Agilent

Agilent OpenLab Server and OpenLab ECM XT

Administration Guide

Notices

Manual Part Number

M8640-90040
Rev B
March 2020

Copyright

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

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

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.

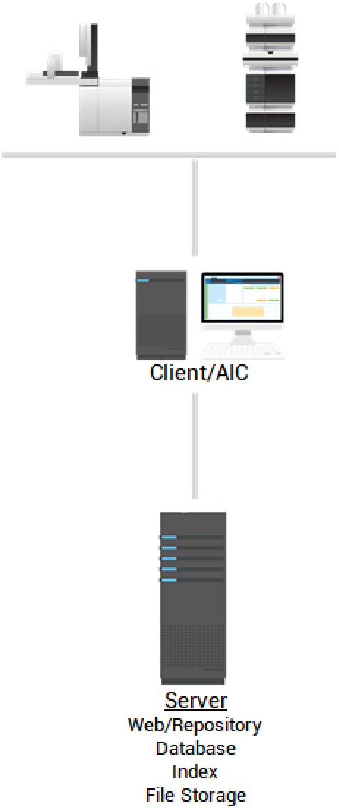


Figure 1. OpenLab Server/ECM XT server all-in-one system architecture

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

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.

Licenses

Table 1 lists the license features in OpenLab Server/ECM XT.

Table 1 Licenses

Description	License features in OpenLab Server/ECM XT
OpenLab Shared Services Server	1 x AgilentOpenLabSharedServices
OpenLab Data Store Server	1 x AgilentOpenLabDataStoreServer

Instrument connectivity licenses (for example, OpenLab Server MS Instrument and OpenLab Server CDS Instrument License) are required for every concurrent instrument that stores data in OpenLab Server/ECM XT.

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.

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 that 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 2** describes the user credentials.

Table 2 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

Table 2 User credentials (continued)

Value	Description	Mandatory
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 3**). 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.

Table 3 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	• Content Management Reader • Content Management Contributer • Content Management Approver • Archivist • System Administrator • Everything
Project: Edit content of project Create, update, and copy files and folders	• Content Management Contributer • Content Management Approver • System Administrator • Everything
Project: E-Signature sign data files Apply electronic signatures to files	• Content Management Approver • System Administrator • Everything
Operations: Manage PDF Templates Apply PDF templates to folders	• Content Management PDF Template Manager • Everything
Administrative: Archive content Online archive, set up automatic archive tasks, and de-archive files and folders	• 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	• System Administrator • Everything

Security policy

With the authentication provider **Internal**, you can set the parameters described in **Table 2** 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 4** describes the security policy settings.

Table 4 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 *10 min*. 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.

3 Securing the System

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

The procedures apply to all-in-one, 2-server, and 4-server topologies.

NOTE

If you upgrade the OpenLab Server/ECM XT server, post-installation server configurations are reset and must be re-applied, including enabling HTTPS. Use the procedures in **"OpenLab Server/ECM XT System Configuration"** on page 24 to reapply your settings.

Create and install certificates

This procedure requires Java SE Development Kit (JDK) 11.0.2. You may download this program from Oracle, or you may use the JDK shipped with Content Management under **C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\java**.

Create the keystore

To generate a keystore, use the following command line:

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

For example:

```
keytool -genkey -alias ecmxtserver -keysize 2048 -keyalg RSA
-keystore ssl.keystore -storetype JCEKS
```

You will be prompted to create a password during this process. Select an appropriate password and take note of it.

Generate a Certificate Signing Request (CSR)

To generate a CSR file for the server where HTTPS will be enabled, use the following command line:

```
keytool -certreq -alias <Alias chosen in previous step> -file
<path_and_createCSRFilename>.csr -keystore ssl.keystore
-storepass <password> -storetype JCEKS
```

For example:

```
keytool -certreq -alias ecmxtserver -file ECMXT-Server.csr
-keystore ssl.keystore -storepass <password> -storetype JCEKS
```

Request the certificate

Go to your trusted certificate provider with your .csr file and request the certificate. Your trusted certificate provider may be within your organization or a commercial vendor like VeriSign/DigiCert.

The trusted provider will deliver your certificate (.p7b), along with the Root CA certificate (.crt). Save both certificates as separate files.

For a 4-server topology, request the certificate that has two hostnames in the SAN section: one for OpenLab Index Server and one for Content Management Server.

Install the certificate into keystore

The trusted provider will deliver your certificate (.p7b), along with the Root CA certificate.

1 Import the Root CA certificate into keystore.

```
keytool -importcert -file <rootcertificateFile> -keystore <your
keystore file name> -alias <choose an alias for the Root CA>
-storetype JCEKS
```

For example:

```
keytool  -importcert -file rootCA.crt -keystore ssl.keystore
-alias agilent -storetype JCEKS
```

2 Import your Server certificate into keystore.

```
keytool -importcert -file <yourcertificateFile> -keystore <your
keystore file name> -alias <an alias for your certificate>
-storetype JCEKS
```

For example:

```
keytool  -importcert -file ecmxt-server.p7b -keystore
ssl.keystore -alias ecmxtserver -storetype JCEKS
```

You should receive the message **Certificate reply was installed in keystore**.

Generate the truststore

To generate the truststore, use the following command line. You may be prompted for passwords.

```
keytool -import -v -trustcacerts -alias <alias for the Root CA>
-file <rootcertificateFile> -keystore <truststore file name>
-storetype JCEKS
keytool -export -keystore <your keystore file name> -alias <alias
for your certificate> -file <a certificate file name> -storetype
JCEKS
```

```
keytool -import -keystore <truststore file name> -alias <alias
for your certificate> -file <a certificate file name> -storetype
JCEKS
```

For example:

```
keytool -import -v -trustcacerts -alias agilent -file rootCA.crt
-keystore ssl.truststore -storetype JCEKS
```

```
keytool -export -keystore ssl.keystore -alias ecmxtserver -file
ecmxt.cer -storetype JCEKS
```

```
keytool -import -keystore ssl.truststore -alias ecmxtserver -file
ecmxt.cer -storetype JCEKS
```

You can view the entries in the keystore by running the following command line:

```
keytool -list  -keystore ssl.keystore -storetype JCEKS
```

At this step, you will have two files: **ssl.keystore** and **ssl.truststore**. These files will be used for further configuration of OpenLab Server/ECM XT Server.

OpenLab Server/ECM XT System Configuration

OpenLab Server/ECM XT repository configuration

For a 4-server solution, perform this procedure only on the Content Management-only Server and OpenLab Index Server. For an all-in-one server or 2-server solution, perform this procedure on the OpenLab Server/ECM XT server.

1 Copy **ssl.keystore** and **ssl.truststore** into the following directory: **C:\Program Files (x86)\Agilent Technologies\OpenLab Data Store\keystore**.

2 Update the **ssl-keystore-passwords.properties** and **ssl-truststore-passwords.properties** to ensure that the alias corresponds to your chosen alias in the steps described earlier.

  For example:

```
aliases=ssl.alfresco.ca,ecmxtserver
# The ssl keystore password
keystore.password=<newPassword>
# The password protecting the ssl repository key
ecmxtserver.password=<newPassword>
# The password protecting the ssl Alfresco CA key
ssl.alfresco.ca.password=Pt4HeMk2jx
```

3 Update the **ssl-truststore-passwords.properties** to ensure that the alias corresponds to your chosen alias in the steps described earlier.

  For example:

```
aliases=alfresco.ca,ecmxtserver
# The ssl truststore password
keystore.password=<newPassword>
# The password protecting the ssl repository key
ecmxtserver.password=<newPassword>
# The password protecting the ssl Alfresco CA strust
certificate
alfresco.ca.password=Pt4HeMk2jx
```

4 Open the **server.xml** file in **C:\Program Files (x86)\Agilent Technologies\ OpenLab Data Store\tomcat\conf**, and update the passwords and alias used for generating the keystore.

   a Update the connectors information for ‘Catalina’ service.

```
<!-- SSL port for Solr -->

<Connector URIEncoding="UTF-8"
protocol="org.apache.coyote.http11.Http11Nio2Protocol"
maxThreads="200" scheme="https" SSLEnabled="true"
sslImplementationName="org.apache.tomcat.util.net.jsse.JSSEI
mplementation" maxHttpHeaderSize="32768"
maxSavePostSize="-1" port="8443">

<SSLHostConfig sslProtocol="TLS" protocols="TLSv1.2"
certificateVerification="optional"
truststorePassword="<newPassword>" truststoreType="JCEKS"
truststoreFile="C:/Program Files (x86)/Agilent
Technologies/OpenLAB Data Store/keystore/ssl.truststore">

<Certificate certificateKeystorePassword="<newPassword>"
certificateKeyAlias="ecmxtserver"
certificateKeystoreType="JCEKS" type="RSA"
certificateKeystoreFile="C:/Program Files (x86)/Agilent
Technologies/OpenLAB Data Store/keystore/ssl.keystore" />
</SSLHostConfig>
</Connector>

<!-- SSL port for web server -->

<Connector URIEncoding="UTF-8"
protocol="org.apache.coyote.http11.Http11Nio2Protocol"
maxThreads="200" scheme="https" SSLEnabled="true"
sslImplementationName="org.apache.tomcat.util.net.jsse.JSSEI
mplementation" connectionTimeout="240000"
maxHttpHeaderSize="32768" compression="on"
compressionMinSize="1024"
compressableMimeType="text/html,text/xml,text/plain,text/jav
ascript,text/css,application/json,application/atom+xml"
port="443">

<SSLHostConfig sslProtocol="TLS" protocols="TLSv1.2"
certificateVerification="none" honorCipherOrder="true"
truststorePassword="<newPassword>" truststoreType="JCEKS"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_E
CDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CB
C_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_W
ITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA3
84,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_
AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_EC
```

```
DHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_
SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_DHE_RSA_WIT
H_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS
_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_S
HA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_
256_CBC_SHA256" truststoreFile="C:/Program Files
(x86)/Agilent Technologies/OpenLAB Data
Store/keystore/ssl.truststore">

<Certificate certificateKeystorePassword="<newPassword>"
certificateKeyAlias="ecmxtserver"
certificateKeystoreType="JCEKS" type="RSA"
certificateKeystoreFile="C:/Program Files (x86)/Agilent
Technologies/OpenLAB Data Store/keystore/ssl.keystore" />
</SSLHostConfig>
</Connector>
```

