central License Server is Still Available)

If the central data storage and/or Domain Controller are unavailable, and the central license server (on the OpenLab Shared Services server host machine) is still available, the central license server can still be used. However, it is necessary to use the local Shared Services instance with the authentication mode **None** or **Internal**. Example: OpenLab ECM server is unavailable, license server is available. Using local authentication is necessary since authentication cannot be against OpenLab ECM, but licenses can still be retrieved from the central license server.

The central license server needs to be declared in the local Shared Services instance.

1   Connect to the local instance of Shared Services (see "Prepare Local Authentication Mode" on page 122).

2   Go to **Administration >Licenses**.

3 Click **Change Server**. In the **Change License Server** dialog, enter the name of the central license server to be used.
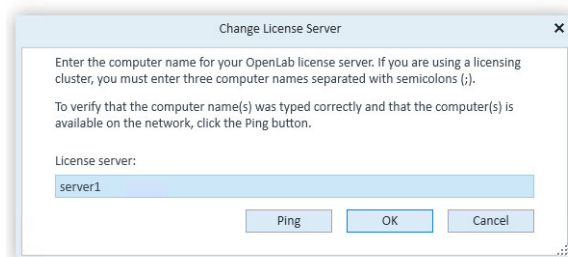
Figure 31   Change License Server dialog

4 Once the central license server has been declared in the local Shared Services instance, reconnect to the central OpenLab Shared Services server.

Prepare Local Methods and Sequences

For a system with central data storage, please ensure that you maintain a local copy on your workstation of all methods, sequence templates and report templates that are required if the central repository is unavailable. As mentioned before, this may require periodic updates of the local files from the master data kept in the central repository (see "Prepare the Local Instrument Configuration" on page 123).

Connect to the Local Server in Case of a Fail Over

If the OpenLab Control Panel cannot communicate with the OpenLab Shared Services server or with its authentication backend, the start-up screen will show a corresponding message (see). You can connect to the local server instead.

If OpenLab Control Panel cannot communicate with its authentication backend (OpenLab ECM server and/or Domain Controller), the OpenLab Control Panel application will not start. If this happens, disconnect the ChemStation workstation PC from the network while starting the OpenLab Control Panel. When starting a ChemStation workstation PC disconnected from the network, OpenLab Control Panel shows a dialog box that allows users to connect to the local server.

1 Select the **[Server]** entry, and click **Info** button. This will give you some diagnostics information. Click **Check connection** to ping the server.

2 If it has become clear that the network or server outage is going to be longer, login to the **[Local]** machine. If authentication is setup on the local Shared Services instance you will be asked for your credentials.

3 Since the instruments and licenses have been made available in the preparation steps, instruments can immediately be used. All instrument-related data, methods and configurations are available at their original locations. In addition, the instrument configuration is also available at its original location.

WARNING   **Inconsistencies between the local Shared Services configuration and the central Shared Services configuration**

✓ **Do not create new instruments or delete existing ones while connected to the local Shared Services instance.**

Restore the Connection

Once the connection to the central OpenLab Shared Services server or authentication backend is restored, the OpenLab Control Panel can be reconnected to the central OpenLab Shared Services server.

Preparations   Shut down ChemStation instances running on the local Shared Services instance before reconnecting to the central OpenLab Shared Services server.

1   When starting the OpenLab Control Panel, the default connection configured in the OpenLab Shared Services Maintenance will be used. If this is not the central OpenLab Shared Services server, select the **[Server]** entry under **Connect to**, and log in with the required user credentials.

    OR

    Alternatively, you can connect to the central Shared Services instance in OpenLab Control Panel under **Administration >Local Configuration**.

2   OpenLab Control Panel will connect to the remote OpenLab Shared Services server.

NOTE   Instruments are already available in the remote OpenLab Shared Services server and do not need to be reconfigured.

Distributed Systems

Preparations for Distributed Systems

If any of the required authentication backends (OpenLab Shared Services server, OpenLab ECM server or Domain Controller) is not available, or in case of a network outage, it is not possible to work directly on the client or the AIC.

There are different approaches for the distributed system. In general, the system offers a workstation-based approach to remediate server unavailability. It requires dedicated failover workstation licenses that are commercially available. Different scenarios that have to be considered include:

- No authentication provider
- No central OpenLab Shared Services Server
- No network

For instruments that are required to run continuously (24/7), Agilent suggests to set up a Networked Workstation on a separate PC using failover licenses, and to use this workstation in case of a fail over. This *fail over workstation* allows controlling instruments in case of a failure of any of the authentication back-ends as well as a network outage.

