



Agilent OpenLab Server and OpenLab ECM XT

Administration Guide

Notices

Document Identification

DocNo D0013947 Rev. C.00
02/2024

Copyright

© Agilent Technologies, Inc. 2024

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

Agilent Technologies, Inc.
5301 Stevens Creek Blvd.
Santa Clara, CA 95051

Software Revision

This guide is valid for the 2.7 revision of the Agilent OpenLab Server and OpenLab ECM XT program until superseded.

Warranty

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

Technology Licenses

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

Restricted Rights Legend

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

Safety Notices

CAUTION

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

WARNING

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

Content

1	Introduction and Overview	7
	OpenLab Server/ECM XT Server System Architecture	8
	21 CFR Part 11 Support	9
2	Control Panel and Security	10
	License Management	11
	FlexNet Publisher Suite	11
	Diagnostics	13
	Administrative Reports	14
	Security	15
	System Activity Log	15
	Authentication provider	16
	Users, groups, and roles	16
	Security policy	20
	Reactivate Content Management After Changing Host Server	21
3	Securing the System	22
	Overview	23
	Procedures for Securing OpenLab Server/ECM XT Servers	25
	Generate certificates	25
	Create the keystore	26
	Generate a Certificate Signing Request (CSR)	27
	Request the certificate	27
	Install certificates into keystore	28
	Configure OpenLab Server/ECM XT Reverse Proxy	29
	Configure port 52088 to use a commercial certificate	31
	Reconfigure AlfrescoTomcat Shared Services connection	32
	Optional: Reconfigure access to Content Management or for a DNS alias	32
	Force traffic to HTTPS for OpenLab Server/ECM XT	33
	Configure a CSRF (Cross-Site Request Forgery) filter	35
	Reboot and reactivate from OpenLab Control Panel	35

Index Server Configuration - 4-Server Systems Only	37
TLS/SSL Disabling	38
4 Maintenance	39
Routine Server Maintenance	40
Update database statistics	40
Maintenance Procedures for PostgreSQL database	40
Maintenance Procedures for SQL Server	42
Monitor resource use on OpenLab Server/ECM XT server	44
Additional best practices	45
Windows Domain	46
Update the Domain, User name, or Password for your server	46
Enable read permission for a user	46
Server Settings	47
FTP Server Protocol	48
Enable the OpenLab Server/ECM XT server as an FTP server	48
Connect to the OpenLab Server/ECM XT server through an FTP protocol	48
Disable the OpenLab Server/ECM XT server as an FTP server	49
Archiving	50
Modify Automatic Archiving Execution Schedule	50
Quarantine	52
5 Backup and Restore Procedures	54
Important Information about Backup and Restore	55
Using Amazon Web Services S3 as a backup location	56
Creating a Disaster Recovery Plan	57
Using the Backup and Restore Utilities	59
Back Up OpenLab Server/ECM XT Using the Backup Utility	61
Procedures for using the Backup Utility	63
Backup verification	67

Incremental backup of PostgreSQL databases	69
Configure incremental backup using Incremental Config Tool	69
Configure custom data directory of PostgreSQL database	70
Configure custom data directory of Data Repository PostgreSQL database	71
Restore OpenLab Server/ECM XT Using the Restore Utility	72
Restore a system with PostgreSQL or Microsoft SQL database	73
Reconfiguration during restore	78
Using the Backup and Restore Scripts	80
System preparation	81
Back up OpenLab Server/ECM XT using the backup script	83
Restore OpenLab Server/ECM XT using the restore script	85
Change temporary database location for backup and restore procedures	89
6 Manual Backup and Restore Procedures	90
Manual OpenLab Server/ECM XT Server Backup Procedure	91
Perform a manual system backup	92
Manual Data Repository database backup	98
Manual OpenLab Server/ECM XT Server Restore Procedure	100
Data Migration of Manual Backup on Different Server	108
7 Manual Hot Backup Procedures	110
Backup Guidelines	111
Overview	112
Back Up the Solr Index	113
Scheduled Backups	113
Manually Back Up the Database	117
Back up an SQL Server database	118
Back up a PostgreSQL database	121
Back up an Oracle database	124

Back Up the Data Repository	128
Manually Back Up the Content Store	129
Manually Back Up OpenLab Server/ECM XT Server and Index Server Configuration Information	130
Back Up Custom Certificates	130
Store the Back Up Files	131
Manually Restore the System	132
Restore the Solr Index	133
Restore an SQL Server database from a backup	133
Restore a PostgreSQL database from a backup	136
Restore an Oracle database from a backup	138
Restore the Data Repository	139
Rebuild the Activity Log Index	139
8 Upgrading and Reconfiguration	141
Upgrading the OpenLab Server/ECM XT Server when the Operating System Changes	142
OpenLab Server/ECM XT Server Reconfiguration	142
Bring Down OpenLab Server/ECM XT	143
Make Changes to the Infrastructure	143
Run the OpenLab Server Configuration Utility	150
Bring Up OpenLab Server/ECM XT	154
Add Additional Content or Archive Store	154
9 Appendix	155
Sales and Support Assistance	156
Agilent Community	156

OpenLab Server/ECM XT Server System Architecture 8

21 CFR Part 11 Support 9

This guide is targeted for the system administrator of OpenLab Server/ECM XT. Basic administrative knowledge of the underlying database management system is required. In addition, familiarity with Windows Backup and Restore is also required.

This guide provides information about administrative and maintenance procedures that must be taken to ensure that OpenLab Server/ECM XT remains stable and performs well over time.

It also provides guidelines for 21 CFR Part 11 support, using the Control Panel to access Shared Services control features, taking regular backups of your server, and restoring your server if a disaster such as a server hardware failure occurs.

Tools mentioned in the document are for demonstration of the concepts. If your organization has standardized on other tools, you may use them as long as you can confirm that they perform the identical tasks.

OpenLab Server/ECM XT Server System Architecture

The OpenLab Server/ECM XT server is installed on a server running a Microsoft Windows Server operating system. Refer to the *Agilent OpenLab Server and ECM XT Hardware and Software Requirements Guide* for a list of supported operating systems. The OpenLab Server/ECM XT server includes Shared Services (OLSS) and the Content Management databases, which are automatically installed on the same machine.

Changing the server domain after the installation requires direct consultation with Agilent Support.

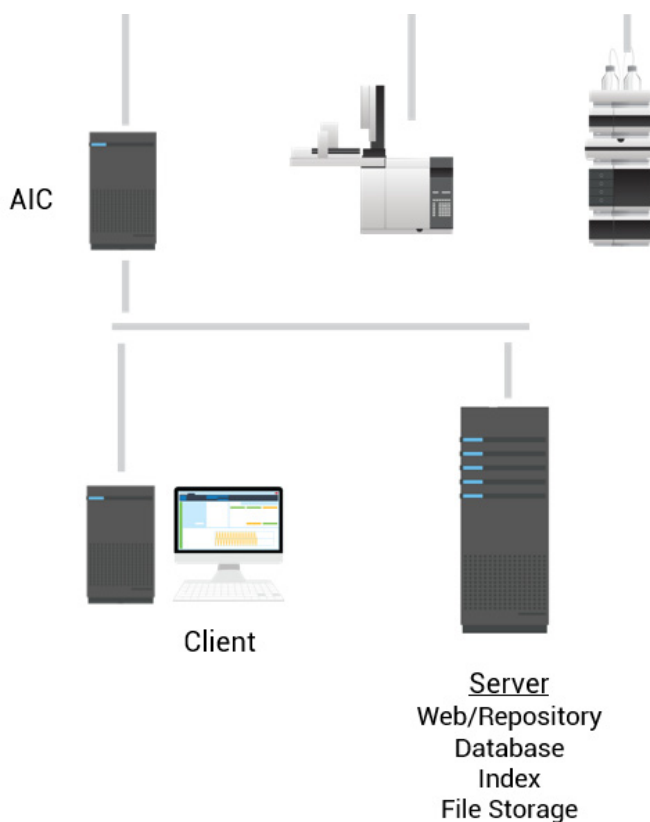


Figure 1. OpenLab Server/ECM XT server all-in-one system architecture

Client machines that access the OpenLab Server/ECM XT server use the following components:

- **Content Management Web client** - OpenLab Server/ECM XT provides a thin client Web-based user interface that can be accessed using a Web browser. The Web interface provides access to the Content Management folders and files.
- **Control Panel** -The Control Panel is the user interface that provides access to administrative functions used for managing the OpenLab Server/ECM XT server and Shared Services.

21 CFR Part 11 Support

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



2

Control Panel and Security

License Management 11

Diagnostics 13

Administrative Reports 14

Security 15

Reactivate Content Management After Changing Host Server 21

Use the Control Panel to access Shared Services control features such as security policy and central configuration. These features are described in more detail in this chapter.

License Management

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

FlexNet Publisher Suite

OpenLab Server/ECM XT uses a third party tool called *FlexNet Publisher Suite* from Flexera to manage the licenses. The required licensing server components are installed by default on the OpenLab Server/ECM XT Server.

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

Before adding a license file, you must first purchase the license and generate the license file using SubscribeNet. For more information on generating new license files, see the *Agilent OpenLab Server and OpenLab ECM XT Installation Guide*.

License management in the Control Panel provides the following functions:

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

For more information on adding license files and viewing the license properties, see the Control Panel online Help.

The following properties are shown for installed licenses:

- **Feature:** This indicates the type of license used.
- **Version:** If a license is versioned, you can see the version number. For licenses that are not versioned, the version is always shown as 2.0.
- **In Use (Available):** This indicates the number of licenses that are currently in use and, in brackets, the total number of licenses. With OpenLab Server/ECM XT licensing strategy, a license is only in use as long as a software instance is running (see **“License Management”** on page 11).
- **Expiration:** If the license is only valid for a certain period, the expiration date is displayed.
- In the **Alerts** pane, you are informed if the number of available licenses has gone down to zero for a specific feature, or if you have started a software instance that requires a license that is unavailable.

Diagnostics

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

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

Content Management registers failed uploads in the server logs. Depending on the upload failure, the debug information will be written either into:

- C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\logs\alfresco.log
- or
- C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\logs\datastore.log

Administrative Reports

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

- **Roles and Privileges Report**

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

- **User's and Group's Role Assignment Report**

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

Security

System Activity Log

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

The following types of events are recorded:

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

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

NOTE

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

Authentication provider

Authentication providers are used to prove the identity of users who log in to the system.

During the installation, OpenLab Server/ECM XT is automatically activated and configured using internal authentication with a default user, **admin**, and password, **openlab**. On first login, the system will require the user to change this password before proceeding. You may then change the authentication mode, if necessary.

OpenLab Server/ECM XT supports the following Authentication providers:

- **Internal**

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

- **Windows Domain**

You import existing Windows users into Shared Services. The authentication is done by a Windows Domain within the Enterprise. Shared Services only use the identity and password of the mapped users; roles and privileges for OpenLab Server/ECM XT are still configured with Shared Services.

Users, groups, and roles

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

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

The roles are equipped with numerous specific privileges, which define what the users, are allowed to view or do in Control Panel and in Content Management.

Table 1 describes the user credentials.

Table 1. User credentials

Value	Description	Mandatory
Name	Username to log in to the system	Yes
Description	Additional information about the user (e.g. department, function etc.)	No
Password	Password for the user; minimum password length is defined in the Security Policy	Yes
Email	Email address of the user	No
Full name	The full (long) name of the user	No
Contact information	General contact information (e.g. telephone number, pager etc.)	No
Account is disabled	Select the check box to disable a user. Disabled users cannot log in. Users may be automatically disabled after too many failed login attempts. If a user is disabled, a corresponding message is displayed instead of the check box. After a given time (see Account lock time in the Security Policy settings), the user is automatically enabled again.	No
User cannot change password	Flag that indicates whether the user can change their own password. The flag is false by default (that is, users CAN change their passwords).	No
User must change password at next logon	If set to true, the user has to change their 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
Password never expires	If set to true, the user never needs to change their password.	No
Group Membership	Assign the user to the relevant groups.	No
Role Membership	Assign roles directly to the user.	No

Users

If you use Windows domain as an external authentication provider you cannot create 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 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, unmap the user in the Control Panel. The user continues to exist in the external authentication system.

Groups

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

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

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

Roles and privileges

Roles are used to assign privileges to a user or a user group globally. The system contains a list of predefined roles, which are installed as part of the system installation (see [Table 2](#)). Each role has certain privileges assigned.

When you assign privileges to a role, 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.

NOTE

Starting with v2.7, Content Management users will be required to have the “View Activity Log” privilege to view the activity log and all its entries. During an upgrade from previous versions, all users will be assigned the “Access Activity Log” role, so users do not lose functionality. After an upgrade, if you do not want a user to have access to the activity log, you must remove that role from the user.

Table 2. Content Management predefined roles

Privileges	Content Management Roles
Project: View Project or Project Group View projects in Control Panel; view, preview, download Content Management content	<ul style="list-style-type: none"> • Content Management Reader • Content Management Contributor • Content Management Administrator • Content Management Approver • Archivist • System Administrator • Everything
Project: Edit Content of Project Create, update, and copy files and folders	<ul style="list-style-type: none"> • Content Management Contributor • Content Management Administrator • Content Management Approver • System Administrator • Everything
Project: E-Signature Sign Data Files Apply electronic signatures to files	<ul style="list-style-type: none"> • Content Management Approver • System Administrator • Everything
Project: Delete Content of Project Delete or move content associated with a project	<ul style="list-style-type: none"> • Content Management Administrator • Everything
Project: Access Content Using Web Client Access project content using the Web client	<ul style="list-style-type: none"> • Content Management Reader • Content Management Contributor • Content Management Administrator • Content Management Approver • Everything
Administrative: Manage Templates Apply PDF templates to folders	<ul style="list-style-type: none"> • Content Management PDF Template Manager • Everything
Administrative: Archive Content Online archive, set up automatic archive tasks, and de-archive files and folders	<ul style="list-style-type: none"> • Archivist • Everything
Administrative: Manage Security Create users, groups, and roles; assign security roles; move files and folders in Content Management, delete files and folders in Content Management that are not in a project	<ul style="list-style-type: none"> • System Administrator • Everything
Administrative: View Activity Log Access activity logs	<ul style="list-style-type: none"> • Activity Log Access • System Administrator • Everything

Security policy

With the authentication provider **Internal**, you can set the parameters described in **Table 1** in the Control Panel. With **Windows Domain** authentication, you can only set the inactivity time in the Control Panel; all other parameters are defined by the external system. **Table 3** describes the security policy settings.

Table 3. Security policy settings

Setting	Description
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 .
Password expiration period (days)	The default value is 0 days. This period can be reset by the OpenLab system administrator. When the user tries to log in after this period, the system will ask them 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 .
Maximum unsuccessful login attempts before locking account	If a user tries to log in with invalid user credentials a defined number of times, the user is locked out of the system for a certain period (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 .
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 they 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 is also used to set the time-based session lock in ChemStation. The default setting is <i>10 min</i> . Set the value to zero to never lock.
Single Sign-On	With Single Sign-On enabled, the user will not see the Control Panel login screen. Only available for authentication provider Windows Domain . Single Sign-On is not supported with OpenLab ECM XT backends.

Reactivate Content Management After Changing Host Server

To reactivate Content Management after specifying a new host server, use the following procedure.

- 1 Log into Control Panel. If upgrading, make sure to log in as a user that existed before the upgrade.
- 2 Click **Administration > System Configuration > Edit System Settings**.
- 3 In the **Please select another option from the list if you wish to use a different storage type** drop-down list, select **Content Management**, and then click **Next**.
- 4 Select **Change Server** and enter the URL of the Content Management server you wish to use.
- 5 Click **Activate**.
- 6 In the **Enter credentials** dialog box, type your Username and Password, and (if required) select your Domain.
- 7 Click **OK**.
- 8 You will see a message that Content Management was successfully activated. Click **OK**.



3 Securing the System

Overview 23

Procedures for Securing OpenLab Server/ECM XT Servers 25

Index Server Configuration - 4-Server Systems Only 37

TLS/SSL Disabling 38

Use these procedures to create and install certificates for Content Management and configure the OpenLab Server/ECM XT Server.

Overview

The procedures in this section apply to All-in-one server, 2-server, and 4-server topologies.

Certificates are required to enable trusted, secure network communication between OpenLab components - Server, AICs, and Clients. Clients can trust a server if the server can prove its identity using a valid certificate. OpenLab CDS relies on secure network communication via HTTPS. At installation, the OpenLab Certificate Service on the OpenLab Server generates an Agilent OpenLab Root Certificate Authority, which issues self-signed certificates for OpenLab Server/ECM XT, OpenLab CDS AICs, and OpenLab CDS Clients. These certificates enable trusted, secure communication of AICs and Clients to the Server, as the OpenLab RootCA certificate is automatically installed to the 'local machine' Windows certificate store of every OpenLab machine connected to this server. Even though self-signed OpenLab certificates technically allow for trusted, secure communication within the OpenLab ecosystems, you may choose to further improve the trust level of the secure communication using commercial certificates.

Using commercial certificates to secure the OpenLab Server can provide the following advantages:

- Compliance with your IT security policy.
- PCs without OpenLab CDS installed or other devices with web browsing capabilities being configured by your IT will trust the OpenLab Server/ECM XT server when trying to access Content Management via the web interface or when using the Sample Scheduler web interface.
- Switching Clients between two OpenLab Servers will not require manual installation of the second OpenLab Server/ECM XT root certificate to the respective Client's certificate store.
- Required for OpenLab CDS cloud installations, which do not rely on VPN only networks.

NOTE

When upgrading an OpenLab Server/ECM XT system that was secured using commercial certificates, Agilent recommends to maintain all Subject Alternative Name (SAN) entries in the new commercial server certificate when upgrading. Be aware that a required secured connection from existing AICs or Clients can only be established if the server address specified for the connection to the server is part of the Subject Alternative Names of the installed commercial certificate. Adjust the AIC and Client connection to the OpenLab Server/ECM XT system before starting the in place upgrade of an AIC or Client.

NOTE

At the end of an OpenLab Server/ECM XT in-place upgrade with a commercial certificate, the system will be in the state of using an internal certificate. After the upgrade, reconfigure and install the commercial certificate.

Procedures for Securing OpenLab Server/ECM XT Servers

Use the procedures in this section in the order presented to secure your system using certificates.

Generate certificates

Prepare a Java keystore in which your certificate will be stored.

Prerequisites: Java Development Kit (JDK) 11

JDK can be downloaded from Oracle or any other provider or you can use the JDK shipped with OpenLab Server/ECM XT under C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\java\bin.

You can use the Certificate Store from Windows Server, part of the Microsoft Management Console (MMC), as an alternative to the keytool. This is not described here.

NOTE

Certificates issued by your Certificate provider or company internal Private Key Infrastructure must be Base64 encoded. Typically these certificates are provided in a PKCS #7 binary certificate package (.p7b) including all intermediate certificates up to the root authority. The procedure describes the generation of the required certificates using a .p7b package, however the same result can be achieved using a Base64 encoded certificate of .crt or .cer file types. In the latter case it may be required to install intermediate Root Authority certificates manually.

For further information on certificate formats, you can visit: [Certificate formats](#)

The keystore will be created as PKCS #12 binary certificate package and is required to create a certificate signing request, import issued certificates from your Certificate Authority, and export information compatible to OpenLab CDS.

Create the keystore

- 1 Open an administrative command prompt.
- 2 Create a working directory on your server to allow for better traceability. The examples will use the directory c:\https.

Example:

```
mkdir c:\https
```

- 3 Navigate to the keytool directory C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\java\bin.

```
cd "C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\java\bin"
```

- 4 Use the following parameters to generate the keystore in PKCS #12 binary certificate package format.

```
keytool -genkey -alias <choose an alias> -keysize 2048 -keyalg RSA -keystore <choose a keystore file name> -storetype pkcs12
```

For an OpenLab Server / ECM XT with hostname ecmxtserver joined to domain agilent.com,

```
keytool -genkey -alias ecmxtserver.agilent.com -keysize 2048 -keyalg RSA -keystore c:\https\ssl.keystore -storetype pkcs12
```

During this process, you will be prompted for a password. Choose an appropriate password and take note of it. Keytool will ask for your first and last name, which refers to the Common Name (CN) of the OpenLab Server/ECM XT server. It is recommended to enter the Fully Qualified Domain Name of the Server, for example, ecmxtserver.agilent.com.

Generate a Certificate Signing Request (CSR)

To generate a CSR file for the server where HTTPS will be enabled, use the following keytool parameters. You will be prompted for the password entered earlier.

```
keytool -certreq -alias <Alias chosen in step Create the
Keystore> -keysize 2048 -keyalg RSA -keystore <your keystore
filename including path> -storetype pkcs12 -ext
"san=dns:<Server-Fully-Qualified-Domain-Name>,dns:<Optional DNS
Alias FQDN>" -file <Certificate Signing request including path>
```

For example,

```
keytool -certreq -alias ecmxtserver.agilent.com -keysize 2048
-keyalg RSA -keystore c:\https\ssl.keystore -storetype pkcs12
-ext "san=dns:ecmxtserver.agilent.com" -file
c:\https\ecmxtserver.agilent.com.csr
```

Request the certificate

Go to your trusted certificate provider with the created .csr file and request the certificate. The provider may be the PKI (Private Key Infrastructure) within your organization or a commercial vendor like VeriSign/DigiCert.

The trusted provider will deliver your PKCS #7 binary certificate package (.p7b), along with the Root CA certificate (.crt). Save both certificates to separate files.

Server Certificate,

```
c:\https\ecmxtserver.p7b
```

Root Certificate Authority Certificate,

```
c:\https\RootCA.crt
```

Install certificates into keystore

- 1 Import the Root CA certificate into keystore using the following keytool parameters.

```
keytool -importcert -alias <choose a new alias for the Root CA>  
-keystore <your keystore file name> -storetype pkcs12 -file  
<root certificate file>
```

For example,

```
keytool -importcert -alias agilent.com -keystore  
C:\https\ssl.keystore -storetype pkcs12 -file  
c:\https\RootCA.crt
```

You will be prompted for the password for the keystore. Confirm by typing "yes", that you trust this certificate.

- 2 Import your Server certificate into keystore using the following keytool parameters.

```
keytool -importcert -alias <Alias chosen in step Create the  
Keystore> -keystore <your keystore file name> -storetype pkcs12  
-file <your provided server certificate package>
```

For example,

```
keytool -importcert -alias ecmxtserver.agilent.com -keystore  
C:\https\ssl.keystore -storetype pkcs12 -file  
c:\https\ecmxtserver.p7b
```

You will be prompted for the password for the keystore. The message "Certificate reply was installed in keystore" appears. The creation of ssl.keystore as a PKCS #12 binary certificate package including the private key is complete.

Configure OpenLab Server/ECM XT Reverse Proxy

NOTE

OpenSSL v.1.1.1 is required for this step, and is provided in the installation folder as described in the following procedure.

