UNICORN™ 7.5

Administration and Technical Manual

Table of Contents

1 Introduction

Purpose of the Administration and Technical Manual

The UNICORN 7.5 Administration and Technical Manual describes how to install, set up, and maintain the UNICORN software.

The installation is assumed to be in a network environment. A system administrator must be able to refer to this manual for the information that is necessary to make sure that the network and all UNICORN clients operate smoothly.

Ordinary users, not assigned as system administrators, can refer to parts of this manual. This is explained below.

Intended readers

System administrators

The general intended reader is a designated UNICORN system administrator, responsible for the network.

In a large organization, the system administrator can be a specific individual, either exclusively responsible for the UNICORN network, or also for the support for other networks or related systems (e.g. LIMS, Laboratory Information Management Systems).

In a smaller organization, the system administrator can be a regular user, who performs other duties and the duties described in this manual. The system administrator must be familiar with all the contents of this manual.

Ordinary users

UNICORN 7.5 can be installed on a stand-alone workstation, with no network connection to other workstations. In this scenario, the UNICORN database and license server software, and the client and instrument server software, are installed on the local computer. In other words, all component parts of a UNICORN network are included in a single installation.

- The user of a stand-alone installation can refer to this manual for information on how to perform administrative UNICORN duties, for example how to maintain the database, install new instrument configurations etc.
- Normally, ordinary users can refer only to selected, relevant parts and do not need to be familiar with all the contents of this manual.

Software declaration of conformity

UNICORN 7.5 is technically compatible with all relevant sections of FDA 21 CFR Part 11.

A part 11-system assessment checklist is available on request from your local GE Healthcare representative.

Typographical conventions

Menu commands, field names and other text items from the software are quoted exactly as they appear on the screen, in a bold italic typeface:

Example: ***Result Navigator***, ***Method Navigator***, ***Method Navigator***, ***UNICORN User Setup*** etc.

Menu paths are shown in a bold italic typeface with a separating colon between each level:

Tools:UNICORN User Setup i.e., the menu option ***UNICORN User Setup*** from the ***Tools*** menu.

Controls on the instrument, computer or keyboard keys are shown with a bold, regular typeface:

Example: Press the **Delete** key.

Text that the user must either type exactly as shown in the manual, or that UNICORN displays as a response (not a regular part of the graphic user interface), is represented by a monospaced typeface:

Example: `Connection change`

File system paths are represented by a monospaced typeface:

Example: `C:\Program Files\GE Healthcare\UNICORN\`

In this chapter

This chapter contains these sections:

1.1 Administration functions – overview

Administration areas

The table below describes the main areas of UNICORN administration:

Area	Concerns
User administration	User properties and authorization of access to the system, see *Section 3.2 UNICORN User setup, on page 128* and *Section 3.3 Access groups and network users, on page 143*. ***Note:*** *It is recommeded to have one responsible person, or a small group, at least in larger installations.*
System administration	• Maintenance of software aspects of UNICORN, including - definition of connected systems, see *Section 3.1.1 System properties, on page 102*. - monitoring of system usage (logs), see *Section 3.1.4 UNICORN and System logs, on page 122*.
Database administration	Set up and maintenance of one or many instances of the UNICORN database, see *Chapter 4 Database management, on page 165*.
Network administration	Setup of the network functions relevant to UNICORN, see *Section 2.4 Network installation and configuration, on page 54*. ***Note:*** *In a network installation, this is normally carried out by the IT staff responsible for the company's network.*
E-mail Setup	Setup of administrator e-mail accounts for sending and recieving messages. See *Section 3.5 E-mail Setup, on page 162*.

Actions before UNICORN is installed

Before UNICORN is installed, the administrator must perform the actions in this table to prepare the network environment:

Step	Action
1	Prepare a dedicated network, see *Section 2.4.4 Configure the network, on page 70*.
2	Configure all client computers in the network, see *Section 2.4.5 Configure and set up the client computers, on page 73*.