Prepare a Fail Over Workstation

The fail over workstation will be used in case ChemStation remote desktop sessions on the AIC are no longer accessible.

1 Determine required workstations and licenses.

As part of a business continuity plan, assess how many and which workstations and instruments need to be available as part of the fail over plan. Based on the assessment determine the required number of failover licenses.

An option to reduce hardware costs is to use fail over workstations as client PCs in a distributed system.

| NOTE | The OpenLab ChemStation hardware and software requirements for Networked Workstations apply. It is recommended to use a PC with two LAN cards: |

- One to connect directly to the instrument.

- One to connect to the laboratory network: This allows easy retrieval of data once systems have been restored to normal operation.

2 Determine IP address needs.

The fail over workstation may need a different IP address to connect to the instrument to support fail over mode.

Ensure common network settings for the LAN cards of the fail over workstation and the AIC. Thus you can reuse the instrument's IP address.

If the instrument is set up on the LAN (that is, not directly connected to the AIC), the IP-address of the instrument needs to be adapted to the subnet of the fail over workstation's network card.

After the fail over has occurred, and systems have been restored, the instrument's configuration needs to be restored before it is reconnected to the AIC.

3 Determine additional equipment needs

You may require additional hardware such as switches, network cabling, etc.

4 Install a ChemStation Networked Workstation on each fail over workstation. Add central data storage and configure the same database server as for the AIC. Register in the central Shared Services database.

5 Execute IQ/OQ procedure if required.

6 While connected to the central OpenLab Shared Services server, configure all instruments for which you require continued operation in case of an anomalous event.

Use a different instrument name, e.g. "<instrument name>_failover".

Start a session for each instrument (online or offline) and configure the upload path in the preferences.

7 Lock all failover instruments using the **Lock** function in OpenLab Control Panel.

During normal operation these instruments remain locked.

8 Close OpenLab Control Panel, and start it again. This time, connect to the *local* Shared Services database.

9 Recreate the instruments on the local server using the script OlssFailover.bat developed for networked workstations (see "Prepare the Local Instrument Configuration" on page 123).

10 If required, prepare the authentication mode on the local server.

On the fail over workstation, the local Shared Services must use the authentication mode **None** or **Internal**.

In case of internal authentication, you must set up fail over users and roles (see "Prepare Local Authentication Mode" on page 122).

11 Install failover licenses (see "Prepare Local Failover Licenses (In Case the Central License Server Becomes Unavailable)" on page 124).

- If the license server remains available (that is, only the authentication provider becomes unavailable):

  The central license server needs to be declared in the local Shared Services (see *Change the license server* in the OpenLab Control Panel Help).

- If the license server becomes unavailable, too:

  Failover licenses need to be available in the license pool. Generate the corresponding license file in SubscribeNet, and add it to the fail over workstation using the local Shared Services instance.

  This licenses file is then bound to the MAC address of the fail over workstation.

12 Make all required methods, sequence and report templates available locally.

Consider using acquisition only methods for the anomalous event, and to postpone processing until the system has been fully recovered.

13 When the anomalous event is over:

- If you want to use the workstation as a normal client or Networked Workstation, switch back to the central OpenLab Shared Services database.

- If the PC is a dedicated fail over workstation, turn the workstation off.

In your Standard Operating Procedures, define that the usage or changed purpose of the machine needs to be documented.

NOTE   Fail over workstations need regular maintenance. They require the same level of operating system updates and application software updates as the distributed system.

Use the Fail Over Workstation

During an anomalous event, the ChemStation instances on the AIC continue to run even if the server is unavailable.

To make an instrument available during an anomalous event, follow the instructions below.

1 Check whether the sequences running on the AIC are completed and the instrument is idle. To confirm this, open the sequence folder and review the log files.

2 Reconfigure the instrument. This step depends on the topology used.

- The AIC has two network cards; the instrument is directly connected to one of them.

    Disconnect the instruments from the AIC (by removing the network cable from the instrument) and connect the instrument directly to the fail over workstation.

- The instrument is connected to the laboratory network.

    You may need to change the instrument's IP address.

3 On the AIC, close the ChemStation sessions using the Windows Task Manager.

4 Power on the fail over workstation, or use the dedicated Networked Workstation, and connect to the local server.

Since the instruments and licenses have been made available in the preparation steps, instruments can immediately be used on the fail over workstation.

5 Start acquiring data.

The instrument name now includes the term *failover*. The data is securely buffered in the queue.