You need the PKCS #12 binary certificate package: `ssl.keystore`, created in the previous step.

Keep the password for `ssl.keystore` available for the private key.

The following procedure leverages the installed OpenSSL to extract the PEM certificate and key files from the keystore. OpenSSL is installed on OpenLab Server in the following folder: `C:\Program Files (x86)\Agilent Technologies\Certificate Service\Bin\libressl`.

- 1 Go to the `openssl` directory.

```
cd "c:\Program Files (x86)\Agilent Technologies\Certificate Service\Bin\libressl"
```

- 2 Configure the current command session for OpenSSL.

```
set OPENSSL_CONF=C:\Program Files (x86)\Agilent Technologies\Certificate Service\Bin\libressl\openssl.cnf
```

- 3 Export the server certificate and the respective private key of the keystore. Provide the `ssl.keystore` password when prompted.

Run the following command to export the private key:

```
openssl pkcs12 -in <your keystore filename> -nocerts -out <your privatekey file> -nodes
```

For example,

```
openssl pkcs12 -in c:\https\ssl.keystore -nocerts -out c:\https\ecmxtserver.key -nodes
```

The message "MAC verified OK" appears as confirmation.

Run the following command to export the server certificate:

```
openssl pkcs12 -in <your keystore file name> -nokeys -out <your server certificate file>
```

For example,

```
openssl pkcs12 -in c:\https\ssl.keystore -nokeys -out c:\https\ecmxtserver.crt
```

The message "MAC verified OK" appears as confirmation.

4 Configure the Reverse Proxy Server using the Server Configuration Utility.

NOTE

Make sure the default OLSS password in Control Panel after installation was changed before running the Server Configuration Utility.

- a You can find the Server Configuration Utility under the Windows Start Menu after you have installed OpenLab Server/ECM XT server. In the Server Configuration Utility, navigate to the Certificate Setup page.
- b Select **Use existing custom certificate**.
- c Enter the exported server certificate file (for example, ecmxtserver.crt).
- d Enter the exported private key (for example, ecmxtserver.key).
- e Enter the Root CA certificate (for example, RootCa.crt).
- f Enter the Server Name/Alias as described in the certificate (for example, ecmxtserver.agilent.com).

After completing the Server Configuration Utility configuration steps, the Reverse Proxy service will use the values entered to secure inbound OpenLab Server/ECM XT traffic.

Once applied and you proceed with the configuration, you will be prompted to enter the OpenLab Shared Services (OLSS) Administrator credentials.

After the services are stopped and the changes are applied, the commercial certificate configuration is complete.

The above procedure can be reversed, if "Use Agilent OpenLab's internal certificate" is selected in step "Certificate Setup".

NOTE

If no entry fields are shown during the "Deploy Content Management permission" step, it is likely that the <Server-FQDN> is missing from the certificate Subject Alternative Names section or is misspelled.

Configure port 52088 to use a commercial certificate

Import the certificate into Windows Certificate Store using Certificate Service:

- 1 Start an administrative command prompt.
- 2 Make a copy of the ssl.keystore file and rename it to ssl.pfx, using the following command:
`copy c:\https\ssl.keystore c:\https\ssl.pfx`
- 3 To start the Certificate Import Wizard, double-click **ssl.pfx** located in c:\https.
- 4 Install the PKCS #12 certificate package to Certificate Store Location "Local Machine" and select **Automatically select the certificate store based on the type of certificate** to finalize the import.

A message "The import was successful" will appear.

- 5 Open the command prompt as an administrator, and go to the C:\Program Files (x86)\Agilent Technologies\Certificate Service\bin folder. Run the following commands to install the certificate:

```
cd "C:\Program Files (x86)\Agilent Technologies\Certificate
Service\Bin"

Agilent.OpenLab.CertService.CertServiceCore.exe
useexternalcert -certfilename c:\https\ssl.pfx -certpassword
<Password defined for ssl.keystore>
```

The certificate Service will restart and display the thumbprint of the used certificate.

To reverse the above step and revert to Agilent OpenLab certificates, use the following command:

```
Agilent.OpenLab.CertService.CertServiceCore.exe useinternalcert
```

Reconfigure AlfrescoTomcat Shared Services connection

This procedure is mandatory on the OpenLab Server/ECM XT server. Changes are not implemented until after you reboot the system (see **“Reboot and reactivate from OpenLab Control Panel”** on page 35).

- 1 Using the administrative notepad, open the AlfrescoTomcat configuration file, located at C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco-global.properties.

- 2 Change the olss.host property from localhost to:

```
olss.host=<Server-FQDN>
```

For example,

```
olss.host=ecmxtserver.agilent.com
```

Optional: Reconfigure access to Content Management or for a DNS alias

This procedure is required to access Content Management on the OpenLab Server/ECM XT server via an optional DNS alias. Prerequisite: the DNS alias must be part of the Subject Alternative Names of your server certificate.

Changes are not implemented until after you reboot the system (see **“Reboot and reactivate from OpenLab Control Panel”** on page 35).

- 1 Using the administrative notepad, open C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco\web-extension\share-config-custom.xml.
- 2 Add |https://<DNS Alias FQDN>.* as last entry to the assertReferer and asserOrigin sections.

```
<config evaluator="string-compare" condition="CSRFPolicy" replace="true">
  <filter>
    <rule>
      <action name="assertReferer">
        <param name="referer">https://localhost/.*|http://localhost/.*|http://<hostname>.*|https://<hostname>.*|https://<DNS Alias FQDN>.*</param>
```



```

</action>
<action name="assertOrigin">
  <param name="origin">https://localhost|http://localhost|
  http://<hostname>.*|https://<hostname>.*|https://<DNS
  Alias FQDN>.*</param>
</action>
</rule>
</filter>
</config>

```

For example, the server ecmxtserver.agilent.com should be reachable via the DNS alias openlab.agilent.com

```

<config evaluator="string-compare" condition="CSRFPolicy" replace="true">
  <filter>
    <rule>
      <action name="assertReferer">
        <param name="referer">https://localhost/.*|http://
        localhost/.*|http://ecmxtserver.*|https://ecmxtserver.*|
        https://openlab.agilent.com.*</param>
      </action>
      <action name="assertOrigin">
        <param name="origin">https://localhost|http://localhost|
        http://ecmxtserver.*|https://ecmxtserver.*|https://
        openlab.agilent.com.*</param>
      </action>
    </rule>
  </filter>
</config>

```

Force traffic to HTTPS for OpenLab Server/ECM XT

To prevent unsecured HTTP communication, manually add an entry in the Proxy Configuration Service config file, as follows.

- 1 Using the administrative notepad, open the Proxy Configuration Service config file, located at:

```

c:\Program Files (x86)\Agilent Technologies\OpenLab Reverse Proxy
Configuration Service\ConfigurationService\Agilent.OpenLab.ReverseProxy.C
onfigurationService.dll.config

```

Ensure that the VirtualHost configuration for Port 80 contains only three values.

```
<VirtualHost>
<add name="ServerName" value="*" />
<add name="PortNumber" value="80" />
<add name="Redirect" value="permanent / https://<Server-FQDN>" />
</VirtualHost>
```

For example,

```
<VirtualHost>
<add name="ServerName" value="*" />
<add name="PortNumber" value="80" />
<add name="Redirect" value="permanent /
https://ecmxtserver.agilent.com" />
</VirtualHost>
```

- 2 Save the file.
- 3 Using the administrative notepad, open the OpenLab Reverse Proxy configuration file, located at:

C:\Program Files\OpenLab Reverse Proxy\Apache24\conf\httpd.conf

Under the <VirtualHost *:80> block, modify it so that the port 80 configuration contains only the entries shown:

```
<VirtualHost *:80>Redirect permanent / https://Server-FQDN/
#<partnerconf80>
IncludeOptional "c:\programdata\agilent\openlab reverse
proxy\customconf\http*.conf"
#</partnerconf80>
</VirtualHost>
```

For example,

```
<VirtualHost *:80>
Redirect permanent / https://ecmxtserver.agilent.com/
#<partnerconf80>
IncludeOptional "C:\ProgramData\Agilent\OpenLab Reverse
Proxy\customconf\http\*.conf"
#</partnerconf80>
</VirtualHost>
```

- 4 Save the httpd.conf file.

This change will force all incoming http traffic to https. For example, if you type in the link: <http://ecmxtserver.agilent.com>, it will automatically get routed to <https://ecmxtserver.agilent.com> after completing the steps in Securing the system. This is not implemented until after you Reboot the system (see **"Reboot and reactivate from OpenLab Control Panel"** on page 35).

Configure a CSRF (Cross-Site Request Forgery) filter

Perform this procedure on the OpenLab Server/ECM XT server. These changes do not take effect until after you reboot and reactivate the system (see **“Reboot and reactivate from OpenLab Control Panel”** on page 35).

- 1 Using the administrative notepad, open the AlfrescoTomcat configuration file, located at C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco-global.properties and change the following properties.

By default, the **csrf.filter.origin** and **csrf.filter.referer** properties contain the “.*” wildcard operator value, which is used to imply that all domains are allowed by default.

To add the origin and referer headers, change the * wildcard operator to the valid Fully Qualified Domain Name for the **csrf.filter.referer** and **csrf.filter.origin** properties.

The following is an example configuration where ECM XT runs on the fully qualified host and port 443:

```
csrf.filter.origin=https://<Server-FQDN>/.*
csrf.filter.referer=https://<Server-FQDN>/.*
```

For example,

```
csrf.filter.referer=https://ecmxtserver.agilent.com/.*
csrf.filter.origin=https://ecmxtserver.agilent.com/.*
```

Reboot and reactivate from OpenLab Control Panel

- 1 From the Windows Start Menu, under Agilent Technologies, click **Shared Services Maintenance** and select the **Server Settings** tab.
 - a Add the server.
 - b Enter a name for the server.
 - c Server: <Server-FQDN>
 - d Optionally, add a description of the server.
 - e Set the added Server as default.
- 2 Reboot the system.

- 3 Activate Content Management communication via HTTPS using OpenLab Control Panel.
 - a Open OpenLab Control Panel, and go to **Administration > System Configuration > Edit System Settings**.
 - b In the **Please select another option from the list if you wish to use a different storage type** drop-down list, select **Content Management**, and then click **Next**.
 - c Select **Change server**.
 - d Enter the Content Management server URL with 'https' and the fully qualified domain name of the host.
Example: https://ecmxtserver.agilent.com
 - e Click **Activate**.

All AICs and Clients must be registered to the <Server FQDN>. The hostname on its own is not permitted and not part of your created certificate.

Index Server Configuration - 4-Server Systems Only

For 4-server systems, use the following procedure to configure security on your index server.

- 1 Copy the Root Authority certificate used on the OpenLab Server/ECM XT server to the Index Server.
- 2 Change the Startup type of the Agilent OpenLab Shared Services service from disabled to manual.
- 3 Start the Server Configuration Utility from the **Windows Start Menu > Agilent Technologies**. (Available after installation of the OpenLab Index server.)
- 4 In the Server Configuration Utility, navigate to the **Certificate Setup** page.
- 5 On the **Server Configuration** screen, enter and verify the (primary) Content Management fully qualified domain name (FQDN).
- 6 On the **Certificate Setup** screen, select **Use existing custom certificate from Content Management host**, browse to the Root Authority Certificate, and select RootCa.crt.
- 7 Complete the Server Configuration Utility.
- 8 Change the Startup type of the Agilent OpenLab Shared Services service from manual to disabled.
- 9 Reboot the Index server.

TLS/SSL Disabling

Some organizations require older security protocols to be disabled in Windows. TLS 1.0, TLS 1.1, and SSL 3.0 are not required by OpenLab Server/ECM XT and may be disabled according to instructions from Microsoft.

If you disable a security protocol, make sure you disable it on all computers in the system (Content Management, Index, file server, DB server, AIC and CDS client).

4

Maintenance

Routine Server Maintenance 40

Windows Domain 46

Server Settings 47

FTP Server Protocol 48

Archiving 50

The **OpenLab Shared Services Maintenance utility** program is automatically installed with your OpenLab software to help administrators manage the system.

To open the program, select **Windows Start > Agilent Technologies > OpenLab Shared Services > Shared Services Maintenance**.

A user must have Windows administrator rights to access this program.

Routine Server Maintenance

Update database statistics

To maintain optimal database performance, periodically update the OpenLab Server\ECM XT server database statistics. These statistics are used by the database engine to determine the most optimal way to execute queries.

Update statistics for the OpenLab Server/ECM XT server and OpenLab Shared Services databases. If custom database names were chosen during installation, use the correct names from your installation notes.

Maintenance Procedures for PostgreSQL database

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

Running the PostgreSQL data management tool

- 1 Go to **Windows > PostgreSQL 14 - OLCM > pgAdmin 4**. If this is the first time you are running pgAdmin, set the Master Password and add a server to the server group. Right-click **Servers** and select **Create > Server** to create a server.
- 2 On the **General** tab, enter *localhost* in the **Name** field.
- 3 On the **Connection** tab, enter *localhost* as the **Host name/address**, and enter the password for the postgres user. The password was set up during installation. Select **Save password?** to save the password.
- 4 Click **Save**. *localhost* is now shown under the **Servers** group.
- 5 Expand *localhost*, and then expand **Databases**.
- 6 Double-click **OLDataStore** and **OLSharedService** to connect both databases.

Updating statistics using the Maintenance Wizard

- 1 Start **PostgreSQL pgAdmin**, connect as the database administrator, and select the database for which you want to update the statistics. The default database administrator user name is 'postgres' and the default password is the password set in **Step 1 - Install or Upgrade Software Prerequisites** of the OpenLab Server/ECM XT installation process.
- 2 Right-click the database, and select **Maintenance**. The following form is displayed.

Figure 2. 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 more details about these commands.

CAUTION

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

Maintenance Procedures for SQL Server

Ensure that at least 4 GB is reserved for the Windows operating system.

Performance tuning for Microsoft SQL server

As the number of documents reaches more than 10 million, OpenLab Server/ECM XT with SQL Server may become slow in the following areas, caused by SQL Server's parameter sniffing being set to ON:

- 1 Bootstrap time
- 2 Initial file listing on both Web and DA after server restart

If you experience any of the above, do not turn parameter sniffing OFF, as this is not supported.

Inadequate covering indexes can often be the root cause of parameter sniffing. SQL Server may choose a Key Lookup plan for a small number of values, and a clustered index seek or scan for a large number of values. With a covering index, the optimizer will not make those choices, and often you will end up with a more stable execution plan.

Add the following two indexes manually in SQL Server Management Tool to improve performance.

- 1 Create this index to improve bootstrap time:

```
USE [DataStore]
GO

SET ANSI_PADDING ON
GO

/***** Object:  Index [idx_alf_cass_qnln]      Script Date:
12/7/2018 8:00:46 PM *****/

CREATE NONCLUSTERED INDEX [idx_alf_cass_qnln] ON
[dbo].[alf_child_assoc]
(
    [parent_node_id] ASC,
    [qname_ns_id] ASC,
    [qname_localname] ASC,
    [qname_crc] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
SORT_IN_TEMPDB = OFF, DROP_EXISTING = OFF, ONLINE = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
GO
```

- 2 Create this index to improve initial file listing time on Web and DA after server restarts:

```
USE [DataStore]
GO

/***** Object:  Index [idx_alf_node_tqn_id]      Script Date:
12/10/2018 5:20:05 PM *****/

CREATE NONCLUSTERED INDEX [idx_alf_node_tqn_id] ON
[dbo].[alf_node]
(
    [type_qname_id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
SORT_IN_TEMPDB = OFF, DROP_EXISTING = OFF, ONLINE = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
GO
```

- 3 Rebuild indexes based on the following recommendations. Run an index fragmentation check, and:
 - Rebuild anything that is >30% fragmented.
 - Re-organize anything that is between 5 and 30% fragmented. See <https://docs.microsoft.com/en-us/sql/relational-databases/indexes/reorganize-and-rebuild-indexes> for more information.

Optimizing Microsoft SQL Server to work with Content Management

To ensure that your performance does not degrade, perform the following weekly maintenance operations on your SQL server.

- Recompute statistics by running the command: `EXEC sp_updatestats`
- Clear the buffers by running the command: `DBCC DROPCLEANBUFFERS`
- Clear the cache by running the command: `DBCC FREEPROCCACHE`

Updating statistics using Maintenance Plan Wizard

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

- 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 OpenLab Server/ECM XT server database (DataStore) and the Shared Services database (OLSharedServices) as the database against which the task will be executed.

Moving your server

To move your server from a domain to a workgroup, or from one domain to another domain, the SQL Server must be configured to a local account (not a domain account). Contact Agilent Support for help with moving your server.

Monitor resource use on OpenLab Server/ECM XT server

The data files, indexes, and database are stored on the server hard disk or in AWS S3. Depending on your server's configuration, these may be on one or more disk drives.

Administrators of the system must regularly monitor disk space use on all disks where data is stored. When the disks get close to 80% full, consider increasing disk space. CPU, memory, and network use must be monitored to check for performance bottlenecks on the server.

Recommended best practices for monitoring resource use

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

Additional best practices

- Apply third-party updates and patches on the OpenLab Server/ECM XT server.
On the Agilent SubscribeNet, Agilent regularly posts information on third-party updates and patches that have been validated for use with the OpenLab software suite. These include OS security patches and updates, database updates, and application updates.
The Customer Care Portal is available at:
<https://agilent.subscribenet.com>
- Apply Agilent software updates.
Apply software updates for Content Management and Shared Services on your OpenLab Server/ECM XT 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.

Windows Domain

Update the Domain, User name, or Password for your server

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

Use **Windows Domain** to specify or change the credentials that OpenLab will use to access your Windows domain server. This feature can only access credentials that are stored on the computer where you opened the Shared Services Maintenance utility program.

To specify or change the **Domain**, **User name**, or **Password** for the windows account that will be used to access your windows domain server, use the **Shared Services Maintenance utility** program that is installed on the server.

Enable read permission for a user

When using Windows domain authentication, OpenLab Server/ECM XT reads user attributes to get information as to whether or not users must change their OpenLab password. If read permission is not granted to the user, OpenLab Server/ECM XT assumes that the user's password has expired and will refuse access.

To enable read permission for a user:

- 1 On a domain controller, open **Active Directory Users and Computers**.
- 2 Select **View > Advanced Features**.
- 3 Under **Users**, right-click a user, and select **Properties**.
- 4 On the **Security** tab, select **Authentication Users**.
- 5 Select the **Read** permission, and click **OK**.

Server Settings

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

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

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

FTP Server Protocol

The OpenLab Server/ECM XT server can be used as an FTP server and accessed through any FTP server protocol.

CAUTION

FTP is disabled by default. If you enable FTP services, this may be considered as a data integrity risk, and impacted customers are advised to disable or block FTP services when not needed. See “Disable the OpenLab Server/ECM XT server as an FTP server” on page 49.

Enable the OpenLab Server/ECM XT server as an FTP server

- 1 On your server, navigate to **C:\Program Files (x86)\Agilent Technologies\OpenLab Data Store\tomcat\shared\classes**.
- 2 Open the `alfresco-global.properties` file in any text editor.
- 3 Change **`ftp.enabled=false`** to **`ftp.enabled=true`**.
- 4 Save the file.
- 5 Restart tomcat service.

Connect to the OpenLab Server/ECM XT server through an FTP protocol

- 1 Access your FTP Client.
- 2 Within the FTP protocol, use:
 - The OpenLab Server/ECM XT server address as the FTP host name
 - The OpenLab Server/ECM XT server port
 - Your Control Panel username and password
- 3 Connect according to your FTP protocol.

Disable the OpenLab Server/ECM XT server as an FTP server

To block FTP access on the server, you must block the FTP port in your firewall. For a workstation installation, you must disable the FTP services.

- 1 On your server, navigate to **C:\Program Files (x86)\Agilent Technologies\OpenLab Data Store\tomcat\shared\classes**.
- 2 Open the alfresco-global.properties file in any text editor.
- 3 Change **ftp.enabled=true** to **ftp.enabled=false**.
- 4 Save the file.
- 5 Restart the tomcat service.

Archiving

Modify Automatic Archiving Execution Schedule

Use this procedure to change the automatic archive task execution date and time in the Content Management properties file. When an automatic archive task runs, user-specified archive rules assigned to the content folders are enforced, and the content is moved to the destination archive location. By default, automatic archive tasks run once a month, but any schedule supported by a Quartz cron expression can be used.

The following is required to modify the automatic archiving execution schedule:

- An operating system user credential with read/write permission for the **<INSTALLATION PATH>\tomcat\shared\classes\alfresco-global.properties** file. In a default installation, the file is in the following location:
C:\Program Files (x86)\Agilent Technologies\OpenLab Data Store\tomcat\shared\classes\alfresco-global.properties.
- Permission to start and stop the alfrescoTomcat service.

Change execution values

- 1 Stop the alfrescoTomcat service.
- 2 Open the file: **<INSTALLATION PATH>\tomcat\shared\classes\alfresco-global.properties.**
- 3 Find the property: **archive-job.cron**. For example,


```
### Archive Job Cron Expression
# default runs first sunday at 2:30 AM of every month
archive-job.cron=0 30 2 ? * 1#1 *
```
- 4 Modify the expression to meet your requirements. See **"Cron expressions"** on page 51.
- 5 Save the file.
- 6 Restart the alfrescoTomcat service.

The task will execute automatically at the date and time described by the cron expression.

Cron expressions

A cron expression is a string consisting of six or seven fields that describe individual details of the schedule.

These fields, separated by white space, can contain any of the allowed values with various combinations of the allowed characters for that field.

Seconds	Minutes	Hours	Day Of Month	Month	Day Of Week	Year
0	0	0	?	*	*	*

Table 4 contains examples of cron expressions for automated archiving.

Table 4 Cron expression examples

Description	Cron Expression
Run every day at 2:30 a.m.	0 30 2 ? * * *
Run every Sunday at 2:00 a.m.	0 0 2 ? * 1 *
Run twice a day at noon and midnight	0 0 */12 ? * *
Run on the 2 nd and 17 th of each month at 11:00 p.m.	0 0 23 2,17 * ? *

Where:

- * = all values
- ? = no specific value

It is not recommended to run an automatic archive task more than once a day. It is recommended to schedule automatic archive tasks to run during off-hours.

Quarantine

Quarantine during archive

Interruption to the archive/de-archive process can result in a file existing in both the source and target location. If this occurs, when the archive/de-archive is rerun, the following steps are taken automatically:

- 1 Upon detecting that the file exists in the target location, that file is moved to a quarantine folder. This quarantine process is transparent to the user. It is assumed that the source file is always the original, “good” version of the file.
- 2 A log entry is created indicating that a file was quarantined. The entry description says:

<'File'/'Folder'><file/folder path and name> was quarantined to <quarantine folder location> during <'archive'/'de-archive'>

where *<file/folder path and name>* is the logical path with the file name as it is seen in the content management interface, and *<quarantine folder location>* is the physical path to the quarantine folder, including the physical file’s obfuscated name (.bin file).