Note: *See also the document UNICORN Installation checklist (29-1091-89).*

Actions before the UNICORN program can be used

When UNICORN has been installed, the administrator must perform the actions in this table before other users can use the program:

Step	Action
1	Set up system definitions for the instruments, see *Section 3.1.1 System properties, on page 102*. ***Note:*** *The systems can also be defined as part of the UNICORN installation procedure, when the software is installed on the instrument server computer.*
2	Define new users with assigned access groups, see *Section 3.2 UNICORN User setup, on page 128*.

1.2 Network terms and concepts

Introduction

In this section, some important network terms and concepts are explained.

Administrator categories and duties

The administrator duties can be divided into two categories with different responsibilities:

- Network administrator: Responsible for network setup, software installation and software maintenance.
- System administrator (or UNICORN administrator): Responsible for the use of UNICORN to control instruments.

The network administrator and the system administrator can be the same person, but the tasks can also be carried out by two different persons.

Administrator security responsibilities

The different security responsibilities of the network administrator and the UNICORN (system) administrator are listed below.

Area	Network administrator responsibilities	System administrator responsibilities
Data storage security (backup routines)	Backup routines for network servers.	Backup routines for the UNICORN database.
Network access security	Maintenance of user passwords and access rights to shared general network resources.	-
UNICORN security	-	Maintenance of UNICORN user passwords and access rights to UNICORN resources.

Local and remote stations

When UNICORN 7.5 is used in a network deployment (as illustrated for example in *Dedicated network for UNICORN only, on page 15*), client computers can be categorized as either local stations or remote stations.

Station type	Description
Local station	A PC to which an instrument is physically connected. The local station is the *Instrument Server* for the connected instrument.
Remote station	A PC to which no instrument is physically connected, but which can control systems over a network link.

Note: *A local station can be used to control other instruments than the one that is connected physically. When controlling other systems than the local system, the station operates as a remote station.*

Network terms and general concepts

In the table below are explanations for some network and general concepts which are important to understand when working with UNICORN in a network environment.

Term	Explanation
Storage of data	All UNICORN data (i.e. methods, results, log files, system and user data) are stored in an SQL database. Several installations of the UNICORN database can be running simultaneously in a large deployment. However, the database instances do not communicate with each other.
Communication	The local and the remote UNICORN clients and servers use TCP/IP to send commands and data between them.
LAN	A *Local Area Network* (LAN) supplies networking capability to a group of computers in close proximity to each other such as in an office building or a lab. A LAN is used for sharing network resources like files, printers or applications.
Workstation	A PC with a UNICORN software installation. A stand-alone workstation can operate independently of any other UNICORN computer. See *Stand-alone workstation* below.

Term	Explanation
Stand-alone workstation	A stand-alone workstation has a locally connected instrument and contains all the software components necessary to operate UNICORN as an independent unit, that is • the UNICORN client software • the instrument server software • the database server software and a local UNICORN database and • the license server software. The workstation can be connected to a network to be able to access other network resources, but it is not set up to interact with other UNICORN clients or common UNICORN servers.
Instrument server	The service that controls a connected instrument. The UNICORN instrument server service is installed as a part of the UNICORN client installation.
Real-Time Unit (RTU)	The RTU is used to separate the run-time critical parts of UNICORN from the network during UNICORN system setup. This is to avoid the network related activities that can disturb ongoing runs.
Control system access mode	Users with ***Control*** access to a system can assume control over the instrument, either using the local, instrument server computer, or from a remote station.
View system access mode	Users with ***View*** access to a system can monitor all activities on the instrument, but cannot control the activities without changing the access mode first.
Instrument configuration	The complete dataset defining the properties and enabling the control of an instrument. The instrument configuration consists of • strategy • process picture • phase library or wizards and • embedded software. This is described further in *Section 3.1.2 Instrument Configurations, on page 112*.

Term	Explanation
Strategy	The strategy defines the available method and manual instructions, system settings, run and curve data. It is part of the *Instrument Configuration*.
Process picture	The process picture contains the necessary elements which are used to create the process pictures in the ***Method Editor*** and ***System Control*** modules.
Phase library	The phase library contains predefined phases and methods. It is available for some instruments as a part of the *Instrument Configuration* and adapted to the properties and available options for a specific instrument or group of instruments.
E-licenses	There are different types of e-licenses. A node locked license can be used on one workstation only and a floating license can be used on any workstation in a network, however only on one workstation at the time. The licenses are described further in *Section 2.3.2 Configure an e-license, on page 39*.