Restore the Connection

Once connection to the OpenLab Shared Services server or central data storage is reestablished, proceed as follows:

NOTE   Once systems have been restored to normal operation, instruments may need to be reconfigured to their original IP-addresses before connecting them to the AIC again.

1 On the fail over workstation, connect to the central OpenLab Shared Services server.

2 Start the online or offline ChemStation instrument sessions and resume the queue.

Acquired data will be uploaded to the central repository.

The data acquired during the anomalous event will have the user configured in the failover mode as the Acquisition User.

- If authentication mode **None** was configured in the local Shared Services database, the user **System** will be the Acquisition User.

- If a fail over user was set up for the failover scenario, this fail over user will be the Acquisition User.

3 Close the instrument sessions.

4 Power off the fail over workstation.

5 Reconnect the instruments to the AIC by unplugging the network cable from the fail over workstation and connecting the LAN cabling with the AIC. If applicable, reassign IP addresses to the instruments.

6 On the ChemStation Client, launch OpenLab Control Panel and connect to the central OpenLab Shared Services server. Check the status of the individual instruments in the **Instruments** panel to ensure they are connected and available.

8 Troubleshooting

The chapter gives some troubleshooting hints. Please see also the OpenLab ChemStation Workstation Maintenance Guide (CDS_CS_maintenance.pdf) and the Troubleshooting section in the OpenLab ChemStation Networked and Distributed System Installation Guide (CDS_CS_Install_NwWS-DS.pdf).

Error messages at OpenLab Control Panel Startup

Connection to Shared Services failed

When both the ECM server and the OpenLab Shared Services server are not available, the user cannot start the OpenLab Control Panel. Since ChemStation is launched from OpenLab Control Panel, working with ChemStation is not possible and the fail over procedure might need to be utilized.

Probable cause	Suggested actions
1 The ECM server or Shared Services server is not available.	In the OpenLab Control Panel start screen, log in to the local instance of the OpenLab Shared Services. For details on this failover scenario, refer to the chapter on *Fail Over Procedures* in this guide.

Alerts and Error Messages at ChemStation Startup

Your Transfer Settings (Remote Data Path) differ from the current connection. Change Transfer Settings now?

At every startup, Agilent ChemStation checks whether all necessary information is provided for transferring data to the central data storage. This message is shown if the information on the Server provided in the Transfer Settings differs from the server configured in OpenLab Control Panel.

Probable cause	Suggested actions
1 The Transfer Settings in ChemStation differ from the configuration in OpenLab Control Panel.	Make sure that the correct information on Server, Account, and Path is provided in the Transfer Settings (**ECM >Preferences >Transfer Settings** or **CM >Preferences >Transfer Settings**, click **Get Server**).

OpenLab ECM or OpenLab Server is not available after login

If the connection to the ECM or OpenLab Server is interrupted after login to the OpenLab Control Panel, the user has already been authenticated by the external system. In this case, ChemStation knows the current logged-in user.

When the ECM or OpenLab Server becomes unavailable, ChemStation automatically tries to reestablish the user login.

The **Load and Save** functions are accessible, but an alert informs the user about the interrupted connection to the central data storage system.

While acquiring data, the automatic transfer of data to the central data storage cannot be completed. The user is notified by an error message and must manually resume the queue to upload the data as soon as the connection is reestablished (**ECM >Manage Queue** or **CM >Manage Queue**).

As soon as the ECM or OpenLab Server is available again, all tasks are available without restarting the application. A new login is not required.

For further troubleshooting, please contact the administrator for the central data storage system.

Error Messages in the Queue Management

Independent of Storage Type

`The queue already contains items`

Probable cause	Suggested actions
1 There are items in the queue that have been queued before the current item.	Process queue in the correct order. If necessary, export items that can't be resolved.

`Invalid URI: The format of the URI could not be determined`

Probable cause	Suggested actions
1 In the preferences, the ECM or OpenLab Server is missing or has been entered by name only, not as URI (http:\\servername\).	Correct the server in the preferences, e.g. by using **Get Server**. Save existing items in the queue to the local file system. After correcting the server setting, reprocess the data.

OpenLab ECM-Specific Messages

`Current connection to '<account1>', expected connection to '<account2>'`

Probable cause	Suggested actions
1 ECM Account setting in Preferences differs from current connection.	Correct the Transfer Settings.

Currently no connection, expected connection to '<server>'

Probable cause	Suggested actions
1 The ECM Server is not available.	Contact your ECM administrator.
2 In the OpenLab Control Panel, the storage is not set to ECM.	Select ECM as the storage type in OpenLab Control Panel, or ask your system administrator to do so.