b Update the connector information for the ‘Share’ service.

```
<Connector URIEncoding="UTF-8"
protocol="org.apache.coyote.http11.Http11Nio2Protocol"
SSLEnabled="true" maxThreads="150" scheme="https"
connectionTimeout="240000" maxHttpHeaderSize="32768"
port="9443" address="127.0.0.1">

<SSLHostConfig sslProtocol="TLS" protocols="TLSv1.2"
certificateVerification="none">

<Certificate certificateKeystorePassword="<newPassword>"
certificateKeyAlias="ecmxtserver"
certificateKeystoreType="JCEKS" type="RSA"
certificateKeystoreFile="C:/Program Files (x86)/Agilent
Technologies/OpenLAB Data Store/keystore/ssl.keystore" />
</SSLHostConfig>
</Connector>
```

5 Update the **alfresco.host** and **solr.host** properties in **C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco-global.properties**, and make sure the fully qualified domain name of actual host of the server is used.

OpenLab Server/ECM XT Solr6 configuration

For a 4-server solution, perform this procedure only on the OpenLab Index Server. For an all-in-one server or 2-server solution, perform this procedure on the OpenLab Server/ECM XT server.

1 Copy **ssl.keystore** and **ssl.truststore** to the following directories:

   - **\Agilent Technologies\Content Management Search Services\solrhome\templates\rerank\conf**
   - **\Agilent Technologies\Content Management Search Services\solrhome\alfresco\conf**
   - **\Agilent Technologies\Content Management Search Services\solrhome\archive\conf**

2 Rename the **ssl.keystore** file to **ssl.repo.client.keystore**.

3 Rename the **ssl.truststore** file to **ssl.repo.client.truststore**.

4 Update the **alfresco.host** property in **solrcore.properties** to correspond to the actual host name. For example:

   - In a 4-server solution, change “localhost” to the fully qualified name of the Index and Search server.
   - In an all-in-one server solution or a 2-server solution, change “localhost” to the fully qualified name of the OpenLab Server/ECM XT server machine name.

5 Update the **ssl-keystore-passwords.properties** to ensure that the alias corresponds to your chosen alias in the steps described earlier.

   For example:

```
aliases=ssl.alfresco.ca,ecmxtserver
# The ssl keystore password
keystore.password=<newPassword>
# The password protecting the ssl repository key
ecmxtserver.password=<newPassword>

# The password protecting the ssl Alfresco CA strust
certificate
ssl.alfresco.ca.password=Pt4HeMk2jx
```

6 Update the **ssl-truststore-passwords.properties** to ensure that the alias corresponds to your chosen alias in the steps described earlier.

   For example:

```
aliases=alfresco.ca,ecmxtserver
# The ssl truststore password
keystore.password=<newPassword>
# The password protecting the ssl repository key
ecmxtserver.password=<newPassword>
# The password protecting the ssl Alfresco CA strust
certificate
alfresco.ca.password=Pt4HeMk2jx
```

7 Open the file **\Agilent Technologies\Content Management Search Services\solr\server\etc\jetty-ssl.xml**, and update the Sets **KeyStorePassword** and **TrustStorePassword** default passwords.

```
<Set name="KeyStorePassword"><Property
name="solr.jetty.keystore.password"
default="<newpass>"/></Set>
<Set name="TrustStorePassword"><Property
name="solr.jetty.truststore.password"
default="<newpass>"/></Set>
```

Configure a CSRF (Cross-Site Request Forgery) filter

For a 4-server solution, perform this procedure only on the Content Management-only Server. For an all-in-one server or 2-server solution, perform this procedure on the OpenLab Server/ECM XT server.

Open **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 host 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://<fully qualified hostname>/.*
```

```
csrf.filter.referer=https://<fully qualified hostname>/.*
```

Configure CORS (Cross-Origin Resource Sharing) to prevent cross-domain requests

For a 4-server solution, perform this procedure only on the Content Management-only Server. For an all-in-one server or 2-server solution, perform this procedure on the OpenLab Server/ECM XT server.

1 To prevent cross-domain requests, open the file **C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\webapps\alfresco\WEB-INF\web.xml**.

2 Search for the **cors.allowOrigin** parameters, and update the **param-value** to your domain. For example:

```
<init-param>
<param-name>cors.allowOrigin</param-name>
<param-value>http://agilent.com,
https://agilent.com</param-value>
</init-param>
```

Disable HTTP Protocol

For a 4-server solution, perform this procedure only on the Content Management only server. For an all-in-one server or 2-server solution, perform this procedure on the OpenLab Server/ECM XT server.

Use the following procedure if you want to completely disable 'http' usage.

1 Add the following to the **OpenLab Data Store\tomcat\webapps\datastore\WEB_INF\web.xml** file before the `</web-app>` line:

```
<security-constraint>
  <web-resource-collection>
  <web-resource-name>Secure URLs</web-resource-name>
  <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

2 Add the following to the **OpenLab Data Store\tomcat\webapps\alfresco\WEB-INF\web.xml** file:

```
<security-constraint>
  <web-resource-collection>
  <web-resource-name>Secure URLs</web-resource-name>
  <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

Reactivate from Control Panel

1 Reboot your system, including the OpenLab Server/ECM XT server and the Index server (if using a 4-server solution).

2 From the OpenLab Control Panel, select **Administration > System Configuration**, then click **Edit System**.

3 Select Change Server, enter the Content Management server URL with https and the fully qualified name of the host.

Configure port 52088 to use a commercial certificate

For a 4-server solution, perform this procedure only on the Content Management-only Server. For an all-in-one server or 2-server solution, perform this procedure on the OpenLab Server/ECM XT server.

1 Export the certificate from the Java keystore. Use the following command in a cmd window to convert the certificate.

```
keytool -importkeystore -srckeystore <keystore file name>
-srcstorepass <password> -srckeypass <password> -srcalias
<alias for your certificate> -destalias <alias for your
certificate> -destkeystore <filename for exported certificate>
-deststoretype PKCS12 -deststorepass <password> -destkeypass
<password>
```

For example,

```
keytool -importkeystore -srckeystore ssl.keystore
-srcstorepass <password> -srckeypass <password> -srcalias
ecmxtserver -destalias ecmxtserver -destkeystore
ecmxtserver.p12 -deststoretype PKCS12 -deststorepass
<password> -destkeypass <password>
```

where <password> is the password specified previously with keytool.

Once this command has run successfully, the exported certificate is the file ecmxtserver.p12.

2 Import the certificate into Windows Certificate Store using Certificate Service. In the cmd window, change to **C:\Program Files (x86)\Agilent Technologies\OpenLab Certificate Service\bin**, and run the following command:

```
Agilent.OpenLab.CertService.CertServiceCore.exe
useexternalcert -certfilename <filename for exported
certificate> -certpassword <password>
```

For example,

