Agilent

OpenLab Server and OpenLab ECM XT

Installation Guide

Notices

Document Identification

DocNo D0035353 Rev. A.00
EDITION 03/2024

Copyright

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

Software Revision

This guide is valid for the 2.8 revision or higher of the OpenLab Server and OpenLab ECM XT program and compatible OpenLab Server and OpenLab ECM XT programs, until superseded.

Warranty

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

Technology Licenses

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

Restricted Rights Legend

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

Safety Notices

CAUTION

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

WARNING

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

Agilent Community

Agilent Community

To get answers to your questions, join over 10,000 users in the Agilent Community. Review curated support materials organized by platform technology. Ask questions to industry colleagues and collaborators. Get notifications on new videos, documents, tools, and webinars relevant to your work.

https://community.agilent.com/

Table of Contents

1 Introduction

This chapter gives you an overview of this guide and the installation requirements.

About This Guide

This installation guide is designed to help system administrators install the Agilent OpenLab Server or OpenLab ECM XT software. The information provided here applies to both products unless otherwise specified.

Installation Workflows for Different Topologies

This following tables summarize the installation workflows for the various topologies of OpenLab Server and ECM XT.

All-in-one and Basic Server

Table 1. Installation steps for All-in-one and Basic Server

Step	See section
1 Prepare the server.	See **"Before You Begin"** on page 11 and **"Set up your server computer or computers"** on page 13.
2 Install OpenLab Server/ECM XT.	See **"Install the OpenLab Software"** on page 23

2-Server with external database and local file storage

Table 2. Installation steps for 2-server with external database and local file storage

Step	See section
1 Prepare the database server.	See **"Before You Begin"** on page 11 and **"Set up your server computer or computers"** on page 13. PostgreSQL is installed by the Installer. For other database servers, see **"Prepare Your Microsoft SQL Server"** on page 14.
2 Install the database server.	See **"Configure a remote MS SQL database server"** on page 16 and **"Configure a remote PostgreSQL database server"** on page 18.
3 Prepare the application server.	See **"Set up your server computer or computers"** on page 13.
4 On the application server, install the OpenLab Server/ECM XT software.	See **"Install the OpenLab Application Server Software"** on page 25.

2-Server with local database and external file storage

Table 3. Installation steps for 2-server with local database and external file storage

Step	See section
1 Prepare the file server.	See **"Before You Begin"** on page 11 and **"Set up the shared storage on Windows file server"** on page 21.
2 Prepare the application server.	See **"Set up your server computer or computers"** on page 13.
3 On the application server, install the OpenLab Server/ECM XT software.	See **"Install the OpenLab Application Server Software"** on page 25.

3-Server with external database and external file server

Table 4. Installation steps for 3-server with external database and external file server

Step	See section
1 Prepare the database server.	See **"Before You Begin"** on page 11 and **"Set up your server computer or computers"** on page 13. PostgreSQL is installed by the Installer. For other database servers, see **"Prepare Your Microsoft SQL Server"** on page 14.
2 Install the database server.	See **"Configure a remote MS SQL database server"** on page 16 and **"Configure a remote PostgreSQL database server"** on page 18.
3 Prepare the file server.	See **"Set up your server computer or computers"** on page 13 and **"Set up the shared storage on Windows file server"** on page 21.
4 Prepare the application server.	See **"Set up your server computer or computers"** on page 13.
5 On the application server, install the OpenLab Server/ECM XT software.	See **"Install the OpenLab Application Server Software"** on page 25.

Before You Begin

Acquire administrator privileges for all computers that you will use in your system

Installation requires that you have system administrator privileges on all servers and clients where the installation will be performed. Make sure all servers are members of a domain and the local administrator used for installation is at least a domain user.

The administrator doing the installation or upgrade must also have the following privileges: SeDebugPrivilege (Debug programs), SeBackup (Back up files and directories), and SeSecurity (Manage auditing and security log).

Download the OpenLab Server/ECM XT software

1. Go to SubscribeNet at: https://agilent.subscribenet.com.
2. Log in with your SubscribeNet user ID and password. If you are a new user, use the authorization code provided with your product purchase to register and create a new SubscribeNet account and login ID.
3. In the Product List, locate the OpenLab Server/ECM XT software you want to download, and download the software to a local drive.
4. Unzip the software package to your local hard drive.

Review the hardware and software requirements

To confirm that you have the correct hardware and software to support your chosen system and review the *Agilent OpenLab Server and OpenLab ECM XT Hardware and Software Requirements Guide*. This can be opened from the Planning page of the OpenLab Server/ECM XT Installer (setup.exe). It can also be found in the documentation folder on the installation media at setup\docs\EN.

NOTE

Server name cannot be longer than 15 characters.

Password setup and verification

During installation, the installer will verify that passwords for Agilent components adhere to the following general guidelines:

- Minimum 8 characters
  - At least one uppercase letter
  - At least one lowercase letter
  - At least one number
  - Only contains allowed characters
- Overall Allowed Characters:
  - Uppercase letters A-Z
  - Lowercase letters a-z
  - Numbers 0-9
  - Special characters: !@#$%^&-+_=

Decide on the database server that you will use

The following server database software is supported:

- **PostgreSQL Server**: This database is provided with the OpenLab software and can be installed and configured during installation. Or, you can configure an existing PostgreSQL server previously installed by the OpenLab software. Any PostgreSQL server that you have installed outside of OpenLab must be removed before installing the provided OpenLab PostgreSQL Server. Make sure you back up any data from an existing PostgreSQL server prior to installing OpenLab Server/ECM XT, as the existing PostgreSQL database may be deleted during uninstallation of PostgreSQL. See **"Configure a remote PostgreSQL database server"** on page 18.
- **Microsoft SQL Server**: This database can be configured during installation, but it must be installed before installing the OpenLab software. See **"Prepare Your Microsoft SQL Server"** on page 14.

NOTE When using an SQL Server named instance, the port used by that database must be open. Refer to the Microsoft SQL Server documentation for how to set up a named instance.

NOTE Database passwords must meet the requirements of the individual database installed. For information, see the documentation for your database. The following characters are not allowed in database passwords:

- For SQLServer:] ["
- For PostgreSQL: single quotes, double quotes, and multi-byte UTF-8 characters

Set up your server computer or computers

1 Join an existing domain. Changing the server domain after the installation requires direct consultation with Agilent Support.

2 Disconnect the server from the Internet until you have installed the latest security fixes and virus protection.

3 Install and configure your server operating system. See your Windows user information for details.

4 Ports 80 and 443 should be set free before installation of any configuration. If the World Wide Web Publishing Service is enabled on the operating system, disable it before starting any OpenLab installation.

CAUTION

Older security protocols Transport Layer Security (TLS) 1.0, TLS 1.1, and SSL 3.0 are not required by OpenLab Server/ECM XT and present a security risk. Disable them according to instructions from Microsoft and your IT policies.

NOTE

Some OpenLab CDS components require Microsoft .Net 3.5. By default, this version of framework does not enforce the usage of TLS 1.2 or higher. In most IT environments, TLS 1.2 is enabled for .Net 4.5 or older frameworks. Run the System Preparation Tool prior to a new or an upgrade installation. It verifies that TLS 1.2 (or higher) is enabled for .Net frameworks. A script to assist making these changes has been provided on the installation media under \Setup\Tools\Support\TLS\FixTLSVersions.ps1. Please contact your system administrator for assistance in running the script.

NOTE

TLS 1.2 (or higher) supports a wide selection of cipher suites, some of which may be vulnerable to attack. OpenLab Server/ECM XT supports all TLS 1.2 (or higher) cipher suites and is not impacted if any weak or vulnerable cipher suite is disabled by your IT policies.

5 Run the **System Preparation Tool**. The tool can be found on the OpenLab installation media under \Setup\Tools\SPT.

The System Preparation Tool (SPT) is always run as part of the installation. However, to avoid time-consuming activities and any associated reboots during the installation itself, Agilent recommends running the System Preparation Tool first.

a Copy the entire contents of the media to a local drive.

b To run the tool from the command line, run the following command (for Windows 2019, substitute Win2019):

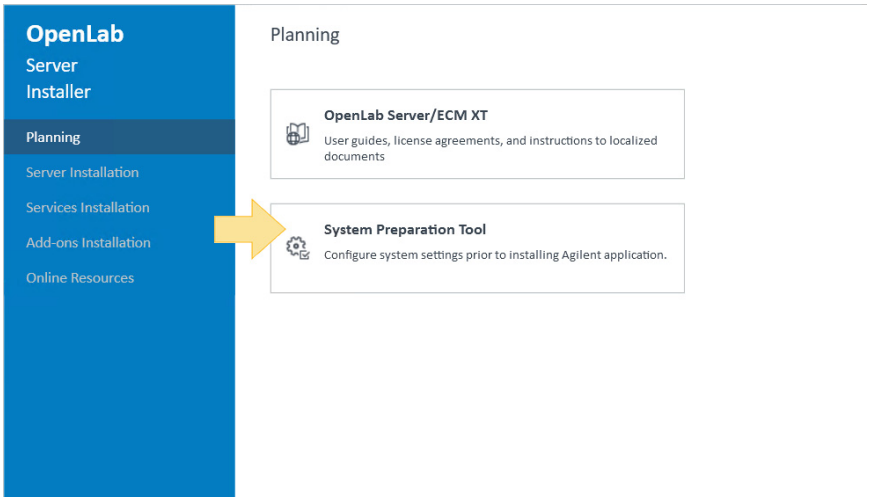
```
SystemPreparationTool.exe -silent ConfigurationName="OpenLab (CDS,
ECMXT)~Server~Win2022"
```

OR

c To run the SPT from the installer, right-click the **setup.exe** file, and run it as an administrator. If User Account Control (UAC) is on, this step requires active confirmation to continue.

Select **OpenLab Server/ECM XT > Standard**, and click **OK**.

From the **Planning** screen, click **System Preparation Tool**.



d Select your product configuration, and click **Continue**.

e The tool checks all settings and displays the current status (Pass or Fail) on the Current Configuration page.

You can clear the check boxes for recommended settings. Mandatory settings cannot be cleared. Recommended actions are selected by default and be will applied unless they are cleared.

Once all settings are selected, click **Apply Fixes**.

f The System Preparation Tool attempts to fix the selected settings and displays the new status on the Update Configuration page.

Click **Open Log File** to view a log of all the actions taken.

Click **Next**.

g A system preparation report lists the new status for all selected settings and provides instructions for settings that you must fix manually.

To print the report, click **Print Report**.

To close the System Preparation Tool, click **Finish**. If the SPT made configuration changes that require a reboot, a message appears asking if you want to reboot. If this message appears, it is recommended to reboot.

6 If using an antivirus program, make sure it is configured as outlined in **"Configure the Antivirus Program"** on page 56.

7 Obtain the server name. You will need to enter this information during the installation. The software will not install to a server that uses an underscore character in its name.

8 Obtain the server administrator credentials. You will need to enter this information during the installation.

9 Decide on a directory or Amazon Web Service location to be used for the database content. You will need to enter this information during installation.

Prepare Your Microsoft SQL Server

If you plan to use a Microsoft SQL server as your OpenLab database, complete these procedures before installing the OpenLab software. Review the *Agilent OpenLab Server and OpenLab ECM XT Hardware and Software Requirements Guide* for supported versions of SQL Server.

NOTE

The XACT_ABORT property in the database server configuration must be set to off. By default, this is already set. However, if you have a custom installation, be sure this property is set to off.

See your Microsoft documentation for details on your SQL server software.

1. Install the Microsoft SQL server.
2. During installation, change the server authentication to mixed mode. Ensure that the server-level collation is **SQL_Latin1_General_CP1_CI_AS**.
3. Enable the login for user *sa*.
4. Restart the **SQL Server** service, and log in with **SQL Server Authentication**.
5. Disable the **Reporting Services** feature. These services use port 80 and will conflict with the OpenLab secure storage Web server. See the SQL user information for details.

If the Database server is separate from the OpenLab application server, configure the Database server to allow the remote access request from the OpenLab application server.

Using Scripts to Prepare your Database

You can use the prepare_db_mssql.sql script to create the OLSharedServices database for the OpenLab Server or ECM XT. Use the dr-mssql-create-database.sql script to create the datarepo database that contains secure storage. Instructions are provided in the script.

Scripts do not create the full database structure (tables, for example). You will need to be a domain user with full access to the databases when running the installer. Make sure you have the database names, users, and passwords (for example, olss and dsadmin) before you run the installer. Mixed mode must be enabled.

Configure a Remote Database Server

Use the procedures in this section to configure a remote database server.

NOTE

The procedures in this section do not apply to a Basic server or All-in-one server.

Configure a remote MS SQL database server

If you have already installed an MS SQL server, follow the instructions in this section. Otherwise, install MS SQL Server and set up mixed mode when configuring the installation.

Step 1. Configure SQL Server Network

1 Click **Start > Microsoft SQL Server > SQL Server Configuration Manager**.

   a Expand **SQL Server Network Configuration**.

   b On the left panel, select **Protocols** for <instancename>.

   c On the right panel, right-click **Named Pipes** and select **Enable** (if it is disabled).

   Named pipes are a windows system for inter-process communication. In the case of SQL server, if the server is on the same machine as the client, then it is possible to use named pipes to transfer the data, as opposed to TCP/IP.

2 Select **SQL Server Services** and run Stopped services.

   The SQL ServerBrowser program runs as a Windows service and listens for incoming requests for Microsoft SQL Server resources and provides information about SQL Server instances installed on the computer.

   The SQL Server Agent is a Microsoft Windows service that executes scheduled administrative tasks, which are called jobs in SQL Server.

3 For any service that was stopped,

   a Right-click the service and select **Properties**.

   b On the **Service** tab, in the **Start Mode** drop-down menu, select **Automatic**.

Step 2. Restart SQL services

Restart all SQL services or restart the PC. If you choose to restart all SQL services, there are two ways to open Services:

- Click **Start** and enter **Services** in the search field, then open Services and restart all SQL services.
- Click **Start**, then open **Control Panel > Administrative Tools > Services**, and restart all SQL services.

Step 3. Configure antivirus settings

If you have an antivirus installed, you must configure it for the MS SQL server to work with remote TCP connections via the port for 1433 (default) and 1434 (custom instance).