1.3 Network environment

Who can perform the network setup?

The personnel performing the network setup must experience in Windows® and network installations. It is recommended to involve a skilled network administrator for the network setup, the installation of the UNICORN software, and the maintenance of the network.

Tip: *Network recommendations are listed in Appendix A.1 Computer recommendations, on page 232.*

UNICORN versions

For UNICORN versions and the supported operating systems and database versions, see the UNICORN compatibility matrix at http://www.gelifesciences.com/UNICORNcompatibility.

UNICORN networks as parts of other Local Area Networks

In most cases, UNICORN computers are connected to a Local Area Network (LAN) to access other network resources and, where applicable, the Internet.

Stand-alone workstations can or can not be connected to a network depending on the need for access to other resources. Since such workstations contain all necessary components for independent operation, the external network connection is not essential when using UNICORN. Network connection between the computer and the instrument is however essential.

A UNICORN network, consisting of several client stations sharing common servers, can either be a totally independent network with no external access or connected to an external LAN. The external LAN connection is necessary for example to provide Internet access and access to other network resources.

The scenarios described above are illustrated in *Section 1.4 Deployment examples, on page 14*.

Note: *UNICORN does not work in a network environment where some UNICORN computers are connected in a workgroup and others are in a domain.*

1.4 Deployment examples

Introduction

This section shows three examples of how UNICORN can be deployed in different environments.

Stand-alone deployment

The figure below illustrates a stand-alone workstation:

The workstation is a stand-alone unit which can operate independently of any other UNICORN workstation or server. It contains all the necessary software components, that is

- the UNICORN software
- the instrument server software
- local database server
- software for license authentication

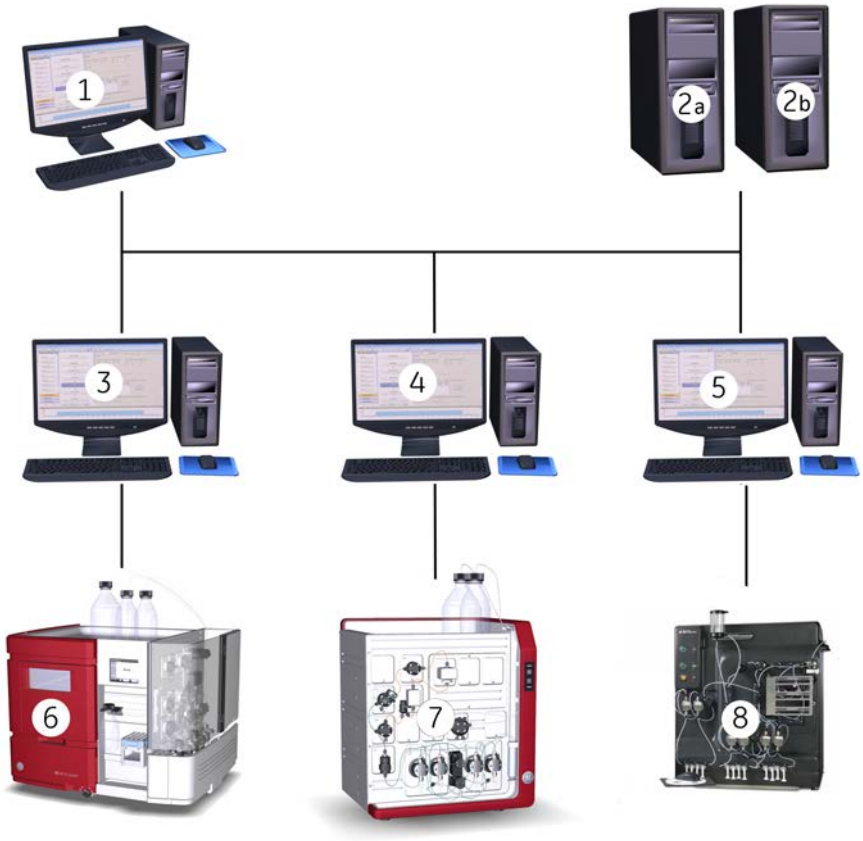
In this deployment example, the workstation can also be connected to a local network. The computers delivered by GE Healthcare are equipped with two network interface cards as a standard feature. One card is used for the communication with the instrument and the other for communication with a network. The connected network can be a UNICORN network as described in the other deployment examples below, or a LAN.