One log entry is created for each .bin file associated with the file being quarantined. For example, if a file has two versions, then there are two .bin files associated with the file. Two log entries are created when the file is moved to the quarantine folder.

- 3 After quarantine, the archive/de-archive proceeds as if the duplicate file was never detected, and users see no difference in the content management interface.

Quarantine folder

The quarantine folder is structured to match the folder structure in content management. Files added to the quarantine folder will have the same path as they did in the source folder. In cases where a file with the same name is already present in the quarantine folder, the new file is placed inside a numbered subfolder. So, files are not overwritten, and no data is lost.

The quarantine folder is named “contentstore.quarantined,” and its location is based on how the system storage locations are set up.

- When both the primary content location and the primary archive location reside in the same place (either on-premises or AWS S3), then the quarantine folder is created in the primary content location.

- When the primary content location and the primary archive location reside in different places (a mix between on-premises and AWS S3), then there is a quarantine folder in both locations. The quarantine folder is created in the location where the duplicate files are found (the target location). For example, for configurations with the primary content location on-premises and the primary archive location on AWS S3:
 - If there are files that failed to get properly archived, then the quarantine folder will reside in the AWS S3 archive location. (This happens if duplicate files are detected in the archive location when the archive is rerun.)
 - If there are archived files that failed to get properly de-archived, then the quarantine folder will reside in the on-premises content location. (This happens if duplicate files are detected in the content location when the de-archive is rerun.)



5

Backup and Restore Procedures

Important Information about Backup and Restore	55
Creating a Disaster Recovery Plan	57
Using the Backup and Restore Utilities	59
Back Up OpenLab Server/ECM XT Using the Backup Utility	61
Restore OpenLab Server/ECM XT Using the Restore Utility	72
Using the Backup and Restore Scripts	80

Important Information about Backup and Restore

It is mandatory that every OpenLab Server/ECM XT server is backed up regularly. Periodic full backups and differential backups between the full backups are created by OpenLab Server/ECM XT server administrators. These backups are the only way to restore an OpenLab Server/ECM XT server if a hardware or software failure occurs.

The backup only reduces the amount of data loss if a catastrophic system failure occurs. Performing backups guarantees that any data that was committed at the time of the backup can be restored. Data that was queued for upload and not yet committed or was added or updated in the system after the backup was performed will not be recoverable by restoring a backup.

It is also mandatory that the restore procedures are tested to ensure that the backups are performed properly, and can be used for a restore. To do an effective restore, a disaster recovery plan must be created. See **“Creating a Disaster Recovery Plan”** on page 57.

CAUTION

In cases where a restored system will run at the same time as the source system (where the backup was taken), make sure that the restored system is on a network that is isolated from the source system. For example, if a test system is created from a backup of the production system, it must be on a network that is isolated from the production system. If the test system and the production system are on the same network, it may cause the two servers to create a cluster and interact with each other. This can lead to data corruption and loss.

In addition, it is important to turn clustering off on the restored system using the following steps:

- 1 On the restored server, open C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco-global.properties.
- 2 Find the `alfresco.cluster.enabled` property and set it to false, as follows:
`alfresco.cluster.enabled=false`
- 3 Restart the AlfrescoTomcat service.

OpenLab Server/ECM XT stores files and indexes on your server's file system. The location of this folder is determined when the product is installed. Other data, such as folder information, audit trails, and signatures are stored in a relational database.

A full backup captures a complete set of data from OpenLab Server/ECM XT, including uploaded files and its databases. An incremental backup contains changes that have occurred since the last full backup. The incremental backup process is faster than the full backup because only the changed elements are backed up.

If you are upgrading your server, perform the following procedures on your machine before upgrading. Clear all work areas and file upload queues before the upgrade procedure. Do not have data in any queues when performing the upgrade to a different operating system. Make sure all file uploads are complete. Clear the file buffer upload queue before the upgrade.

The Backup Utility can be used for performing immediate backup or backup by a schedule for OpenLab Server/ECM XT Server (All-in-one or 2-server).

Using Amazon Web Services S3 as a backup location

- Ensure that the S3 bucket is not 'publicly' accessible over the internet. Use centralized controls to limit access.
- Follow principles of 'least privileged access'. Grant only the permissions required to perform the task
- If you plan to use S3 as the backup location for your system using OpenLab Backup/Restore tools, assign the following permissions (in addition to the permissions defined above) to the bucket that will contain the backups.

s3:DeleteObjectVersion

s3:GetObjectVersionTagging

s3:ListBucketVersions

s3:PutObjectVersionTagging

s3:DeleteObjectVersionTagging

- Enable Server-side encryption.
- Enable versioning of objects.

Creating a Disaster Recovery Plan

Prepare a recovery plan for the unlikely case that OpenLab Server/ECM XT becomes inoperable due to a hardware or software failure. This plan must include information and procedures for completely restoring the operating system, the OpenLab Server/ECM XT software and data - if necessary, to a physically different server. Ensure that the disaster recovery plan has been tested and confirmed to be working.

In developing your disaster recovery plan, consider the following:

- Determine the frequency of backups you require. For example, what is the maximum acceptable number of lost samples in case of a failure (samples that would require repeating)? Generally, there is a tradeoff between frequency of backup and cost/effort to restore, especially for large systems.
- What is the best backup/restore method, based on your system topology and availability requirements?
 - Backup/Restore Utility (Available for All-in-one and 2-server topologies only). Utilities provide full or incremental daily backups.
 - Backup and Restore Scripts. The scripts do not support incremental backups, so they may not be appropriate for larger systems.
 - Manual Procedure (usually the best option for larger systems). This is a procedure for configuring backup solutions other than the Agilent Backup/Restore Utilities.

OpenLab Server/ECM XT backup and restore is supported only for the exact same type of database configuration. If you attempt to backup and restore between different types of archived databases (including the same databases with different configurations), the Control Panel will display an error. The "Disaster Recovery Plan" must include the following:

- Server hardware information: CPU, Memory, and Hard disk configuration information
- Server identity: Name, IP, domain, URL, and so forth
 - Server administrator information: username and passwords for logging into the server. If applicable, usernames and passwords for the database.
- Server software information: OS version, Patch level

- OpenLab Server/ECM XT Installation Parameters:
 - Installation folder
 - Installation log file
 - OpenLab Server/ECM XT database type
 - OpenLab Server/ECM XT content and archive folders
 - OpenLab Server/ECM XT indexes folder
 - OpenLab Server/ECM XT Content Management database name
 - Shared Services language
 - Shared Services database name
 - Installed licenses
 - Registered applications
- 3rd party software information: applications and their revisions and install paths
- Procedures for your topology. See **“Using the Backup and Restore Utilities”** on page 59 or **Chapter 6**, “Manual Backup and Restore Procedures”.
- Backup media location and organization details
- Remote database server is configured correctly. See “Configure a Remote Database Server” in the *OpenLab Server/ECM XT Installation Guide*.

Using the Backup and Restore Utilities

The Backup and Restore Utilities are tools that make it easy to back up and restore your OpenLab Server/ECM XT system.

For All-in-one and 2-server topologies, you can use the automated tools for backup and restore described in the following sections. To back up and restore a 4-server, you can use the scripts provided for backup and restore (see **"Using the Backup and Restore Scripts"** on page 80) or a manual method. For scalable topology, use the manual backup and restore procedures described in **Chapter 6**, "Manual Backup and Restore Procedures". The following table describes the OpenLab Server/ECM XT topologies supported by the Backup and Restore Utilities.

CAUTION

Anti-virus scanning during backup can prevent successful completion of the backup. Make sure that the backup location is excluded for both regular/scheduled scans and real-time protection. If the backup location cannot be excluded from real-time protection and real-time protection cannot be turned off, it is possible the final backup tasks might not finish successfully.

To help avoid these failures, there is a Delay and Retry setting. By default, it is set to 3 tries with 10 seconds delay. You can modify this setting in the Backup > BackupFinalizationSettings section of the configuration.xml file located in the %ProgramData%\Agilent\Installation folder. System Administrator privileges are required to update this file. Acceptable values are Delay greater than 0 and Retry greater than 1. Delay and Retry is applied during a "Backup now" at the Processing page before the first step and when a backup is started from a "Backup by schedule."

If you have an anti-virus running during backup, you can verify that the backup finished successfully with these steps:

After the backup completes, check that the backup location contains only "Current" (or "Current" and "Incremental") sub-folder(s)

Check that the log file corresponding to the backup time contains an entry stating "The backup has completed" at the end. Backup logs are placed in the "C:\ProgramData\Agilent\LogFiles\Backup" folder.

Table 5. Supported topologies for Backup and Restore Utilities

Topology	Backup Utility	Restore Utility	Notes
All-in-One	+	+	Scripts and manual procedures also available. Scripts do not support incremental backup.
2-Server	+	+	Scripts and manual procedures also available. Scripts do not support incremental backup. Oracle database backup and restore uses manual procedure
4-Server	Scripts available, manual optional	Scripts available, manual optional	Scripts do not support incremental backup. Oracle database backup and restore uses manual procedure
Scalable system	Manual only	Manual only	Oracle database backup and restore uses manual procedure

Back Up OpenLab Server/ECM XT Using the Backup Utility

Use the Backup Utility to perform immediate or scheduled backups for supported topologies. The Backup Utility supports full and incremental backups. For a list of topologies supported by the Backup Utility, see **“Using the Backup and Restore Utilities”** on page 59.

The backup captures a complete set of OpenLab data, including:

- Configuration file
- Databases for Shared Services, Content Management, and Data Repository
- Solr Indexes
- Local Content and Archive storage locations
- Alfresco cache
- Certificate server

NOTE

The Backup Utility backs up the OpenLab data only. The customer is responsible for backing up core database elements, such as Master and MSDB, as part of general database maintenance.

NOTE

The Backup Utility does not back up data from an AWS S3 Storage location.

NOTE

In case of a non-domain (workgroup) environment with remote database server (PostgreSQL or MSSQL), make sure that LocalAccountTokenFilterPolicy is enabled on the database server. Create or update the registry DWORD value “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy” to 1.

NOTE

Use of the Backup Utility for Oracle databases is not supported. In case of Oracle database, the database backup will be skipped and must be backed up manually. See the Oracle documentation for instructions on how to back up an Oracle database. Oracle database backups should be performed before backup of other parts of the system.

NOTE

The Backup Utility does not back up custom certificates used for secure connection. If custom certificates are used, back them up manually and keep them in a secure location for use during the restore process.

The custom certificates are located at C:\Program Files\OpenLab Reverse Proxy\Apache24\conf\ssl\custom\.

NOTE

The user should have “Logon as a batch”, “Logon as a service” permissions and be an administrator on ECM XT Server and Database server if the system is configured with a specified (non-system) user account.

CAUTION

If you use the Agilent OpenLab Backup Utility to schedule backups, do not use SQL Server Management Studio, SQL Scripts, or tools to back the OpenLab Content Management databases. This will prevent the tool from performing incremental backups.

Space required

The free space required for the backup procedure depends on different factors, including the server configuration, backup location, and database backup size. In the most resource-intensive case, make sure free space in the backup location is at least twice as large as the sum of all on-prem file storage and database size. This is needed to avoid rewriting a previous successful backup with a backup that finished in the middle for any reason.

Backup and Restore Utilities use specific database folders as temporary backup locations during backup/restore to/from AWS S3 backup location:

- Data directory for PostgreSQL database. See **“Configure custom data directory of PostgreSQL database”** on page 70 and **“Configure custom data directory of Data Repository PostgreSQL database”** on page 71.
- Default backup location for MS SQL database. Follow the MS SQL guide to configure default backup location. Make sure the new location has permissions for Access Credentials and MSSQLSERVER (NT Service\MSSQLSERVER).

Make sure the space on the specified location is enough for temporarily storing the database backup.

Configure databases for Incremental Backup

If you plan to use incremental backups, you must configure the OLCDS and Data Repository PostgreSQL databases first. See **“Incremental backup of PostgreSQL databases”** on page 69.

Troubleshooting

The Backup Utility collects logs in the %ProgramData%\Agilent\LogFiles\Backup folder. During the backup procedure, all steps are checked, and the procedure will stop on the first failed step. A link with the failed step opens the current backup log file to help identify the issue. In case of a failed backup, the partial backup is stored in a Temp folder in the backup location.

Procedures for using the Backup Utility

Back up using Backup Utility

Steps	Options	Notes
1 Start Backup Utility from Start > Agilent Technologies > Backup Utility. If a request for User Account Control access appears, click Yes. Click Next.	The Status page displays the date and time of the latest successful backup. Click the link to go to the backup location.	<ul style="list-style-type: none">• System administrator privileges are required to run and execute the Backup Utility• If a backup is scheduled, the page displays the current backup status and the next backup start date and time.• If a backup is currently running, the status shows Running. If a scheduled backup has failed, the status shows Failed.• The Last successful backup shows the date/time when the latest successful backup ("by scheduler" or "backup now" types) was taken and its location. The link points to the backup location (on-prem or AWS S3). it will contain information right after the first successful backup.• Reboot system if time zone has been changed. Otherwise, date/time on the Status page can show mismatched values.

Back up using Backup Utility (continued)

Steps	Options	Notes
2 On the Backup option page, select the backup option.	<ul style="list-style-type: none"> Set backup schedule 	<ul style="list-style-type: none"> Use this option as part of an automatic backup procedure. Provide the backup type and schedule settings. The schedule time uses a 24-hour format. Scheduling automatic backups is recommended. To disable automatic backups during maintenance periods, clear the Enable backup schedule check box. Be sure to enable the scheduled backups when maintenance is completed.
	<ul style="list-style-type: none"> Backup now <ul style="list-style-type: none"> Hot backup Cold backup 	<ul style="list-style-type: none"> Back up using hot or cold backup starts immediately. There is no impact on a scheduled backup. This option can be helpful for checking the correctness of the backup settings, how much disc space and how much time a single backup requires. In addition, this option can be a part of the testing of the whole recovery procedure.
3 On the Configure page, configure your backup settings.	<ul style="list-style-type: none"> For backup schedule, enable and set up schedule for backups Select if you want your system to be available during backup <ul style="list-style-type: none"> Yes for hot backup No for cold backup Select to enable incremental backups. Enter the time and days for incremental backups 	<ul style="list-style-type: none"> It is highly recommended to enable the backup by schedule. Clearing the Enable backup schedule check box turns the scheduled backup off. When full and incremental backups are scheduled on the same day, the full backup will be performed. Incremental backups require at least one full backup performed first. If a scheduled full backup fails, the subsequent incremental backups will fail until the next successful scheduled full backup. To prevent failure of the incremental backups, perform an immediate backup to the location designated for the scheduled backups.

5 Backup and Restore Procedures

Procedures for using the Backup Utility

Back up using Backup Utility (continued)

Steps	Options	Notes
	<ul style="list-style-type: none"> For Backup now, select if you want your system to be available during backup <ul style="list-style-type: none"> Yes for hot backup No for cold backup 	<ul style="list-style-type: none"> Hot backup: System remains operational during backup Cold backup: Requires stop of all OpenLab Server/ECM XT operations. The Backup Utility does this automatically.
4 Provide backup location		The backup can be configured to a folder without permissions for the current Windows user. The backup executes from the System user, which allows saving of a successful backup. In this case of scheduled backup, the backup will be executed, but the current Windows user will not be able to view the results without the appropriate privileges.
	<ul style="list-style-type: none"> File system 	<ul style="list-style-type: none"> Backup location is for on-prem backup, local or on a Windows share. Network drive is not supported. If you are using a network share, server should be configured with a specified user account. To configure Server with this setting, run the Server Configuration Utility > Access Credentials. The user should have Logon as a batch permissions and be an administrator. Server configuration with SYSTEM account supports local folders only.
	<ul style="list-style-type: none"> AWS S3 (Amazon AWS S3 location) <ul style="list-style-type: none"> Provide S3 bucket region, name, and access keys 	<ul style="list-style-type: none"> Enable Versioning of objects in the AWS S3 Bucket setting. Make sure that AWS S3 settings are valid. A message will appear in AWS S3 if service is unreachable or settings are invalid.
5 Set up notifications. If you selected to Backup now, this is skipped.	<ul style="list-style-type: none"> Enable backup notifications From address To address 	<ul style="list-style-type: none"> Use a "From" address that is configured in the Control Panel. For information on how to set up email addresses, see the Control Panel online help. Use a comma to separate multiple "To" addresses. Each address can be represented in long-form (name and email) or in short-form (only email).

5 Backup and Restore Procedures

Procedures for using the Backup Utility

Back up using Backup Utility (continued)

Steps	Options	Notes
	<ul style="list-style-type: none">• Subject starts with text	This specifies a prefix in the notification e-mail subject.
	<ul style="list-style-type: none">• Send a test message	Use Sent test message to ensure that the Notification settings are correct.
6 Review and start backup. To start backup, click Apply .		Progress is tracked on the Processing page.
7 When backup is complete, click Done .		

NOTE

If you are using Sample Scheduler, the Sample Scheduler services must be restarted after a cold backup.

Backup folders are created in the location specified when you run the Backup utility.

Name	Date modified	Type	Size
CertificateService	3/1/2021 3:22 PM	File folder	
DR	3/1/2021 3:22 PM	File folder	
DSArchiveDir	3/1/2021 3:22 PM	File folder	
DSContentDir	3/1/2021 3:22 PM	File folder	
DSIndexDir	3/1/2021 3:21 PM	File folder	
Installation	3/1/2021 3:22 PM	File folder	
PostgreSQLDataDir	3/1/2021 3:22 PM	File folder	
Verification	3/1/2021 3:22 PM	File folder	
backup.xml	3/1/2021 3:22 PM	XML Document	1 KB
Backup_log_03-01-2021(15_21_59.037231...	3/1/2021 3:22 PM	Text Document	39 KB

In the event of a failed backup, the partial backup is saved in a Temp folder in your backup location.

NOTE

In some cases, antivirus scanning can prevent the final step of renaming the Temp folder to Current. In this case, the creation of the backup.xml file was successful, even though the backup “failed.” If this was the reason for the failure, you can manually rename the Temp folder to Current (if full backup was performed.) If incremental backup was performed, rename the Temp folder to Incremental.

Backup verification

The backup verification step verifies the backed-up data after the completion of the backup procedure.

This step generates two reports. Both reports are located in the Verification sub folder.

- VerificationReport.xml - This file contains the technical information about the backup, including information about backed-up entities such as files, their hashes, databases' entities, and so on. In case of restoration, this report will be used for comparison of the files and databases' entities.
- VerificationReport.html - This report contains information about backup, number of verified files, information about failed file verification, database entity verification results in a human-readable view.

The verification step checks that main entities (uploaded files, database entities) are backed up properly. The number of files for verification is specified in the configuration file after backup configuration (10% or 10000 by default). Backing up an Oracle database is not supported by the Backup Utility, so the validation of database entities will be skipped.

Files stored in On-Prem locations will be verified and included in the report after the backup procedure. Files from AWS S3 storage locations will not be verified because they are backed up using the AWS procedure and are not part of verification. In case of a mix of on-prem and AWS S3 file storage, file verification is also not performed, and only the total number of files in Content Management are listed and compared.

In case of restoration, all entities which have been included in the backup report will be verified.

Any entity (or its version) modified after the backup start time will not be included in the reports and will not be verified during the restoration procedure.

Files Verification

For File Verification, the following logic is used:

- The Backup Utility first counts all backed up files and randomly takes minimum of 10% of the amount of the files and upper limit files for verification. The taken percent of the files for the verification is always rounded up, for example, for 3 files 10% is 0.3, and this value rounded to 1. It is useful for a small amount of the files in the Content Management, the tool guarantees that at least 1 file will be verified.

- Then the utility takes a random version of each file. For example, if a file in Content Management has three revisions (1.0, 2.0, and 3.0), the utility will randomly take one of them.
- The verification excludes deleted files.
- The verify procedure compares checksum and size of backed up files with file information from Content Management. If the checksums are equal, the verification is passed. Otherwise, the verification is failed.

The amount of files for verification can be configured with the following properties in the Backup section of the configuration.xml file, located in the %ProgramData%\Agilent\Installation folder. You must be a System Administrator to modify this file.

- PercentFilesVerification - The percentage of files verified (default 10%), range 1 - 100.
- TotalFilesVerificationLimit - The upper limit files for verification (default 10,000), value must be greater than 0. Negative and fractional values are not allowed.

The new value is applied during a "Backup now" at the Processing page before the first step and when a backup is started from a "Backup by schedule."

Database Verification

Verification includes checking of number of database entities for:

- Methods
- Samples with unique names
- Shared Services Activity Log
- Content Management Activity Log

Incremental backup of PostgreSQL databases

Cumulative incremental backup is a process that saves data files and objects that have been modified since the last full backup. It is a data backup technique that only updates modified data rather than the complete data. Perform these steps on the PostgreSQL Database server-side for System PostgreSQL (olcm-postgresql-x64-14) and locally for Data Repository PostgreSQL.

PostgreSQL does not have a tool that performs incremental backup but has an incremental backup strategy. This strategy means that you can combine a file-system-level backup with a backup of the WAL files.

To recover successfully using continuous archiving (also called “online backup” by many database vendors), you need a continuous sequence of archived WAL files that extends back at least as far as the start time of your backup. To start, set up and test your procedure for archiving WAL files before you make your first base backup.

Configure incremental backup using Incremental Config Tool

The Incremental Config Tool configures incremental backup support automatically. It allows you to configure all PostgreSQL instances used by OpenLab Server/ECM XT at once. The Incremental Config Tool performs following actions:

- Updates settings for support of incremental backups for Content Management PostgreSQL (if installed) and Data Repository PostgreSQL.
- Requires a restart of PostgreSQL services after updating.
- Updates the BackupUtility.config file for supporting incremental backups by the Backup Utility.

The tool is located by default at C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Incremental Config Tool\PgIncrementalConfigTool.exe.

PgIncrementalConfigTool can be run from the command line. Run PgIncrementalConfigTool as administrator and configure the access credentials according to **“Reconfiguring Access Credentials”** on page 79

Parameters:

- -on - mandatory, enable incremental backup, set up default paths
- -off - mandatory, disable incremental backup
- -olcmWalDir <path> - optional, set up specified path for OLCM PostgreSQL, applicable only with on parameter
- -drWalDir <path> - optional, set up specified path for Data Repositories PostgreSQL, applicable only with on parameter

For example,

PgIncrementalConfigTool.exe -on

Enable incremental backup, set up default paths.

PgIncrementalConfigTool.exe -off

Disable incremental backup.

PgIncrementalConfigTool.exe -on -olcmWalDir D:\wal\olcm -drWalDir "D:\wal\dr files"

Enable incremental backup, set up specified paths.