Also, add sqlservr.exe to the exceptions. This allows the application to work both in the domain network and public and private.

This is necessary for the SQL server because the antivirus can block "unwanted" network traffic.

For example, add path %ProgramFiles%\Microsoft SQL Server\MSSQL15.CUSTOMINSTANCE\MSSQL\Binn\sqlservr.exe.

If you don't have an antivirus, you must configure Windows Defender Firewall:

1. Navigate to **Control Panel > System and Security > Windows Defender Firewall > Advanced Settings > Inbound Rules**.
2. Right-click **File and Printer Sharing (SMB-In)** from the list and select **Enable Rule**.
3. On the left panel, right-click **Inbound Rules**, and select **New Rule.**
4. Select **Program**, and then click **Next**.
5. Select **This program path**, enter the path to sqlservr.exe, and click **Next**
6. Select **Allow the connection** and click **Next.**
7. Select all check boxes and click **Next**.
8. Add name and click **Finish** to create the rule.

You must also add a rule for TCP port 1433 and UDP port 1434 if they have another instance.

1. Select **Port** and click **Next**.
2. Add the port and click **Next**.
3. Select **Allow the connection** and click **Next**.
4. Select all check boxes and click **Next.**

Step 4. Configure SQL Server logins settings

If you add a new user, for example, after adding PC to Domain, you can use MS SQL Management Studio to create a login.

1. Open Management Studio.
2. Connect to the server.
3. Select **Security > Logins**.
4. To add a local or domain user, right-click **Logins**, and select **New Login**.
5. Click **Search**, enter a user name, and click **OK**.
6. Open the **Server Roles** tab for this user and select the sysadmin role.

NOTE

If a domain user is used, there cannot be a local user with the same name.

These types of users can only be used with Windows Authentication settings for a database.

After completing all these instructions, go through steps 1 and 2 of the server installation for OpenLab Server/ECM XT, specifying the desired server address, instance name, and use the login added in the MS SQL Management studio.

Configure a remote PostgreSQL database server

NOTE The procedures in this section do not apply to a Basic or All-in-one server installation.

From the OpenLab Installer, run Step 1 - Install or upgrade software prerequisites. See**"Step 1 - Install or upgrade software prerequisites"** on page 25. When completed, reboot the computer, and perform the following configuration steps.

NOTE Install and configure the database server before running the OpenLab Installer Step 1 on the application server.

Step 1. PostgreSQL Server Network Configuration

1 If you changed the default port, open the file C:\ProgramData\Agilent\OpenLab Platform\PostgreSQL\15\postgresql.config and edit the following:

```
listen_addresses = '*'
  port=<port specified in Installed Step 1>
```

2 Edit the C:\ProgramData\Agilent\OpenLab Platform\PostgreSQL\15\pg_hba.config file so that the remote machines can connect to the PostgreSQL server. By default, the PostgreSQL instance is configured to only allow connections from the PostgreSQL host itself. To allow remote OpenLab Server/ECM XT application servers to connect to the PostgreSQL database, you must add four lines to pg_hba.conf for each remote OpenLab Server/ECM XT application server. Method md5 is mandatory for all PostgreSQL servers that are deployed using Step 1 of the OpenLab Server/ECM XT installer.

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

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

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

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

Consult the PostgreSQL pg_hba.conf documentation if more information is required: **https://www.postgresql.org/docs/current/auth-pg-hba-conf.html**.

Restricting PostgreSQL database access to OpenLab Server/ECM XT hosts will enhance security. A similar configured firewall will restrict database server remote access even more effectively.

Step 2. Configure a Custom User

A domain account with administrative permissions must be used to restore a system with remote PostgreSQL server. For 3-server topologies, this is required to enable access to system administration resources needed for starting and stopping of PostgreSQL services during the "cold" backup and the restore procedure.

To create or configure an account, follow the instructions below. If you already have an administrator, skip this step and go **"Step 3. Configure firewall settings"** on page 19.

You can use any custom name for the account.

1. Add account to PC:
   a. Click **Start > Settings > Accounts > Other users > Add someone else to this PC > Users**.
   b. Right-click **Users** and select **New User.**
   c. Add user information and password, then click **Create**. (Setting the user password to **never expire** is recommended.)
2. Add account to Administrators group:
   a. Click **Start > Settings > Accounts > Other users > Add someone else to this PC > Groups**.
   b. Right-click **Administrators**.
   c. Select **Properties.**
   d. Click **Add**, and enter the new account.

Step 3. Configure firewall settings

If you have a third-party firewall installed, you must configure it for the PostgreSQL server to work with remote TCP connections via the port specified during installation. If you are using Windows Defender Firewall, follow the instructions below.

1. Navigate to **Control Panel > System and Security > Windows Defender Firewall > Advanced Settings > Inbound Rules**.
2. Right-click **File and Printer Sharing (SMB-In)** from the list and select **Enable Rule**.
3. Right-click **File and Printer Sharing (Echo Request - ICMPv4-In)** from the list and select **Enable Rule**.
4. On the left pane, right-click **Inbound Rules** and select **New Rule**.
5. Select **Port** and click **Next**.
6. Add default port 5432 or a custom port used during install, and click **Next**.
7. Select **Allow the connection** and click **Next**.
8. Select all (Domain, Public, Private) check boxes and click **Next**.
9. Add name and click **Finish**.

Step 4. Restart PostgreSQL service

Restart the PostgreSQL service or restart the PC. To restart service, there are two ways to open Services:

- Click **Start** and enter Services in the search field, and then open Services.
- Click **Start**, then go to **Control Panel > Administrative Tools > Services**.

Right-click the PostgreSQL service PostgreSQL 15.1.1.96 (x64), and select **Restart**.

Tuning the external PostgreSQL server

The following procedure is an example for an external PostgreSQL server with 32GB memory.

PostgreSQL is installed at C:\Program Files (x86)\PostgreSQL\15\.

PostgreSQL Data is installed at E:\ProgramData\Agilent\OpenLab Platform\PostgreSQL\15\.

Configure the WAL (Write-Ahead log) to another disk

1. Stop PostgreSQL 15.51.96 (x64) service.
2. Move WAL folder - E:\ProgramData\Agilent\OpenLab Platform\PostgreSQL\pg_wal to F:\pg_wal.
3. Using command prompt (as Administrator) – run the following command:

```
mklink /D "E:\ProgramData\Agilent\OpenLab Platform\PostgreSQL\15\pg_wal" F:\pg_wal
```

4. Update and uncomment (if they are commented) the following parameters in E:\ProgramData\Agilent\OpenLab Platform\PostgreSQL\15\postgresql.conf.

Table 5. PostgreSQL configuration

	Database for 2 Server Solution	Database for 3 Server Solution
	2xCPU–2.6Ghz or higher Minimum of 16 vCPU 32 GB	2xCPU–2.6Ghz or higher Minimum of 16 vCPU 64 GB
max_connections	150	300
shared_buffers	8 GB	16 GB
effective_cache_size	24 GB	48 GB
maintenance_work_mem	2097151 kB	2097151 kB
checkpoint_completion_target	0.9	0.9
wal_buffers	16 MB	16 MB
default_statistics_target	100	100
random_page_cost	1.1 (using SSD storage)	1.1 (using SSD storage)
work_mem	9175 kB	18495 kB
min_wal_size	2 GB	2 GB
max_wal_size	8 GB	8 Gb
max_worker_processes	12	12
max_parallel_workers_per_gather	4	4
max_parallel_workers	12	12
max_parallel_maintenance_workers	4	4

Set up the shared storage on Windows file server

This section applies if you are installing a server topology that includes a separate file server.

A shared storage is set for keeping OpenLab Server/ECM XT content. The shared storage is secured by allowing only the access from the planned Windows domain user, which is the service account for the OpenLab Server/ECM XT application servers.

To set a shared storage folder on the server:

1. Log in to the Windows file server as the Windows domain user, who is the member of the local administrators group.
2. Create a shared storage folder.
3. Right-click the shared storage folder, and select **Properties**.
4. Select the **Sharing** tab.
5. Click **Share**.
6. Add the planned windows domain user account (the service account), and give Read/Write permission.
7. Open **Server Manager**.
8. Select **File and Storage Services > Shares**.
9. Right-click the shared storage set, and select **Properties**.
10. Select **Settings**.
11. Select **Enable access-based enumeration**.
12. Clear **Allow caching of share**.
13. Click **OK**.

    The file server can be set on different operating systems or on a NAS that supports storage sharing using SMB protocol.

Prepare Amazon Web Services S3

Review the following information if you are planning to use Amazon Web Services S3 for file storage.

Bucket naming

Bucket names must be between 3 and 63 characters long. Bucket names can consist only of lowercase letters, numbers, and hyphens (-).

Although it is possible to use a period(.) in a bucket, it is not recommended because it is not DNS name friendly. Additionally, virtual hosting or certificate validation will not work correctly with a period(.)

Permissions and best practices

- Ensure that the S3 bucket is not 'publicly' accessible over the internet. Use centralized controls to limit access.
- Follow principles of 'least privileged access'. Grant only the permissions required to perform the task.
- For OpenLab Server/ECM XT the minimum privileges required to store content in an S3 bucket are as follows:

  s3:PutObject
  s3:GetObject
  s3:ListBucketMultipartUploads
  s3:ListBucket
  s3:DeleteObject
  s3:GetObjectVersion
  s3:ListMultipartUploadParts
- Enable versioning of objects.
- If an EC2 instance is accessing the S3 bucket and the EC2 instance has an IAM role assigned, the IAM role of the EC2 instance takes precedence over the configuration done in the Server Configuration Utility.
- An AWS PostgreSQL instance requires the prepared transactions feature to be enabled.

2 Install the OpenLab Software

Use these procedures to install your OpenLab Server or OpenLab ECM XT software in a standard topology. Installation procedures for Enterprise systems are provided in the *OpenLab Server and OpenLab ECM XT Enterprise System Installation Guide*.

A Windows domain user is required as the service account for OpenLab Server/ECM XT.

NOTE

During the installation, restarts are required. You must log in using the same user account that was used to start the installation.

NOTE

For procedures to upgrade your system, see **"Upgrading Your System"** on page 59.

Start the OpenLab Installer

If you have not done so already, use the following procedure to start the OpenLab Installer.

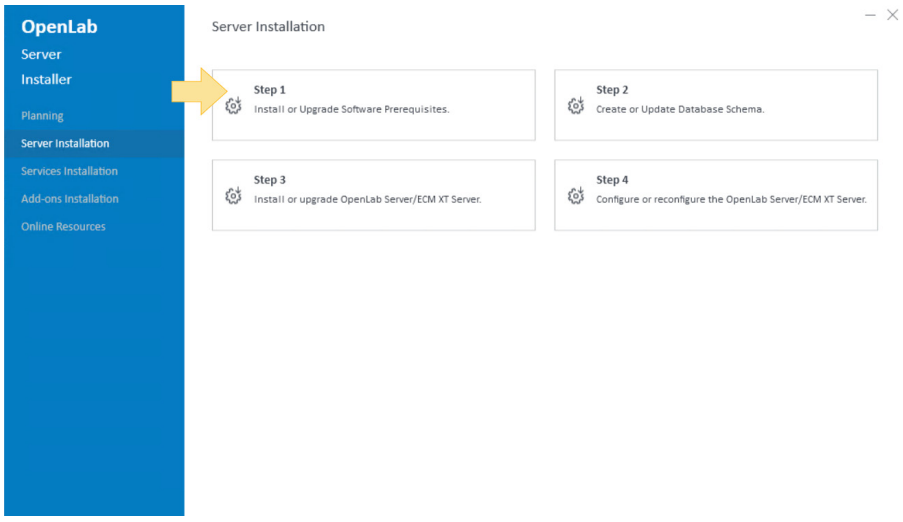
1. Unzip the software package to a local drive. Right-click the **setup.exe** file, and run it as an administrator. If User Account Control (UAC) is switched on, this step requires active confirmation to continue.
2. From the drop-down menu, select **OpenLab Server/ECM XT > Standard**, and click **OK**.

Install the OpenLab Application Server Software

CAUTION **Record and store the selections that you use during this installation in a different physical location. This information is needed to restore your system in the unlikely case of your system becoming inoperable due to a hardware or software failure.**

Step 1 - Install or upgrade software prerequisites

1 From the **Server Installation** screen, click **Step 1 - Install or Upgrade Software Prerequisites**.



2 On the **Database Type** tab, select the server database you have decided to use, and click **Next**.

Select **Install a Local PostgreSQL Server** if you are installing an all-in-one topology and want the Installer to install PostgreSQL on the local machine.

Select **External PostgreSQL Server** if you are using a remote PostgreSQL database server. If you select this option, skip to **step 6** to enter component credentials.

Select **Microsoft SQL Server** if you are using a Microsoft SQL server. If you select this option, the installer skips to the Component Credentials tab.

3 On the **PostgreSQL** tab, if this is a new installation, enter the **Server Name** and **Port**, and click **Next**. If you are configuring a remote PostgreSQL database, the **Server Name** must be the name of the database machine and the port must be configured for the PostgreSQL communication.
If this is an update, this screen is not displayed.

4 On the **PostgreSQL Settings** tab, enter the **Installation** and **Database location** paths. Create and confirm a PostgreSQL superuser password. If this is an upgrade, this screen is not displayed.

NOTE

The PostgreSQL installation path and the database location cannot contain folder names that start with the letters “t”, “r”, or “n”.

For example, a PostgreSQL installation path “C:\Program Files (x86)\test\Agilent Technologies” or a PostgreSQL database location “C:\Program Files (x86)\test\PostgreSQL” are not allowed.

NOTE

The following characters are not allowed in database passwords:

- For SQLServer:] [“
- For PostgreSQL: single quotes, double quotes, and multi-byte UTF-8 characters

5 Click **Next**.

6 On the **Component Credentials** tab, enter and confirm a password for software components. In case of an upgrade, the new password will reset an existing password. Make sure to document the password in a secure location.