```
Agilent.OpenLab.CertService.CertServiceCore.exe
useexternalcert -certfilename ecmxtserver.p12 -certpassword
<password>
```

3 Reboot your system, including the OpenLab Server/ECM XT server and the Index server (if using a 4-server solution).

NOTE

Upgrading the OpenLab Server/ECM XT Server will reset configurations. To re-enable the HTTPS, the configurations need to be reapplied.

4 Maintenance

The **Agilent OpenLab Server 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 OLSharedServices databases. If custom database names were chosen during installation, use the correct names from your installation notes.

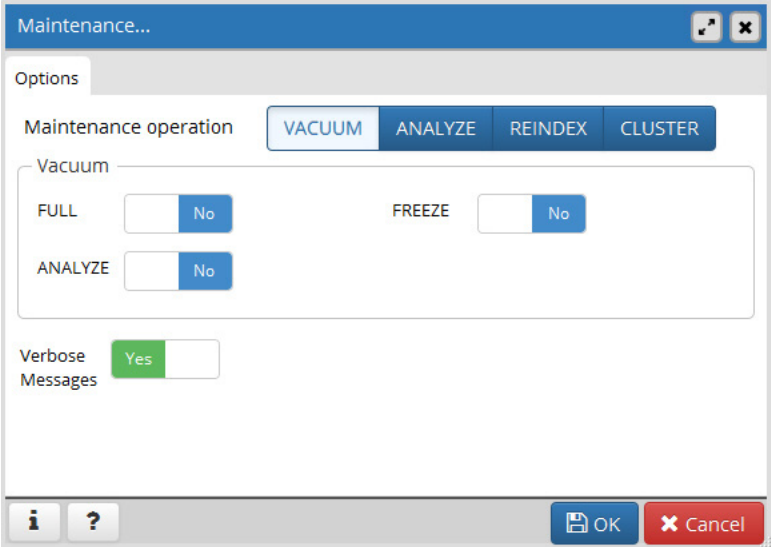
Procedures for PostgreSQL database

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.

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.



Maintenance operation: VACUUM

FULL: No

FREEZE: No

ANALYZE: No

Verbose Messages: Yes

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.

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 Server 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 **Server 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 **Server 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 **Server 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 **Customers subject to regulations from US FDA or similar organizations are cautioned that FTP services are enabled by default. 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 42.**

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.

Automatic 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:

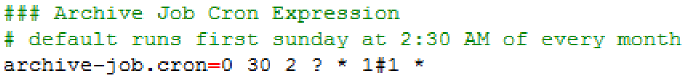
- An operating system user credential with read/write permission for the **<INSTALLATION PATH>\tomcat\shared\classes\alfresco-global.properties** file. In a default installation, the file is in the following location: **C:\Program Files (x86)\Agilent Technologies\OpenLab Data Store\tomcat\shared\classes\alfresco-global.properties**.
- 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 44.

5 Save the file.

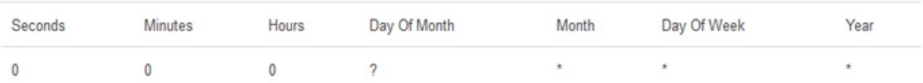
6 Restart the alfrescoTomcat service.

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 5 contains examples of cron expressions for automated archiving.

Table 5 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 2nd and 17th 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.

5 Backup and Restore Procedures

Disaster Recovery Planning

Prepare a recovery plan for the unlikely case of OpenLab Server/ECM XT becoming 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.

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 directory
  - OpenLab Server/ECM XT indexes folder
  - Shared Services language
  - Shared Services database name
  - Installed licenses
  - Registered applications
- Third party software information: applications and their revisions and install paths
- **“OpenLab Server/ECM XT Server Backup Procedure”** and **“OpenLab Server/ECM XT Server Restore Procedure”**
- Backup media location and organization details

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 (**“OpenLab Server/ECM XT Server Restore Procedure”** on page 57) 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.

There are some differences in procedure for systems with multiple storage. See **“Backup and Restore with Multiple Storage Locations”** on page 65.

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.

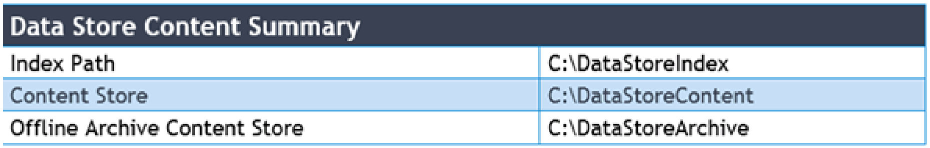
There are two databases that need to be backed up. The OpenLab Server/ECM XT server database and the Shared Services database. The names of these databases can be retrieved from the Server Configuration page.

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 > OpenLab Data Store > Server Configuration**.

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



Data Store Content Summary	
Index Path	C:\DataStoreIndex
Content Store	C:\DataStoreContent
Offline Archive Content Store	C:\DataStoreArchive

Figure 3. OpenLab Server/ECM XT Server Content Summary

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.

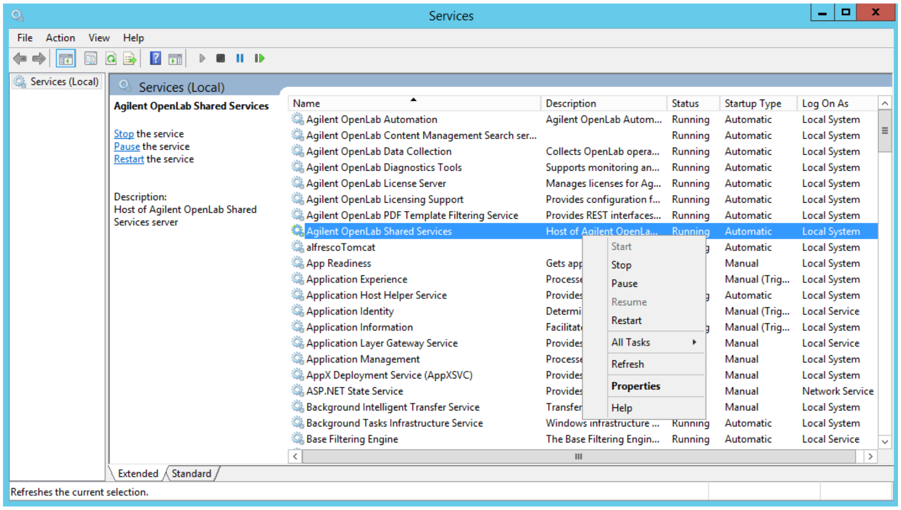
```
dir.root=\\\\HA-ContentStore\\ContentStore# content store 1
dir2.root=\\\\HA-ContentStore\\ContentStore2 # content store 2 (current)
```

Step 2 Stop OpenLab Server/ECM XT services:

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

- Content Management Search service
- alfrescoTomcat
- Agilent OpenLab Shared Services
- olcm-postgresql-x64-10 (only applicable when using PostgreSQL database for OpenLab Server/ECM XT)

  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.



Agilent OpenLab Shared Services

Stop the service
Pause the service
Restart the service

Description:
Host of Agilent OpenLab Shared Services server

Name	Description	Status	Startup Type	Log On As
Agilent OpenLab Automation	Agilent OpenLab Autom...	Running	Automatic	Local System
Agilent OpenLab Content Management Search ser...		Running	Automatic	Local System
Agilent OpenLab Data Collection	Collects OpenLab opera...	Running	Automatic	Local System
Agilent OpenLab Diagnostics Tools	Supports monitoring an...	Running	Automatic	Local System
Agilent OpenLab License Server	Manages licenses for Ag...	Running	Automatic	Local System
Agilent OpenLab Licensing Support	Provides configuration f...	Running	Automatic	Local System
Agilent OpenLab PDF Template Filtering Service	Provides REST interfaces...	Running	Automatic	Local System
Agilent OpenLab Shared Services	Host of Agilent OpenLa...	Running	Automatic	Local System
alfrescoTomcat		g	Automatic	Local System
App Readiness	Gets app		Manual	Local System
Application Experience	Processe		Manual (Trig...	Local System
Application Host Helper Service	Provides	g	Automatic	Local System
Application Identity	Determi		Manual (Trig...	Local Service
Application Information	Facilitat	g	Manual (Trig...	Local System
Application Layer Gateway Service	Provides		Manual	Local Service
Application Management	Processe		Manual	Local System
AppX Deployment Service (AppXSVC)	Provides		Manual	Local System
ASP.NET State Service	Provides		Manual	Network Service
Background Intelligent Transfer Service	Transfer		Manual	Local System
Background Tasks Infrastructure Service	Windows infrastructure ...	Running	Automatic	Local System
Base Filtering Engine	The Base Filtering Engin...	Running	Automatic	Local Service

Refreshes the current selection.

Figure 4. Stop OpenLab Server/ECM XT Services

Step 3 Backup databases

This section provides a simple and interactive approach to backup databases. Please see PostgreSQL, MS SQL Server, or Oracle 12c 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. By default, it is **C:\ProgramData\Agilent\PostgreSqlData-10-OLCM**. If customized during installation, you can find the location information in the Server Configuration (**Start > All Programs > Agilent Technologies > OpenLab Data Store > Server Configuration**).

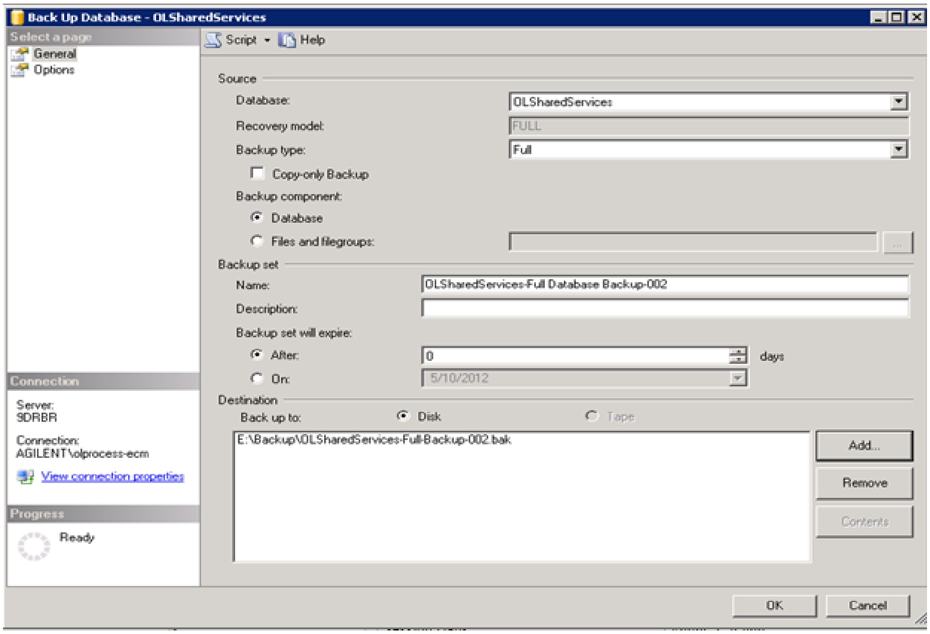
This information is also recorded in Windows registry at:

`“HKEY_LOCAL_MACHINE\SOFTWARE\PostgreSQL\Installations\postgresql-x64-10\Data Directory”.`
Back up the PostgreSQL database by backing up the database folder (**C:\ProgramData\Agilent\PostgreSqlData-10-OLCM**) using **Windows Server Backup** or any other tool of your choice.

CAUTION

If your server is configured to use PostgreSQL 9.3 and you upgrade your system in place to the latest version, the PostgreSQL database will be upgraded to version 10.3 and database data will be migrated to C:\ProgramData\Agilent\PostgreSqlData-10.3. Any backup and restore activity should occur on the upgraded system.

Procedure for MS SQL Server Use **SQL Server Management Studio** to backup 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**.



Back Up Database - OLSharedServices