Tool output

The tool configures PostgreSQL databases depending on topology, restarts PostgreSQL services, and displays message "Configuration completed successfully".

In case of errors, it displays "PgIncrementalConfigTool has failed. The log files: <log file path>"

Configure custom data directory of PostgreSQL database

- 1 Get the current PostgreSQL service setting.
 - a Run the command line and on machine where the PostgreSQL database installed, execute the following command: `sc qc olcm-postgresql-x64-14`
 - b The next value after the -D option shows the current data location.
- 2 Stop PostgreSQL service: `olcm-postgresql-x64-14`
- 3 Move content in the current data location to the new location.

- 4 Modify PostgreSQL service settings based on the current. Set up a new data location. For example: `sc config olcm-postgresql-x64-14 binPath= "\"C:\Program Files (x86)\PostgreSQL-14-OLCM\bin\pg_ctl.exe\"" runservice -N \"olcm-postgresql-x64-14\" -D \"E:\NewDataLocation\" -w"`
- 5 Update the registry value for PostgreSQL service. Set up the new data location to:
 - HKEY_LOCAL_MACHINE\SOFTWARE\PostgreSQL\Installations\olcm-postgresql-x64-14\DataDirectory
 - HKEY_LOCAL_MACHINE\SOFTWARE\PostgreSQL\Services\olcm-postgresql-x64-14\DataDirectory
- 6 Start PostgreSQL service: `olcm-postgresql-x64-14`
- 7 Reboot the computer.

Configure custom data directory of Data Repository PostgreSQL database

- 1 Get the current PostgreSQL service settings.
 - a Run the command line and execute the following command:
`sc qc postgresql-x64-14-dr`
 - b The next value after the -D option shows the current data location
- 2 Stop PostgreSQL service: PostgreSQL 14.1.1 (x64).
- 3 Move content in the current data location to the new location.
- 4 Modify PostgreSQL service settings based on the current. Set up a new data location. For example: `sc config postgresql-x64-14-dr binPath= "\"C:\Program Files\PostgreSQL\14\bin\pg_ctl.exe\"" runservice -N \"postgresql-x64-14-dr\" -D \"E:\NewDataLocation\" -w"`
- 5 Update the registry value for PostgreSQL service. Set up the new data location to:
 - HKEY_LOCAL_MACHINE\SOFTWARE\PostgreSQL\E998E784-031A-4F94-9A3A-AB474D21C135\Installations\postgresql-x64-14\DataDirectory
 - HKEY_LOCAL_MACHINE\SOFTWARE\PostgreSQL\E998E784-031A-4F94-9A3A-AB474D21C135\Services\postgresql-x64-14\DataDirectory
- 6 Start PostgreSQL service: PostgreSQL 14.1.1 (x64).
- 7 Reboot the computer.

Restore OpenLab Server/ECM XT Using the Restore Utility

Use these procedures to restore your system from an existing backup if the OpenLab Server/ECM XT server becomes inoperable due to a hardware or software failure.

If you are upgrading your server, perform the following procedures on your machine before the upgrade.

The restore procedure will restore only committed data captured by the successful backup procedure. Any data that was queued for upload and not yet committed or was added or updated after the backup was performed are not recovered by restoring a backup.

CAUTION

Make sure the restore system has the same OpenLab Server/ECM XT update as the system where the backup was created.

CAUTION

In cases where a restored system will run at the same time as the source system (where the backup was taken), make sure that the restored system is on a network that is isolated from the source system. For example, if a test system is created from a backup of the production system, it must be on a network that is isolated from the production system. If the test system and the production system are on the same network, it may cause the two servers to create a cluster and interact with each other. This can lead to data corruption and loss.

In addition, it is important to turn clustering off on the restored system using the following steps:

- 1 On the restored server, open C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco-global.properties.
- 2 Find the `alfresco.cluster.enabled` property and set it to false, as follows:
`alfresco.cluster.enabled=false`
- 3 Restart the AlfrescoTomcat service.

Verification

When restoring to an existing installation, you can also verify the restoration was performed correctly. Verification reports are saved at C:\ProgramData\Agilent\Restore\Verification.

Troubleshooting the restore procedure

The Restore Utility collects logs in the "%ProgramData%\Agilent\LogFiles\Restore" folder. During the restore procedure, all steps are checked and the whole restore procedure stops on the first failed step. A link with the failed step opens the current restore log file to help identify the root cause of the problem. There are validations on each page during restore configuration to prevent possible errors with incorrect credentials, no access to content and archive locations, incorrect format, and other common configuration issues.

Restore a system with PostgreSQL or Microsoft SQL database

Use the Restore Utility to restore a supported OpenLab Server/ECM XT system with a PostgreSQL or MS SQL Server database. For a list of topologies supported by the Restore Utility, see **"Using the Backup and Restore Utilities"** on page 59.

In all other cases follow the manual restore procedure described in **"Manual OpenLab Server/ECM XT Server Restore Procedure"** on page 100.

During the restore procedure, validations on each page prevent possible errors, such as incorrect credentials, no access to content and archive locations, incorrect formats, and other common configuration issues.

For supported topologies, use the following procedure to restore your system using the Restore Utility.

CAUTION

The same update level of OpenLab Server/ECM XT must be installed as on the system where the backup was created. This is required to ensure the patch level of the restored database matches the patch level of the application.

NOTE

The Restore Utility can restore a system from cold and hot backups created with the Backup Utility. The Restore Utility can be run on systems with OpenLab Server/ECM XT installed or on clean systems (see **“Restore on a clean machine without OpenLab Server/ECM XT installed”** on page 76).

NOTE

The Restore Utility does not restore custom certificates used for a secure connection. After restoring, the system will be configured with internal certificates. To configure custom certificates, follow **step 4** in **“Configure OpenLab Server/ECM XT Reverse Proxy”** on page 29. For Index server on 4-server or scalable systems, see **“Index Server Configuration - 4-Server Systems Only”** on page 37.

NOTE

The Restore Utility does not support restoring an Oracle database. See the Oracle documentation for instructions on how to restore an Oracle database.

NOTE

If you are using Sample Scheduler, the Sample Scheduler services must be restarted after the restore procedure.

NOTE

If you are using non-default paths for configuring PostgreSQL for incremental backup in a backed-up system, follow the instructions in **“Configure incremental backup using Incremental Config Tool”** on page 69 after the restore.

Using the Restore Utility for systems with OpenLab Server/ECM XT installed

Use the procedure below to restore a previously-installed system that was backed up using the Backup Utility.

CAUTION

Stop all OpenLab Server/ECM XT operations before performing the restore process. Make sure that any clients, instruments, or other parts of the system are not using the server during the restore process.

Restore to an existing installation using Restore Utility

Steps	Options	Notes
1 Start Restore Utility from Start > Agilent Technologies > Restore Utility.		You must have System Administrator privileges to run and execute the Restore Utility.
2 On the Backup Location page, choose your backup location.	<ul style="list-style-type: none"> Select File system as the Backup location if the backup is located locally or on Windows share. Select the backup folder that was used by the Backup Utility, and click Next. Select AWS S3 as the Backup location if the backup is located on Amazon AWS S3 storage. Specify the AWS S3 backup bucket region and name, keys, and then click Next. Restore and Verify are selected by default. For normal recovery, select Restore only. 	<ul style="list-style-type: none"> The Restore Utility first restores the full backup from the Current folder, then restores any incremental backups from the Incremental folder. Verification reports are saved at C:\ProgramData\Agilent\Restore\Verification. Verification is available only for systems on which the OpenLab software has already been installed. If Verify only is selected, the next page will be Review followed by the Processing page.
3 The Database Server page settings are pre-populated based on the backed-up system.	<ul style="list-style-type: none"> If the current environment state has changed since the backup, modify these settings. For SQL Server, provide the server name and database administrator credentials. For PostgreSQL, provide connection settings and database administrator credentials. For more information about reconfiguring during Restore, see "Reconfiguration during restore" on page 78 	Restoration of Oracle database is not supported and must be restored manually. See your Oracle documentation for instructions on how to restore an Oracle database.
4 The Access Credentials page settings are pre-populated based on the backed-up system.	<ul style="list-style-type: none"> If the current environment state has changed since the backup, modify these settings. Click Verify to confirm the credentials you entered are valid. 	
5 The Content Paths page settings are pre-populated based on the backed-up system.	<ul style="list-style-type: none"> Only file system storage locations can be changed on this screen. Click Verify to confirm the credentials you entered are valid. 	Multiple Content and Archive locations are supported.
6 Review the settings and click Apply.		Progress is tracked on the Restore page.

Restore to an existing installation using Restore Utility (continued)

Steps	Options	Notes
7 The restore procedure progress is tracked on the Restore page.	When prompted at the Run Server Configuration Utility step, enter the Shared Services administrator credentials.	If you selected "Restore and Verify" or "Verify only", a verification step is displayed as the last step. Click the verification status "done" link to open the verification report.
8 When the restore procedure is complete, click Done.		
9 Reboot the system after restore.	Click Yes to reboot the system immediately. Click No to postpone reboot and reboot it manually.	Rebooting the system is recommended after a completed restore on an already-installed system.
10 Perform Step 6- Step 7 starting on page 104.		

Restore on a clean machine without OpenLab Server/ECM XT installed

Use this procedure to restore a backed up OpenLab Server/ECM XT system to a machine that does not have OpenLab Server/ECMXT installed.

NOTE

If you plan to use an MS SQL database, MS SQL Server must be installed prior to running the Restore Procedures. Otherwise, an error will occur during the database server setting step, and the restore process cannot continue.

For PostgreSQL, the utility will restore all PostgreSQL databases on a clean system along with other ECM XT data. You will need to install the software after the restore is complete.

Procedure to restore using Restore Utility on a clean machine

Steps	Options	Notes
1 From the OpenLab Server/ECM XT Server installation media, go to Setup > Tools > RestoreTool and launch RestoreUtility.exe.		For information on how to download and unzip your software installation media, see the OpenLab Server/ECM XT Installation Guide.

Procedure to restore using Restore Utility on a clean machine (continued)

Steps	Options	Notes
2 On the Backup Location page, choose your backup location.	<ul style="list-style-type: none"> Select File system as the Backup location if the backup is located locally or on Windows share. Select the backup location that had been used by the Backup Utility. Select AWS S3 as the Backup location if the backup is located on Amazon AWS S3 storage. Specify the AWS S3 backup bucket region and name, and keys. 	When restoring to a machine where OpenLab Server/ECM XT is not installed, verification is not available.
3 The Database Server page settings are pre-populated based on the backed-up system.	<ul style="list-style-type: none"> If you are restoring a PostgreSQL server on a machine without PostgreSQL installed, you will be prompted to continue the restore process. Click Yes to continue. PostgreSQL will be installed after the restore procedure is complete and OpenLab Server/ECM XT is installed. If a Microsoft SQL database is configured, MS SQL Server must be installed to continue the restore procedure. 	<ul style="list-style-type: none"> For more information about reconfiguration during restore, see “Reconfiguration during restore” on page 78. Do not change the pre-populated server settings.
4 The Access Credentials page settings are pre-populated based on the backed-up system.	<ul style="list-style-type: none"> If the current environment state has changed since the backup, you can modify these settings. 	
5 The Content Paths page settings are pre-populated based on the backed-up system.	<ul style="list-style-type: none"> Only file system storage locations can be changed on this screen. 	Multiple Content and Archive locations are supported.
6 Review the settings and click Apply.		
7 The restore procedure progress is tracked on the Restore page. When the restore procedure is complete, click Done.		.After the OpenLab Server/ECM XT software is installed, run the Restore Utility with the Verify only option selected. This will check data and generate a verification report.

After a successful restore procedure, proceed with standard installation of OpenLab Server/ECM XT. All the values reviewed and configured during restore procedure will be automatically captured during OpenLab Server/ECM XT installation and should not be changed during the process.

Reconfiguration during restore

Reconfiguration may be needed:

- If the server with the database has moved to another computer
- The port or administrative credentials have changed
- A user restores the backup from another server
- Database moved to another instance on the server
- Storage locations have changed
- Content management index path changed

It is possible to reconfigure PostgreSQL and MS SQL settings during the restore procedure. On the Database Server page, the preloaded information about the connection to a database is displayed. If you change anything on this page, you must be sure that this information is correct. The utility will check values and will show a message with details in case of a problem. The reconfiguration of Oracle database settings is not supported and must be done separately.

Reconfiguring a PostgreSQL database server

On the Database Server page, you can change and verify the server name, port, super user, and password. If another user is used, they must have the same privileges as the default super user (postgres).

To check the entered values, click **Verify** or **Next**.

Reconfiguring a Data Repository PostgreSQL password

On the Database Server page, you can change and verify the password of the Data Repository PostgreSQL database super user.

To check the entered values, click **Verify** or **Next**.

Reconfiguring MS SQL database server

On the Database Server page, you can change and verify the server name, named instance, port, super user, and password. If another user is used, they must have the same privileges as the default super user (sa).

A named instance is the name that a user specifies when installing the MS SQL server (if it differs from the default.)

To use the Windows user, it must be added to the MS SQL server security settings. See the OpenLab Server/ECM XT Installation Guide section on Configuring a Remote Database Server.

To check the entered values, click **Verify** or **Next**.

Reconfiguring Access Credentials

On this page, you can change an account that has been used to access all content storage paths. Make sure this account is in the Administrator group on both ECM XT Server and Database server machines.

Separate accounts for individual storage locations are not supported.

Make sure the user has "Log on as a service" permission.

To check the entered values, click **Verify** or **Next**.

Reconfigure Content Paths

In the Content Paths page, you can change any storage location for the restored data by entering a new path as the Restore Location.

You can also specify a new index location by entering a new path as the restore location. The Index Path must be an absolute or UNC path.

NOTE

Network drives are not supported for the index location.

To check the entered values, click **Verify** or **Next**.

Review and start the restore

On the Review page, review the summary of OpenLab Server settings you are configuring.

If everything is correct, click **Apply** to start the restore process. Click **Back** if you want to change something.

Using the Backup and Restore Scripts

If the Backup and Restore Utilities cannot be used for your system for any reason, Backup and Restore Scripts can be used for backing up and restoring.

For All-in-one, 2-server and 4-server topologies, use Backup and Restore scripts for backup and restore described in the following sections. To back up and restore a scalable topology, use the manual backup and restore procedures described in **“Manual Backup and Restore Procedures”** on page 90. The following table describes the OpenLab Server/ECM XT topologies supported by the Backup and Restore Scripts.

Table 6 OpenLab Server/ECM XT topologies supported by the Backup and Restore Scripts

Topology	Backup script	Restore script	Notes
All-in-one	+	+	
2-server	+	+	Oracle database backup and restore uses manual procedure
4-server	+	+	Oracle database backup and restore uses manual procedure
Scalable system	Manual only	Manual only	

4-Server topology includes the following servers:

- OpenLab Server/ECM XT Content Management server (Content Management server)
- OpenLab Index Server (Index Server)
- Database server
- Windows file server and/or AWS S3 storage

Backup and Restore scripts support the following:

- PostgreSQL and Microsoft SQL databases
- File system and AWS S3 storage
- File system backup destination and restore source
- Full immediate backup only

Before you perform any backup and restore operation, review the following sections:

- **“Important Information about Backup and Restore”** on page 55
- **“Creating a Disaster Recovery Plan”** on page 57

NOTE

In case of an Oracle database, the database backup/restore will be skipped and must be done manually. See the Oracle documentation for instructions on how to back up and restore an Oracle database. Perform Oracle database backups before backup of other parts of the system. Use the same order for restore procedures in case of Oracle database.

CAUTION

The Backup and Restore scripts do not support custom certificates used to secure a system. If custom certificates are used, back them up manually and keep in a secure location for use during the restore process. The custom certificates are located in C:\Program Files\OpenLab Reverse Proxy\Apache24\conf\ssl\custom\.

After restoration, the system is configured with internal certificates. To restore custom certificates, use the custom certificates that were backed up and follow step 4 in “Configure OpenLab Server/ECM XT Reverse Proxy” on page 29. For index server on 4-server or scalable systems, see “Index Server Configuration - 4-Server Systems Only” on page 37.

System preparation

Configure the system before starting the backup and restore scripts. To configure the system, use the following instructions.

- 1 On the Content Management server, add the following rows to the C:\ProgramData\Agilent Technologies\OpenLab Platform\Data Repository\postgresql\14\data\pg_hba.conf file:
 - host replication postgres 127.0.0.1/32 md5
 - host replication postgres ::1/128 md5
- 2 In case of PostgreSQL, on the Database server, add the following rows to the C:\ProgramData\Agilent\PostgreSQLData-14-OLCM\pg_hba.conf file:
 - host replication postgres <CM Node IPv4>/<CM Node IPv4 CIDR> md5
 - host replication postgres <CM Node IPv6>/<CM Node IPv6 CIDR> md5

- 3 On the Index and Database servers, go to Windows Defender Firewall with Advanced Security > Inbound Rules and enable the following rules:
 - File and Printer Sharing (SMB-In)
 - File and Printer Sharing (Echo Request - ICMPv4-In)
- 4 On the Content Management and Index servers,
 - a Go to **Windows Defender Firewall with Advanced Security > Inbound Rules > New rule**.
 - b Choose the following options: **Port, UDP, 137** and leave other options at their default values.
 - c Set any name, and click **Finish**.
 - d Verify that the new rule is enabled.
- 5 Configure PowerShell to run signed scripts.
 - a Go to **Start > Windows PowerShell**.
 - b Right-click on **Windows PowerShell**, and select **More > Run as administrator**.
 - c In the opened PowerShell window, run the command: `Set-ExecutionPolicy -ExecutionPolicy AllSigned -Scope LocalMachine`. If the Do **you want to change the execution policy?** question appears, type **A** and click **Enter**.

CAUTION

The backup/restore script initiator user must be an administrator on the Content Management, Database, and Index servers. The user must have access (granted Read and Write permissions) to Content and Archive storage locations and also a backup location.

NOTE

The Backup and Restore scripts are delivered as a .zip archive. Upload the .zip file to the Content Management server. Before extracting it, right-click on it, go to **Properties > General**, and make sure there is no **Security** section with an **Unblock** check box in it. If the **Security** section with an **Unblock** check box is shown, select the **Unblock** check box and click **Apply**.

Back up OpenLab Server/ECM XT using the backup script

Supported backup scenarios

The backup script (Secure_OpenLABCDS_backup.ps1) can be executed on the system to back up the following data:

- Configuration files for Content Management and Index servers
- Databases for Shared Services, Content Management, and Data Repository
- Solr Indexes
- Content and Archive storages
- Alfresco cache
- Certificate Service certificates

Space required

The free space required for the backup procedure depends on various factors, including the server configuration, backup location, and database backup size. In the most resource-intensive case, make sure free space in the backup location is at least twice as large as the sum of all on-prem file storage and database size. This is needed to avoid rewriting a previous successful backup with a backup that finished in the middle for any reason.

Procedure for using the backup script

The backup procedure is performed by executing the Secure_OpenLABCDS_backup.ps1 script on the Content Management server using Windows PowerShell.

- 1 Go to **Start > Windows PowerShell**, right-click on **Windows PowerShell**, and select **More > Run as different user**.
- 2 In the opened dialog window, set the login and password of the user you want to run the backup. Click **OK**.
- 3 Type the following command in the PowerShell window to perform the script in the privileged mode:

```
Start-Process -FilePath "powershell" -Verb RunAs
```

If a request for User Account Control access appears, click **Yes**.

- 4 In the new opened PowerShell window, navigate to the folder where the Backup script is located (C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Backup and Restore Scripts by default).

For example, use the command: `cd "C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Backup and Restore Scripts"`

- 5 Execute the `Secure_OpenLABCDS_backup.ps1` script. Provide the parameters: `.\Secure_OpenLABCDS_backup.ps1 -backupDestinationDir "<destination_path>" [-hotBackup]`

where the following parameters are used:

- `<destination path>` - the backup destination path. For example, `C:\BackupDir`. The absolute local folder and network share paths are supported by the script.
- `[hotBackup]` - an optional parameter to choose Hot backup or Cold. By default, the parameter is absent and the cold backup is run. Hot backup means that the system remains operational during backup. In case of Cold backup all the OpenLab Server/ECM XT operations are stopped automatically before the backup starts and run after the backup is completed.

- 6 Wait until the Backup script finishes. If the backup is successful, the "Backup has completed" message is displayed and the backup folders are created in the `<destination_path>` location.

In case of a failed backup, the partial backup is saved in a Temp folder in your backup location. The unsuccessful backup attempt does not overwrite and corrupt the previous successful backup in the Current folder.

Troubleshooting the backup

Whenever the backup script is run, the execution log is written into the `%AppData%\Agilent\LogFiles\Backup` folder using the "Backup_log_" prefix and timestamp at the end. In case of the script failure, the message "The backup has failed." will be printed in the log and provides log file path for the current execution. A current backup log file can help to identify an issue. In case of a failed backup, the partial backup is stored in a Temp folder in the backup location.

In case of script execution errors, follow this procedure:

- 1 Ensure that all actions from **“System preparation”** on page 81 were performed on required system components before running the backup procedure.
- 2 Ensure that the user who is running script has appropriate permissions according to **“System preparation”** on page 81.
- 3 Ensure that all machines are up and running and accessible from the machine where the script is executed (for example, Database server, Index server, or Windows file server).
- 4 Ensure the Database server account has database administrator privileges/super user.
- 5 Ensure that antivirus scanning is not preventing the successful backup completion. Exclude the backup location for both regular/scheduled scans and real-time protection.
- 6 Ensure there is enough C drive space on Content Management and Database servers. If there is not enough space on the C drive for a temporary database backup, you can use other local drive for this purpose. To do this, follow the instructions in **“Change temporary database location for backup and restore procedures”** on page 89.
- 7 In case none of the above steps help, collect the log files from the %AppData%\Agilent\LogFiles\Backup folder and contact Agilent support.

Restore OpenLab Server/ECM XT using the restore script

This section describes how to restore an All-in-one, 2-server, and 4-server topology using the restore script.

Supported restoration scenarios

The restore script (Secure_OpenLABCDS_restore.ps1) can be executed on the following environments:

- To restore existing system after disaster occurred, to restore data at the moment of the backup
- To restore system from backup on a new clean system (no OpenLab/ECM XT Server installed)
- To restore system from backup on a newly installed environment

- For all supported cases, the script can be executed without installing additional software

CAUTION

The database server, Index node, and data storages server(s) must have the same names as at the moment of backup. The installation\configuration.xml file from the backup can be reviewed to get names of the database server, Index node, and storage locations.

Procedure for using the restore script

The restoration procedure for supported topologies is performed by executing the Secure_OpenLABCDS_restore.ps1 script using Windows PowerShell on the machine which is used as a Content Management server.