The password must be a minimum of eight characters, including at least one uppercase letter, at least one lower case letter, and at least one number, and may contain only the following special characters: !@#$%^&-+_=

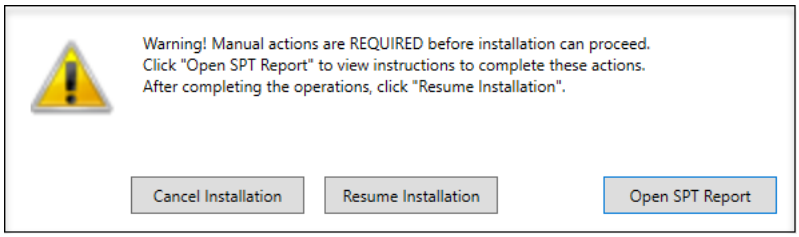
Click **Next**.

7 The **System Preparation** page applies the mandatory and recommended Windows settings. The installer shows the list of recommended settings for the system. You may clear items that you do not want to apply on the system. Other mandatory settings will be applied automatically during installation.

If you choose to resume the installation, click **Next**.

8 The **Review** tab displays a list of components that will be installed. The items listed depend on the selected database type. Click **Install**.

If there are manual actions to be performed, you will be prompted to cancel the installation, resume the installation, or open the SPT Report.



Options to proceed:

- *Recommended*: Click **Open SPT Report** to view instructions to complete these actions. After completing the operations, click **Resume Installation**.
- Click **Cancel Installation** to abort the installation. Make the necessary updates, and restart the installation.

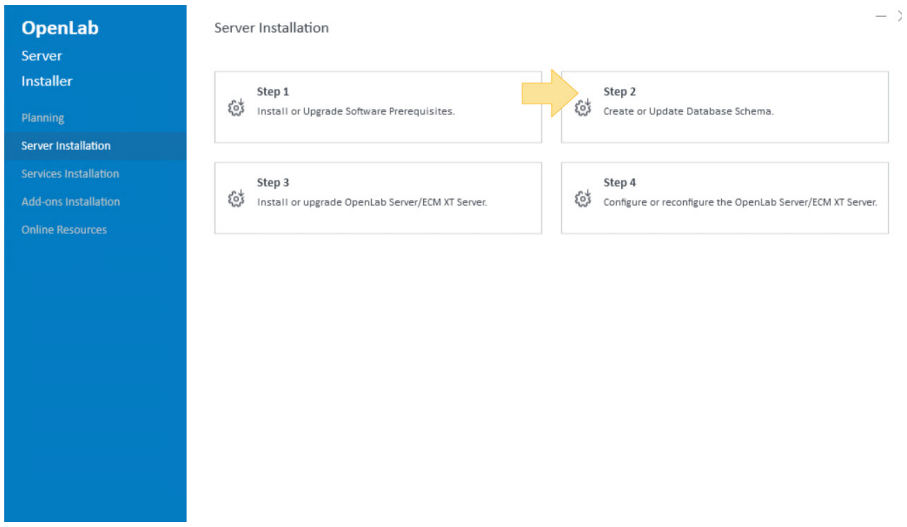
9 Click **Resume Installation** to close this dialog box. The installation continues even if a setting was not applied.

10 When the installation progress bar indicates 100%, click **Next**.

11 On the **Finish** tab, click **Finish**.

Step 2 - Create or update your database schema

1 Click **Step 2 - Create or Update Database Schema**.



2 If you are installing a **PostgreSQL Server**, see **"For a PostgreSQL server"** on page 27.

If you are installing a **Microsoft SQL Server**, see **"For a Microsoft SQL server"** on page 28.

For a PostgreSQL server

By default, the information you entered in **"Step 1 - Install or upgrade software prerequisites"** on page 25 will be displayed.

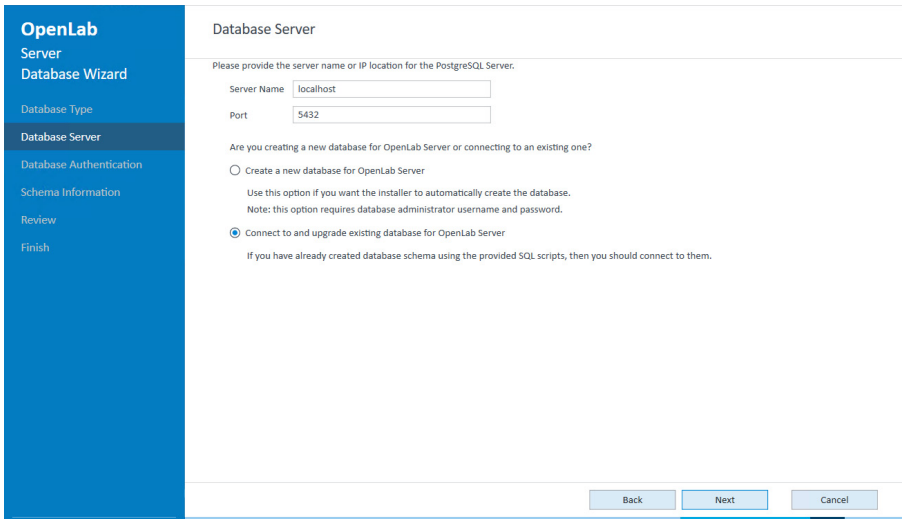
1 On the **Database Server** tab, enter the **Server Name** and **Port**.

Select whether you are creating a database for the OpenLab Server/ECM XT or are connecting to an existing database.

- **Create a new database for OpenLab server**: Select this option if you want to installer to automatically create the database. This option requires the database administrator user name and password.
- **Connect to and upgrade existing database for OpenLab Server**: Select this option if you already created the database schema using the provided SQL scripts.

NOTE

The software will not install to a server that uses an underscore character in its name.



Click **Next**.

2 On the **Database Authentication** tab, the superuser credentials created in **"Step 1 - Install or upgrade software prerequisites"** are filled in. To reset the superuser password, enter a new password, and select Reset Super User password. Click **Next**.

If you are connecting to an existing database, this tab is skipped.

3 On the **Schema Information** tab, enter the information for the OpenLab Shared Services database.

The OpenLab Shared Services database is used for software administration and access control.

Create and confirm the password for OpenLab Shared Services.

Agilent recommends that the default Database User name remains unchanged.

Click **Next**.

4 On the **Review** tab, verify the information and click **Create Database**.

5 When the database is created successfully, click **Finish**.

For a Microsoft SQL server

By default, the information you entered in **"Step 1 - Install or upgrade software prerequisites"** on page 25 will be displayed.

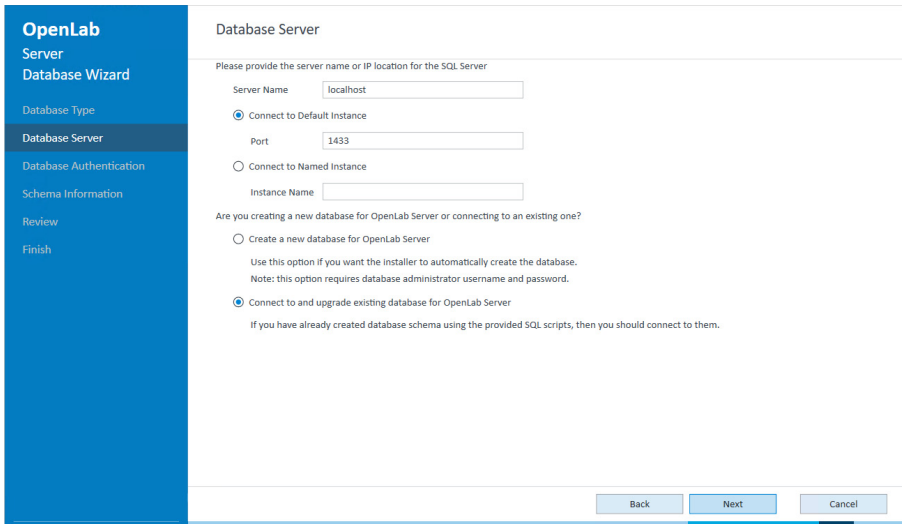
1 On the **Database Server** tab, enter the server name or IP location for the SQL Server. Select one:

- **Connect to Default Instance**: Enter the **Port** number**.**
- **Connect to Named Instance**: Enter the **Instance Name**.

Select whether you are creating a database or are connecting to an existing database.

- **Create a new database for OpenLab Server**: Select this option if you want to installer to automatically create the database. This option requires the database administrator user name and password.
- **Connect to and upgrade existing database for OpenLab Server**: Select this option if you already created the database schema using the provided SQL scripts.

NOTE The software will not install to a server that uses an underscore character in its name.



Click **Next**.

2 On the **Database Authentication** tab, select the authentication mode. If you select **Use SQL Server database administrator account (sa)**, complete the **Super User** and **Password** fields.

Click **Next**.

3 The **Schema Information** tab displays information to be used to connect to OpenLab Server databases. It is recommended that you keep the default **Database User**.

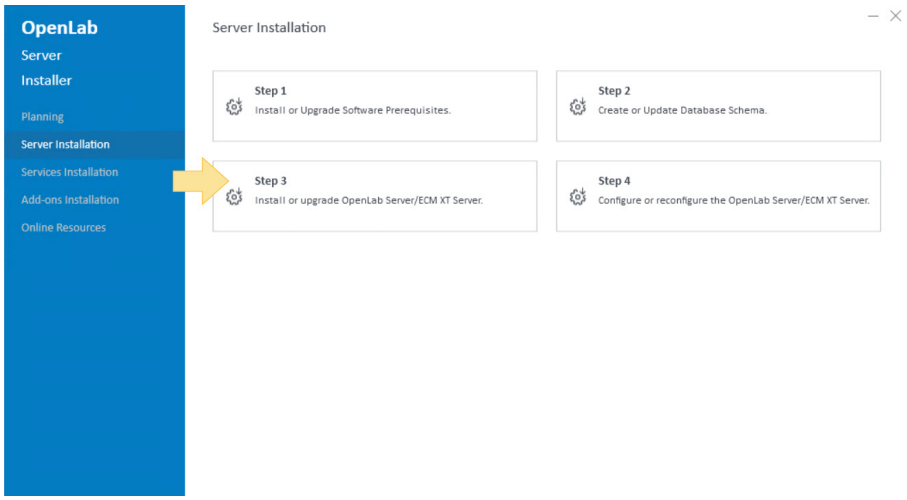
Click **Next**.

4 On the **Review** tab, review the information and click **Create Database**.

5 On the **Finish** tab, click **Finish**.

Step 3 - Install or Upgrade OpenLab Server/ECM XT Server

1 Click **Step 3 - Install or upgrade OpenLab Server/ECM XT Server**.



2 On the **License Agreement** tab, review and agree to the license terms and click **Next**.

3 On the **Installation Folders** tab, select the **Installation Folder** and click **Next**.

4 The **Review** tab displays the components that will be installed. To start the installation, click **Install**.

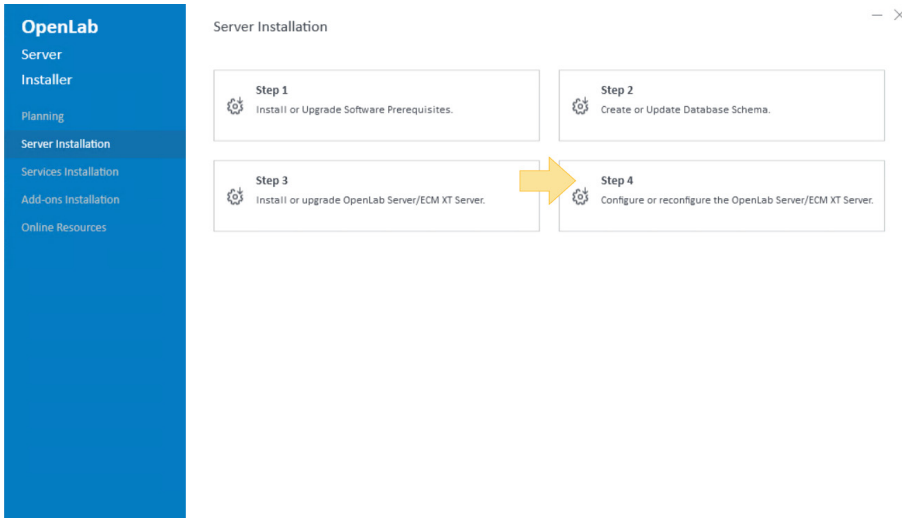
5 The **Install** tab displays the status of the installation. When the installation is complete, click **Next**.

6 On the **Finish** tab, click **Run Software Verification** to verify the software was installed correctly. **Reboot the computer now** is selected by default and is recommended. If the check box is selected, when you click **Finish**, the system reboots and Step 4 - Configure or reconfigure the OpenLab Server/ECM XT Server is started automatically.

Step 4 - Configure or reconfigure the OpenLab Server/ECM XT Server

Step 4 uses the Configuration utility to configure or reconfigure an OpenLab application server.

1 Click **Step 4 - Configure or reconfigure the OpenLab Server/ECM XT Server**.



2 If you have previously installed OpenLab Server or OpenLab ECM XT and have saved your settings as a configuration file, you can reuse those settings by importing the configuration file on the **Welcome** tab. Click **Next**.

3 On the **Access Credentials** tab, choose a Windows account to run the secure storage service. This account must have access to all storage locations and must have Windows "Log on as a service" permission. In order to back up to a network share, this account must also have the "Log on as a batch job" permission. All non-AWS S3 instances must use the same credentials for the storage path. Separate accounts for individual storage paths are not supported.

   If you are using an external PostgreSQL database server, use the Windows domain user as the service account that was created in **"Step 2. Configure a Custom User"** on page 19.

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

4 On the **Storage Locations** tab, type a descriptive name for the content storage location. This is the path that is used for storage of files generated by applications such as OpenLab CDS. Do not use special characters or symbols.

NOTE

After installation, you can change or add storage locations using the Storage Administration web client at https://localhost/OpenLab-Storage.

   For the **Storage Location Path**, if you do not want to use the default path, type or select the desired path. The path must be an absolute local path or UNC share.

   Click **Next**.

5 On the **Certificate Setup** tab, an Agilent OpenLab internal certificate is selected and installed by default. Then, click **Next**. For information on generating certificates, see the *OpenLab Server and OpenLab ECM XT Administration Guide*. When upgrading, this setting resets to the Agilent OpenLab internal certificate. You must reconfigure any custom certificate by launching the Configuration Utility from the **Start menu > Agilent Technologies > Configuration Utility**.

NOTE

During initial installation, you cannot select to use a custom certificate. This selection is only possible during reconfiguration of a server after installation.