Source
Database: OLSharedServices
Recovery model: FULL
Backup type: Full
☐ Copy-only Backup
Backup component:
● Database
○ Files and filegroups:

Backup set
Name: OLSharedServices-Full Database Backup-002
Description:
Backup set will expire:
● After: 0 days
○ On: 5/10/2012

Destination
Back up to: ● Disk ○ Tape
E:\Backup\OLSharedServices-Full-Backup-002.bak

Connection
Server:
SDRBR
Connection:
AGILENT\olprocess-ecm

Progress
Ready

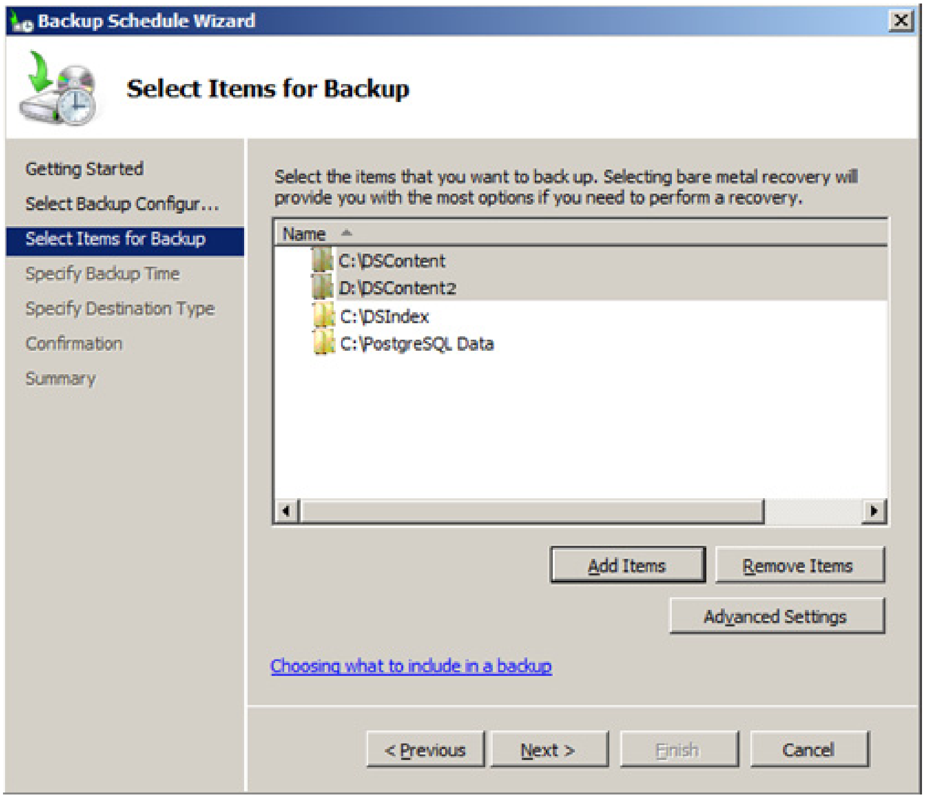
Figure 5. Using SQL Server Management Studio for backup

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

Step 4 Backup 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:\DSContent**), index folder (**C:\DSIndex**), and Archive folder (**C:\DataStoreArchive**).

If you have multiple content stores, you have to backup each additional content folder (**D:\DSContent2**).



Select the items that you want to back up. Selecting bare metal recovery will provide you with the most options if you need to perform a recovery.

Name
C:\DSContent
D:\DSContent2
C:\DSIndex
C:\PostgreSQL Data

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.

Step 6 Start OpenLab Server/ECM XT services

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

- olcm-postgresql-x64-10 (only applicable when using PostgreSQL database for OpenLab Server/ECM XT)

  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

Create a 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.

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\OpenLab DataRepository\Base\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.

Set up an automated system backup

Use the **Windows Task Scheduler** to set up an automated PostgreSQL database backup for the OpenLab Server/ECM XT server. Only an administrator of the local PC can perform this procedure.

Information required in this procedure can be found on the Server Configuration page.

1 Click **Windows Start > Agilent Technologies > OpenLab Data Store > Server Configuration**.

2 Log on to the local PC with Administrator privileges.

3 Create a directory on disk to which you want the backups to be copied. Make sure to record the complete path to this directory.
This is your <BACKUPDESTINATIONDIR>.

4 Record the complete path to the OpenLab Server/ECM XT content directory using the information in the Server Configuration. If the content location is an Amazon S3 storage location, there is no need to record the path.
This is your <DSCONTENTDIR>.

5 Record the complete path to the OpenLab Server/ECM XT Indexes directory using the information in the Server Configuration.
This is your <DSINDEXDIR>.

6 Record the complete path to the OpenLab Server/ECM XT archive directory using the information in the Server Configuration. If the archive location is an Amazon S3 storage location, there is no need to record the path.
This is your <DSARCHIVEDIR>.

7 Record the complete path to the PostgreSQL database files directory. By default, this directory is located at
C:\ProgramData\Agilent\PostgreSqlData-10-OLCM
This is your <POSTGRESQLDATADIR>.

8 Record the complete path to the Installation Root directory.
For example, **C:\Program Files (x86)\Agilent Technologies**
This is your <AGILENTHOMEDIR>.

9 Copy the Backup Scripts folder (by default, this folder is located at **C:\Program Files (x86)\Agilent Technologies\OpenLab Data Store\Backup Scripts**) with scripts to a location on Disk (for example, **C:\BackupScripts**).

10 To open the Windows Tasks Scheduler, open your Windows Control Panel, click **Administrative Tools**, and double-click **Task Scheduler**.

11 Click **Create Basic Task** in the **Actions** panel. The **Create Basic Task Wizard** opens.

12 Enter a **Name** and **Description**, and then click **Next**.

13 Select the time period that you want to run the backup, and then click **Next**.

14 More options may be available depending on the time interval selected. Complete the options, and then click **Next**.

15 Select **Start a program**, and then click **Next**.

16 Browse to and select the **Secure_OpenLabCDS_Data_Backup_TaskScheduler.bat** file from the **Backup Scripts** folder.

17 Ensure that the script contains only the name of the script and not the full path. For example, **Secure_OpenLabCDS_Data_Backup_TaskScheduler.bat**.

18 Enter the path of the script in the **Start In** field. For example, if the script resides in **C:\Backup\Backup Scripts**, enter **C:\Backup\Backup Scripts**. Do not enclose this path in quotes and do not include a \ character at the end of the path.

19 In the **Add Arguments** box, enter the following values (with quotes)
"<BACKUPDESTINATIONDIR>"
"<DSCONTENTDIR>"
"<DSINDEXDIR>"
"<POSTGRESQLDATADIR>"
"<AGILENTHOME>"
"<DSARCHIVEDIR>"

For example:
"E:\BackupLocation" "C:\DsData\DsContent" "C:\DsData\DSIndex" "C:\ProgramData\Agilent\PostgreSqlData-10-OLCM" "C:\Program Files (x86)\Agilent Technologies" "C:\DsData\DSArchive"

If the content or archive location is an Amazon S3 storage location, put double quotes ("") as the parameter. Do not leave the parameter blank.

For example:
"E:\BackupLocation" "" "C:\DsData\DSIndex" "C:\ProgramData\Agilent\PostgreSqlData-10-OLCM" "C:\Program Files (x86)\Agilent Technologies" ""

Amazon S3 storage locations are not backed up using this procedure.

20 Click **Next**.

21 Select **Open the Properties dialog for this task when I click Finish**.

22 Click **Finish**. The Properties window for your newly created task appears.

23 On the **General** tab, select **Run with highest privileges**.

24 Click **OK**.

A message will appear before the backup is scheduled to start. To dismiss the message and continue with the backup, click **OK**. A command prompt appears and displays the progress of the backup, and a log file is created in your <BACKUPDESTINATIONDIR>.

You can also run your task manually from the Task Scheduler window outside of the scheduled times. Select your task from the **Task Scheduler Library** and click **Run**.

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.

Step 1 Restore the databases

Procedure for a PostgreSQL Server

Determine your database folder (for example, **C:\ProgramData\Agilent\PostgreSqlData-11-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 9.3 and you upgrade your system in place to the latest version, the PostgreSQL database will be upgraded to version 11.5 and database data will be migrated to C:\ProgramData\Agilent\PostgreSqlData-11.5. 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.

1 Restore the Shared Services database and the OpenLab Server/ECM XT server database using the SQL Server Management Studio.

2 Modify Shared Services database settings using the SQL Server Management Studio.

   a Remove the database user from **Shared Services database > Security > Users**.

   b Go to **Security > Logins > User Mappings**.

   c Select **Map** for **OLSharedServices** database.

- **d** The user selected as the DB administrator in Step 2 of the installation should be assigned the **db_owner** role. The user selected as the Shared Services DB user should be assigned the **db_datareader** and **db_datawriter** roles. If you are using Windows Authentication, the selected user is “NT AUTHORITY\SYSTEM”.
- **e** Set the **Default Schema** to **dbo**.

3 Modify OpenLab Server/ECM XT server database settings using the SQL Server Management Studio.

- **a** Go to **Datastore > Security > Users**.
- **b** Remove **DSAdmin**.
- **c** From **Security > Logins**, assign the **DSAdmin** user as the **db_owner**. If the **DSAdmin** user does not exist, you must create that user.

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\OpenLab DataRepository\Base\Scripts\PostgreSQL\Backup\dr-db-restore.ps1**.