NOTE

Ensure that all actions from **"System preparation"** on page 81 were performed on required system components before running the restoration procedure.

- 1 Go to **Start > Windows PowerShell**, right-click on **Windows PowerShell**, and select **More > Run as different user**.
- 2 In the opened dialog window, set the login and password of the user you want to run the backup. Click **OK**.
- 3 Type the following command in the PowerShell window to perform the script in the privileged mode:

```
Start-Process -FilePath "powershell" -Verb RunAs
```

If a request for User Account Control access appears, click **Yes**.

- 4 In the new opened PowerShell window, navigate to the folder where the Restore script is located (C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Backup and Restore Scripts by default on installed system).

For example, use the command: `cd "C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Backup and Restore Scripts"`

In case of restoring to clean system find, the script in media: `.\Setup\Scripts\Server Restore`.

- 5 Execute the Secure_OpenLABCDS_restore.ps1 script, providing backup location path:

```
.\Secure_OpenLABCDS_restore.ps1 -backupDir "<path_to_backup>"
```

where the <path_to_backup> is a file system path for a stored backup. The absolute local folder and network share paths are supported by the script.

- 6 Wait until script finishes. If the restore is successful, the "The restore has completed" message is displayed.
- 7 Reboot the system.

NOTE

If performing the restore procedure on a system with ECM XT server already installed, it is possible that a window requesting ECM XT Administrator credentials pops up during the Server Configuration Utility execution. The window appears if ECM XT Administrator credentials were changed since the last execution of the Server Configuration Utility.

NOTE

In case of a 4-server or scalable system, run the System Configuration Utility for the Index server after restoration to apply system settings.

NOTE

For restoration on an already installed ECM XT Server, if the Content Management server name differs from the name used at backup, you must:

- Open Shared Services Control Panel and activate Content Management with the new server name on the Content Management server.
- Navigate to the Index node machine and run the Server Configuration Utility to apply system settings.

NOTE

In case the -backupDir parameter is not specified, the script will prompt to provide the path for a backup. Type the path to the backup and press **Enter**.

Troubleshooting the restore

Whenever the restoration script is run, the execution log is written into the %AppData%\Agilent\LogFiles\Restore folder with the "Restore_log_" prefix and timestamp at the end. In case of the script failure, the message "The restore procedure has failed." will be printed in the log and provides the log file path for the current execution.

In case of script execution errors, use the following procedure:

- 1 Ensure that all actions from **"System preparation"** on page 81 were performed on required system components before running the restoration procedure.
- 2 Ensure that the user who is running script has appropriate permissions according to **"System preparation"** on page 81.

- 3 Ensure that all machines are up and running and accessible from the machine where the script is executed (for example, Database server, Index server, or Windows file server.)
 - The Database server, Index server, and Windows file server must have the same names as during backup. The Installation\configuration.xml file from the backup can be reviewed to get names of the Database server, Index server, and storage locations.
- 4 Ensure that Database server account used at the moment of backup is present with same credentials on the Database server and has database administrator privileges/super user.
- 5 Ensure there is enough space on the C drive of the Content Management and Database servers. If there is not enough space on the C drive for a temporary database backup, you can use other local drive for this purpose. To do this, follow the instructions from **“Change temporary database location for backup and restore procedures”** on page 89.

In case of none of the troubleshooting steps help, collect the log files from the %AppData%\Agilent\LogFiles\Restore folder and contact Agilent support.

Change temporary database location for backup and restore procedures

By default, backup/restore scripts use the C:\ProgramData\Agilent\Backup and C:\ProgramData\Agilent\Restore folders to store a database backup during the backup/restore procedure. A database backup needs enough free space on the C drive for its temporary location. If the drive C space is not big enough and backup/restore fails because of this, another local drive can be used. To do this, run the LinkTempFolderForBackupAndRestoreDatabase.ps1 script. It is located in C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Backup and Restore Scripts by default.

NOTE

The "LinkTempFolderForBackupAndRestoreDatabase.ps1" script is executed on the Database server in case of remote MSSQL, otherwise it is executed on the Content Management server. The script is executed once.

To change the temporary database backup location using the LinkTempFolderForBackupAndRestoreDatabase.ps1 script:

- 1 Go to **Start > Windows PowerShell**, right-click on **Windows PowerShell**, and select **More > Run as Administrator**.
- 2 In the opened PowerShell window, navigate to the folder where the script is placed (C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Backup and Restore Scripts by default).

For example, use the command: `cd "C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Backup and Restore Script"`

- 3 Run the command: `.\LinkTempFolderForBackupAndRestoreDatabase.ps1 -tempFolderForBackupAndRestoreDatabase "<new_temporary_DB_path>"`

where the following parameter is used:

<tempFolderForBackupAndRestoreDatabase> - a new temporary database backup location. Only local path is supported, for example, "E:\New temp folder"

- 4 Wait until the script finishes.



6

Manual Backup and Restore Procedures

Manual OpenLab Server/ECM XT Server Backup Procedure	91
Manual OpenLab Server/ECM XT Server Restore Procedure	100
Data Migration of Manual Backup on Different Server	108

Manual OpenLab Server/ECM XT Server Backup Procedure

It is mandatory that every OpenLab Server/ECM XT server is backed up regularly. Periodic full backups and differential backups between the full backups must be created by OpenLab Server/ECM XT server administrators. These backups are the only way to restore an OpenLab Server/ECM XT server if a hardware or software failure occurs.

The backup only reduces the amount of data loss if a catastrophic system failure occurs. Performing backups guarantees that any data that was committed at the time of the backup can be restored. Any data that was queued for upload and not yet committed or was added or updated in the system after the backup was performed will not be recoverable by restoring a backup.

It is also mandatory that the restore procedures (**"Manual OpenLab Server/ECM XT Server Restore Procedure"** on page 100) are tested to ensure that the backups are performed properly, and can be used for a restore. To do an effective restore, a disaster recovery plan must be created.

OpenLab Server/ECM XT stores files and indexes on your server's file system. The location of this folder is determined when the product is installed. Other data, such as folder information, audit trails, and signatures are stored in a relational database.

A full backup captures a complete set of data in OpenLab Server/ECM XT, including uploaded files and its databases. A differential backup contains changes that have occurred since the last full backup. The differential backup process is faster than the full backup since it is backing only the changed elements.

If you are upgrading your server, perform the following procedures on your machine before upgrading. All work areas and file upload queues should be cleared before the upgrade procedure. You should not have data in any queues when performing the upgrade to a different OS. All file uploads should be complete. The file buffer upload queue should be cleared before the upgrade.

Perform a manual system backup

Step 1 Determine your database, content, and index folders

To backup and restore OpenLab Server/ECM XT, you need to know the name of your databases, the location of the stored content folder, the location of the stored indexes folder, and other installation and configuration information.

There are two databases that need to be backed up. The OpenLab Server/ECM XT server database and the Shared Services database. The names of these databases can be retrieved from the Server Configuration page.

Similarly, the content folder path is also a parameter that is specified during the server installation. You can use the following procedure to determine these paths.

- 1 Go to the OpenLab Server/ECM XT server machine.
- 2 Click **Start > All Programs > Agilent Technologies > Configuration Viewer**.

A webpage appears and provides the paths for contentstore, index, and the offline archive.

Content Management Content Summary	
Server Configuration	Content Management with Index and Search Services
Primary Content Storage Location	C:\DataStoreContent
Secondary Content Storage Location(s)	None
Primary Archive Storage Location	C:\DataStoreArchive
Secondary Archive Storage Location(s)	None
Index Path	C:\DataStoreIndex
Index hostname	

Figure 3. OpenLab Server/ECM XT Server Content Summary

NOTE

If your topology has a separated Index Node Server, then the index path may be found on that Index Node Server.

If your repository has multiple content stores, then you need to back up each of the additional content stores. To determine if your system has multiple content stores and their locations:

- 1 Open the **alfresco-global.properties** file from **<INSTALLATION PATH>\OpenLab Data Store\tomcat\shared\classes** (the default location is C:\Program Files (x86)\Agilent Technologies\OpenLab Data Store\tomcat\shared\classes directory of your OpenLab Server/ECM XT server).

- 2 Search for **dir.root** property. If there are multiple content stores, they will be listed as shown below, where we see two content stores defined.

```
dir.root=\\\\HA-ContentStore\\ContentStore# content store 1
dir2.root=\\\\HA-ContentStore\\ContentStore2 # content store 2 (current)
```

Step 2 Stop OpenLab Server/ECM XT services:

Open **Windows Services** (services.msc) and **Stop the services**:

- Agilent OpenLab Content Management Search service. Skip this service if it is disabled.
- alfrescoTomcat
- Agilent OpenLab Shared Services
- olcm-postgresql-x64-14 (only applicable when using PostgreSQL database for OpenLab Server/ECM XT). Skip this service if the database is on a separate host.

NOTE

If your topology has several ECM XT Servers or a separated Index Node Server, then these services should be stopped on all ECM XT Servers.

For MSSQL Server or Oracle, please see the vendor database documentation on how to stop services. If the database is on a separate host, then this step must be performed on that host.

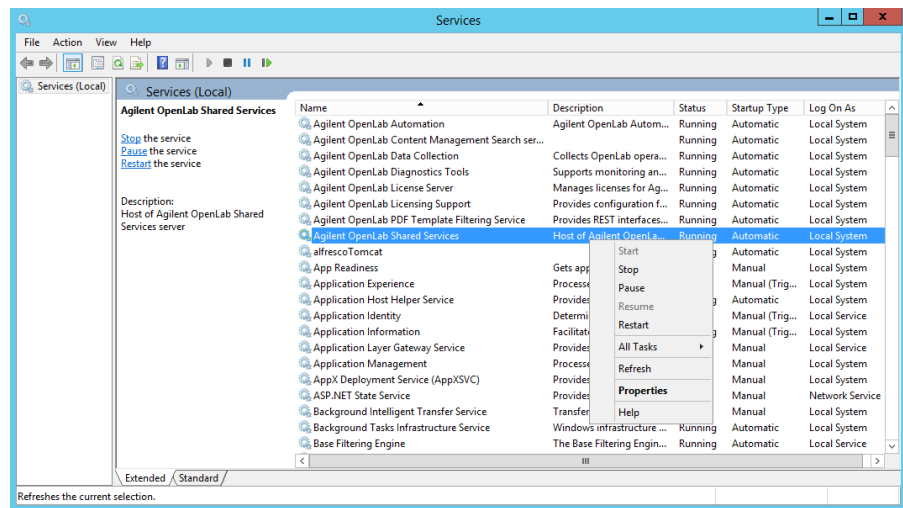


Figure 4. Stop OpenLab Server/ECM XT Services

Step 3 Back up databases

This section provides a simple and interactive approach to backup databases. Please see PostgreSQL, MS SQL Server, or Oracle documentation for other options, some of which may allow you to automate the process as well.

Procedure for PostgreSQL The location where the database files are stored is specified during the server installation. In the case of the local PostgreSQL database, by default, it is C:\ProgramData\Agilent\PostgreSqlData-14-OLCM. If customized during installation, you can find the location information in the Server Configuration (Start > All Programs > Agilent Technologies > Server Configuration Viewer).

This information is also recorded in Windows registry at:

```
"HKEY_LOCAL_MACHINE\SOFTWARE\PostgreSQL\Installations\postgresql-x64-14\Data Directory".
```

For a remote PostgreSQL database, this information is recorded in the Windows registry at:

```
"HKEY_LOCAL_MACHINE\SOFTWARE\PostgreSQL\Installations\postgresql-x64-14\Data Directory"
```

Back up the PostgreSQL database by backing up the database folder (C:\ProgramData\Agilent\PostgreSqlData-14-OLCM) using **Windows Server Backup** or any other tool of your choice.

CAUTION

If your server is configured to use PostgreSQL version before 14.1 and you upgrade your system in place to the latest version, the PostgreSQL database will be upgraded to version 14.1 and database data will be migrated to C:\ProgramData\Agilent\PostgreSqlData-14-OLCM. Any backup and restore activity should occur on the upgraded system.

Procedure for MS SQL Server Make sure that MSSQL Service is started. Use **SQL Server Management Studio** to back up the Shared Services database (OLSharedServices) and the OpenLab Server/ECM XT server database (DataStore). The tool allows users to perform **Full Backups** as well as **Differential Backups**.

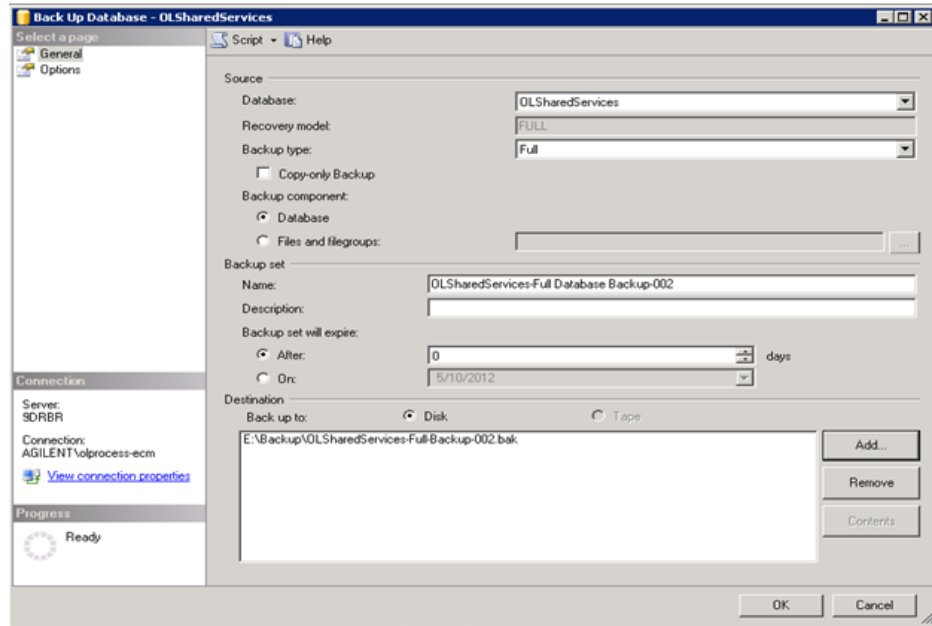


Figure 5. Using SQL Server Management Studio for backup

Procedure for Oracle Server See the Oracle documentation for backing up an Oracle database.

Step 4 Back up content, index, and archive folders

Use the **Windows Server Backup** or any other tool of your choice to backup the OpenLab Server/ECM XT content folder (**C:\DataStoreContent**), index folder (**C:\DataStoreIndex**), and Archive folder (**C:\DataStoreArchive**).\

If your topology has a separated Index Node Server, back up the index from that Index Node.

If you have multiple content stores, you have to back up each additional content folder (**D:\DataStoreContent2**).

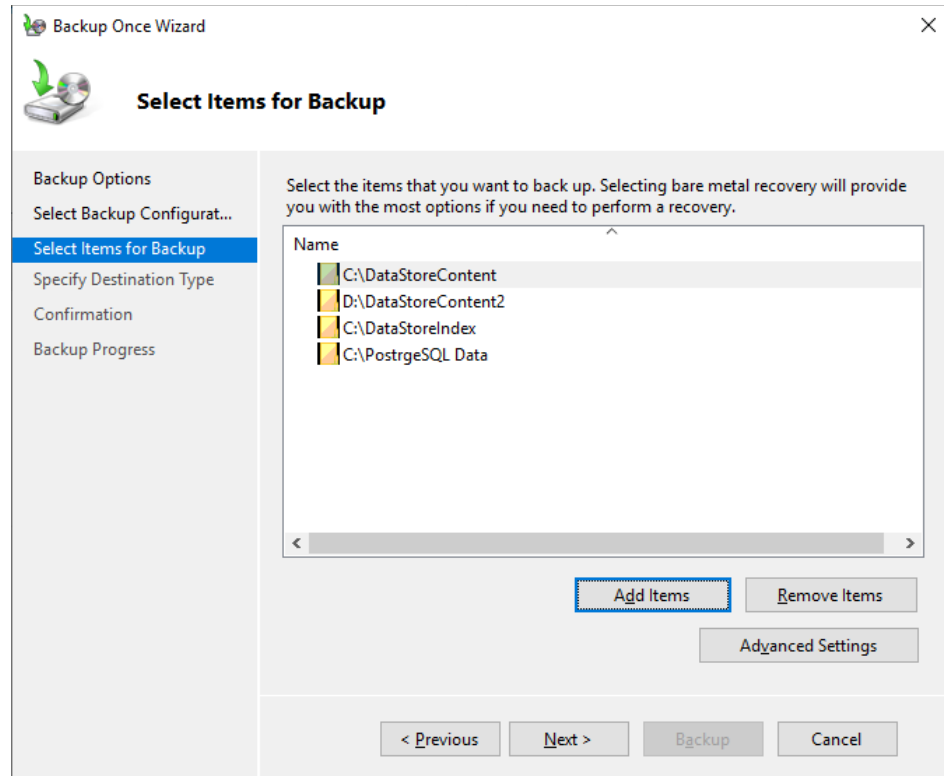


Figure 6. Using Windows Server Backup

Step 5 Backup OpenLab Server/ECM XT server configuration information

- 1 Locate the **<Installation Directory>\OpenLab Data Store\tomcat\temp\com.agilent.datastore.cache** file, and copy it to the **C:\ProgramData\Agilent\Installation** folder.

The **<Installation Directory>** can be found in the **Installation Summary** on the **Server Configuration** page.

- 2 Backup the **C:\ProgramData\Agilent\Installation** folder. This will be used to reconfigure the system at a later point.

NOTE

If your topology has a separated Index Node Server, then the index path may be found on that Index Node Server.

NOTE

If your topology has several ECM XT Servers or a separated Index Node Server, then back up these files from all ECM XT and Index Node Servers.

Step 6 Backup custom certificates

If you are using custom certificates for a secure connection, back up these certificates. Copy the **C:\Program Files\OpenLab Reverse Proxy\Apache24\conf\ssl\custom** folder to the backup location.

Step 7 Back up OpenLab Certificate Server

Copy the **C:\ProgramData\Agilent\OpenLab Certificate Service** folder to the backup location.

Step 8 Start OpenLab Server/ECM XT services

Open **Windows Services** (services.msc) and **Start the services**:

- olcm-postgresql-x64-14 (only applicable when using PostgreSQL database for OpenLab Server/ECM XT). Skip this service if the database is on a separate host.

If the database is on a separate host, then this step must be performed on that host.

- Agilent OpenLab Shared Services
- alfrescoTomcat
- Content Management Search service. Skip this service if it is disabled.

NOTE

If you are using Sample Scheduler, the Sample Scheduler services must be restarted after the restore procedure.

NOTE

If your topology has several ECM XT Servers or a separated Index Node Server, then start these services on all ECM XT and Index Node Servers.

Manual Data Repository database backup

Data Repository supports automatic backups and manual recovery by means of PowerShell scripts. The Data Repository backup and restore procedure enables a full database backup to a custom compressed backup file and a full database restoration from that custom backup file. This procedure relies on the built-in commands `pg_dump` and `pg_restore`.

To support scheduled backups, Data Repository 1.4 stores user credentials in the Windows Registry in encrypted form.

To complete this procedure, you will need the following:

- A PostgreSQL database that was installed and configured within the authority of Data Repository
- Read access on all database objects
- Write access to the backup target folder.

NOTE

In order to avoid unnecessary errors when the script is executed, run PowerShell in a mode that does not restrict the execution. Use the following command to force unrestricted script execution.

```
PowerShell.exe Set-ExecutionPolicy UnRestricted -Force
```

Using Group Policies, an administrator can prevent bypassing the execution policy. In this case, PowerShell scripts cannot be executed.

NOTE

If your topology has several ECM XT Servers or a separated Index Node Server, then these services should be stopped on all ECM XT Servers.

Create the backup

The Data Repository backup script is located in the Data Repository installation folder at:

```
C:\Program Files (x86)\Agilent Technologies\OpenLab Platform\Data
Repository\Data Repository\Service\Scripts\PostgreSQL\Backup
\dr-db-backup.ps1
```

SYNOPSIS

Agilent Technologies - OpenLab Data Repository Backup Utility

SYNTAX

```
dr-db-backup.ps1
[[-hostname] <String>]
[[-port] <String>]
[[-database] <String>]
[-path] <String>
```

DESCRIPTION

Create a backup of a running PostgreSQL database using the `pg_dump` custom compressed format.

PARAMETERS

```
-hostname <String>
    Specifies the PostgreSQL server.
-port <String>
    Specifies the PostgreSQL server port.
-database <String>
    Specifies the PostgreSQL database.
-path <String>
    Specifies the backup directory.
```

Example backup call

```
./dr-db-backup -path c:\temp
```

Backup output

This script creates a full PostgreSQL backup using the built-in command **pg_dump** and stores the result in the custom backup file format **.bakpgdc**. This is a compressed archive of all database objects, including a table of contents.

If the backup operation is successful, the exit code is **0**. If the backup directory is invalid, the exit code is **2**. The error code is **1** on any other error.

Manual OpenLab Server/ECM XT Server Restore Procedure

Use these procedures to restore your system from an existing backup if the OpenLab Server/ECM XT server becomes inoperable due to a hardware or software failure.

If you are upgrading your server, perform the following procedures on your machine after the upgrade.

The restore procedure will restore only committed data captured by the successful backup procedure. Any data that was queued for upload and not yet committed or was added or updated in the system after the backup was performed will not be recoverable by restoring a backup.

Step 1 Restore the databases

Procedure for a PostgreSQL Server Determine your database folder (for example, **C:\ProgramData\Agilent\PostgreSqlData-14-OLCM**), and restore the PostgreSQL databases to it from your backup. It is recommended to keep the original paths to simplify further configuration.

CAUTION

If your server is configured to use PostgreSQL version before 14.1 and you upgrade your system in place to the latest version, the PostgreSQL database will be upgraded to version 14.1 and database data will be migrated to C:\ProgramData\Agilent\PostgreSqlData-14-OLCM. Any backup and restore activity should occur on the upgraded system.

Procedure for an MS SQL Server Use these procedures to restore the database and modify the settings for each restored database.

Restore databases

Restore the Shared Services database (OLSharedServices) and OpenLab Server/ECM XT server database (DataStore) using SQL Management Studio.

Configure Shared Services database settings using SQL Management Studio

- 1 Check database user in **Shared Services database > Security > Users** (review users to re-use existing user, or remove and create a new one).
- 2 Check and Grant db_owner for the database user used in Step 1.

3 Check MS SQL Server logins

a Go to **Security > Logins**.

b Ensure the Shared Service login is present on the MS SQL Server (create it if it is required).

If MS SQL Server authentication was used in Step 2 of the installation procedure, ensure the existence of the login used on this step.