6 On the **Review**, tab, review the server configuration summary. To apply the configuration, click **Apply**.

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

3 Install OpenLab Client Services

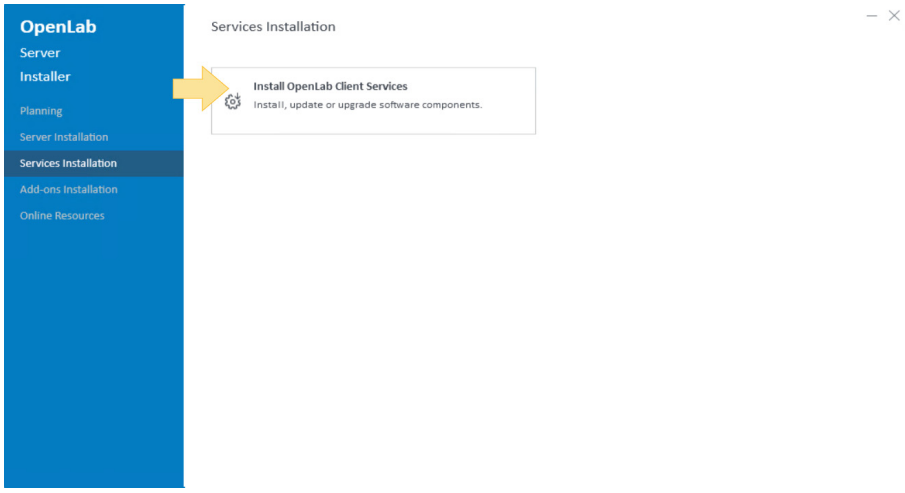
Use these procedures to install the software to any number of clients connected to the server.

OpenLab Client Services does not need to be installed when using OpenLab CDS.

If upgrading the software (**"Step 3 - Install or Upgrade OpenLab Server/ECM XT Server"** on page 30), all uploads from the client must be stopped and the File Upload Queue on the client must be empty before upgrading. Run a software upgrade on any client that was not upgraded at the same time as the server.

Install OpenLab Client Services

1. From the software package, right-click the **setup.exe** file, and run it as an administrator. If User Account Control (UAC) is switched on, this step requires active confirmation to continue.To start the OpenLab Installer, run **setup.exe**.
2. From the drop-down menu, select **OpenLab Server/ECM XT > Standard**, and click **OK**.
3. Select **Services Installation > Install OpenLab Client Services**.



4. Read the terms of the **License Agreement**.

   Select **I agree with the terms and conditions**. You cannot proceed with the installation until you agree to these terms.

   Click **Next**.
5. On the **Installation Folder** tab, type the folder name or browse to the folder where you want to store the application components. Type or select the location for the Cache Folder. This folder contains internal data used by your selected storage. Click **Next**.
6. On the Server Information tab, enter the hostname of the OpenLab application server and click **Connect**. Click **Next**.
7. The **System Preparation** tab applies the mandatory and recommended Windows settings.

   The installer shows the list of recommended settings for the system. You may unselect items that you do not want to apply on the system. Other mandatory settings will be applied automatically during installation.

   Click **Next**.
8. On the **Installation Preview** tab, review the components to be installed, and click **Install**.
9. The installation progress is displayed on the **Installation** tab. When the installation is complete, click **Next**.
10. On the **Finish** tab, click **Run Software Verification** to verify that the software was installed correctly. **Reboot the computer now** is selected by default. Click **Finish** to reboot the computer.

    After a successful installation, you can access the OpenLab Content Management Web interface by going to the following URL: **https://<<server>>/openlab-storage/content/** where <<server>> is the server address on which OpenLab Server/ECM XT was installed.

4 Configure the Control Panel

Access the Control Panel

1 Start the **Control Panel** shortcut on the desktop, or go to **Start > Agilent Technologies > Control Panel**.

2 During the installation, the application server is automatically activated and configured using internal authentication with a default user.

Log in with the user, **admin**, and password, **openlab**.

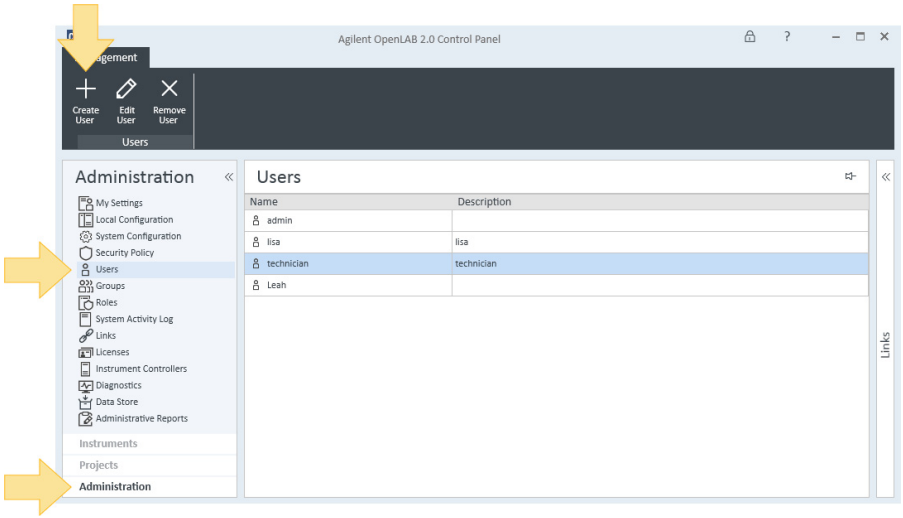
On first login, the system requires the user to change this password before proceeding. You may now change the authentication mode, if necessary.

See the Control Panel online Help for more information.

Create Users

Add users (Internal authentication only)

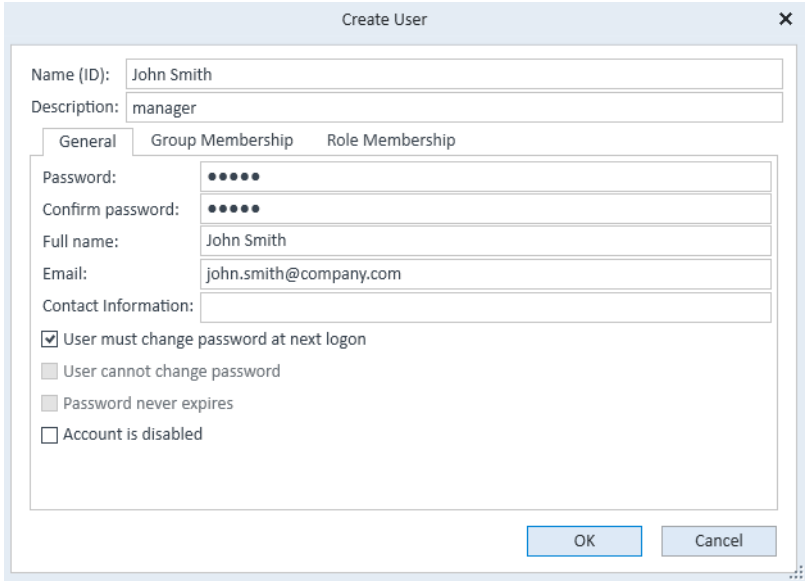
1 Click **Administration > Users > Create User**.



2 Enter a **Name** and **Description** for the user.

3 Enter a **Password** for the user. Confirm the password. Password length is set under Security Policy.

4 Enter the user's **Full Name**, **Email**, and **Contact Information** if desired. The full name is used in activity log entries and the welcome message at the lower right of the Control Panel.

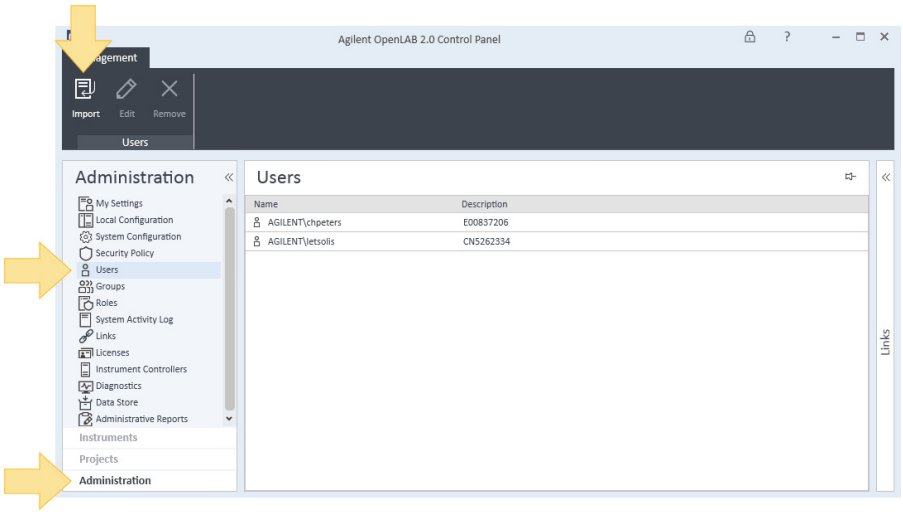


5 Select password options.
   - To prevent the user from changing the assigned password, select **User cannot change password**.
   - To require the user to create a password the next time they log on, select **User must change password at next logon**.
   - To allow the user to use the assigned password or change it at any time, clear **User cannot change password** and **User must change password at next logon**.
   - To set the password to never expire, select **Password never expires**.
6 To create a user profile, but prevent the user from logging on to the Control Panel, select **Account is disabled**.
7 Click **OK**.

Import users (Windows Domain authentication only)

To import users to your system, you must have privileges to obtain user and group information from the domain.

1 Click **Administration > Users > Import**.



2 Search within your domain or local computer, and add users to the list of authenticated OpenLab users. The user's domain password will be required to log in to Control Panel.
3 Click **OK**.

Add users to a role

Use the Control Panel to manage the roles and privileges that affect Secure Storage users. You can create custom roles, or assign one or more of the following predefined Secure Storage roles to give users varying degrees of access to the Content Browser and Storage Administration interface.

Table 6. Secure Storage privileges and roles

Privilege	Description	Roles with this privilege
Check-in/out	Check out, check in, and undo check out of files. In Content Browser: • Undo check out	Secure Storage Administrator Secure Storage Contributor
Copy files/folders	Copy files and folders to another location in secure storage. In Content Browser: • Copy	Secure Storage Administrator Secure Storage Contributor
Create/Rename folder	Create or rename folder. In Content Browser: • Create folder • Rename folder	Secure Storage Administrator Secure Storage Contributor
Delete files/folders	Delete files and folders from secure storage. In Content Browser: • Delete	Secure Storage Administration Secure Storage Delete Content
Download files/folders	Download files and folders. In Content Browser: • Download • Download as zip • Preview files • Create file/folder link • Use file/folder link	Secure Storage Administrator Secure Storage Approver Secure Storage Archivist Secure Storage Contributor Secure Storage Viewer
E-Sign files	Add e-signature to data files. In Content Browser: • Electronic Signature	Secure Storage Approver
Lock files/folders	Lock files and folders so that they cannot be changed or deleted. In Content Browser: • Lock	Secure Storage Administrator Secure Storage Archivist
Move files/folders	Move files and folders to another location in secure storage. In Content Browser: • Move	Secure Storage Administrator Secure Storage Contributor
Undo checkout for other users	Undo checkout for files checked-out by other users	Secure Storage Administrator
Unlock files/folders	Unlock files and folders. In Content Browser: • Unlock	Secure Storage Administrator Secure Storage Archivist
Upload files/folders	Upload files and folders to secure storage. In Content Browser: • Upload	Secure Storage Administrator Secure Storage Contributor

Table 6. Secure Storage privileges and roles (continued)

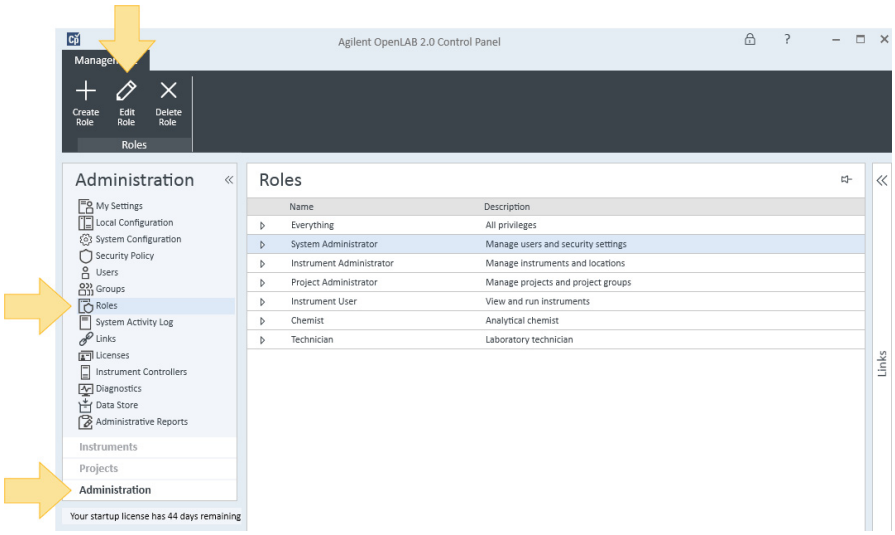
Privilege	Description	Roles with this privilege
View content	Access core capabilities. In Content Browser: • Log in • Browse content • View file properties • View folder properties • Quick Search	Secure Storage Administrator Secure Storage Approver Secure Storage Archivist Secure Storage Contributor Secure Storage Delete Content Secure Storage Viewer
View project or project group	(Shared Services privilege) View a project and project details in Control Panel but cannot edit.	Secure Storage Administrator Secure Storage Approver Secure Storage Archivist Secure Storage Contributor Secure Storage Delete Content Secure Storage Viewer