You do not have permission to create a new Drawer/Folder.

Probable cause	Suggested actions
1 You do not have appropriate privileges to create the Drawer or Folder in ECM.	Ask your administrator to give you the corresponding privileges or to create the needed directories.

You do not have permission to add files.

Probable cause	Suggested actions
1 You do not have appropriate privileges to save files to the specified location in ECM.	Ask your administrator to give you the corresponding privileges.

Unable to upload (filename). This file is currently checked out to another user and may not be updated. (error -1).

Probable cause	Suggested actions
1 Another user has checked out the file from ECM.	The other user has to check in the file before you can upload the file.

OpenLab Server-Specific Messages

No connection to remote storage established

Probable cause	Suggested actions
1 The Content Management service is not available.	Contact your Content Management administrator.

Connection to remote storage is broken.

Probable cause	Suggested actions
1 The connection to OpenLab Server has become unavailable during the current session.	• Wait for the connection to be reestablished. • Contact your OpenLab Server administrator.

You cannot upload a file that is checked out by another user

Probable cause	Suggested actions
1 The file you want to upload is currently checked out by another user.	Ask the other user to check in the file, then upload again.

You do not have appropriate permissions to create a folder

Probable cause	Suggested actions
1 You do not have the privilege to create content in the Content Management system.	Ask your administrator to give you the **Save data to storage** privilege.

Other Error Messages

Access to the path <local ChemStation path> is denied.

Probable cause	Suggested actions
1 ChemStation folders are protected by Secure File I/O, and the password for the Secure File I/O user has expired.	• Shut down the ChemStation. Update the password for the Secure File I/O user account. Provide the new password in the ChemStation Administration Tool. Then start the ChemStation again.
	• See the chapter about *Folder Protection with Secure File I/O* in the *ChemStation Workstation Administrator's Guide*.

9 Appendix

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. With ChemStation, the following additional default roles are available:

- ChemStation Administrator
- ChemStation Lab Manager
- ChemStation Analyst
- ChemStation Operator

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 10   Project Management

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

Table 11   E-Signature

Name	Description
E-Signature Sign Data Files	User can sign data files if user authentification is on.

Table 12   Intelligent Reporter templates

Privilege	Description
Edit Intelligent Reporter report template	Only relevant for OpenLab ECM Intelligent Reporter: This privilege is required to edit report templates in the Reporter Client

Table 13   ChemStation: Control

Privilege	Description
Run Acquisition	Start acquisition (single sample or sequence).

Table 14   ChemStation: Data

Privilege	Description
Delete Data	User can delete data files in the navigation table.
Load data using not configured path	If Secure File IO is enabled, this privilege is required for … • loading data from unprotected paths • adding paths that are not empty to the ChemStation (**Preferences** dialog)
Manual Integration	User can perform manual integration.
Save data to storage	Interactive saving of data to the central data storage system.

Table 15   ChemStation: Instrument

Privilege	Description
Modify instrument configuration	User can modify the instrument configuration parameters.

Table 16   ChemStation: Logbook

Privilege	Description
Clear Logbook	Clear the current logbook.
Save Logbook	Save the current logbook.

Table 17   ChemStation: Method

Privilege	Description
Edit calibration table	Create and modify the calibration table; change calibration settings.
Delete method	Delete a master method from the disk through the file menu.
Edit integration events	Modify integration events and perform Auto Integration.
Edit ion labels	Edit options for ion labels (LC/MS only).
Edit system suitability	Edit noise ranges and performance limits.
Enable audit trail	Enable the audit trail for a specific method.

Table 17   ChemStation: Method

Privilege	Description
Load method from not configured path	If Secure File IO is enabled, this privilege is required for … • loading a method from an unprotected path • saving a method to an unprotected path • adding paths that are not empty (**Preferences** dialog)
Modify instrument method	Modify instrument method parameters.
Modify method properties	Modify Run Time Checklist and Method Information.
Perform method recalibration	Perform interactive recalibration.
Save method changes	Save method changes (includes Update Sequence/Master Method in Data Analysis view).

Table 18   ChemStation: Report

Privilege	Description
Preview/print report	User can preview/print a report.
Modify report	User can modify report calculation/print style and can edit Instrument Curves dialog.
Lock/unlock report template items	Only relevant with Intelligent Reporting: User can lock or unlock report items and composite groups in a report template.