If Windows Authentication was used in Step 2 of the installation procedure, check the following predefined logins:

- For local MS SQL Server database (MS SQL Server and ECM XT Server are installed on the same machine), use 'NT AUTHORITY\SYSTEM' login.
- For remote MS SQL Server database (MS SQL Server and ECM XT Server are installed on 2 different machines), use the 'DOMAIN\ECM XT Server machine name\$' from Windows login. (For example, if Domain is Agilent and ECM XT Server is installed on the 'ECMServer' machine, then the 'Agilent\ECMServer\$' from Windows login should be used/created.)

4 Map the Shared Service user with the MS SQL Server login.

a Select **Map** for OLSharedServices database.

b Map the MS SQL login to the Shared Services database use from Step 1.

Configure DataStore database settings using SQL Management Studio

1 Check the database user in **DataStore database > Security > Users** (review users to re-use existing user, or remove and create a new one).

2 Check and Grant db_owner for the database user used in Step 1.

3 Check MS SQL Server logins.

a Go To **Security > Logins**.

b Ensure the DataStore login used in a Step 2 of the installation procedure is present on the MS SQL Server (create it if it is required.)

4 Map the DataStore user with the MS SQL Server login.

a Select **Map** for DataStore database.

b Map the MS SQL login to the DataStore database user from Step 1.

Procedure for an Oracle Server See the Oracle documentation for restoring the database from a backup.

Restore the Data Repository database To complete this procedure, you will need the following:

- A PostgreSQL database that was installed and configured using Data Repository
- All applications that have been covered by the specified backup must have been installed and registered with Data Repository according to their documentation
- Read and write access to the backup directory

Restore the backup The Data Repository restore script is located in the Data Repository installation folder at:

C:\Program Files (x86)\Agilent Technologies\OpenLab Platform\Data Repository\Data Repository\Service\Scripts\PostgreSQL\Backup.

SYNOPSIS

Agilent Technologies - OpenLab Data Repository Restore Utility

SYNTAX

```
dr-db-restore.ps1
[[-hostname] <String>]
[[-port] <String>]
[[-database] <String>]
[-path] <String>
[-quiet]
```

DESCRIPTION

Restore a backup of a running PostgreSQL database using the pg_dump custom compressed format.

PARAMETERS

```
-hostname <String>
    Specifies the PostgreSQL server.
    - optional, default: 'localhost'
-port <String>
    Specifies the PostgreSQL server port.
    - optional, default: 5433
-database <String>
    Specifies the PostgreSQL database.
    - optional, default: 'datarepo'
-path <String>
    Specifies the backup directory.
-quiet
    Restore will be done without user interaction.
    - optional
```

Example restore calls `./dr-db-restore -path c:\temp`

Restore output Data Repository uses the built-in command **pg_restore** to restore the custom PostgreSQL database backup **pg_dump**, starting with the most recent backup file in the target directory path.

When you specify the parameter **-quiet**, Data Repository will restore the latest backup without any user interaction.

If the backup operation is successful, the exit code is **0**. If the backup directory is invalid, the exit code is **2**. The error code is **1** on any other error.

Step 2 Restore content, index, and archive folders

Determine the locations of your OpenLab Server/ECM XT content folder (**C:\DataStoreContent**) and index folder (**C:\DataStoreIndex**), and Archive folder (**C:\DataStoreArchive**), and restore them from your backup. It is recommended to use the original paths to simplify further configuration.

If you have multiple content storages, each additional content storage must be restored to its own location.

For topologies where storages are located in shared network resources, the user, after restoring the storages, also needs to restore permissions or take care of their availability for the server.

Rebuild the Activity Log Index Use the following procedure to rebuild the OpenLab Shared Services Activity Log Index when the Activity Log table or data is corrupted or when the Shared Services database has been restored with an existing OpenLab installation.

The Activity Log Index is automatically rebuilt in the following scenarios:

- You are using a file-based Workstation configuration using a Firebird database
- The Shared Services database has been restored with a fresh installation
- You are migrating or updating your data

The time required to rebuild the index depends on your database type and the amount of Activity Log records. It may take up to a few hours. During this time, you cannot search the Activity Log in the application.

To rebuild the Activity Log,

- 1 Start the Command Prompt as an Administrator.
- 2 Execute the following command:

```
net stop SharedServicesHost && del /s /f /q
%ProgramData%\Agilent\OLSS\Index\ActivityLog && net start
SharedServicesHost
```

Possible errors include:

- **Message**

The Agilent OpenLab Shared Services service is not started. More help is available by typing NET HELPMSG 3521.

Solution

Use the following command instead:

```
del /s /f /q %ProgramData%\Agilent\OLSS\Index\ActivityLog &&
net start SharedServicesHost
```

- **Message**

System error 5 has occurred. Access is denied.

Solution

Make sure the Command Prompt has been started as an Administrator.

Step 3 Restore OpenLab Server/ECM XT configuration information

Restore the installation/configuration related file to

C:\ProgramData\Agilent\Installation.

For scalable systems, restore this folder for each node.

Step 4 Restore OpenLab Certificate Services

Copy the backup of the Certificate Services folder to the "C:\ProgramData\Agilent\OpenLab Certificate Service" folder.

Step 5 Install OpenLab Server/ECM XT using original configurations

Follow the installation procedures to install and configure a new OpenLab Server/ECM XT on the machine. The following procedure describes how to install an OpenLab Server/ECM XT using restored information using a PostgreSQL database as an example; the procedure is similar for other databases as well.

- 1 Run **Step 1 - Install or Upgrade Software Prerequisites** from the installer.
- 2 On the **Database Type** screen, check that **PostgreSQL Server (v14)** is selected, and click **Next**.
- 3 On the **PostgreSQL** screen, keep the default Server Name and Port, and click **Next**.
- 4 On the **PostgreSQL Settings** screen, do not change the PostgreSQL installation path. Ensure that the database file locations correspond to the locations where the database files were restored.

- 5 Enter a **superuser password**, and complete the prerequisites installation.
- 6 Run **Step 2 - Create or Update Database Schema** from the installer.
- 7 On the **Server Information** screen, select **Connect to and upgrade existing databases for Content Management**, and click **Next**.
- 8 Complete the database schema configuration.
- 9 Run **Step 3 - Install or Upgrade the OpenLab Content Management Server Software**.
- 10 Run **Step 4 - Configure the OpenLab Content Management Server**. Please be ready to provide Shared Services admin credentials during this step.
- 11 On the **Content Paths** screen, check that all database file locations match the actual data folder locations. Click **Verify**, and then click **Next**.
- 12 Review the overall configuration summary carefully. If it is OK, click **Apply**.

Step 6 Change the license server in OpenLab Control Panel

Follow this procedure if the license server is moved to a computer to a different name.

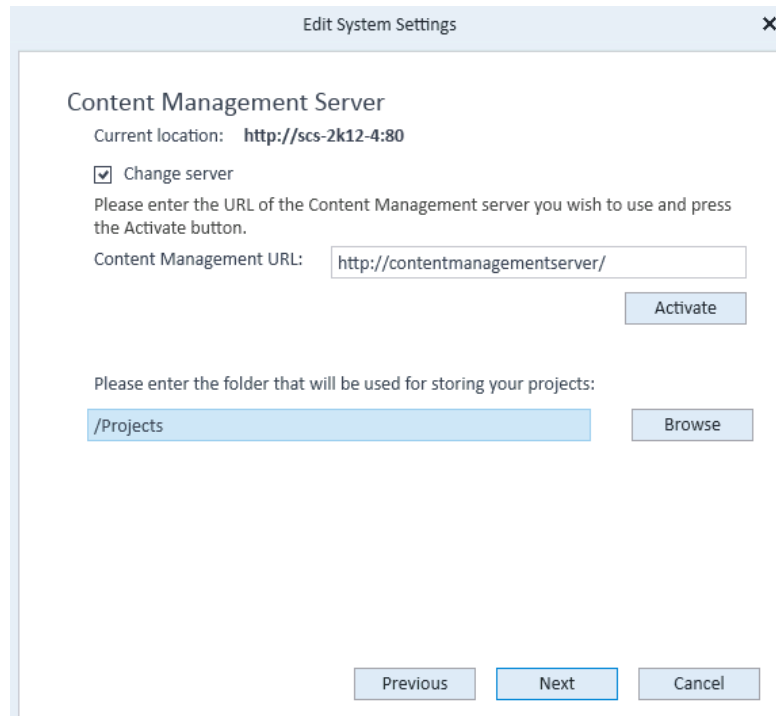
- 1 Log in to OpenLab Control Panel as an administrator.
- 2 Click **Administration > Licenses > Change Server**.
- 3 Type the name of the license server.
- 4 Click **Ping** to make sure that the new server is correct.
- 5 Click **OK**.
- 6 Restart the machine.

Step 7 Activate OpenLab Server/ECM XT

If the Restore is being done on the same host name, OpenLab Server/ECM XT does not need to be re-activated. However, if the server is moved to a new machine, OpenLab Server/ECM XT may require reactivation.

- 1 Open the **OpenLab Control Panel >Administration**.
- 2 Click **System Configuration > Edit System Settings**.
- 3 Select either **Internal** or **Windows domain** for the authentication provider. If you had already configured with one of these values previously, you can choose **Keep current configuration**. If you select **Windows domain**, see **"Windows Domain"** on page 46.
- 4 Select **Content Management** as the storage type, and click **Next**.

- 5 If you did not keep the current configuration for the authentication provider, enter the **Authentication Parameters** for the administrator account.
- 6 Click **Next**.
- 7 Select **Change server**, provide the OpenLab Server/ECM XT URL, and click **Activate** to re-activate the OpenLab Server/ECM XT synchronization.



Edit System Settings

Content Management Server

Current location: **http://scs-2k12-4:80**

☒ Change server

Please enter the URL of the Content Management server you wish to use and press the Activate button.

Content Management URL:

Please enter the folder that will be used for storing your projects:

Figure 7. OpenLab Server/ECM XT Activation

- 8 Click **Next**, and then click **Apply**.

NOTE

If you are using Sample Scheduler, the Sample Scheduler services must be restarted after the restore procedure.

Step 8 Client Configuration

If the OpenLab Server/ECM XT server was restored to a different host, every client in the setup has to be configured to the new OpenLab Server/ECM XT server. This procedure must be repeated from each client machine.

- 1 Select **Windows Start > All Programs > Agilent Technologies > Shared Services Maintenance**.
- 2 Click the **Server Settings** tab.
- 3 Click **Add Server**, and provide a Name and optional Description.
- 4 Enter the new hostname in the **Server** field, and click **Test Connection**.
- 5 Click **OK**, and set this server as the default. You can now log into Control Panel.

Step 9 Restore custom certificates

If your backup contains a folder with custom certificates, configure them by following **step 4** in **"Configure OpenLab Server/ECM XT Reverse Proxy"** on page 29. For index server on 4-server or scalable systems, see **"Index Server Configuration - 4-Server Systems Only"** on page 37.

Step 10 Check the License in Control Panel

If your server MAC address changed during a server upgrade, the license for the new server will be different from the old server.

- 1 From the **Control Panel**, select **Administration > Licenses**.
- 2 In the **Licensing** toolbar, click **View Licenses**. The information will display in an Internet window.

Re-apply the license, if needed. See the Control Panel Help for more information.

Data Migration of Manual Backup on Different Server

This section covers migration of data from a manual data backup on a different server. Use this procedure when upgrading from an OpenLab Server/ECM XT v2.4 system (Win2012 server) to a v2.7 server with a newer operating system (Win2016, Win2019, or Win2022.)

The following steps apply to an All-In-One OpenLab Server/ECM XT 2.4 server.

NOTE

The new server inheriting data should be on a server operating system supported by OpenLab Server/ECM XT v2.7, for example, Win2022.

- 1 Install All-In-One OpenLab Server/ECM XT 2.4 and software updates on a new server.
- 2 Follow the 2.4 *OpenLab Server/ECM XT Administration Guide* section “Perform a manual system backup” to backup old server data.
- 3 Transfer and restore data to the new server using Windows Server Backup or other tools of your choice.
- 4 Manually replace the C: drive folders and files with the backup folders and files.
 - a Stop the following services. This is required to successfully replace C: folders.
 - AlfrescoTomcat
 - Agilent OpenLab Content Management Search Service
 - Agilent OpenLab Shared Services
 - olcm-postgresssql-x64-10
 - b Replace the C: folders and files with corresponding backup data:
 - PostgreSQLData-10-OLCM - **C:\ProgramData\Agilent\PostgreSQLData-10-OLCM**
 - DSContent - **C:\DSContent**
 - DSIndex - **C:\DSIndex**
 - DataStore Archive - **C:\DataStoreArchive**
 - Installation Folder - **C:\ProgramData\Agilent\Installation**

- c Restart the services in reverse order:
 - olcm-postgresql-x64-10
 - Agilent OpenLab Shared Services
 - Agilent OpenLab Content Management Search Service
 - AlfrescoTomcat
- 5 Reconfigure the new server with the original schema by running Step 2 and Step 4 of the OpenLab Server/ECM XT v2.4 installer.
 - On Step 2, select **Connect to a upgrade existing database for Content Management** and ensure old server logins schema are connecting to the database.
 - On Step 4, check that all database file locations match the actual data folder locations. Click **Validate** and check that it is successful as you proceed through the step.
- 6 Reactivate Content Management in OpenLab Control Panel.

At this point, Content Management is pointing to the old server location and must be changed:

 - a Log in to OpenLab Control Panel with an administrator user.
 - b Access Edit System Settings from **Administration > System Configuration > Edit System Settings**.
 - c Select the drop-down menu under Content Management and select **Content Management**.
 - d Click **Next**.
 - e If the current location of the Content Management Server is pointing to the old server name, select the **Change Server** check box.

Change the Content Management URL to the current server name by searching Windows search bar.

Replace <NewServerName> with the window.

Click **Activate** and check that it was successful.
 - f Click **Next**.
 - g Click **Apply** to save settings.
- 7 Check that all data can be observed in Content Management via the website.
- 8 Download and upgrade to OpenLab Server/ECM XT with the latest v2.7 installer.

Backup Guidelines 111

Overview 112

Back Up the Solr Index 113

Manually Back Up the Database 117

Back Up the Data Repository 128

Manually Back Up the Content Store 129

Manually Back Up OpenLab Server/ECM XT Server and Index Server
Configuration Information 130

Store the Back Up Files 131

Manually Restore the System 132

This chapter is intended for administrators who are skilled in database backup and maintenance and who have some familiarity with Apache Tomcat. The instructions include the necessary information to execute a hot backup of the OpenLab Server/ECM XT system, including hot backup of Solr indexes, database, content store, and configuration information. Information on how to restore the system is also included.

NOTE

The backup and restore utilities provide hot backup for supported systems. Agilent recommends use of the backup and restore utilities whenever possible. See **“Backup and Restore Procedures”** on page 54 for information on how to use the backup and restore utilities.

Backup Guidelines

- Always follow the prescribed order as described in **“Overview”** on page 112 when backing up the system.
- While hot backup is designed to run while users are active on the system, there is a performance impact. It is preferable to run it during periods of lower system activity, such as when archive is not running and the upload rate is at normal or below-normal levels.

Overview

A hot backup allows all the data from OpenLab Server/ECM XT to be copied in a consistent state while the system continues to operate. It is important to perform the backup procedure in the following order.

- 1 **Solr indexes** - Solr indexes are backed up first (before the database). When restored, the system will detect any missing index entries from the database transaction data and generate them as needed.
- 2 **Data Repository** - If your topology has several ECM XT Servers or a separated Index Node Server, back up Data Repositories from all ECM XT Servers.
- 3 **Database** - To ensure consistency between the database and the content store, the database backup must be completed before backing up the files. When doing the database backup, use the backup tools provided by the database vendor OpenLab Server/ECM XT is configured to use.
- 4 **Content Store** - The final step is to back up the actual files. For this you can use any file backup tool.
- 5 **Custom certificates** - If you are using custom certificates for a secure connection, make a backup of these certificates. For this you can use any file backup tool.
- 6 **Configuration Information** - The final step is to back up the configuration file, which will simplify the reinstallation of the software. For this you can use any file backup tool.

NOTE

In a scalable environment, the database and content store (file system) are shared, and the Solr indexes are stored on the Index Server. When you restore the system, you will restore the indexes to the Index Server.

NOTE

Once the backups are completed, it is important that you store the indexes, database, and the content store backup together as a single unit since they must be restored as a set or the system will not work correctly.

Back Up the Solr Index

Do not attempt to back up the solr6/index subdirectory directly using an OS file system copy utility while OpenLab Server/ECM XT is running because this will cause Solr index corruption.

The scheduled Solr backup job is the recommended method of backing up Solr. See **“Scheduled Backups”** for steps to enable automated backups. OpenLab Server/ECM XT can schedule regular Solr index backups, which are configured via system properties.

Scheduled Backups

Use the following steps to enable automated backups.

OpenLab Server/ECM XT with Content Management Servers only

In a configuration that doesn't have a separate Index Server but has Index and Search Services local to Content Management Servers such as an All-In-One or a Two-Server solution, do the following to schedule regular index backups.

- 1 Find out the location of the index by opening the **Server Configuration** application (**Windows Start > Agilent Technologies > Server Configuration**).
- 2 Under **Content Management Content Summary**, you will find the **Index Path**. For example, the index path of the following example shows C:\DataStoreIndex, implying that the index folder is under C:\DataStoreIndex\solr6\index\alfresco:

Table 7 Solr Index Content Management content summary

Server configuration	Content Management with Index and Search Services
Primary content storage location	C:\DataStoreContent
Secondary content storages	None
Primary archive storage location	C:\DataStoreArchive
Secondary archive storage locations	None

Table 7 Solr Index Content Management content summary

Index path	C:\DataStoreIndex
Index hostname	

- 3 Set system properties to enable regular index backups (See “**Modify system properties**” on page 116). For example, if the index path is C:\DataStoreIndex, you will need to configure your backup location to be:
/DataStoreIndex/solr6Backup/alfresco:

Table 8 Set system properties

Property	Description
solr.backup.alfresco.remoteBackupLocation=C:/DataStoreIndex/solr6Backup/alfresco	Index backup location
solr.backup.alfresco.numberToKeep=3	Keep the most current backup plus the 3 prior backups
solr.backup.alfresco.cronExpression=0 0 2 * * ?	The default is to run once per day at 2:00 a.m. See “Cron expressions” on page 51.

- 4 Create the folder C:/DataStoreIndex/solr6Backup/alfresco.
- 5 Restart the Content Management server for the setting to take effect.

NOTE

When restoring, the content of the index backup directory (directory structure and files) will be copied to the Search Service’s <solr6\index> directory specified at install time. The default location is C:\DataStoreIndex.

NOTE

The index backups must be saved regularly before they are automatically removed after three days. Store them as a set with the matching content and database backups. When restoring an index, never use a Solr index that was created after the database backup. Use the one that is closest to the database backup time, but not after.

OpenLab Server/ECM XT with an Index Server

In a configuration that has a separate Index Server such as a Four-Server or Scalable Topology solution, then do the following to schedule regular index backups.

- 1 Find out the location of the index on the Index Server by opening the “Server Configuration” application (**Windows Start > Agilent Technologies > Server Configuration**).
- 2 In the **Content Management Content Summary**, you will find the **Index Path**. For example, the index path of the following example shows C:\DataStoreIndex, implying that the index folder is under C:\DataStoreIndex\solr6\index\alfresco.

Table 9 Content Management content summary

Server configuration	Content Management with Index and Search Services
Primary content storage location	C:\DataStoreContent
Secondary content storages	None
Primary archive storage location	C:\DataStoreArchive
Secondary archive storage locations	None
Index path	C:\DataStoreIndex
Index hostname	

- 3 Set system properties in the Index Server to enable regular index backups. (See **“Modify system properties”** on page 116.) For example, if the index path is C:\DataStoreIndex, you will need to configure your backup location to be C:\DataStoreIndex\solr6Backup\alfresco so that the backup folder will be close to the index folder C:\DataStoreIndex\solr6\index\alfresco.

Table 10 Set system properties

Property	Description
solr.backup.alfresco.remoteBackupLocation=C:\DataStoreIndex\solr6Backup\alfresco	Index backup location on the Index Server
solr.backup.alfresco.numberToKeep=3	Keep the most current backup plus the 3 prior backups
solr.backup.alfresco.cronExpression=0 0 2 * * ?	The default is to run once per day at 2:00 a.m.

- 4 Create the folder C:\DataStoreIndex\solr6Backup\alfresco.
- 5 Apply the same settings to all other Content Management Servers.
- 6 Restart the Index Server only for the setting to take effect. You don't need to restart the other Content Management Servers.

NOTE

It is important that you replicate the same settings you applied on the Index Server to all other Content Management Servers to ensure all the servers behave consistently as they all point to the same database and Index Server and the scheduled job can be invoked by any one of the servers including the Index Server itself (no guarantee which one it will be). The backup is done to the index on the Index Server so the remoteBackupLocation must be a location that the Index Server understands. Having different settings in different servers will introduce inconsistent and unexpected behaviors.

NOTE

When restoring, the content of the index backup directory (directory structure and files) will be copied to the Index Server's <solr6\index> directory specified at install time. The default location is C:\DataStoreIndex.

NOTE

The index backups must be saved regularly, before they are automatically removed after three days. Store them as a set with the matching content and database backups. When restoring an index, never use a Solr index that was created after the database backup. Use the one that is closest to the database backup time, but not after.

Modify system properties

- 1 Open the alfresco-global.properties file from
<INSTALLATION PATH>\OpenLAB Data Store\tomcat\shared\classes
(the default location is C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes directory of your ECM XT server).
- 2 Search for the property you want to change or add the property if it does not exist. Make the change and save the file. The change is in effect the next time the server is restarted.

Manually Back Up the Database

In an OpenLab Server/ECM XT system, the ability to support hot backups depends on the hot backup capabilities of the database product OpenLab Server/ECM XT is configured to use. To do hot backups, the database product being used must have a tool that can "snapshot" a consistent version of the OpenLab Server/ECM XT database. (That is, it must capture a transactional-consistent copy of all the tables in the OpenLab Server/ECM XT database.) In addition, to avoid serious performance problems in the running OpenLab Server/ECM XT system while the backup is in progress, this "snapshot" operation should either operate without establishing locks in the OpenLab Server/ECM XT database or it should complete quickly (within seconds).

Backup capabilities vary widely between relational database products. Make sure that any backup procedures are validated by a qualified, experienced, database administrator before they are put into a production environment.

To back up the database, do the following:

- 1 Ensure that the database is installed and configured as shown in the *Agilent OpenLab ECM Server and ECM XT Installation Guide*.

If you are using an Oracle database, be sure that a Fast Recovery Area (FRA) has been defined, the database mode is set to ARCHIVELOG, and a retention policy is in place.
- 2 Identify the names of the content database and the shared services database that were specified at install time. You can determine these names as follows:
 - a Run the Server Configuration application (**Windows Start > Agilent Technologies > Server Configuration**). This provides a summary of the server configuration.
 - b In the Shared Services Database Summary, you will find the Database Name for shared services.