Table 7. Storage Administration priviliges and roles

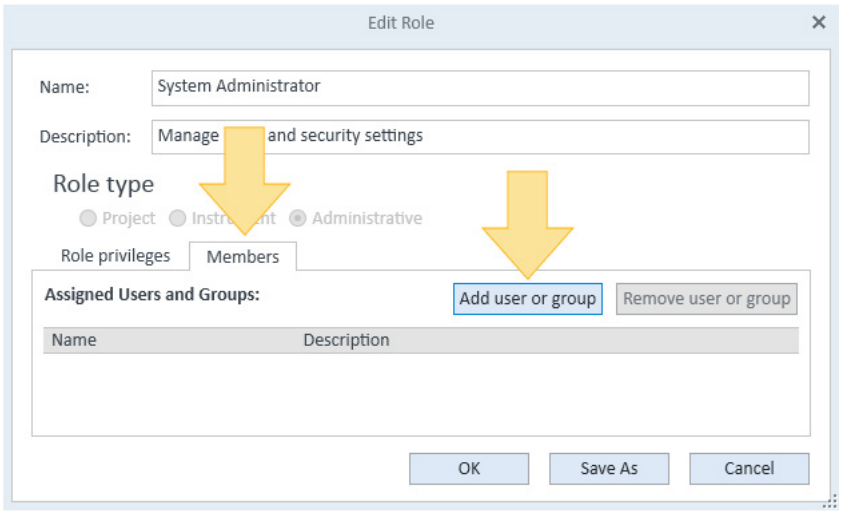
Privilege	Description	Roles with this privilege
Import files/folders	Bulk import files and folders. In Storage Administration: • Log in • Bulk import	Bulk Importer
Manage file storage	Access and move files between storage locations. In Storage Administration: • Log in • Move files between storage locations (relocate files)	File Storage Location Manager Storage Configuration Manager
Manage storage locations	Access and add/edit storage locations. In Storage Administration: • Log in • Add or edit storage locations	Storage Configuration Manager Storage Location Manager
Schedule file locking	Access and manage file locking schedules. In Storage Administration: • Log in • View, add, and edit lock schedules	Lock Scheduler Manager
View project or project group	(Shared Services privilege) View a project and project details in Control Panel but cannot edit.	View Storage Administration Content
View storage administration content.	Browse storage content structure. In Storage Administration: • Browse storage content structure. (Project permission)	View Storage Administration Content

1 Click **Administration > Roles**.

2 Select the role you want to assign to users and click **Edit Role**.

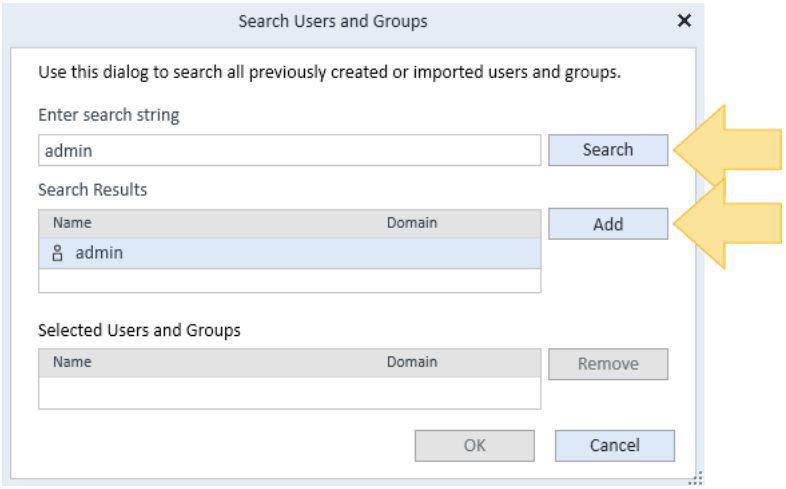


3 On the **Members** tab, click **Add user or group**.



4 Enter a search value and click **Search** to view a list of users and groups in your system.

5 Select a user or group, and click Add.



6 Click OK.

Obtain Your License

The license file contains your software license. This file is installed to the license server, the workstation computer, or the Shared Services Server where your product was installed. The license file is 'bound' to this server address and cannot be moved to another server.

Information in the license file defines the type of data systems connected and type of files stored in the secured storage, the number of instruments that may be connected to the storage, and your ability to access and perform certain activities in the Content Browser or Storage Administration interface.

Obtain your software license online

The most efficient way to manage and maintain your license is through the Internet; however, if you lack an Internet connection, see **"Obtain Your Software License Offline"** on page 45.

Gather the following information from the lavender envelope containing your Software Entitlement Certificate. If you have not received a lavender envelope, contact your vendor or internal support.

- The authorization code label
- The URL for SubscribeNet

Create a SubscribeNet account (new users only)

If you are a new user who has not registered with SubscribeNet, you must first create an account.

If you are already registered with SubscribeNet, skip to the section, **Generate your license**.

1. From any computer with Internet access, enter the SubscribeNet URL in an Internet browser.
2. Click **Click HERE to register**.
3. Enter the authorization code from the label, and complete the profile information. The email address you enter will be your login ID.
4. Click **Submit**.

An account name is generated and displayed. The system will also send an email message with the following information:

- Account name
- Login ID
- Password
- A link to access your license pool at the SubscribeNet site

Generate your license

1. From your OpenLab Content Management server, use the link to open the SubscribeNet site.
2. Log into SubscribeNet using your login ID and password.
3. Select the SubscribeNet account associated with this authorization code, if you have more than one account.
4. Click **Generate licenses** from the left navigation bar and follow the prompts to generate your new license.
   - The computer **HOST NAME** you enter must match the network name of the computer where the Control Panel is running. Do not include any DNS suffix (domain.com) references in the entered machine name. If the computer name or domains are changed after the license is installed, this license must be removed and a new license must be created in SubscribeNet, downloaded, and installed.
   - The MAC address is that of the Shared Services server. To retrieve your MAC address, see the Control Panel online Help topic, **Manage license server > To copy MAC address**. If the network adapter that provides that MAC address used during license creation is removed from the machine, your license will no longer be valid. A new license will need to be generated with a currently available MAC on the license server.
5. When the system generates the license, click **Download License File** and save the license file to your computer and to a backup location (such as a portable storage device).

Obtain Your Software License Offline

If you lack an Internet connection, you or your local onsite service engineer can collect the necessary information from you to allow Agilent to create a license account on your behalf.

1 Collect the required Customer Information.
   - Company name
   - Lab/department name
   - First and last name
   - Email address
   - Phone number
   - Address, city, state/province, postal code, country
   - The authorization code label provided in the lavender envelope containing your Software Entitlement Certificate.

2 Contact your local Agilent sales and service center.

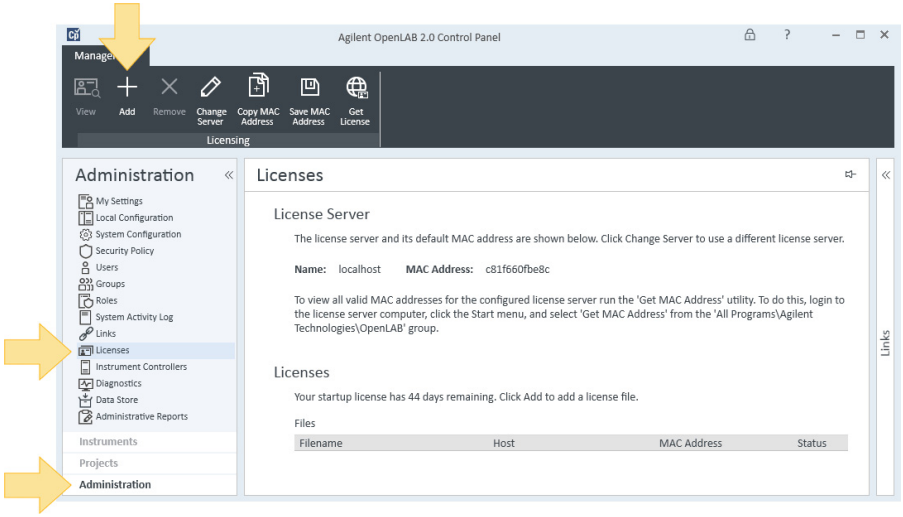
   Once the required information is provided, Agilent will work on your behalf to generate a license file through SubscribeNet. The license file will either be sent to your shipping address on a CD or delivered by your local FSE on a USB stick.

Install Your License

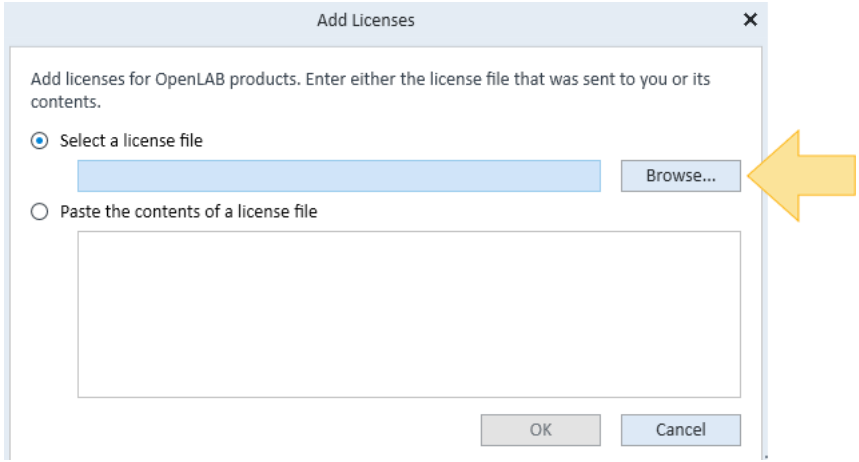
For your system to be fully operational, you must add your license to the Control Panel.

1 Start the **Control Panel** shortcut on the desktop, or go to **Start > All Programs > Agilent Technologies > OpenLab > OpenLab Control Panel**.

2 Click **Administration > Licenses > Add**.



3 Click **Browse**.



4 Navigate to and select the license file (on CD, USB, or network folder), and click **Open**.

5 Click **OK**.

5 Install the OpenLab ECM XT Add-ons

Use these procedures to install the OpenLab ECM XT Add-ons.

The Add-ons can only be installed on a system running OpenLab Server with an ECM XT license. Add-ons can also be installed on a Services for Secure Storage topology.

NOTE

OpenLab Client Services must be installed before installing an ECM XT Add-on. See **"Install OpenLab Client Services"** on page 33.

Start the OpenLab Installer

OpenLab ECM XT add-on software is installed using the OpenLab Installer. To start the OpenLab Installer, copy the OpenLab ECM XT software media to a local drive, and run **Setup.exe**.

Install Import Scheduler

The Import Scheduler add-on program automates the transfer of analytical data within your laboratory to Secure Storage.

For information on installing this add-on, please see the *Agilent OpenLab ECM XT Import Scheduler Installation Guide*.

Install Import Services

Use the Import Services program to easily import files from local folders into Secure Storage directly from your desktop.

1. On the **Add-ons Installation** page, click **Install Import Services**.
2. Select **I agree with the terms and conditions**. You cannot proceed with the installation until you agree to these terms.
3. Keep the default **Installation Folder**, or type the folder name or browse to the folder where you want to store the application components, and click **Next**.
4. Review the **Installation Preview**, and click **Install**.
5. When the installation is complete, click **Next**.
6. Agilent recommends that you reboot your system after the installation is completed. Select **Reboot the computer now**, and click **Finish** to exit the installer.

To start Import Services, go to Start > Agilent Technologies > ECM XT Import Services. For information on how to use Import Services, see the Import Services online Help.

6 Installation and Configuration for Cloud Deployments

This section serves as guidance for installation and post-installation configuration of an OpenLab CDS client/server system to a cloud platform.

Installation and Configuration in the Cloud

Perform the following steps to install in a cloud deployment.

Step 1 Preparation for cloud installation

Before installation, you must address the following:

- Your virtual private cloud is implemented and meets the requirements set out in the *OpenLab CDS Requirements Guide* and *OpenLab Server and ECM XT Hardware and Software Requirements Guide*, including networking and required ports. Follow the best practices guidelines provided by your cloud services supplier and Agilent Technologies.
- Review Agilent guidance for what components must be installed on-premise and what components can be installed in the cloud. The *OpenLab Server and ECM Hardware and Software Requirements Guide* includes comprehensive information for the different supported topologies.
- Network communication between cloud instances and on premises computers must follow network requirements specified in the *OpenLab Server and ECM XT Hardware and Software Requirements Guide*.
- An AWS PostgreSQL instance requires prepared transactions feature enabled.

Step 2 Install and prepare your cloud computers

Create Windows systems, database server, and file storage on cloud instances following the requirements specified in the *OpenLab Server and OpenLab ECM XT Hardware and Software Requirements Guide*. See **"Before You Begin"** on page 11 and **"Configure a Remote Database Server"** on page 16 sections.

When installing AWS RDS, apply the following configuration:

1. Create a new custom parameter group.
2. Set max_prepared transaction = 300.
3. Save changes and reboot the database instance.

Step 3 Obtain a commercial certificate

Using the instructions in the *Securing the System* chapter of the *OpenLab Server and OpenLab ECM XT Administration Guide*, obtain your commercial certificate and have it available for installation.

Step 4 Install OpenLab Server/ECM XT in the cloud

Following the instructions in this guide for your topology, install OpenLab Server/ECM XT. Make sure you followed the instructions in the **"Before You Begin"** on page 11 and **"Configure a Remote Database Server"** on page 16 sections. For cloud installations, a commercial certificate is recommended.

NOTE

Always use fully qualified domain names (FQDN) during installation.

Install a commercial certificate

By default, Agilent installs an Agilent certificate. For cloud installations, a commercial certificate is recommended. The procedures for obtaining and installing a commercial certificate are found in the *OpenLab Server and ECM XT Administration Guide*, in the Securing the System chapter.

Step 5 (AWS only) Add AWS storage location

1 On the application server, open Storage Administration from https://<Server FQDN>/openlab-storage-admin.
2 On the **Manage Storage** tab, add a storage location.
   a Select AWS S3 for the Storage Location Type. Fill in the fields with the information for your AWS S3 instance
      - In the **Storage Name** field, type a unique name for the new storage location.
      - In the **Storage Path** field, type the folder name in the AWS S3 bucket for the new storage location.
   b Make this the main storage location.

Step 6 Configure your system

1 Restart the application server.
2 On the application server, perform the following configuration steps.

Update OpenLab Shared Services configuration

1 On the OpenLab application server, from the start menu launch Agilent Technologies > Shared Services Maintenance.
2 Add a new server with the server's fully qualified domain name and set it as default.
   a Select **Add Server**.
   b Name: Enter a name for the server.
   c Server: Enter the Server's fully qualified domain name.
   d Description (optional).
   e Click **Test Connection** and continue if the connection was successful.

f Select the added server from the list and click **Set as Default.**

3 Click **Apply**. This restarts OpenLab Shared Services.

Change the license server

1 Launch the Control Panel for OpenLab.
2 Navigate to the Administration tab and select **Licenses**.
3 In the top ribbon, click **Change Server**.
4 Update the License server to the fully qualified domain name of the license server and click **OK**.