```
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 bak1`

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 Sever/ECM XTcontent folder (**C:\DSContent**) and index folder (**C:\DSIndex**), 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.

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**.

Step 4 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 (v11)** 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 **Validate**, and then click **Next**.

12 Review the overall configuration summary carefully. If it is OK, click **Apply**.

Step 5 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**.

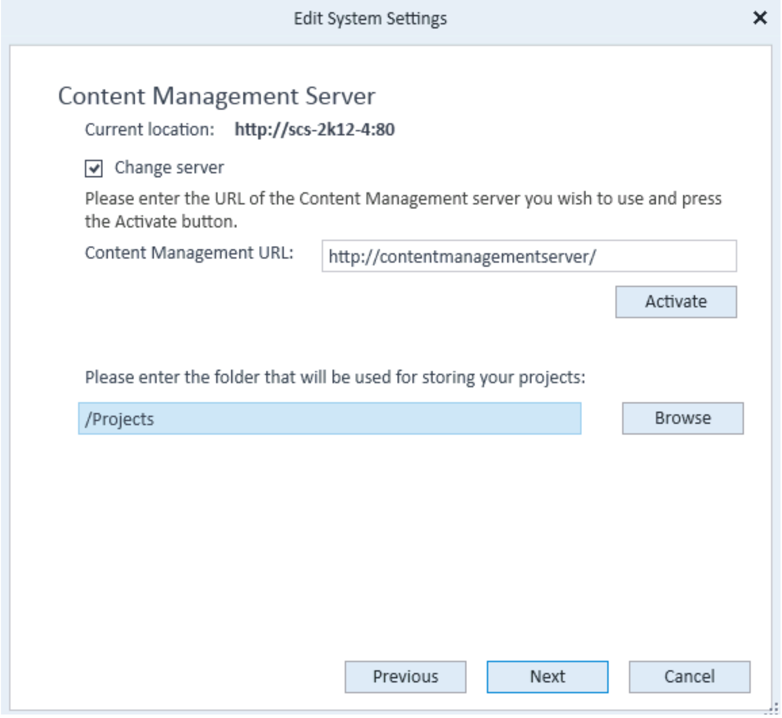
3 Select either **Internal** or **Windows domain** for the authentication provider. If you had already configured with one of these values previously, you can choose **Keep current configuration**. If you select **Windows domain**, see **"Windows Domain"** on page 39.

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: http://contentmanagementserver/

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

/Projects

Figure 7. OpenLab Server/ECM XT Activation

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

Step 6 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 > OpenLab Shared Services > 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 7 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**. The information will display in an Internet window.

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

Backup and Restore with Multiple Storage Locations

For systems with multiple storage locations, the backup script can get several paths for <DSCONTENTDIR> and <DSARCHIVEDIR>. Multiple paths should be separated by a semicolon and enclosed in quotation marks.

For example, “C:\DataStoreContent;E:\DataStoreContent-New”

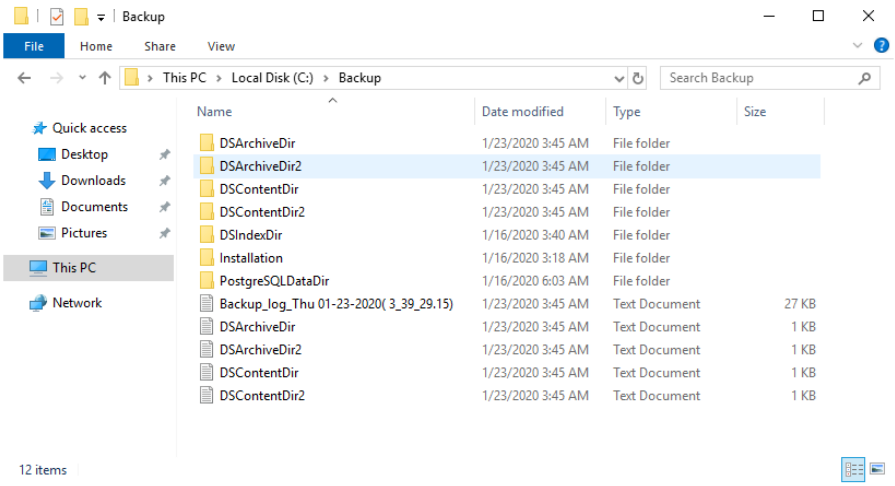
The following is an example of parameters for the run backup script:

"E:\BackupLocation" "C:\DsData\DsContent;D:\NewContent" "C:\DsData\DSIndex" "C:\ProgramData\Agilent\PostgreSqlData-11-OLCM" "C:\Program Files (x86)\Agilent Technologies" "C:\DsData\DsArchive;D:\NewArchive"\

If a backup system has multiple content or archive storages, the backup contains subfolders for each additional storage. The first content and archive storages are backed up to the DSContentDir and DSArchiveDir sub-folders in the backup location. Then, the second content and archive storages are backed up to the subfolders in the backup location with an added suffix containing a number.

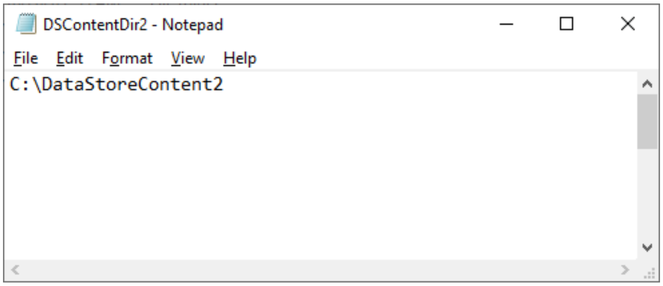
A text file with the same name as the subfolder is placed in the backup location. The text file contains the storage location path from where it was backed up.

The following is an example of a backup system with two content and two archive storages:



Name	Date modified	Type	Size
DSArchiveDir	1/23/2020 3:45 AM	File folder	
DSArchiveDir2	1/23/2020 3:45 AM	File folder	
DSContentDir	1/23/2020 3:45 AM	File folder	
DSContentDir2	1/23/2020 3:45 AM	File folder	
DSIndexDir	1/16/2020 3:40 AM	File folder	
Installation	1/16/2020 3:18 AM	File folder	
PostgreSQLDataDir	1/16/2020 6:03 AM	File folder	
Backup_log_Thu 01-23-2020(3_39_29.15)	1/23/2020 3:45 AM	Text Document	27 KB
DSArchiveDir	1/23/2020 3:45 AM	Text Document	1 KB
DSArchiveDir2	1/23/2020 3:45 AM	Text Document	1 KB
DSContentDir	1/23/2020 3:45 AM	Text Document	1 KB
DSContentDir2	1/23/2020 3:45 AM	Text Document	1 KB

The file DSConentDir2.txt contains the information that the files that were placed in the DSContentDir2 sub-folder were backed up from the content location “C:\DataStoreContent2”.



```
C:\DataStoreContent2
```

6 Hot Backup Procedures

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.

Backup Guidelines

- Always follow the prescribed order as described in **“Overview”** on page 69 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 OpenLabe 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. 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.

3. Content Store

   The final step is to back up the actual files. For this you can use any file backup tool.

4. 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 6 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 6 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 73). For example, if the index path is C:\DataStoreIndex, you will need to configure your backup location to be: /DataStoreIndex/solr6Backup/alfresco:

Table 7 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.

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 8 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 73.) 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 9 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.

Backup 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 10 Shared Services database summary

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

Table 10 Shared Services database summary

Database administrator	postgres
Database user	Olss

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

Table 11 Content Management database summary

Database type	PostgreSQL
Server name	loaclhost
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 79.

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 12 Backup destination

Tool	Property	Notes
Text Editor	Set backupdestination=<Path\to\backupfolder> OR 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. 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-10-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 13 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-x64-10 Windows service.

The default path to the file is: C:\ProgramData\Agilent\PostgreSqlData-10-OLCM.

Table 14 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 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 84.
- SQL*Plus or another tool for executing SQL commands. See **"How to connect SQL*Plus to the database"** on page 84.
- 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 84. 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 82.

Back up the database and archive log

Table 15 Back up database

Tool	Command
Not applicable	Connect RMAN to the database. See **"How to connect RMAN to the database"** on page 84.
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 16 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 login 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 17 Connect RMAN to the database

Tool	Command

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

How to connect SQL*Plus to the database

Table 18 Connect SQL*Plus to the database

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

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 19 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.

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.

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 Content and Archive Store
4 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.

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, 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.

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.xxxxxxxxxxxxxxxxx. 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.

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

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:

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

This section provides the steps for restoring from a backup to the same Oracle installation from which it was taken and where the goal is to replace the existing data with the data from the backup. This may occur when recovering from an operational error where data changes were made inadvertently, and you need to bring the system back to a point before the error occurred.

1 Execute the following commands to restore the database.

Table 20 Restore an Oracle database

Tool	Command
SQL	`SHUTDOWN IMMEDIATE` To execute SQL commands, connect SQL*Plus to the database. See **"How to connect SQL*Plus to the database"** on page 84.
SQL	`STARTUP MOUNT`
SQL	`RESTORE DATABASE` This restores the most recent backup.
SQL	`RECOVER DATABASE`

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

Restoring from a backup after a loss of data

This section provides the steps for restoring from a backup to the same Oracle installation from which it was taken, but where data loss has occurred due to a system failure. For the purposes of this section, the failure is assumed to be a total loss of the Oracle data (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, unless the archive logs generated since the last backup have been saved. See **Log backup** in the **"More backup considerations"** on page 83.

Before starting the restore process,

- Ensure that the FRA folder that contains your most recent backup is accessible to Oracle.
- Confirm that the FRA parameters are set, and, if not, execute the Oracle hot backup configuration instructions from the *Agilent OpenLab Server and OpenLab ECM XT Installation Guide*.