Table 19   ChemStation: Security

Privilege	Description
Break session lock	Unlock a ChemStation session locked by other users.
Command line	Turn on / off the command line
Manage transfer queue	Access to the Transfer Queue and the Queue Management.

Table 19   ChemStation: Security

Privilege	Description
Modify storage transfer preferences	Modify transfer settings for data upload to the central data storage system.
Take over ChemStation Remote Session	Only relevant for ChemStation in a Distributed System: User can take over a running remote session.

Table 20   ChemStation: Sequence

Name	Description
Change priority in run queue	User can submit samples or sequences to the front of the queue, and change the order of items in the run queue.
Delete entries from run queue	User can remove queued samples or sequences from the run queue.
Delete sequence	User can delete sequence templates from disk through the file menu
Edit sequence summary	User can modify the classic sequence summary report and extended statistics settings.
Load sequence from not configured path	If Secure File I/O is enabled, this privilege is required for … • loading sequence templates from unprotected paths • saving sequence templates to unprotected paths • adding paths that are not empty (**Preferences** dialog)
Reprocess	User can reprocess a sequence.
Save sequence template	User can save sequence templates locally (on workstation or AIC).

Table 21   ChemStation: View Access

Privilege	Description
Access Data Analysis view	User has access to Data Analysis view.
Access Diagnostic view	User has access to Diagnostic view.

Table 21   ChemStation: View Access

Privilege	Description
Access Method & Run Control view	User has access to Method and Run Control view.
Access retention time lock	User has access to the Retention Time Lock menu (GC only).
Access retention time search	User has access to Retention Time Search menu (GC only).
Access Review view	User has access to Review view
Access Tune view	User has access to Tune view (LC-MSD ChemStation only).
Access Verification view	User has access to Verification (OQ/PV) view.
Access Report Layout view	User has access to Report Layout View, ability to create/edit/save report templates.
Enable Batch view	Enables all operations in Batch view.

Instrument Privileges

Table 22   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 23   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	Can change security settings. Can edit (add, change etc) users, groups and roles. *Note:* A user with this privilege can grant himself access to all settings in OpenLab Shared Services. Be careful who you grant the Manage Security privilege.
Manage instrument controllers	Can edit AIC configuration, manage the AICs in configuration UI.
Unlock any locked UI	Can login into any locked portal or instrument session (will be a re-login), even if privately locked.

Table 24   Content Management

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

OpenLab ECM Privileges related to ChemStation

The privileges described in the following table must be assigned to at least one of your roles in order to become active.

Table 25   List of ECM related privileges

Privilege	View	Edit	Delete	Add	Run	Description
Content: File	X			X		Minimum privilege for ChemStation to access ECM • View ECM Properties in ChemStation
Content: File Filtering		X				Minimum privilege for ChemStation to access ECM • Add files manually to an ECM folder
Content: File Revisions	X					• View revisions in ChemStation
Content: File Type [XLSX]		X		X		• Add and check in files with an .xlsx extension
Content: Folder	X	X		X		Minimum privilege for ChemStation to access ECM • View ECM Properties in ChemStation
Content: Folder Access Properties		X				• View and change any folder property tab
Content: Rekey File					X	• Rekey files in ECM e.g. with XML Filters
System: Advanced Search					X	• Use the Advanced Search in ChemStation
System: Audit Trail	X					• View ECM Properties in ChemStation
System: Filtering Configuration	X					• View or change the filtering configuration • Use attribute extraction services and to manage user-defined attributes
System: indexing Configuration	X					Minimum privilege for ChemStation to access ECM. • Privilege to view ECM Properties in ChemStation

Table 25   List of ECM related privileges

Privilege	View	Edit	Delete	Add	Run	Description
System: Quick Search					X	• Use Quick Search in ChemStation
System: Super Object	X					Privilege is mandatory for OLIR
System: Project	X					• View projects in OLIR
System: Project Access	X					• Access projects in OLIR

Sales and Support Assistance

Please check the following web site for your local sales and support contact:

https://www.agilent.com/en/support

Agilent Community

To get answers to your questions, join over 10,000 users in the Agilent Community. Review curated support materials organized by platform technology. Ask questions to industry colleagues and collaborators. Get notifications on new videos, documents, tools, and webinars relevant to your work.

https://community.agilent.com/

In This Book

This guide details on administration and maintenance for distributed systems of LTS 01.11 with a content management system (OpenLab ECM, OpenLab Server, or OpenLab ECM XT). It also describes the settings required by 21 CFR Part 11, and it provides information on the workflows for ChemStation using a central data storage.

Agilent