Change the hostname

1 Navigate to the Administration tab and select **System Configuration**.
2 In the top ribbon, click **Edit System Settings**.
3 In the Edit System Settings dialog, change the storage type drop-down to **Secure Storage**.
4 Click **Next**.
5 Select the **Change server** check box. Update the Secure Storage URL to be the fully qualified domain name of your secure storage server, and then click **Activate**. A message appears informing you that Secure Storage has been successfully activated.
6 Click **Apply** and confirm the changes.

Step 7 On premises AIC and CDS client installation

1 Follow the *OpenLab CDS Client and AIC Guide* to install the AIC and CDS client on premises.
2 Follow the *OpenLab Server and OpenLab ECM XT Installation Guide* to install OpenLab Client Services and add-ons.

NOTE

Always use the OpenLab Server/ECM XT application server's FQDN when prompted during the installation.

Known issues with cloud configuration

This section contains descriptions of known issues, with workarounds.

If the OpenLab Server Configuration Utility is executed after applying changes described above, the changes from **"Update OpenLab Shared Services configuration"** on page 53 will be overwritten and need to be reapplied. This includes the manual changes relating to fully qualified domain name in the OpenLab Shared Services Maintenance Utility tool. For example, this can occur when applying a certificate post-installation.

7 Post Installation Tasks

This chapter describes tasks that are relevant after finishing the installation.

Configure the Antivirus Program

You can use any antivirus program to protect your system. The following information was developed using the antivirus programs tested by Agilent and listed in the *OpenLab Server and OpenLab ECM XT Hardware and Software Requirements Guide*.

1 Open the firewall ports listed in **"Set up your server computer or computers"** on page 13.

2 The following folders should be excluded from an antivirus scan. If you want to have these folders scanned, scan them while the system is not acquiring or performing data analysis, as scanning may cause slowness and runs to be aborted due to concurrent access to the same file by the antivirus program and the CDS application. (Default drive is shown. Change this if needed.)

   - Exclude any configured storage locations (for example, C:\SStorage)
   - [C:\]Program Files (x86)\Agilent Technologies
   - [C:\]ProgramData\Agilent
   - [C:\]ProgramData\Agilent Technologies, Inc
   - [C:\]ProgramData\Firebird
   - [C:\]ProgramData\IsolatedStorage

   Refer to your specific antivirus software documentation on how to configure folder exclusions.

NOTE

For antivirus software with network intrusion prevention, expect to see some degradation in general system performance. To disable network intrusion prevention, refer to your antivirus software instructions.

Settings for Trend Micro antivirus software

OpenLab CDS can be used with other antivirus programs as well. If you use Trend Micro, the following settings are recommended to optimize system performance. In addition, white-list certain applications to improve performance, especially if your antivirus software consumes a high amount of CPU resources. Other antivirus programs may require the same level of configuration.

1 If your version of Trend Micro has **Web Reputation**: Turn off to maximize performance.

   The risk of turning off Web Reputation is that web traffic through browsing from the machine will not be checked.

   Ensure that there is another URL/web scanner on the gateway level to protect the endpoint, or ensure that the endpoints have limited access to Internet. These production machines should not have access to Internet websites where most of the infections are coming from.

2 **Real time scan**: Add exclusions, and modify scan direction from **Created/Modified/Retrieved** to **Created/Modified**.

   Exclusions ensure that the working directory of Agilent Technologies will not be scanned, thus improving performance.

The risk is that only files that are created and changed on this machine are scanned. Files that are just accessed will be bypassed. Dormant Files that got infected without being noticed at the time they were created or written to the machine will not be scanned.

Increase scheduled scan to daily to ensure all files on the machine are being checked for infections that are dormant or not moving.

3 **Behavior Monitoring**: White-list the following folders so they are excluded from the automated scan. Refer to the information provided by your antivirus program. Note that if any of the excluded files get infected, it will not be detected. To avoid risks, trigger a scheduled scan on a daily basis to cover these files.

- Program Files (x86)\Agilent Technologies\Certificate Service\
- Program Files (x86)\Agilent Technologies\Data Collection Agent\
- Program Files (x86)\Agilent Technologies\OpenLab\Services\
- Program Files (x86)\Agilent Technologies\OpenLab Services\
- Program Files (x86)\Agilent Technologies\OpenLab Backup Utility
- \Program Files (x86)\Agilent Technologies\OpenLab Restore Utility
- Program Files (x86)\Agilent Technologies\OpenLab Platform\Data Repository\Data Repository\
- Program Files (x86)\Agilent Technologies\OpenLab Platform\Reverse Proxy
- Program Files (x86)\Agilent Technologies\OpenSearch\
- Program Files (x86)\Agilent Technologies\Test Services

Add the following list of programs to **Approved programs**.

- OpenLab\Services\Distributed Transaction Coordinator Service\Agilent.OpenLab.DistributedTransactionCoordinator.Rest.exe
- OpenLab Backup Utility\Monitoring Service\Agilent.OpenLab.BackupRestore.BackupMonitoringService.exe
- OpenLab Backup Utility\Notification Service\Agilent.OpenLab.BackupRestore.NotificationService.exe
- OpenLab Backup Utility\Task Status Cache Service\Agilent.OpenLab.BackupRestore.TaskStatusCacheService.exe
- OpenLab\Services\Electronic Signature Service\Agilent.OpenLab.ESignature.Rest.exe

4 **Realtime monitoring**: Add below folder to the exclusion list of Realtime Monitoring setting: C:\Program Files (x86)\Agilent Technologies\

Run an Installation Verification

About the Software Verification Tool

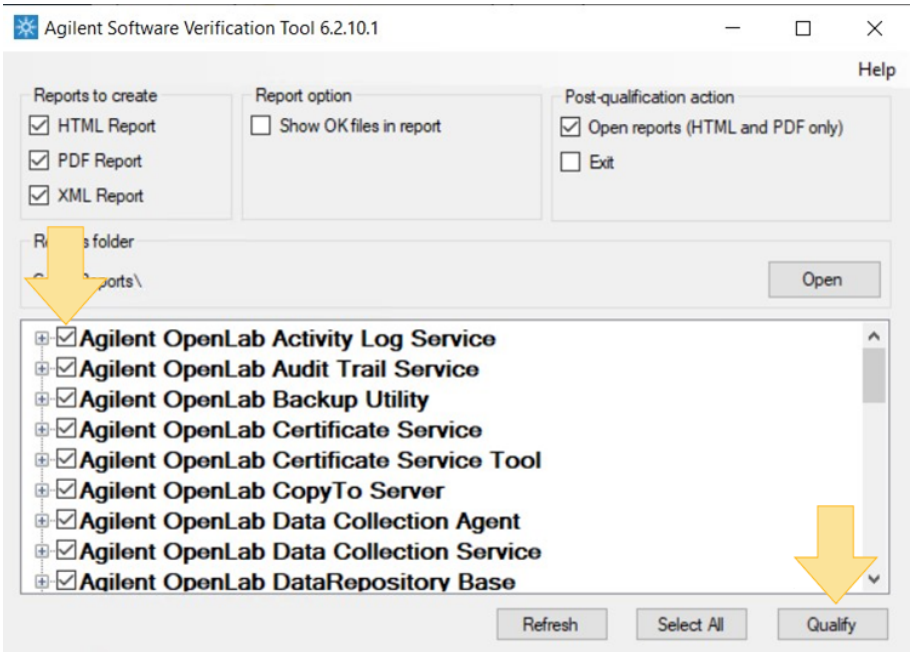
Because there is a separate installation procedure for each client computer in your system, you may choose to run the Software Verification Tool during installation or sometime after your system is completely installed.

Use this procedure if your system is completely installed, and you want to verify that your system has been built and installed correctly and that all design specifications have been met.

Run the Software Verification Tool

1 Go to **Start > Agilent Technologies > Software Verification Tool**.

2 Select products to qualify, and click **Qualify**. The system will run the application and generate a Software Verification Report. If the report indicates failure, verify the computer requirements, and reinstall the data system. Do not use the system until the Software Verification Report gives a pass result.



8 Upgrading Your System

Overview

The procedure for upgrading an OpenLab Server/ECM XT system from v2.5, v2.6, or v2.7 to v2.8 generally involves several steps to ensure a fully functional upgraded system.

Important notes:

- Perform a full backup of your existing system before you begin. Use the backup procedures and utilities provided with your existing system.
- Make sure that your hardware and software meets or exceeds the hardware and software requirements for v2.8.
- Execute *all steps* in the procedure in the order presented.
- In order to perform the upgrade, you must have a valid license for your existing system (current valid license or unexpired startup license).
- SQL Server 2022 is not supported for in-place upgrades.

Backup

It is crucial to have a complete backup of your existing system before you start.

Upgrade the software

When you run the OpenLab Installer to upgrade your software, various tasks are executed automatically in the background. These tasks include checking compatibility and disk space, upgrading and installing database, checking connections, removing old software, and migrating some components. When you finish running the Installer, the upgrade is not complete although the updated software and components are installed.

Run the OpenLab Database Import/Transfer Service

This important step transfers and transforms data from your legacy system to the v.2.8 system. Individual data transformation tasks are executed in a specific order. When completed, a summary report is generated.

Data transformation verification checks that entries for a file in the source database are present in the destination database and that the physical file can be found. By default, 5% of the files are verified. To change the % of files verified, modify the following parameter in the datatransformation_appsettings.json file in C:\Program Files (x86)\Agilent Technologies\OpenLab SDMS Data Transformation Tool\Bin. If the value is set to “0”, the verification is skipped.

"PostVerificationPercentage": 5

Obtain and install your upgraded license

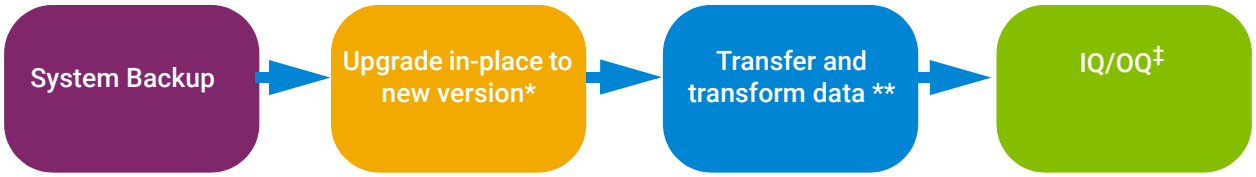
Use the procedure in **“Upgrading your licenses”** on page 71 to upgrade your license.

Backup

Perform a complete backup of your upgraded system.

Workflow for an in-place upgrade

For details, see **"Upgrade a system in-place"** on page 64.



* Includes transfer and transform of some data

** Background process - server functional at this point

‡ IQ/OQ can begin while transfer is in progress

Figure 1. Workflow for in-place upgrade

Workflow for upgrade to new hardware

For details, see **"Workflow to Upgrade In-place to New Hardware"** on page 69.

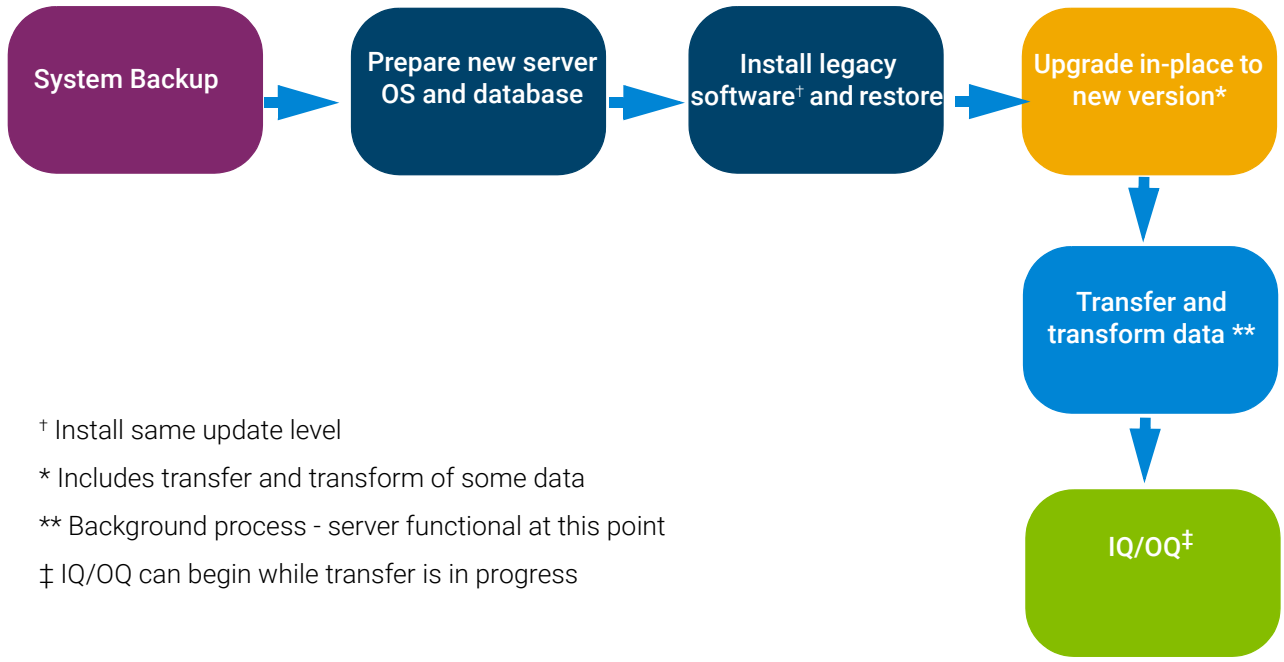


Figure 2. Workflow for upgrading to new hardware

Pre-upgrade Tasks For All Systems

If you changed the superuser password

If you are using a PostgreSQL database and you changed your superuser password after installing your current version, you must update the configuration.xml file with the new password before starting the upgrade. Edit the configuration.xml file as follows:

Under `SharedServices//DataBase//PostgreSQL` and `DataStore//DataBase//PostgreSQL`, update the configuration file tag `<ObfuscatedAdminPassword>` with the new password using the format `plain-password:NewPassword`.