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	`CREATE PFILE='<Oracle Installation>\database\PFILE<YOURINSTANCENAME>.ORA' FROM SPFILE='<Oracle`
	`Installation>\database\SPFILE<YOURINSTANCENAME>.ORA`
Text Editor	Edit tnsnames.ora to add (UR = A) clause The default location is: <Oracle Installation>\network\admin\tn snames.ora

	`<YOURINSTANCENAME> =`
	`(DESCRIPTION =`
	`(ADDRESS_LIST =`
	`(ADDRESS = (PROTOCOL = TCP)(HOST = YourServerName)(PORT = 1521))`
	`)`
	`(CONNECT_DATA = (SERVER = DEDICATED)`
	`(SERVICE_NAME = <YOURINSTANCENAME>)`
	`(UR = A)`
	`)`
	`)`

SQL	`STARTUP NOMOUNT` If the database is already running, `SHUTDOWN IMMEDIATE` instead. Then run `STARTUP NOMOUNT` and reconnect RMAN and SQL.

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.

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.

7 Upgrading and Reconfiguration

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 **“OpenLab Server/ECM XT Server Backup Procedure”** on page 47.
3. On the new machine, perform the server restore procedure. See **“OpenLab Server/ECM XT Server Restore Procedure”** on page 57.

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 DB server (local or remote), and you have decided to upgrade the DB server software to a newer version or upgrade the hardware, which involves relocating the DB server software to a new machine. You must tell OpenLab Server/ECM XT how to connect to the new DB 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 97“
2. **“Make Changes to the Infrastructure”** on page 97
3. **“Run the OpenLab Server Configuration Utility”** on page 104
4. **“Bring Up OpenLab Server/ECM XT”** on page 112

To add additional content or archive store, see **“Add Additional Content or Archive Store”** on page 112.

Bring Down OpenLab Server/ECM XT

Stop services in the following order:

1. alfrescoTomcat
2. 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 11.x.x.

For this example,

- Server1 is the source machine
- Server2 is the destination machine

1. On Server1, stop PostgreSQL service (for version 11: **postgresql-x64-11**).
2. Click **Start > All Programs > Agilent Technologies > OpenLab Data Store > Server Configuration**.
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 Windows authentication:

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:

```
# those 4 lines enable remote access for OLSS
host all labuser 0.0.0.0/0  sspi
host all labuser ::/0     sspi
host all SYSTEM  0.0.0.0/0  sspi map=datastore
host all SYSTEM  ::/0     sspi map=datastore
# those two lines will enable remote access for DataStore
host all all    0.0.0.0/0  md5
host all all    ::/0     md5
```

where **labuser** is the domain user that will run the OpenLab ECM XT installer (case-sensitive).

Depending on your network configuration, you may want to replace 0.0.0.0/0 and ::/0 with more restrictive subnet definitions (or even a single IP address) that still include OpenLab Server/ECM XT. Please 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:

```
host  all  all  0.0.0.0/0  md5
```

```
host  all  all  ::/0     md5
```

Depending on your network configuration, you may want to replace 0.0.0.0/0 and ::/0 with more restrictive subnet definitions (or even a single IP address) that still include OpenLab Server/ECM XT. Please consult your network administrator to find the best option for your network.

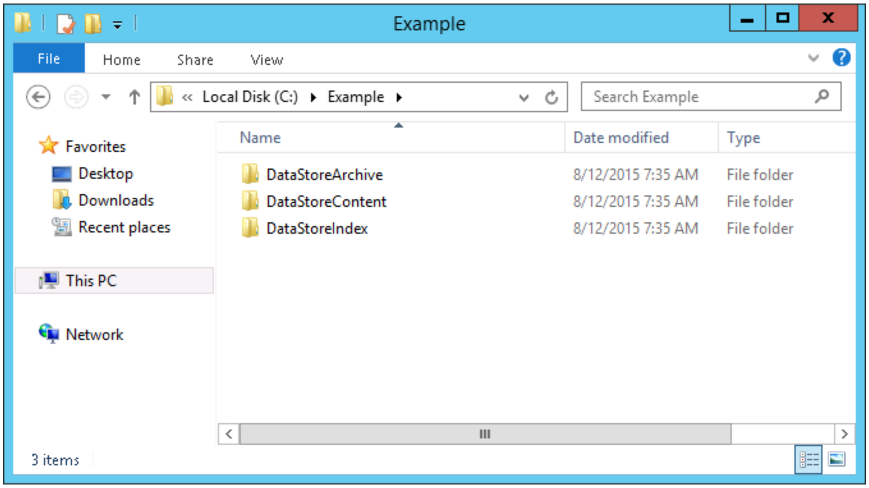
Please see PostgreSQL official documentation to learn more about security features.

8 To apply the changes, click **Start > All Programs > PostgreSQL 11** and click **Reload Configuration**.

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 101

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.



Name	Date modified	Type
DataStoreArchive	8/12/2015 7:35 AM	File folder
DataStoreContent	8/12/2015 7:35 AM	File folder
DataStoreIndex	8/12/2015 7:35 AM	File folder

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.

Create a new user

1 Create the user.

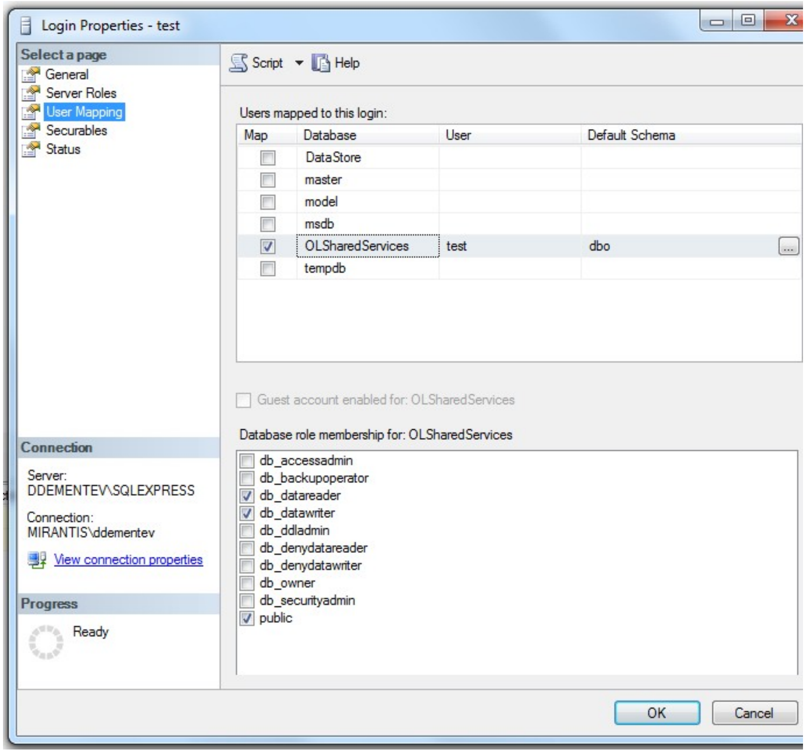
2 Grant the user permissions on database tables.

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.



Users mapped to this login:

Map	Database	User	Default Schema
☐	DataStore		
☐	master		
☐	model		
☐	msdb		
☑	OLSharedServices	test	dbo
☐	tempdb		

☐ Guest account enabled for: OLSharedServices

Database role membership for: OLSharedServices

☐ db_accessadmin
☐ db_backupoperator
☑ db_datareader
☑ db_datawriter
☐ db_ddladmin
☐ db_denydatareader
☐ db_denydatawriter
☐ db_owner
☐ db_securityadmin
☑ public

Connection

Server:
DDEMENTEV\SQLEXPRESS

Connection:
MIRANTIS\ddementev

View connection properties

Progress

Ready

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

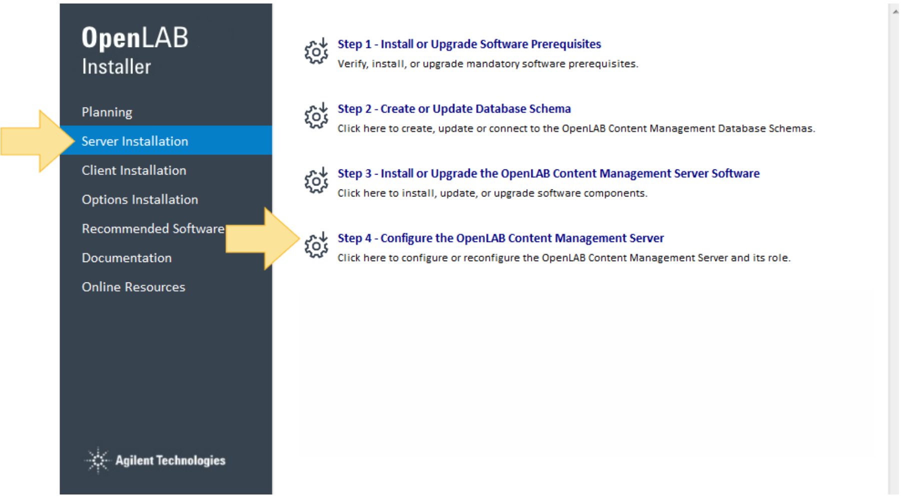
CAUTION

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 97. It is strongly recommended that you do not edit any other values. Changing any other fields could cause the configuration to crash.

1 Insert the USB drive. **Autorun.inf** will automatically run **Agilent.OpenLab.CDSInstaller.exe** and display the **OpenLab Installer screen**. If the program does not start automatically, select **setup.exe** from the USB driver.

2 Select **OpenLab Server**, and click **OK**.

3 From the OpenLab Installer, click **Server Installation > Step 4 - Configure the OpenLab Content Management Server**.



Step 1 - Install or Upgrade Software Prerequisites
Verify, install, or upgrade mandatory software prerequisites.