Table 11 Shared Services database summary

Database type	PostgreSQL
Server name	localhost
Server instance	Not applicable
Server port	5432
Database name	OLSharedServices

Table 11 Shared Services database summary (continued)

Database administrator	postgres
Database user	Olss

- c** In the Content Management Database Summary, you will find the Database Name for the content database.

Table 12 Content Management database summary

Database type	PostgreSQL
Server name	localhost
Server instance	Not applicable
Server port	5432
Database name	DataStore
Database administrator	postgres
Database user	DSAdmin

- 3** Once you have the database names, use the appropriate database backup instructions and tool to back up all the tables.

Back up an SQL Server database

This section provides the details for creating a hot backup of an MS SQL Server OpenLab Server/ECM XT database.

The scripts provided with the system create a full backup of the following types of database objects:

- SQL Server System Databases (for example., master, msdb and model)
- OpenLab Server/ECM XT Databases (DataStore, OLSharedServices)
- The active portion of the transaction log that contains running transactions

Prerequisites

Review the following prerequisites before you back up your database.

- A user credential with system administrator authority
- SQL Server Management Studio (SSMS) or another tool for executing SQL scripts
- SQLCMD
- A folder on a non-local drive to store the backup file (for example, \\NetworkBackups\Database)
- A local folder for creation of the backup file (for example, C:\Backup\Database). This location should be temporary. The backup file will be moved to a storage location after the backup is complete.

Executing the hot backup

SQL Server Management Studio (SSMS) may be used to execute the backup scripts supplied with the system. For default installations, the scripts are stored in **C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\Backup Scripts\Hot Backup\SQLServer**.

Open SSMS and use the File>Open menu to select the backup script you want to run. Run the script by clicking the Execute button in the toolbar.

For each of the scripts you execute, change the term "TO DISK =" to point to the local backup folder you created. The following scripts are provided:

ECMDBHotBackup.sql This script makes a backup of the DataStore and OLSharedServices user databases.

```
-----
-----

ALTER DATABASE OLSharedServices SET RECOVERY FULL

BACKUP DATABASE OLSharedServices TO DISK =
'C:\Backup\Database\OLSharedServices.bak'

WITH INIT

ALTER DATABASE DataStore SET RECOVERY FULL

BACKUP DATABASE DataStore TO DISK =
'C:\Backup\Database\DataStore.bak'

WITH INIT

-----
-----
```

SystemDBHotBackup.sql This script makes a backup of the SQL Server system databases.

```
-----
ALTER DATABASE Master SET RECOVERY SIMPLE

BACKUP DATABASE Master TO DISK =
'C:\Backup\Database\MSSQLBackupMaster.bak'
WITH INIT

ALTER DATABASE MSDB SET RECOVERY FULL

BACKUP DATABASE MSDB TO DISK = 'C:\Backup\Database\
MSSQLBackupMsdB.bak'
WITH INIT

ALTER DATABASE Model SET RECOVERY FULL

BACKUP DATABASE Model TO DISK = 'C:\Backup\Database\
MSSQLBackupModel.bak'
WITH INIT
-----
```

Additional Backup Considerations

- Offsite backup – For more protection, copy the backup files to an offsite location.
- The “WITH INIT” parameter on the BACKUP command removes previous versions of the backup, that is, only a single version of the data is maintained. After each database backup, copy the files to a separate location along with the content file and Solr index backups, so that a matching set is maintained.
- Encryption – To further secure the data, you may encrypt the backup files.
- Schedule database backup jobs – Backup jobs can be scheduled in SSMS using the Management/Maintenance Plan function.
- Log backup – Changes to the database since your last backup are lost unless log backups are made in between full backups. Consider if log backups should be added to your backup scripts.
- Log truncation – Periodically remove log entries so that the log file does not grow too large.
- Copy backup files from the local folder location to the non-local backup storage location.

Back up a PostgreSQL database

This section provides basic database hot backup and restore instructions for OpenLab Server/ECM XT PostgreSQL components. These instructions should not be considered a substitute for a comprehensive database backup strategy, which must be developed by a qualified PostgreSQL professional.

These instructions are for creating a full backup of the following types of database objects:

- System databases
- OpenLab Server/ECM XT Databases (DataStore, OLSharedServices)
- The active portion of the work-ahead-log

Prerequisites

Review the following prerequisites before starting the database backup.

- The postgres user admin password
- A user entry in `pg_hba.conf`. See Hot backup script note
- A utility that can unpack a gzip compressed TAR file
- A folder to store the backup files. It is suggested that the location not be on the same device that stores the PostgreSQL database files.

Executing the hot backup

These instructions allow the PostgreSQL database to be backed up while users continue working on the system. Be aware that running a hot backup may cause a degradation in system performance while the backup is executing, and only data entered before the backup begins are guaranteed to be saved in the resulting backup file.

The high-level steps for creating the database backup are as follows:

- 1 **“Create folder to store backup files”**.
- 2 **“Execute the hot backup script”** on page 122.

Create folder to store backup files

Create a folder on a device that does not contain the PostgreSQL database. Based on the size of your database, make sure that enough space is allocated to hold as many generations of the backup as your backup strategy requires. The backup script compresses the backup file.

Configure the backup script

For default installations, locate the backup script at **C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\Backup Scripts\Hot Backup\Postgres\postgresqlHotBackup.bat**, and customize the script for your environment using a text editor.

- 1 Edit the backup destination with the path to the folder created above.

Table 13 Backup destination

Tool	Property	Notes
Text Editor	Set backupdestination=<Path\to\backupfolder>	The default is to place the folder in the servers root drive in the \PostgreSQLBackup folder, but it is recommended to store it on another device.
	OR Set backupdestination=<\\Path\to\backupfolder>	
		If the destination is a UNC path use this format.

- 2 Add the following location to the Path environment variable: C:\Program Files (x86)\PostgreSQL-11-OLCM\bin. This ensures that the PostgreSQL backup command is found when running the hot backup script.

Execute the hot backup script

For default installations, locate the backup script in the **C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\Backup Scripts\Hot Backup\Postgres** folder, and execute the command. You will be prompted for the “postgres” user password.

Table 14 Backup destination

Tool	Property	Notes
Windows Command Line	postgresqlHotBackup.bat	As the backup runs, the job's progress is reported.

Each time the backup script is executed, a new subfolder is created (for example, Backup-2019-06-28_10_45_14) in the backup destination. Within the created folder you will find two gzip compressed archives:

- base.tar.gz – this file keeps all the data that has been added to the database.

- `pg_wal.tar.gz` – this file contains the `pg_wal` folder, which holds write-ahead-log (wal) records. Each record stores a set of database changes that are written before the change is applied to the database. This mechanism protects the database in the event a failure occurs.

Hot backup script note

`pg_hba.conf`

The hot backup script executes using the “postgres” user account, which has system administrator permission and which by default has replication (backup) permission. Any user who has replication permission must also have a matching entry in the `pg_hba.conf` file. Add the following two lines to the existing file and restart the `olcm-postgresql-x64-11` Windows service.

The default path to the file is: `C:\ProgramData\Agilent\PostgreSQLData-11-OLCM`.

Table 15 Backup destination

# Type	Database	User	Address	Method
host	replication	postgres	127.0.0.1/32	md5
host	replication	postgres	::1/128	md5

Additional backup considerations

- Offsite backup – For more protection, copy the backup files to an offsite location. At a minimum, backups should be stored on a device separate from the PostgreSQL database files.
- For each backup you choose to retain, copy the database backup files to a separate location along with the content file and Solr index backups, so that a matching set is maintained.
- Encryption – To further secure the data, you may consider encrypting the backup files.
- Schedule database backup jobs – Backup jobs can be scheduled using Windows Scheduler, for example.

Back up an Oracle database

The following instructions create a full backup of the following types of database objects:

- Oracle System tablespace
- OpenLab Server/ECM XT Databases (DataStore, OLSharedServices)
- The active portion of the transaction log that contains running transactions

Prerequisites

The *Agilent OpenLab ECM Server and ECM XT Installation Guide* contains one-time configuration steps to enable Oracle's hot backup capability. Those configuration steps must be completed before using this document to run a hot backup.

Review the following prerequisites before starting the database backup.

- An Oracle user credential with system administrator authority
- Oracle Recovery Manager (RMAN). See **"How to connect RMAN to the database"** on page 127.
- SQL*Plus or another tool for executing SQL commands. See **"How to connect SQL*Plus to the database"** on page 127.
- The instance name configured during Oracle installation.

NOTE

All the RMAN and SQL commands require a semicolon (;) at the end of the command.

NOTE

Before executing SQL or RMAN commands, you must first establish a connection to the database. See **"How to connect RMAN to the database"** and **"How to connect SQL*Plus to the database"** on page 127. You may need to re-establish the database connection before executing a SQL or RMAN command if a prior command closes the connection (for example, SHUTDOWN IMMEDIATE).

Executing the hot backup

These instructions allow the Oracle database to be backed up while users continue working on the system. Be aware that running a hot backup may cause a degradation in system performance while the backup is executing.

The high-level steps for creating the database backup are as follows:

- 1 “Back up the database and archive log”.
- 2 “Save the SPFILE” on page 125.

Back up the database and archive log

Table 16 Back up database

Tool	Command
Not applicable	Connect RMAN to the database. See “How to connect RMAN to the database” on page 127.
RMAN	BACKUP AS BACKUPSET DATABASE PLUS ARCHIVELOG The database and archive log are backed up and placed in the Fast Recovery Area (FRA).

You can view the configured FRA location using the SQL SHOW command:
SHOW PARAMETER DB_RECOVERY_FILE_DEST.

To execute SQL commands, connect SQL*Plus to the database. See How to connect RMAN to the database for instructions.

Save the SPFILE

The SPFILE stores Oracle configuration information and is used for recovering the server in the event of a failure. Make an initial backup of the file, and resave it whenever your configuration changes or consider saving it each time you take a backup so that you always have the latest version.

Table 17 Save the SPFILE

Tool	Command
Not applicable	Copy the SPFILE and store it with your backups. The default location is: <Oracle Installation>\database\SPFILE<YOURINSTANCENAME>.ORA Do not include < > in the command. For example, C:\app\orcladmin\product\12.2.0\dbhome_1\database

To show all the available backups, execute the following command: RMAN> LIST BACKUP SUMMARY.

More backup considerations

- Offsite backup – For more protection, copy the backup files to an offsite location. At a minimum, backups should be stored on a device separate from the Oracle database files. The backups are stored in the Fast Recovery Area (FRA) which was created above. Save the entire FRA folder.
- The retention policy configured above keeps backups for seven days. Therefore, consider copying these backups to another location before that are automatically removed. For each backup you choose to retain, copy the database backup files to a separate location along with the Solr index, content files, and configuration backups, so that a matching set is maintained.
- Encryption – To further secure the data, you may encrypt the backup files.
- Schedule database backup jobs – Backup jobs can be scheduled using Oracle Enterprise Manager or Windows Scheduler, for example.
- Log backup sizing – It is critical to allocate enough space to the fast-recovery-area and the log archive destination to avoid system disruptions. Consult with your DBA for proper sizing.
- Log backup – Changes to the database since your last full backup are stored in the log. Daily (or more frequent) backups of the archive log in between full backups is essential to ensure that work is not lost. Oracle supports having log archives copied to more than one location simultaneously for greater resiliency, but it requires extra storage space and configuration.
- Log archive maintenance – Regularly remove unneeded logs so that the log directory does not grow too large; a full archive will cause system disruption.

How to connect RMAN to the database

Table 18 Connect RMAN to the database

Tool	Command
Windows Command Line	<code>rman TARGET SYS@<YOURINSTANCENAME> nocatalog</code> Substitute your Oracle instance name. Do not include < > in the command. For example, <code>rman TARGET SYS@OPENLAB nocatalog</code>

How to connect SQL*Plus to the database

Table 19 Connect SQL*Plus to the database

Tool	Command
Windows Command Line	<code>sqlplus/NOLOG</code>
SQL	<code>CONNECT SYS/<THEPASSWORD> AS SYSDBA</code>

Back Up the Data Repository

Back up the Data Repository using the procedures in **“Manual Data Repository database backup”** on page 98

Manually Back Up the Content Store

To back up the content store, you can use any file backup utility. It is recommended that you use one that can perform differential backups. That way, you do not have to back up the entire content store each time, but rather just do an incremental backup. It is important that you can restore your indexes, database, and file content store to a consistent state. To back up the content files, you will need to identify the location of the content store. To find the location of the content store, do the following:

- 1 Go to the OpenLab Server/ECM XT server machine. In a scalable environment, you can connect to any node.
- 2 Click **Windows Start > Agilent Technologies > Server Configuration**. A webpage appears and provides the paths for contentstore and the archive.

Table 20 Content Store Content Management content summary

Primary content storage location	C:\DataStoreContent
Secondary content storages	None
Primary archive storage location	C:\DataStoreArchive
Secondary archive storage locations	None

- 3 If your repository has multiple content stores, you also need to back up each of the additional content stores.
- 4 Once you have identified all the content store locations, use your file backup tool to back them up.

Manually Back Up OpenLab Server/ECM XT Server and Index Server Configuration Information

For each OpenLab Server/ECM XT server and Index server, perform the following steps.

- 1 Locate the **<Installation Directory>\OpenLAB Data Store\tomcat\temp\com.agilent.datastore.cache** file, and copy it to the C:\ProgramData\Agilent\Installation folder.

The <Installation Directory> can be found in the **Installation Summary** on the **Server Configuration** page.

- 2 Back up the **C:\ProgramData\Agilent\Installation** folder. This will be used to reconfigure the system at a later point.

Back Up Custom Certificates

If you are using custom certificates for a secure connection, make a backup of these certificates. Copy the C:\Program Files\OpenLab Reverse Proxy\Apache24\conf\ssl\custom\ folder to the backup location.

Store the Back Up Files

To ensure that you have a consistent set of database, content, and index files, a process must be put in place to save the output of these backup steps daily and to organize them so that the matched set can be found in the event the system needs to be restored. You may choose to store the files from the same set together or just document the steps for finding the set, keeping in mind the required order for the backups are:

- 1 Solr indexes
- 2 Database
- 3 Data Repository
- 4 Content and Archive Store
- 5 Configuration Information

Since the Solr backup is run on a predetermined schedule and not on-demand, store the database backup with the most recent Solr backup in the event restoration is needed.

Manually Restore the System

Set up a system consistent with the configuration in use at the time of the backup. This can be done manually by following all the same setup and configuration steps you did originally, along with any follow-on steps you made over time. Another approach might be to include a full system backup as a base and update it as you update the configuration. How you set up your disaster recovery plan is up to you. However, you must start with the correct configuration to restore your data set and have a running system.

To restore the data, start with a working system, shut down the services, and restore the index, database, data repository, content and archive store, and Server Configuration file. It does not matter what order you restore them. What is important is that you restore a complete consistent set of data. To do this, consider the following:

- Do not leave any existing files or folders in the index folder before restoring. Start from an empty directory. Be sure to put the index snapshot in the correct directory structure (for example, <DataStoreIndex\solr6\index>). The other directories are created during startup.
- Do not leave any existing data in the database. Start with an empty database.
- Make sure the content stores are empty when starting the restore. If you are using multiple content stores, put the right set of files in each location.

After restoring all the data, reboot the server, and your system will do a final consistency check. Update the indexes as needed, and start up.

NOTE

For the scripts in the following sections, make sure to specify real locations of database backup files before running the scripts.

NOTE

If your backup contains folder with custom certificates, configure them by following **step 4** in **“Configure OpenLab Server/ECM XT Reverse Proxy”** on page 29. For index server on 4-server or scalable systems, see **“Index Server Configuration - 4-Server Systems Only”** on page 37.

Restore the Solr Index

To restore the Solr index from a backup, perform the following steps:

- 1 Locate the index backup you want to restore. Always use a backup that matches the database you are restoring.

The index backup is stored in a folder named `snapshot.xxxxxxxxxxxxxxxxxx`. For example, `snapshot.20190708231001373`.
- 2 Stop the **Agilent OpenLab Content Management Search** service.
- 3 Copy the “snapshot” folder to the location specified by the Index Path in your Server Configuration. The default is `C:\DataStoreIndex\solr6\index\alfresco`.
 - a If this path already exists, delete the index files from under `C:\DataStoreIndex\solr6\index\alfresco\index`, and replace them with the files from the backup.
 - b If this path does not exist, create the path `C:\DataStoreIndex\solr6\index\alfresco`, and copy the “snapshot” folder to it. Rename the “snapshot” folder to “index,” creating a path of `C:\DataStoreIndex\solr6\index\alfresco\index`.
- 4 Start the **Agilent OpenLab Content Management Search** service.

Restore an SQL Server database from a backup

In the event it becomes necessary to recover the system, you must recover all the data types (database, content files, indexes) from the same set to ensure data consistency of the system.

The following scripts are provided for restoring the database:

ECMDBRestore.sql This script replaces the data in the DataStore and OLSharedServices user databases with data from the backup files.

If you are restoring to a fresh installation of SQL Server (for instance, if ECM XT has not yet been installed) you must, at a minimum, first run Step 1 and Step 2 of the OpenLab Server/ECM XT installer, which creates the DataStore and OLSharedServices databases. If these databases do not exist before the restore, you will receive the following message:

“User does not have permission to alter database 'OLSharedServices', the database does not exist, or the database is not in a state that allows access checks.”

If OpenLab Server/ECM XT has already been installed, you can proceed without running Step 1 and Step 2 of the ECM XT installer.

Whether you already have OpenLab Server/ECM XT installed or not before the restoration, you must run Step 4 of the OpenLab Server/ECM XT installer once after the entire restoration is done to allow the system to reconfigure itself or else the system will not run properly.

NOTE

Make sure you use the actual locations of your backup files in the scripts.

```
-----
-----
ALTER DATABASE [DataStore ] SET SINGLE_USER WITH ROLLBACK
IMMEDIATE

RESTORE DATABASE DataStore FROM DISK =
'\\NetworkBackup\Database\DataStore.bak' WITH RECOVERY, REPLACE
ALTER DATABASE [DataStore] SET MULTI_USER WITH ROLLBACK IMMEDIATE

ALTER DATABASE [OLSharedServices] SET SINGLE_USER WITH ROLLBACK
IMMEDIATE

RESTORE DATABASE OLSharedServices FROM DISK =
'\\NetworkBackup\Database\OLSharedServices.bak' WITH RECOVERY,
REPLACE

ALTER DATABASE [OLSharedServices] SET MULTI_USER WITH ROLLBACK
IMMEDIATE
-----
-----
```

SystemDBRestore.sql This script replaces the data in the SQL Server system databases with data from the backup files.

```
-----
-----
ALTER DATABASE [MSDB] SET SINGLE_USER WITH ROLLBACK IMMEDIATE
```

```
RESTORE DATABASE MSDB FROM DISK =
'\\NetworkBackup\Database\MSSQLBackupMsdb.bak'

WITH RECOVERY, REPLACE

ALTER DATABASE [MSDB] SET MULTI_USER WITH ROLLBACK IMMEDIATE

ALTER DATABASE [Model] SET SINGLE_USER WITH ROLLBACK IMMEDIATE
RESTORE DATABASE Model FROM DISK =
'\\NetworkBackup\Database\MSSQLBackupModel.bak'

WITH RECOVERY, REPLACE

ALTER DATABASE [Model] SET MULTI_USER WITH ROLLBACK IMMEDIATE
```

NOTE

The version of SQL Server on the server to be restored must match exactly the version from which the backup was taken to restore system databases. Message 3168 is generated by SQL Server if a mismatch condition exists. If this situation arises, upgrade or downgrade the target server so that the versions match. The 3168 error message contains the version number of the target server and the backup file. Use this information to set the target server to the correct version.

MasterDBRestore.bat This script replaces the data in the SQL Server Master database with data from the backup file. This script is executed from a Windows command line using the SQLCMD utility. Execute the following steps:

NOTE

The path to the SQL Server binary folder is dependent on the SQL Server version. Be sure to verify the path used in the script.

- 1 Open the **Windows System Properties** dialog and select **Environment Variables**. (Search within Windows for "sysdm.cpl" and run the command. Select **Environment Variables** on the **Advanced** tab.)
- 2 Edit the Path environment variable and add the following path: C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Binn
- 3 Set the server to single-user-mode before restoring the Master database.
 - a Using SQL Server Configuration Manager, click the SQL Server Services icon to display a list of services. Right-click the SQL Server (MSSQLSERVER) service, and select the Startup Parameters tab and add: -mSQLCMD

- 4 Restart SQL Server (MSSQLSERVER) service in SQL Server Configuration Manager .
- 5 Execute the restore script.
 - a Using the Windows command line, run MasterDBRestore.bat. You will be prompted to enter the system administrator (SA) password. The command can also be executed by copying the batch file content into the command line.
- 6 After the restore of the Master database is complete:
 - a Remove -mSQLCMD parameter from startup script.
 - b Restart the SQL Server service.

 Run MasterDBRestore.bat from a Windows command line which contains the following:

```
sqlcmd -U SA -S localhost -Q "RESTORE DATABASE Master FROM DISK
= '\\NetworkBackup\Database\MSSQLBackupMaster.bak' WITH
REPLACE "
```

Restore a PostgreSQL database from a backup

In the event it becomes necessary to recover the system, you must recover all the data types (database, content files, indexes) from the same set to ensure data consistency of the system. Depending on the database failure that is compelling the restoration from backup, the needed steps may vary. For the purposes of this document, the failure is assumed to be a total loss of the PostgreSQL database (for example, user and system database files and redo logs no longer exist). In this case, any changes made since the last backup are lost.

Restoration Considerations

- The version of PostgreSQL on the server to be restored must be greater than or equal to the version from which the backup was taken to ensure a successful restore.
- If you are restoring to a new server that previously did not have OpenLab Server/ECM XT installed, you must run Steps 1 through 4 of the OpenLab Server/ECM XT installer before restoring the database from your backup files.

Restore the database

Execute the following steps to restore the database:

- 1 Stop the **alfrescoTomcat** service.
- 2 Stop the **olcm-postgresql-x64-11** service.
- 3 Remove all content from the <PostgreSQL Installation> directory. The default is C:\ProgramData\Agilent\PostgreSqlData-11-OLCM.
- 4 Extract the content of the base.tar.gz archive into the <PostgreSQL Installation> folder.
- 5 Locate the **pg_wal** folder within the <PostgreSQL Installation> folder.
- 6 Extract the content of the **pg_wal.tar.gz** archive into the pg_wal folder.
- 7 Restart the **alfrescoTomcat** service.
- 8 Restart the **Agilent OpenLab Shared Services** service.

After the last command is executed, the database is restored and ready for user activity.