Perform a full backup of your current system

Use the procedures prescribed by your IT department to make a complete backup of your system. These procedures can be those provided in the *OpenLab Server and OpenLab ECM XT Administration Guide* for your current version, or they can be scripted procedures.

Verify the system hardware and software are ready for the upgrade

Work with your Agilent representative to make sure the target system hardware and software are adequate to perform the upgrade and run the upgraded software. Procedures in this section assume like-to-like database upgrade. (That is, if you are using PostgreSQL database, the upgrade will use an upgraded PostgreSQL database.)

NOTE

OpenLab Server/ECM XT v2.8 does not support Oracle databases.

In general, the upgrade will require 2.5x the amount of space taken up by your current database.

Upgrade a system in-place

To upgrade a system in-place, follow the steps in **Table 8**.

NOTE If you are upgrading a system with an external PostgreSQL database, use the procedures provided in the **"Upgrade a System with Remote PostgreSQL Database Server"** on page 72.

CAUTION **You must perform all of the steps for a complete and functional upgrade.**

Table 8. Workflow to Upgrade In-place

Step	Location/page	Procedures and Notes
1 Pre-upgrade - Perform a full backup of the existing system.		See the *OpenLab Server OpenLab ECM XT Administration Guide* for your *current system*. Do a full backup according to the instructions in the Backup and Restore sections of that guide. Make sure you have the most recent updates installed before you back up your system.
2 Pre-upgrade - Check hardware and software requirements and prepare the new hardware		• See the *OpenLab Server and OpenLab ECM XT Hardware and Software Requirements Guide* v2.8 and verify your hardware and software meet the requirements for installing v2.8. • Make sure all of your OpenLab applications are compatible with OpenLab Server/ECM XT v2.8. If you are using Microsoft SQL Server, some software applications may not yet be compatible with OpenLab Server/ECM XT v2.8. Before proceeding, run the compatibility check located at \Setup\Tools\Support\SQL Compatibility Check\SQLserver_compatibiltiy_check.exe. • In addition, for the upgrade, you will need approximately 2.5 x the amount of space required by your current database. • You must have a valid license on your existing system or an upgraded license in order to perform the upgrade. Installing the upgraded license before upgrading is recommended. The upgraded license is required in order for the upgraded system to function.
3 Download the v2.8 software from SubscribeNet and have the software media for your current system available.		**a** Obtain the software media for your current system and extract the provided .zip file to a local drive. **b** Download the v2.8 software from SubscribeNet and extract the provided zip file to a local drive.
4 Obtain and install your upgraded license.		See the **"Upgrading your licenses"** on page 71 for instructions on how to upgrade your license. See **"Install Your License"** on page 46 for instructions on how to install your licenses.
5 Run the OpenLab Installer.		**a** Run setup.exe as a user with administrative privileges. **b** From the drop-down menu, select **OpenLab Server/ECM XT - Standard**. **a** Click **OK**.

Table 8. Workflow to Upgrade In-place (continued)

Step	Location/page	Procedures and Notes
6 Run Installer Step 1 - Install or upgrade prerequisites		On the Server Installation tab, click **Step 1 - Install or upgrade prerequisites.**
	Upgrade Preparation	**a** If you are using Microsoft SQL Server, some Agilent software or services may not yet be compatible with OpenLab Server/ECM XT v2.8. If you have not yet checked, run the compatibility check located at \Setup\Tools\Support\SQL Compatibility Check\SQLserver_compatibiltiy_check.exe. **b** Verify that you have a complete system backup, then select **I confirm that I have a current and valid backup**. **c** Click **Next**.
	Database Type	**a** The database is pre-populated with the database of your existing system. Select the database you are using. Upgrade is supported for like databases only (PostgreSQL to PostgreSQL or SQL Server to SQL Server). **b** Click **Next**. Note: If you are upgrading a system with an external PostgreSQL database, use the procedures in the **"Upgrade a System with Remote PostgreSQL Database Server"** on page 72.
	Component Credentials	**a** Type and confirm a password to use for software components, including Data Repository. Password must be at least 8 characters long and contain 1 upper case letter, 1 lower case letter, and one digit. (Note: This page was previously the Data Repository password page. Data Repository no longer uses a separate database.) **b** Click **Next**.
		Note: for PostgreSQL systems: The PostgreSQL and PostgreSQL Settings tabs are skipped during an upgrade, as this information is provided by the existing system.
	System Preparation	**a** Mandatory checks and settings are applied automatically. Recommended settings are displayed. **b** Click **Next**.
	Review	**a** Click **Install**. If there are manual actions to be performed, you will be prompted to cancel the installation, resume the installation, or view the SPT Report. **b** When ready, click **Resume Installation**.
	Install	When the installation is complete, click **Next**.
	Finish	Review any messages, then click **Finish**.

Table 8. Workflow to Upgrade In-place (continued)

Step	Location/page	Procedures and Notes
7 Run Installer Step 2 - Create or update database schema		On the Server Installation tab, click **Step 2 - Create or update database schema.**
	Database Server (This screen only appears for 2-server and 3-server upgrades.)	**a** Fields are active and prepopulated with the Shared Services database name and authentication type/credentials from the existing system. Keep the default values. **b** Select **Connect to and upgrade existing database for OpenLab Server**. **c** Click **Next**.
	Database Authentication	This screen is prepopulated with your database information. You cannot change it here. Click **Next**.
	Schema Information	**a** Fields are active and credentials are prepopulated with the database name and username/password from the existing system. **b** Click **Apply**.
	Review	Shows the information about this step. Click **Next**.
	Finish	When the database has been successfully updated, click **Finish**.
8 Run Installer Step 3 - Install or upgrade OpenLab Server/ECM XT Server		On the Server Installation tab, click **Step 3- Install or upgrade OpenLab Server/ECM XT Server**.
	License Agreement	**a** Read license agreement. Select **I agree with the terms and conditions**. **b** Click **Next**.
	Review	A list of installed versions and minimum versions required are displayed. Click **Upgrade**.
	Install	Wait for the installation to show 100%, then click **Next**.
	Finish	**a** Click **Run Software Verification** to verify the software was installed correctly. **b** **Reboot the computer now** is selected by default. Agilent recommends you select to reboot the computer now. Otherwise, you must reboot before you run the next step. **c** Click **Finish**.

Table 8. Workflow to Upgrade In-place (continued)

Step	Location/page	Procedures and Notes
9 Run Installer Step 4 - Configure or reconfigure the OpenLab Server/ECM XT Server		On the Server Installation tab, click **Step 4 - Configure or reconfigure the OpenLab Server/ECM XT Server**.
	Welcome	**a** You can select to use the saved configuration file from your old system. If desired, click **Browse** to find and select the configuration file to import. **b** Click **Next**.
	Access Credentials	**a** Select or enter the access credentials to be used. **b** Click Verify to make sure the selections are valid. **c** Click **Next**.
	Storage Locations	Storage locations are transferred from the existing system during the upgrade. **a** Click **Next**.
	Certificate Setup	**a** During upgrade, the certificate is set by default to an Agilent provided certificate. To use a 3rd party certificate, you must set up the custom certificate again using procedures in the *Securing the System* chapter of the *OpenLab Server and OpenLab ECM XT Administration Guide*. **b** Click **Next**.
	Review	**a** A summary of your server configuration is displayed. Click **Apply**.
	Processing	**a** When prompted to Save OpenLab Shared Services credentials, provide the Shared Services admin user credentials. **b** The progress status of the configuration is displayed. When the progress shows 100%, click **Done**.
	Final Steps	**a** Select **I understand that the upgrade is not complete yet. To complete the upgrade, after reboot it is necessary to run the OpenLab Database Import/Transfer Service tool from the start menu**. **b** Click **Finish**. **CAUTION: At this point, the upgrade is not finished. Make sure to perform all of the steps below to complete the upgrade.**

Table 8. Workflow to Upgrade In-place (continued)

Step	Location/page	Procedures and Notes
10 Run the OpenLab Database Import/Transfer Service application.		This application automatically performs transformation of system components, in a specific order. On the application server, launch the OpenLab Database Import/Transfer Service: **Windows Start > Agilent Technologies > Agilent OpenLab Database Import Export Transfer Service**.
	Database Import/Transfer Service	• This application runs a series of tasks that transfer data to the new database. • Before starting the tasks, the application runs checks to make sure connections to the source and destination databases are working. • Once the health checks pass, click **Start**. The transfer tasks are executed in a specific order. • Server can be used during the data transformation.
		• The data transfer process takes significant time. To view the status, click **Open Logs** and look at the console log. • The server can be used during the data transformation. • When the data transfer is complete, click **View Reports** to open the folder containing the task reports.
		• When all data transfer tasks are complete, green check marks are displayed next to each task. To open a folder with reports for the transfers, click **View Reports**. • To close the application, click **Acknowledge**.

		In case of errors:
		• If a transfer task does not return a status within five minutes, the task displays an alert "Data transfer is unresponsive."
		• Click **Open Logs** to examine the log file to check details.
		• After correcting the problem,
		  ◦ Click **Retry Health Check**
		  or
		  ◦ Click **Stop Data Transfer** to skip this task and proceed to the next. After the problem is fixed, run the Database Import/Transfer Service tool again.

11 Perform a full backup of the upgraded system.		Use the Backup and Restore procedures in the *OpenLab Server and OpenLab ECM XT Administration Guide* v2.8 to create a full backup of the upgraded system.
12 At this point, the upgrade is complete and the upgraded system is functional.		

Upgrade in-place to new hardware

To upgrade a system to new hardware, follow the steps in **Table 9**.

CAUTION **You must perform all of the steps for a complete and functional upgrade.**

Table 9. Workflow to Upgrade In-place to New Hardware

Step	Location/page	Procedures and Notes
1 Pre-upgrade - Perform a full backup of the existing system.		See the *OpenLab Server and OpenLab ECM XT Administration Guide* for your *current system*. Do a full backup according to the instructions in the Backup and Restore sections of that guide. Make sure you have the most recent updates installed before you back up your system.
2 Pre-upgrade - Check hardware and software requirements and prepare the new server		• See the *OpenLab Server and OpenLab ECM XT Hardware and Software Requirements Guide* v2.8 and verify your hardware and software meet the requirements for installing v2.8. • Make sure all of your OpenLab applications are compatible with OpenLab Server/ECM XT v2.8. If you are using Microsoft SQL Server, some Agilent client software or services may not yet be compatible with OpenLab Server/ECM XT v2.8. Before proceeding, run the compatibility check located at \Setup\Tools\Support\SQL > SQLserver_compatibiltiy_check.exe. • In addition, for the upgrade, you will need approximately 2.5x the amount of space required by your current database. • You must have a valid license on your existing system or an upgraded license in order to perform the upgrade. Installing the upgraded license before upgrading is recommended. The upgraded license is required in order for the upgraded system to function.
3 Download the v2.8 software from SubscribeNet, and have the software media for your current system available.		**a** Obtain the software media for your current system and extract the provided .zip file to the new server or a local drive. **b** Download the v2.8 software from SubscribeNet and extract the provided zip file to the new server or a local drive.
4 Obtain and install your upgraded license.		See the **"Upgrading your licenses"** on page 71 for instructions on how to upgrade your license.
5 Prepare the new server.		On your new server, follow the instructions in the Installation Guide for your current version to prepare the system.
6 On the new server, install your current software version.		Note: If you are installing on a server with Windows Server 2022, make sure you obtain and follow the instructions for installing the update that is compatible with that operating system. Note: Make sure the software version installed on the new server is the same update level as on the previous server. **a** From the extracted software location, right-click Setup.exe and run as an administrator. **b** Follow the instructions in your current version Installation Guide to run Step 1 through Step 4 of the OpenLab Installer. **c** Install the same OpenLab Server/ECM XT software update on the new server as on the existing server.
7 On the new server, Restore using the backup you created in **"Pre-upgrade - Perform a full backup of the existing system."**		Use the procedures in your current system documentation to perform the Restore. At this point, your new server should mirror your existing system except for the new server hardware and possibly new operating system.
8 On the new server, using the Control Panel for OpenLab, install your upgraded license.		See the **"Upgrading your licenses"** on page 71 for instructions on how to upgrade your license. See **"Install Your License"** on page 46 for instructions on how to install your licenses.

Table 9. Workflow to Upgrade In-place to New Hardware (continued)

Step	Location/page	Procedures and Notes
9 Run Installer Step 1 - Step 4		See instructions for running the Installer in **"Workflow to Upgrade In-place"** on page 64, **"Run Installer Step 1 - Install or upgrade prerequisites"** through **"Run Installer Step 4 - Configure or reconfigure the OpenLab Server/ECM XT Server"**.
10 Run the OpenLab Database Import/Transfer Service application.		This application automatically performs transformation of system components, in a specific order. On the application server, launch the OpenLab Database Import/Transfer Service: **Windows Start > Agilent Technologies > Agilent OpenLab Database Import Export Transfer Service**,
	Database Import/Transfer Service	• This application runs a series of tasks that transfer data to the new database. • Before starting the tasks, the application runs checks to make sure connections to the source and destination databases are working. • Once the health checks pass, click **Start**. The transfer tasks are executed in a specific order. • Server can be used during the data transformation. • When the data transfer is complete, click **View Reports** to open the folder containing the task reports.
11 Synchronize secure storage		**a** Log in as an administrator to Control Panel for OpenLab. **b** Go to **Administration > Secure Storage**. **c** In the command ribbon, click **Synchronize All**.
12 Perform a full backup of the upgraded system.		Use the Backup and Restore procedures in the *OpenLab Server and OpenLab ECM XT Administration Guide* v2.8 to create a full backup of the upgraded system.
13 At this point, the upgrade is complete and the upgraded system is functional.		

Upgrading your licenses

Obtain your licenses for the updated software

Use the following procedure to upgrade your licenses. You must have a valid SMA subscription to upgrade your licenses.

1 For an all-in-one, in-place upgrade, you will need the hostname and MAC address of the current machine. If upgrading to a new server, obtain the hostname or MAC address of the server where OpenLab Server/ECM XT is already installed, as well as the hostname and MAC address of the new server where you will install OpenLab Server/ECM XT v2.8.

   To retrieve the hostname and MAC address of the server where OpenLab Server/ECM XT is already installed, open the Control Panel for OpenLab on the server and go to the **Administration > Licenses** page. Note the hostname and click **Copy MAC Address** or **Save MAC address** in the ribbon to obtain the MAC address.