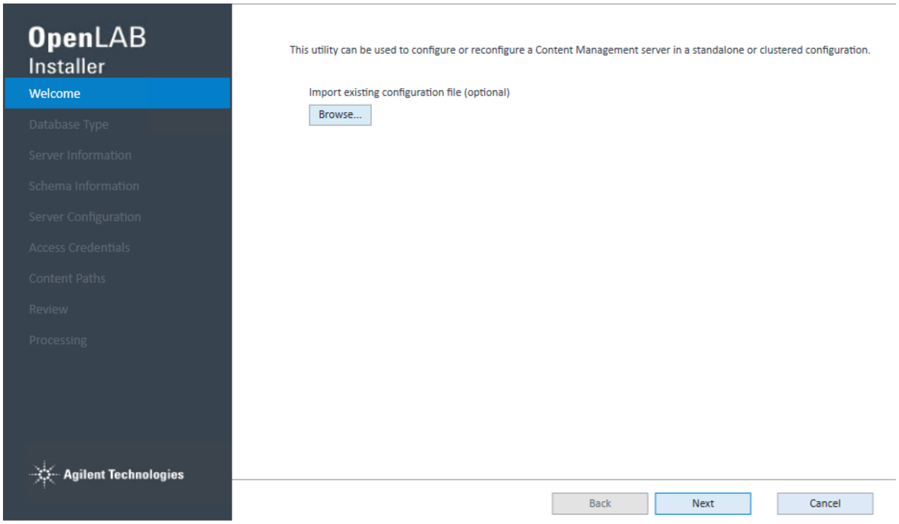
Step 2 - Create or Update Database Schema
Click here to create, update or connect to the OpenLAB Content Management Database Schemas.

Step 3 - Install or Upgrade the OpenLAB Content Management Server Software
Click here to install, update, or upgrade software components.

Step 4 - Configure the OpenLAB Content Management Server
Click here to configure or reconfigure the OpenLAB Content Management Server and its role.

Figure 10. OpenLab Installer Server Installation

4 Click **Next**.

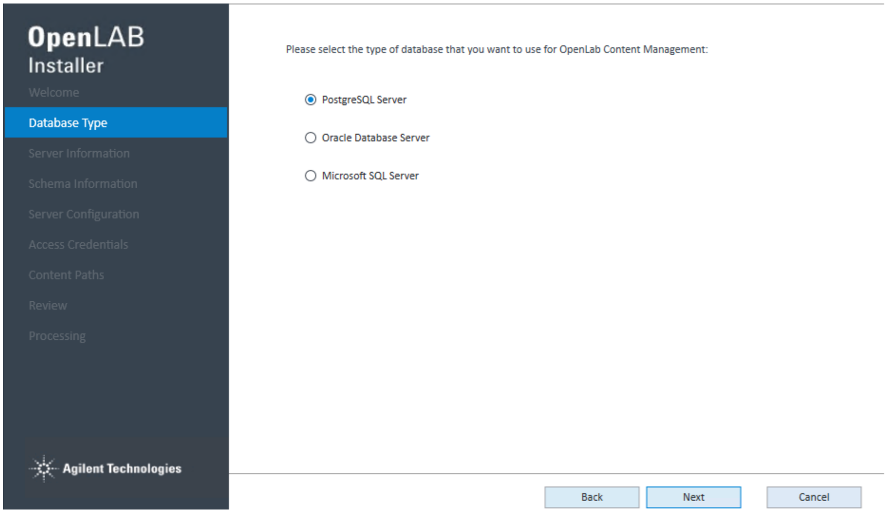


This utility can be used to configure or reconfigure a Content Management server in a standalone or clustered configuration.

Import existing configuration file (optional)

Figure 11. OpenLab Installer Welcome Screen

5 Click **Next**.



Please select the type of database that you want to use for OpenLab Content Management:

● PostgreSQL Server

○ Oracle Database Server

○ Microsoft SQL Server

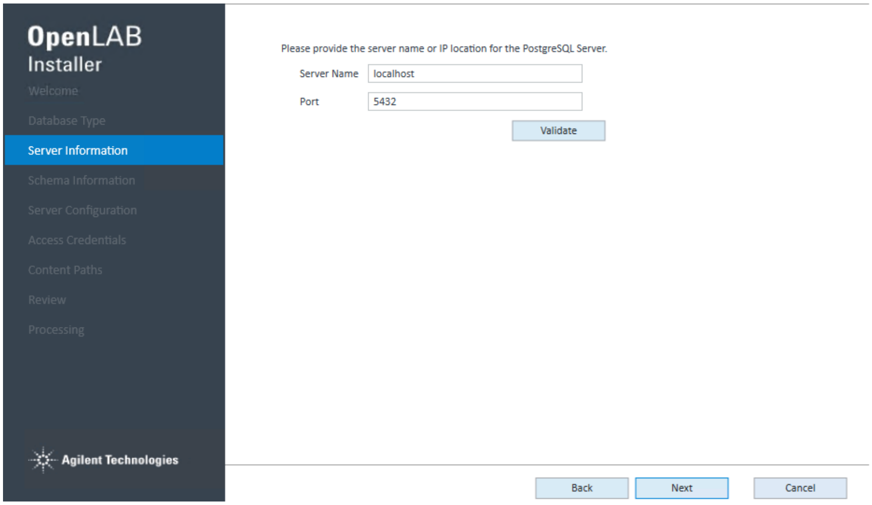
Figure 12. OpenLab Installer Database Type Screen

6 The information displayed on the **Server Information** 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 hostname or port number) has been changed.

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



Please provide the server name or IP location for the PostgreSQL Server.

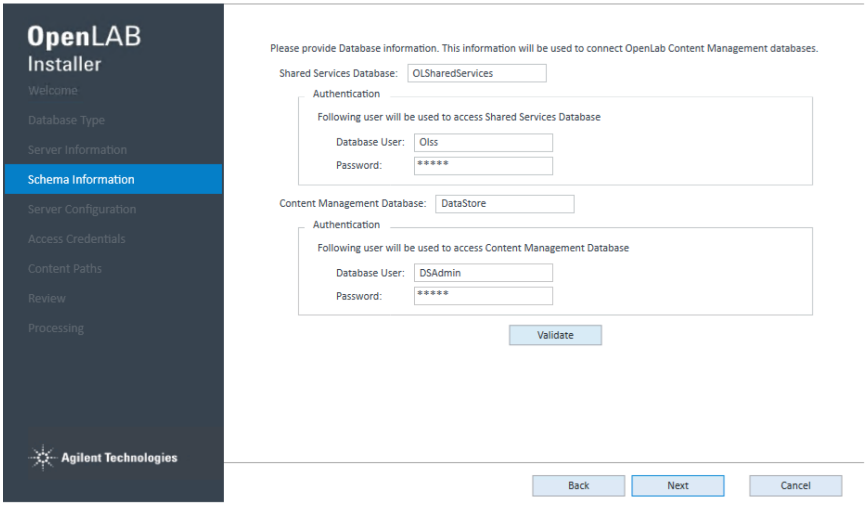
Server Name: localhost

Port: 5432

Figure 13. OpenLab Installer Server Information Screen

7 Edit the **Schema Information** information only if the database users or passwords have been changed.

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



Please provide Database information. This information will be used to connect OpenLab Content Management databases.

Shared Services Database: OLSharedServices

Authentication

Following user will be used to access Shared Services Database

Database User: Olss

Password: *****

Content Management Database: DataStore

Authentication

Following user will be used to access Content Management Database

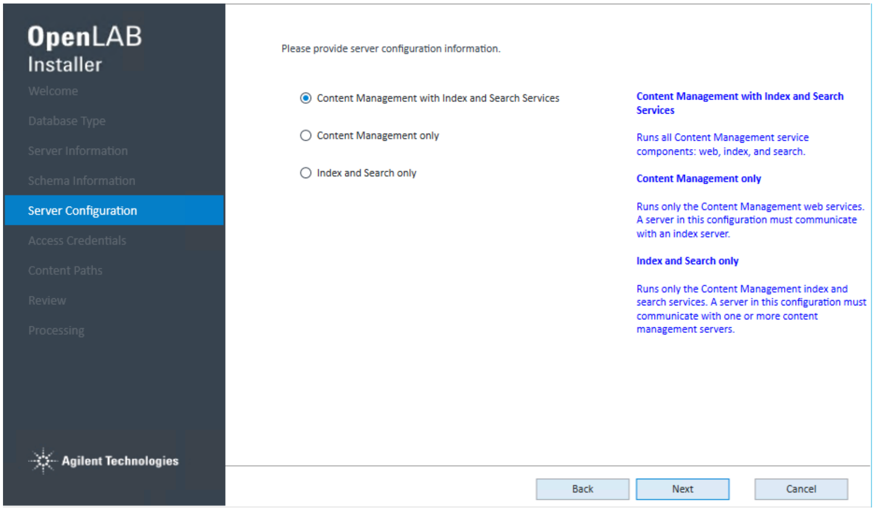
Database User: DSAdmin

Password: *****

Figure 14. OpenLab Installer Schema Information Screen

8 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 and are creating the server to host the Content Management Web services, select **Content Management only**.
- If you are using a scalable system topology and are creating the server to host the indexes and search services, select **Index and Search only**.



Please provide server configuration information.

● Content Management with Index and Search Services

○ Content Management only

○ Index and Search only

Content Management with Index and Search Services

Runs all Content Management service components: web, index, and search.

Content Management only

Runs only the Content Management web services. A server in this configuration must communicate with an index server.