Restore an Oracle database from a backup

See your Oracle documentation for information on how to restore an Oracle database from a backup.

- 1 Execute the following commands to restore the database.

Table 21 Restore an Oracle database after a loss of data

Tool	Command
SQL	SHUTDOWN IMMEDIATE
Not applicable	Copy saved SPFILE to <Oracle Installation>\database\
SQL	<pre>CREATE PFILE='<Oracle Installation>\database\PFIL<YOURINSTANCENAME>.ORA' FROM SPFILE='<Oracle Installation>\database\SPFILE<YOURINSTANCENAME>.ORA</pre>
Text Editor	<p>Edit tnsnames.ora to add (UR = A) clause The default location is: <Oracle Installation>\network\admin\tnsnames.ora</p> <pre><YOURINSTANCENAME> = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST = YourServerName) (PORT = 1521))) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = <YOURINSTANCENAME>) (UR = A)))</pre>
SQL	<pre>STARTUP NOMOUNT</pre> <p>If the database is already running, SHUTDOWN IMMEDIATE instead. Then run STARTUP NOMOUNT and reconnect RMAN and SQL.</p>

- 2 After the last command is executed, shutdown the database and restart the Windows server.

Restoration considerations

In the event it becomes necessary to recover the system, you must recover all the data types (index, database, content, and configuration files) from the same set to ensure data consistency of the system. Depending on the database failure that is compelling the restoration from backup, the needed steps may vary.

Restore the Data Repository

Follow the procedures given in **“Manual OpenLab Server/ECM XT Server Restore Procedure”** on page 100 to restore the Data Repository.

Rebuild the Activity Log Index

Use the following procedure to rebuild the OpenLab Shared Services Activity Log Index when the Activity Log table or data is corrupted or when the Shared Services database has been restored with an existing OpenLab installation.

The Activity Log Index is automatically rebuilt in the following scenarios:

- You are using a file-based Workstation configuration using a Firebird database
- The Shared Services database has been restored with a fresh installation
- You are migrating or updating your data

The time required to rebuild the index depends on your database type and the amount of Activity Log records. It may take up to a few hours. During this time, you cannot search the Activity Log in the application.

To rebuild the Activity Log,

- 1 Start the Command Prompt as an Administrator.
- 2 Execute the following command:

```
net stop SharedServicesHost && del /s /f /q  
%ProgramData%\Agilent\OLSS\Index\ActivityLog && net start  
SharedServicesHost
```

Possible errors include:

- **Message**

The Agilent OpenLab Shared Services service is not started. More help is available by typing NET HELPMSG 3521.

Solution

Use the following command instead:

```
del /s /f /q %ProgramData%\Agilent\OLSS\Index\ActivityLog &&  
net start SharedServicesHost
```

- **Message**

System error 5 has occurred. Access is denied.

Solution

Make sure the Command Prompt has been started as an Administrator.



8 Upgrading and Reconfiguration

Upgrading the OpenLab Server/ECM XT Server when the Operating System Changes 142

OpenLab Server/ECM XT Server Reconfiguration 142

Upgrading the OpenLab Server/ECM XT Server when the Operating System Changes

- 1 Install OpenLab Server/ECM XT on the new machine with the new operating system.
- 2 On the old machine, perform a manual system backup. See **“Back Up OpenLab Server/ECM XT Using the Backup Utility”** on page 61 or **“Manual OpenLab Server/ECM XT Server Backup Procedure”** on page 91
- 3 On the new machine, perform the server restore procedure. See **“Restore OpenLab Server/ECM XT Using the Restore Utility”** on page 72 or **“Manual OpenLab Server/ECM XT Server Restore Procedure”** on page 100.

OpenLab Server/ECM XT Server Reconfiguration

This section covers common scenarios, such as the following:

- You have an OpenLab Server/ECM XT installation with a database server (local or remote), and you have decided to upgrade the database server software to a newer version or upgrade the hardware, which involves relocating the database server software to a new machine. You must tell OpenLab Server/ECM XT how to connect to the new database server and continue to work.
- A file server lacks free space, so you decide to move the content storage to another piece of hardware.
- A corporate security policy change has made it necessary to change system users and passwords used by OpenLab Server/ECM XT.

The following pages describe how to use the OpenLab Server Configuration Utility (OSCU) to accomplish these tasks.

In general, the process consists of four steps:

- 1 **“Bring Down OpenLab Server/ECM XT”** on page 143”
- 2 **“Make Changes to the Infrastructure”** on page 143

3 “Run the OpenLab Server Configuration Utility” on page 150

4 “Bring Up OpenLab Server/ECM XT” on page 154

To add additional content or archive store, see “Add Additional Content or Archive Store” on page 154.

Bring Down OpenLab Server/ECM XT

Stop services in the following order:

- 1 Agilent OpenLab Content Management Search service
- 2 alfrescoTomcat
- 3 Agilent OpenLab Shared Services

Make Changes to the Infrastructure

Move the DB Server

Relocate OpenLab Server/ECM XT and Shared Services databases to the new server. This step is specific to the DB type used. Please see the *Agilent OpenLab ECM XT Hardware and Software Requirements Guide*. Please see vendor documentation for SQL Server and Oracle databases.

Move a PostgreSQL Database The destination and source database server versions must be the same. The major and minor version digits should be equal, for example 14.x.x. For this example,

- Server1 is the source machine
 - Server2 is the destination machine
- 1 On Server1, stop PostgreSQL service (for version 14: **olcm-postgresql-x64-14**).
 - 2 Click **Start > All Programs > Agilent Technologies > Configuration Viewer**.
 - 3 Locate the **PostgreSQL Database** folder in the **Installation Summary** section and back it up.
 - 4 On Server2, unpack the PostgreSQL data folder. Name it **PG_DATA_NEW**.

- 5 Run the PostgreSQL installer. When asked for the data folder, enter **PG_DATA_NEW**.
- 6 Click **Next** until the installation is complete.
- 7 If after reconfiguration, your PostgreSQL server is going to be on a different machine from your OpenLab Server/ECM XT installation, follow these steps. Otherwise, proceed to **step 8**.

To use a remote connection to PostgreSQL using a PostgreSQL database user:

- a Make sure Server1, Server2, and your OpenLab Server/ECM XT server are all connected to the same domain.
- b Open **pg_hba.conf** from the **PG_DATA_NEW** folder, and make sure it contains the following lines:

```
host all "postgres" 172.16.0.111/32 md5
host all "postgres" ::1/128 md5
host all "SYSTEM" 127.0.0.1/32 sspi
host all "SYSTEM" ::1/128 sspi
host all all 127.0.0.1/32 md5
host all all ::1/128 md5
```

Add the following lines for an OpenLab Server/ECM XT server with IPv4 address 172.16.0.111 and IPv6 address fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed:

```
host all "postgres" 172.16.0.111/32 md5
host all "postgres"
    fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed/128 md5
host all all 172.16.0.111/32 md5
host all all fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed/128
    md5
```

For more information on how to configure an external PostgreSQL server, see the "Configure a remote PostgreSQL database server" section in the *Agilent OpenLab Server/ECM XT Installation Guide*. Consult your network administrator to find the best option for your network.

- c Open **pg_ident.conf** from the **PG_DATA_NEW** folder, and add the following lines:

```
# MAPNAME    SYSTEM-USERNAME    PG-USERNAME
datastore    Server1$            SYSTEM
```

where **Server1\$** is the name of the remote system user assigned by PostgreSQL. Usually, the system user name matches the NetBIOS name of the machine where your OpenLab Server/ECM XT is running, followed by a dollar sign (\$).

If it does not match and the OpenLab ECM XT Configuration fails, review the latest messages in the **PG_DATA_NEW > pg_log** folder to find something similar to:

```
2015-06-02 10:05:34 PDT FATAL: SSPI authentication failed
for user "SYSTEM"
```

```
2015-06-02 10:05:37 PDT LOG: provided user name (SYSTEM) and
authenticated user name (WIN-ITGSOV7UQM2$) do not match
```

where WIN-ITGSOV7UQM2\$ is the **SYSTEM_USERNAME** you should put in **pg_ident.conf**.

Please see PostgreSQL official documentation to learn more about security features.

To use a remote connection to PostgreSQL using SQL authentication:

Open **pg_hba.conf** from the **PG_DATA_NEW** folder, and make sure it contains the following lines for an OpenLab Server/ECM XT server with IPv4 address 172.16.0.111 abd IPv6 address fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed:

```
host    all    "postgres"    172.16.0.111/32    md5
host    all    "postgres"
        fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed/128    md5
host    all    all    172.16.0.111/32    md5
host    all    all    fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed/128
        md5
```

It is possible to define subnet ranges instead of single IP addresses in `pg_hba.conf`. The following example allows all connections to the PostgreSQL database server originating from address range 172.16.0.0 to 172.16.0.255 and from `fc00:1ac4:65fb:34cb::/64` IPv6 address range:

```
host all "postgres" 172.16.0.0/24 md5
host all "postgres" fc00:1ac4:65fb:34cb::/64 md5 0.0/24 md5
host all all fc00:1ac4:65fb:34cb::/64 md5
```

Please see PostgreSQL official documentation to learn more about security features.

- 8 To apply the changes, restart postgresQL service.

Change the Location of a Single Content Storage

This procedure covers single content storage locations only. If you have set up multiple content storages, see **“Change the Location of Multiple Content Storages”** on page 147

- 1 Create folders for Content Storage, Index Storage, and Archive Storage. The storage locations must be an absolute or UNC path. Network drives are not supported.

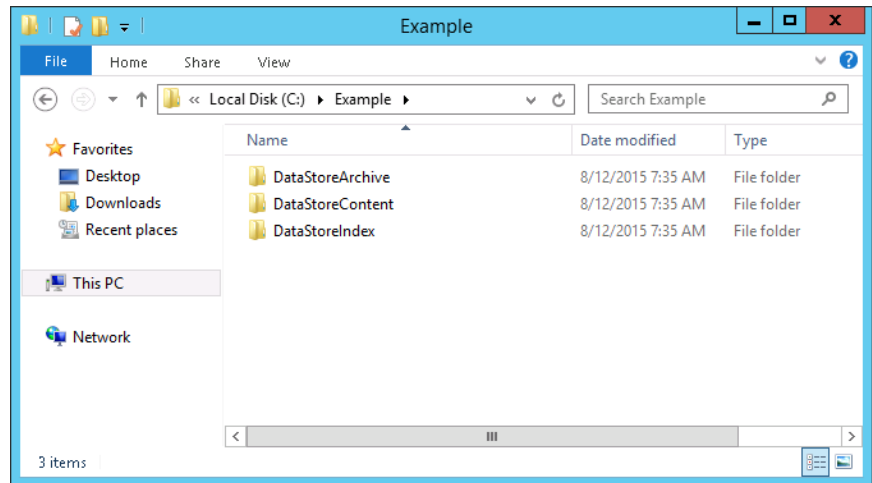


Figure 8. OpenLab ECM XT Storage Folders

- 2 If the Storage folders already exist, move the content from each previous storage location to the new location.

For example:

- The previous folder location for Content Storage is C:\DataStoreContent.
- The new folder location for Content Storage is C:\Example\DataStoreContent.

Move all content from the C:\DataStoreContent folder to the C:\Example\DataStoreContent folder. Also move the content for the Index Storage and Archive Storage folders if needed.

Change the Location of Multiple Content Storages

- 1 Create folders for Content Storage, Index Storage, and Archive Storage. The storage locations must be an absolute or UNC path. Network drives are not supported.
- 2 If the Storage folders already exist, move the content from each previous storage location to the new location.

For example:

- The previous folder location for Content Storage is C:\DataStoreContent.
- The new folder location for Content Storage is C:\Example\DataStoreContent.

Move all content from the C:\DataStoreContent folder to the C:\Example\DataStoreContent folder. Also move the content for the Index Storage and Archive Storage folders if needed.

- 3 Open **alfresco-global.properties**. The default location is **C:\Program Files (x86)\Agilent Technologies\OpenLab Data Store\tomcat\shared\classes**.
- 4 Update all content store paths. For example:

```
dir.root=C:\\Example\\DataStoreContent
dir2.root=C:\\Example\\DataStoreContent
dir3.root=C:\\Example\\DataStoreContent
```

Change OpenLab ECM XT Users or Passwords

You can change the password of database users or create users and set them to be used in OpenLab Server/ECM XT.

If you only want to change the password of an existing database user, use a database integrated development environment (IDE), such as MS SQL Server Management Studio, pgAdmin III, Oracle Developer, etc. using the software's standard procedure. Please see the official documentation for details. Changing the PostgreSQL password might impact backup utility access to the database.

Create a new user

- 1 Create the user.
- 2 Grant the user permissions on database tables.

For example, if you created a "test" user for the Shared Services database, execute the following script to grant privileges on all database tables.

```
DO
$$
DECLARE
    r information_schema.tables%rowtype;
    user_name VARCHAR = 'test'; -- specify username
BEGIN
    FOR r IN SELECT * FROM information schema.tables WHERE tab
schema='public'
    LOOP
        RAISE NOTICE 'EXECUTE "ALTER TABLE % OWNER TO
%";"',r.table_name, user_name; -- for debug
        EXECUTE 'ALTER TABLE ' || quote_ident(r.table_name) || ' OWNER
TO ' || user_name || ';';
    END LOOP;
END
$;$
```

To create a new user for an MS SQL Server database Specify the database login mapping using MS SQL Server Management Studio. Make sure that the user is a member of database roles **db_datareader** and **db_datawriter** for the desired tables.

You must execute queries with Database Administrator credentials.

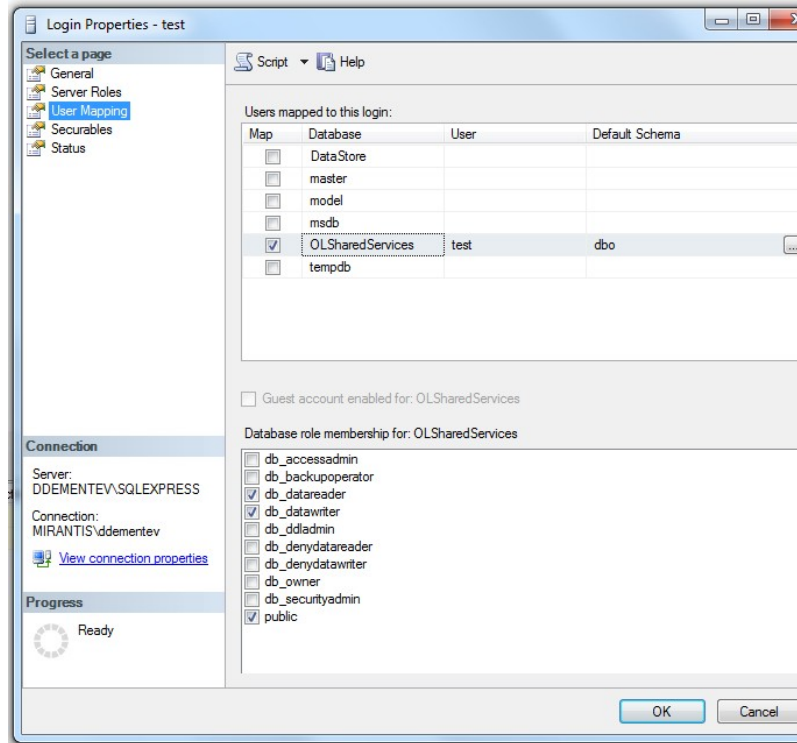


Figure 9. MS SQL Server Management Studio

To create a user for an Oracle database

Migrate all database objects (tables with constraints, sequences, triggers, etc.) from the old schema (user) to the new schema (user). This can be done using Power Designer (import the database schema with data and deploy the adjusted schema).

Depending on the database type, you may need to grant some other permissions. Please see the DB server manual for more information.

Run the OpenLab Server Configuration Utility

The OpenLab Server Configuration Utility is installed on the server and can be run standalone without the installer. The Configuration Utility is listed in Agilent Start Up menu.

CAUTION

Every screen in the OpenLab Server Configuration Utility (OSCU) is prepopulated with defaults that reflect the actual OpenLab Server/ECM XT configuration. Only edit fields that reflect changes made in [“Make Changes to the Infrastructure”](#) on page 143. It is strongly recommended that you do not edit any other values. Changing any other fields could cause the configuration to crash.

- 1 From the Windows Start menu, click **All Programs > Agilent Technologies > OpenLab Server Configuration Utility**.
- 2 On the **Welcome** screen, click **Next**.
- 3 On the **Database Type** screen, the database you are using is selected. Click **Next**.
- 4 The information displayed on the **Database Server** screen depends on the database type chosen for the OpenLab Server/ECM XT server. Check the displayed database server connection information and make changes according to the new configuration.

Edit this screen only if the database server connection information (for example, the Server Name or port number) has been changed.

Click **Verify** to check the entered values, and click **Next**.

- 5 On the **Schema Information** screen, edit the information only if the database users or passwords have been changed.

Click **Verify** to verify the entered values, and click **Next**.

- 6 On the **Server Configuration** tab, enter your configuration information, and click **Next**.
 - If you are using an all-in-one system configuration, select **Content Management with Index and Search Services**. This is the default selection.
 - If you are using a scalable system topology or 4-server topology and are creating the server(s) to host the Content Management Web services, select **Content Management only**.
 - If you are using a scalable system topology or 4-server topology and are creating the server to host the indexes and search services, select **Index and Search only**. Enter the fully qualified domain name of the server where Content Management is installed, and click **Verify**.
Click **Next**.
- 7 On the **Account Credentials** screen, enter your account access credentials. If you are using a 4-server topology, a scalable topology, or an external PostgreSQL database server, use the Windows domain user as the service account. This user must have "Log on as a service" permission.
Click **Verify** to check the credentials, and then click **Next**.

- 8 On the **Content Paths** screen, review information for the content storage, archive storage, and index locations.
 - All location paths must be unique. For example, the same path cannot be used for both the content and archive locations.
 - If UNC paths are used, you must manually validate your path. Validate will not check if the user has read and writer access to the UNC path.
 - If the server is configured as **Content Management only** or **Index and Search only**, configure the same content storage location to use the UNC path of the shared storage location for the Content Storage Locations on all servers.

OpenLab Server Configuration

Content Paths

Content Storage Locations

Location	Type
C:\DSData\DsContent	Primary

Add Content Location

Archive Storage Locations

Location	Type
C:\DSData\DsArchive	Primary

Add Archive Location

* Location type change pending; takes effect upon completion.
 ** Location edits made; changes saved upon completion.

Content Management Index Path

C:\DSData\DsIndex

Verify

Content Storage Location
 Location and type of each content store. Only one content store can be added during a configuration session. Click pencil icon to edit content store information.

Archive Storage Location
 Location and type of each archive store. Only one archive store can be added during a configuration session. Click pencil icon to edit archive store information.

Content Management Index Path
 Location of Content Management search engine index. Absolute or UNC path. Network drive is not supported.

Back Next Cancel

Figure 10. OpenLab Installer Content Paths Screen

To edit a content or archive storage location,

- a Click the **Edit** icon for the location.
- b Edit the location information as desired, and click **Done**.

A double-asterisk (**) indicator is shown next to the name of the location.

To add a new content or archive storage location,

- a Click **Add Content Location** or **Add Archive Location**. Only one new location can be added at a time.
- b Select the type of location, either the file system or Amazon S3.
- c Enter the required information. For S3, the location must be created and accessible before adding it.

- d To add the location and return to the location lists, click **Done**. To cancel adding the new location, click **Cancel**.

The new location is shown as the first item in the list. An asterisk (*) is shown next to the location type (Primary), indicating that this new location will become the location to which files are written.

To remove this new location, click the Remove icon.

An asterisk (*) is also shown next to the location type for the previous primary location. This indicates that the location is now considered secondary and is read-only. Data can be retrieved from this location, but no new data can be saved to it.

The following storage location combinations for content locations and archive locations are supported for Amazon S3:

Table 22 Storage location combinations

Primary	Secondary
S3	on-prem
on-prem	on-prem
S3	(no secondary)

If the server is configured as either a Content Management with Index and Search or an Index and Search only server, then the index location is a local path.

If the server is configured as a Content Management only server, then the hostname of the OpenLab Index server is provided instead of a path. the OpenLab Index server needs to be powered on and ICMP Echo Requests must be allowed during the verification.

Click **Verify** to check the locations, and then click **Next**.

- 9 By default, an Agilent OpenLab internal certificate is installed. Otherwise, select **Use an existing custom certificate**, and enter the certificate information. Then, click **Next**.
- 10 Review the updated configuration summary, and click **Apply**.
- 11 When the configuration is complete, click **Done**.
- 12 Move your content into the new storage location.

Bring Up OpenLab Server/ECM XT

When the OSCU process is complete, OpenLab Server/ECM XT is up and running. To check that the new configuration has been acquired successfully,

- 1 Log in to Control Panel and click **Administration > Content Management > Synchronize**.

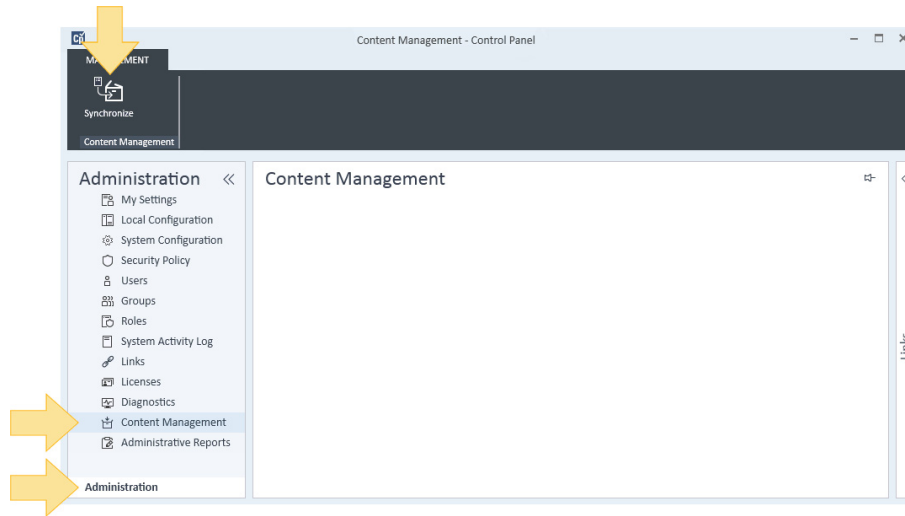


Figure 11. Control Panel Content Management Synchronize

- 2 Log in to Content Management and verify that all content is in place.

Add Additional Content or Archive Store

Use the OpenLab Server Configuration Utility to add an additional content or archive store to an OpenLab Server/ECM XT server. See **"Run the OpenLab Server Configuration Utility"** on page 150 for details.

Sales and Support Assistance 156

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>

www.agilent.com

©Agilent Technologies, Inc. 2024
DocNo D0013947
02/2024