   To retrieve the hostname and MAC address of a new server where OpenLab Server/ECM XT v2.8 will be installed, open the command prompt on the new server and run the "getmac" and "hostname" commands.

2 Log in to your Agilent Electronic Software and License Delivery account (https://agilent.subscribenet.com).

3 Navigate to **Manage Licenses by Host**. In the **Select from Existing Hosts** drop-down, select the entry that matches the hostname and MAC address of the server where OpenLab Server/ECM XT is already installed. If the hostname is not available to select in the drop-down, you may be managing your licenses in multiple SubscribeNet accounts. Log in to those accounts to upgrade or return those licenses.

4 If your licenses are eligible for an upgrade, an **Upgrade All** button is shown. If you do not see **Upgrade All**, contact your Agilent Sales Representative to renew your Software Maintenance Agreement.

5 For an in-place upgrade to OpenLab Server/ECM XT v2.8,

   a Click **Upgrade All** to generate your upgraded license.

   b On the Upgrade All Licenses for License Host page, review the data and click **Upgrade All** to confirm. This upgrades the license files to the most current version. SubscribeNet will send you an email with new licenses.

   c Make sure that the upgraded license files are available to install at the appropriate step in the upgrade workflow.

6 If you are upgrading to a new server, you must first return the licenses.

   a Before returning the licenses, Navigate to View Licenses by Host and note which licenses were generated for the old server.

   b Click **Return All** to return the licenses for the old server.

   c On the Return All Licenses for License Host page, review the data and click **Return All** to confirm. This returns all licenses for the selected license host. If one or more of the licenses do not have a return available, you will be notified via email and you will need to contact SubscribeNet Support (subscribenet_support@agilent.com) to add more returns.

   d Follow the steps in **"Obtain your software license online"** on page 43 to generate and download a license file for the new server with all the returned licenses from the old server.

   e Make sure that the license files are available to install at the appropriate step in the upgrade workflow.

Upgrade a System with Remote PostgreSQL Database Server

The procedures in this section apply only to upgrading a 2-server system with a remote PostgreSQL database server. Although the procedure references v2.7, it is also valid for upgrading v2.6 to v2.8.

NOTE

At the end of the procedure, the original remote database will no longer be used by OpenLab.

1. Before you start, perform all of the tasks listed in **"Pre-upgrade Tasks For All Systems"** on page 63.
2. On the OpenLab Server/ECM XT application server, start the v2.8 installer, and select **OpenLab Server/ECMXT > Standard.**
3. Run Installer **Step 1 - Install or upgrade prerequisites.**
   a. On the Database Type page, select **External PostgreSQL Server** and click **Next**.
   b. On the PostgreSQL page, make sure the PostgreSQL server name and port match the values for your v2.7 installation. The port is 5432 or whatever custom port was used in the v2.7 installation. Click **Next**.
   c. On the Component Services page, the Data Repository password from v2.7 is prepopulated as the Component Password. Verify that the password meets complexity requirements and change it if necessary. Click **Next**.
   d. On the System Preparation page, click **Next**.
   e. On the Review page, click **Install**.
   f. When done, click **Finish**.
   g. Close the installer.
4. On the OpenLab Server/ECM XT application server, run PostgreSQL15-Win64-Agilent.msi. This upgrades and migrates the PGDR instance.
   a. Open a Command Prompt window and Run As Administrator.
   b. Run the following command, where <installation media location> is the location where you unzipped the installation software package, for example, C:\\Package\\ECMXT-2.8.0.1128-Release.

      msiexec /i "<installation media location>\\Setup\\Tools\\PostgreSQL\\PostgreSQL15-Win64-Agilent.msi" ALLUSERS="1" MSIFASTINSTALL="7" INSTALLDIR="C:\\Program Files (x86)\\PostgreSQL\\15" DATA_FOLDER="C:\\ProgramData\\Agilent\\OpenLab Platform\\PostgreSQL\\15" PORT="5433" SUPERUSERNAME="postgres" PASSWORD="<password>"

      - The DATA FOLDER must match the location where it will be on the database server. The example above uses the location used by the installer when doing a new install. This is the recommended location.
      - For the data file location, the "15" subfolder is not added automatically by the PostgreSQL msi. For the app location, the "15" subfolder is not added automatically.
      - The port must be 5433.
      - The SUPERUSERNAME is "postgres". This was hard coded in v2.7.

- The PASSWORD is the DR password used v2.7.
- If the /q command line switch is included it is run in the background.

c If the /q switch is not used, a UI is presented.

d Click **Next**, accept license terms, and then Install without changing any other input values in the UI.

5 Stop the new PG15 instance, PostgreSQL 15.x.x.x (x64).

6 Create a zip file of the data files created for PostgreSQL 15. (In the example above, C:\ProgramData\Agilent\OpenLab Platform\PostgreSQL\15).

7 Copy the zip file to the database server.

8 Unzip the data files.The default completed location is <%programdata%>\Agilent\OpenLab Platform\PostgreSQL\15. This should be the same location used in **step 4**, matching the location on the OpenLab Server/ECM XT application server.

9 Open a Command Prompt window and Run As Administrator. Update the permissions of the PG data files using the following two commands. Adjust the file location if a different location was used.

```
icacls "C:\ProgramData\Agilent\OpenLab Platform\PostgreSQL\15" /grant administrators:F /T
```

```
icacls "C:\ProgramData\Agilent\OpenLab Platform\PostgreSQL\15" /setowner "SYSTEM" /T
```

10 Delete the following three files from the root data file directory on the database server. For the above example the location is C:\ProgramData\Agilent\OpenLab Platform\PostgreSQL\15.

root.crt

server.crt

server.key

11 If .NET 6 is not installed on the database server, run the dotnet-hosting installer from Setup\redist\DotnetCore.

12 On the database server, run PostgreSQL15-Win64-Agilent.msi from the installation media.

a Open a Command Prompt window via the Start menu and Run As Administrator.

b Enter the following command, where <installation media location> is the location where you unzipped the installation software package, for example, C:\\Package\\ECMXT-2.8.0.1128-Release.

```
msiexec /i "<installation media
location>\\Setup\\Tools\\PostgreSQL\\PostgreSQL15-Win64-Agilent.msi" ALLUSERS="1"
MSIFASTINSTALL="7" INSTALLDIR="C:\\Program Files (x86)\\PostgreSQL\\15"
DATA_FOLDER="C:\\ProgramData\\Agilent\\OpenLab Platform\\PostgreSQL\\15"
PORT="5433" SUPERUSERNAME="postgres" PASSWORD="<password>"
```

- The /q param prevents the need to walk through a default installer UI, but it means you need to watch the log files.
- The install directory is a user choice with no restriction.
- The DATA_FOLDER must match the unzipped location. Note that the “15” subfolder is not in the parameter name. It will be added automatically by the installer.
- The SUPERUSERNAME and PASSWORD must match what was used on the OLSS server when installing version 2.7.
- Port 5433 must be used.
- PostgreSQL 15 is installed and new copies of the root.crt, server.crt, and server.key files are created.

13 Create a folder within the C:\ProgramData\Agilent\InstallLogs directory using any folder name. For example, C:\ProgramData\Agilent\InstallLogs\Special.

14 On the database server, install the new version of pgAdmin.

a Open a Command Prompt and Run As Administrator.

b Enter the following command, where <installation media location> is the location where you unzipped the installation media.

<installation media location>\Setup\Tools\DBAdmin\pgadmin4.Windows-x64.exe /VERY-SILENT /SUPPRESSMSGBOXES /ALLUSERS /NORESTART /DIR="C:\Program Files (x86)\pgAdmin4" /LOG="C:\ProgramData\Agilent\InstallLogs\Special\Agilent_OpenLab_-Server_pgAdmin.log"

15 Update the PostgreSQL configuration files so that the installed database instance is accessible from the remote OpenLab Server/ECM XT application server.

In the pg_hba.conf file, add the following lines. Replace the actual addresses to the IPv4 and IPv6 values of the OpenLab Server/ECM XT application server machine:

host all “postgres” {Main Server IPv4 here}/md5

host all “postgres” {Main Server IPv6 here}/md5

host all all {Main Server IPv4 here}/md5

host all all {Main Server IPv6 here}/md5

In the postgresql.conf file, make sure the following entries are present. Add them if necessary.

listen_addresses = '*'

port=5433

16 Using the services.msc dialog or with command line commands, restart PostgreSQL 15.x.x.x (x64).

17 Optional: On the database server, restart the Postgres 14 process.

18 Launch “pgAdmin 4 v6” from the Start menu and confirm the location of the different schemas via port 5433 and 5432:

a The datarepo database is on port 5433.

b OLSharedServices is only present via port 5432.

c The DataStore schema is also present via port 5432.

19 Optional. Install and launch the “pgAdmin 4 v6” application on the OpenLab Server/ECM XT server. Once installed it can be launched from the OpenLab Server/ECM XT application server and a connection made to the two DB instances on the database server machine. This will confirm the remote access was set up correctly.

20 On the OpenLab Server/ECM XT application server, edit the configuration.xml file as follows.

a On the OpenLab Server/ECM XT application server machine, navigate to C:\ProgramData\Agilent\Installation.

b Make a backup copy of the configuration.xml file.

c Open the configuration.xml file in notepad or equivalent text editor.

d Change port from 5432 to 5433 for everything except the DataStore sub-element.

e Update the PostgreSQL installation and data paths to show the PG15 install values and then save the file.

Change

```
<Installation>
  <DataBase>
    <Type>PostgreSQL</Type>
    <InstallFolder>C:\Program Files (x86)\PostgreSQL-14-OLCM</InstallFolder>
    <DataFolder>C:\ProgramData\Agilent\PostgreSqlData-14-OLCM</DataFolder>
  </DataBase>
</Installation>
```

to

```
<Installation>
  <DataBase>
    <Type>PostgreSQL</Type>
    <InstallFolder>C:\Program Files (x86)\PostgreSQL</InstallFolder>
    <DataFolder>C:\ProgramData\Agilent\OpenLab Platform\PostgreSQL</DataFolder>
  </DataBase>
</Installation>
```

21 On the OpenLab Server/ECM XT application server, launch the OpenLab installer and select OpenLab Server/ECMXT > Standard.

22 On the Server Installation tab select **Step 2 - Create or update database schema.**

a On the Database Authentication page the password entered from Step 1 is pre-populated. Do not change these values. Click **Next**.

b The Schema Information page contains the values that were originally used in the 2.7 installation. Do not change these values. Click **Next**.

c On the Review page, the host and port are pre-populated with the name of the database server machine and port 5433. Click **Create Database**.

d Click **Finish**.

23 On the database server, refresh pgAdmin 4 v6 and confirm that the Shared Services schema was created on the database server available via port 5433. The schema name must match what was just used in Installer Step 2. Verify the user specified is also present.

24 On the OpenLab Server/ECM XT application server, run **Step 3 - Install or Upgrade OpenLab Server/ECM XT Server** in the OpenLab installer. When this step is done, reboot.

25 On the OpenLab Server/ECM XT application server, run **Step 4 - Configure or Reconfigure the OpenLab Server/ECM XT Server** in the OpenLab installer.

a Leave default settings.

b The certificate will be set to Agilent internal. If it was previously a custom certificate this will be changed to Agilent internal during the upgrade. The custom certificate will need to be set via the Configuration Utility launched from the Start menu after the upgrade run is complete.

c If Step 4 fails at Migrate PostgreSQL database, click **Cancel** to exit.

- Move the “bin” and “lib” folders from C:\Program Files (x86)\PostgreSQL\15\

to

- C:\Program Files (x86)\PostgreSQL\

d Re-run **Step 4 - Configure or Reconfigure the OpenLab Server/ECM XT Server** in the OpenLab installer. This will fail at Data Transformation.

26 Swap the ports on the database server.

a Stop both PostgreSQL instances.

- PostgreSQL 15.x.x.x (x64)
- PostgreSQL 14

b Edit the postgresql.conf of each instance, reversing ports 5432 and 5433. Save the files.

c Start both PostgreSQL instances.

27 On the OpenLab Server/ECM XT application server, start the installer and run **Step 4 - Configure or Reconfigure the OpenLab Server/ECM XT Server**.

28 Log in to the Control Panel for OpenLab. Verify the secure storage roles are available.

29 On the OpenLab Server/ECM XT application server, from the Start menu, run **Agilent Technologies > Agilent OpenLab Database Import Export Transfer Service**.

30 Log in to confirm the Storage Locations are ready: https://localhost/openlab-storage-admin.

31 Optionally upload a test file: https://localhost/openlab-storage.

9 Uninstall the Software

About Uninstallation

The OpenLab Uninstaller automates the uninstallation of OpenLab Server/ECM XT.

To uninstall, you must have administrator privileges for all servers and clients. Power user privileges are not sufficient (the uninstallation does not start).

If you plan to reinstall OpenLab Server/ECM XT, do not remove PostgreSQL or Microsoft SQL; keep the database intact. Upon reinstallation, select the existing server and OpenLab Shared Services database and content directory as the previously installed version of OpenLab Server/ECM XT.

Uninstall OpenLab Server/ECM XT

To uninstall OpenLab Server/ECM XT on a server or client machine,

1. From the Windows Control Panel, select **Programs and Features**.
2. If you installed any ECM XT add-ons, uninstall them first.
3. Select **Agilent OpenLab Server** or **OpenLab Client Services**, and click **Uninstall**. The **OpenLab Server Uninstaller** opens.
4. Click **Uninstall** to start the uninstallation.

   All listed components are automatically uninstalled. Any components that you must uninstall manually are identified.

   When a component is uninstalled correctly, the status shown in the **Status** field of the **Uninstall** screen changes from **Detected** to **Uninstalled**.

   To abort the uninstallation, click **Cancel**.
5. When the uninstallation has finished, click **Finish** to close the uninstaller.
6. From the **Programs and Features** list, select **Agilent Software Verification Tool**, and click **Uninstall**.
7. Reboot the system to complete the uninstallation.

10 Appendix

Sales and Support Assistance

Please check the following web site for your local sales and support contact:

https://www.agilent.com/en/support

www.agilent.com

DocNo D0035353 Rev. A.00
03/2024

Agilent