Index and Search only

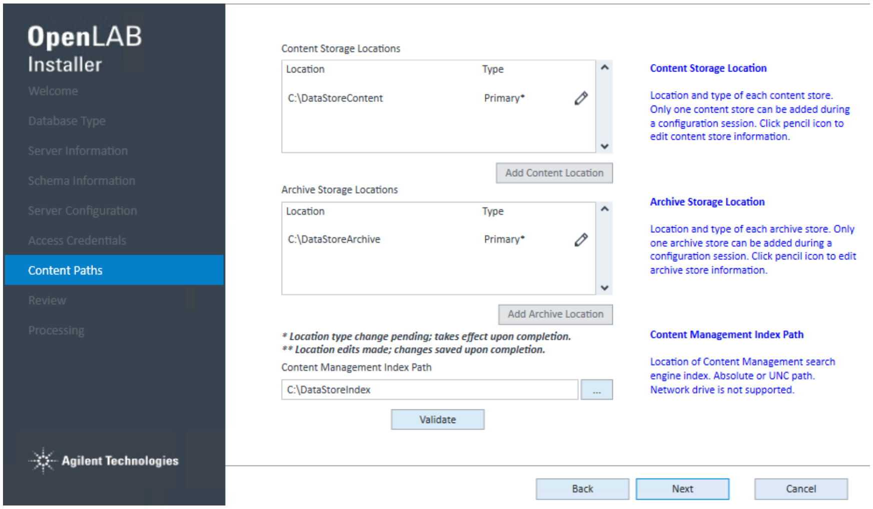
Runs only the Content Management index and search services. A server in this configuration must communicate with one or more content management servers.

Figure 15. OpenLab Installer Server Configuration Screen

9 Enter your account access credentials, and click **Next**.

10 Review path information for the content and archive storage locations and index location. Click **Validate** to verify the index location, and click **Next**.

- If the server is configured as either a **Content Management with Index and Search** or a **Content Management only** server, then the index location will be a path. If the server is configured as an **Index and Search only** server, then the index location will be a hostname.
- 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.



Content Storage Locations

Location	Type
C:\DataStoreContent	Primary*

Archive Storage Locations

Location	Type
C:\DataStoreArchive	Primary*

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

Content Management Index Path: C:\DataStoreIndex

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.

Figure 16. 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.

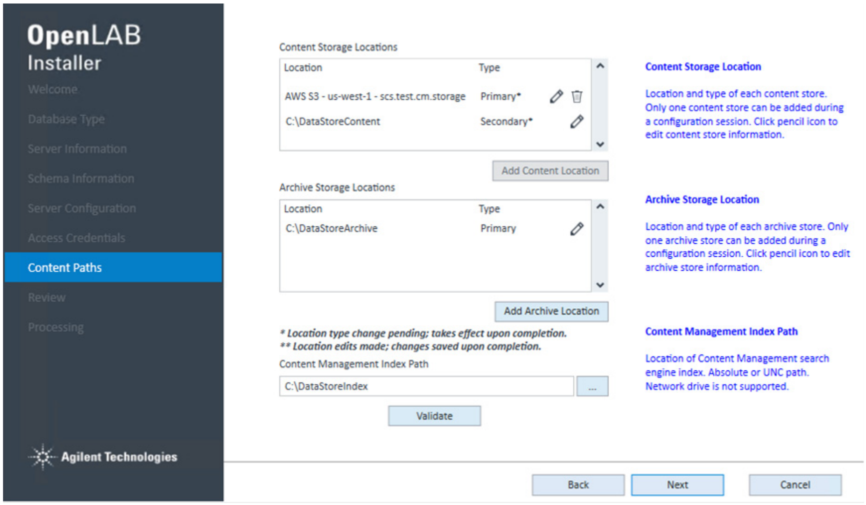
c Enter the required information. For S3, the location must be created and accessible before adding it.

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.



Content Storage Locations

Location	Type
AWS S3 - us-west-1 - scs.test.cm.storage	Primary*
C:\DataStoreContent	Secondary*

Archive Storage Locations

Location	Type
C:\DataStoreArchive	Primary

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

Content Management Index Path: C:\DataStoreIndex

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.

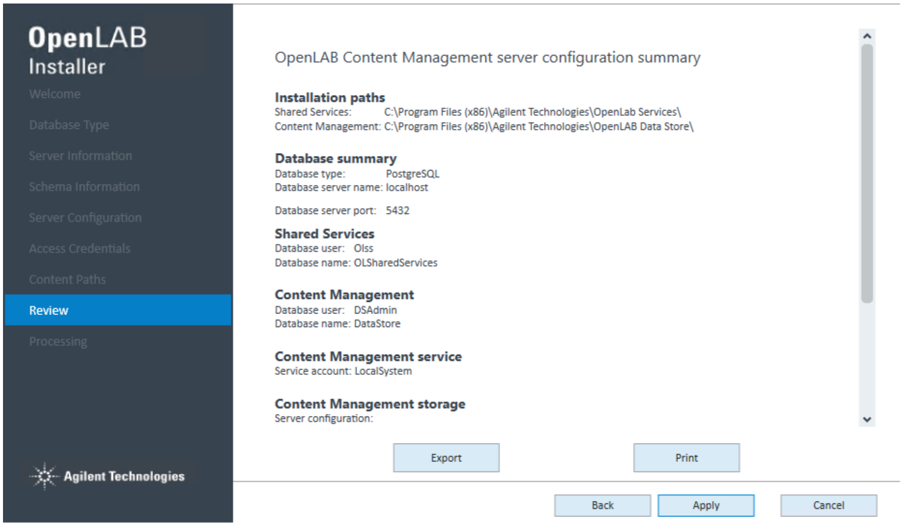
Figure 17. OpenLab Installer Content Paths Screen with New Location

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)

Review the updated configuration summary, and click **Apply**.



OpenLAB Content Management server configuration summary

Installation paths
Shared Services: C:\Program Files (x86)\Agilent Technologies\OpenLab Services\
Content Management: C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\

Database summary
Database type: PostgreSQL
Database server name: localhost

Database server port: 5432

Shared Services
Database user: Olss
Database name: OLSharedServices

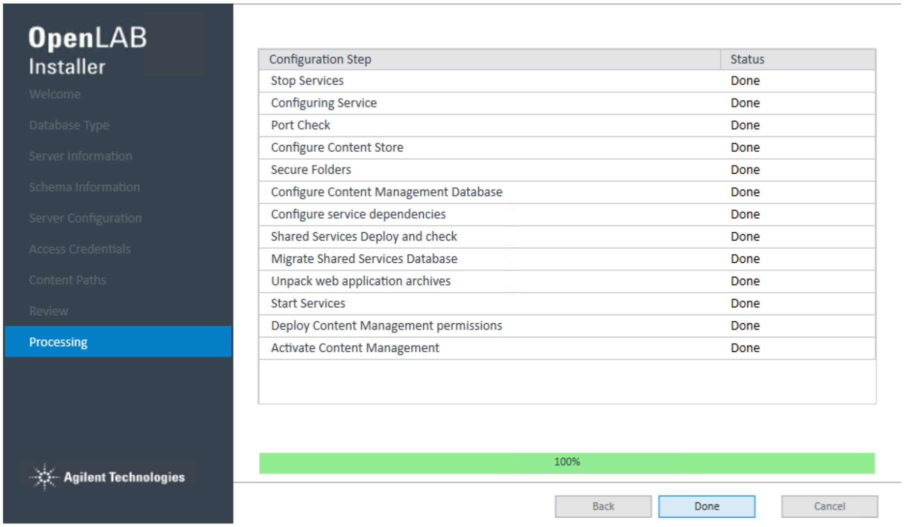
Content Management
Database user: DSAdmin
Database name: DataStore

Content Management service
Service account: LocalSystem

Content Management storage
Server configuration:

Figure 18. OpenLab Installer Review Screen

11 When the configuration is complete, click **Done**.



Configuration Step	Status
Stop Services	Done
Configuring Service	Done
Port Check	Done
Configure Content Store	Done
Secure Folders	Done
Configure Content Management Database	Done
Configure service dependencies	Done
Shared Services Deploy and check	Done
Migrate Shared Services Database	Done
Unpack web application archives	Done
Start Services	Done
Deploy Content Management permissions	Done
Activate Content Management	Done

Figure 19. OpenLab Installer Processing Screen

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**.

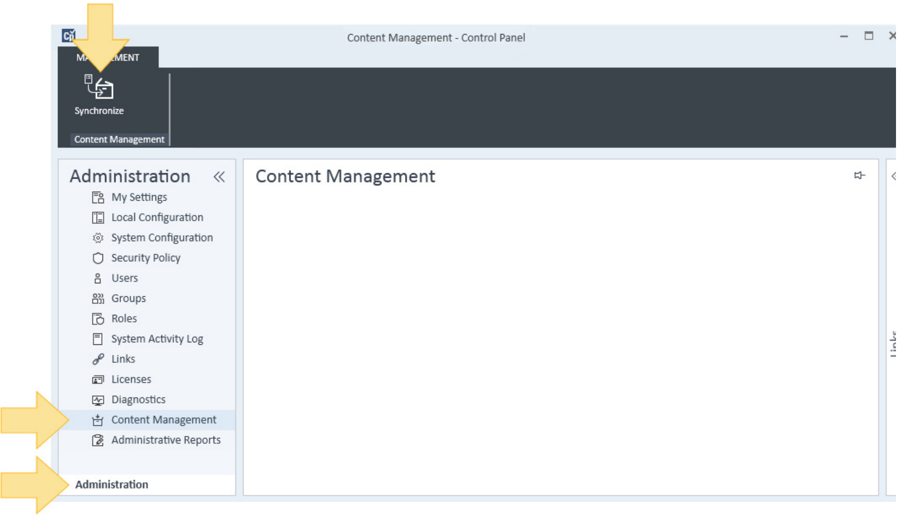


Figure 20. Control Panel Content Management Synchronize

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 104 for details.

www.agilent.com

March 2020

M8640-90040