It is possible to connect the workstation to both the instrument and a network from a single network interface card by using a switch. This solution is not recommended as it can reduce the system performance.

It is possible to use the ***Full Installation*** alternative for this workstation. This option is described in *Section 2.3.1 Install the UNICORN software - Full installation, on page 33*.

Dedicated network for UNICORN only

The figure below illustrates how a network with dedicated servers and several client workstations can be organized for exclusive UNICORN use:

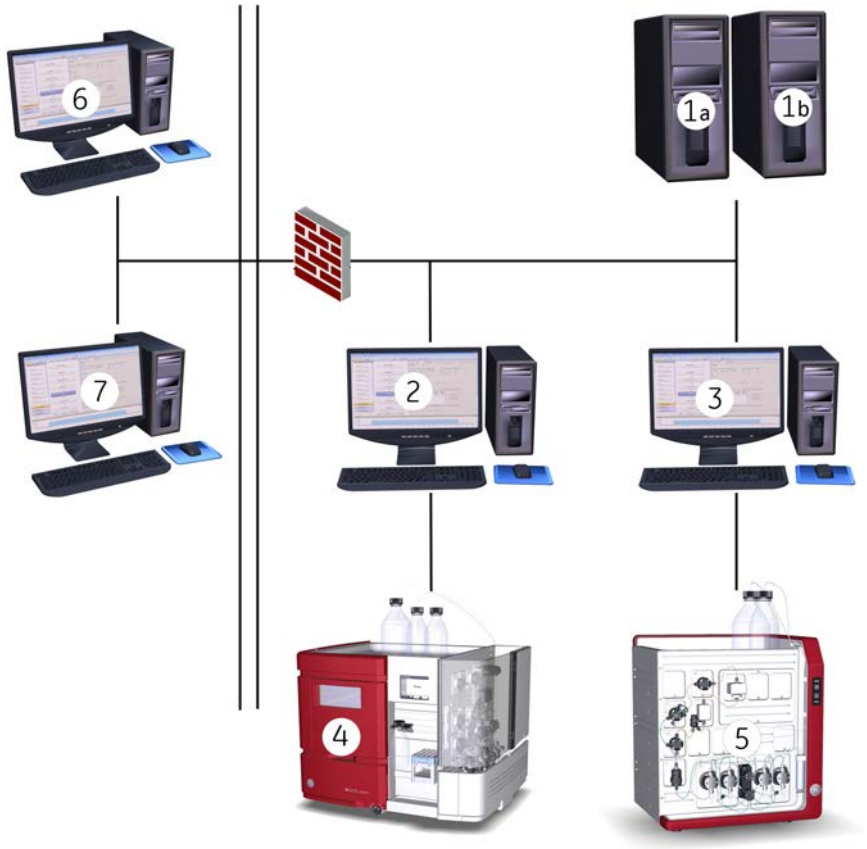


- PC 1 is a *remote station*: it has UNICORN installed but is not directly connected to an instrument. Via the network, remote stations can control the instruments that are connected to local stations.
- PC 2a and 2b are servers. The UNICORN database and the UNICORN license server are installed separately on each of the respective two PCs.
- PCs 3, 4 and 5 are *local stations*: they have UNICORN installed and are connected to instruments 6, 7, and 8 as *instrument servers*. To have an instrument accessible remotely, the computer with the instrument server must be switched on and logged on to the network.

Use different options from the ***Custom Installation*** alternative for each of the client stations and the server in this scenario. The client installation is described in *Section 2.4.1 Install the UNICORN 7.5 software - Custom installation, on page 55*. The server installation is described in *Section 2.4.2 Install the UNICORN database, on page 60*.

UNICORN network as part of larger LAN

The figure below illustrates how a UNICORN network can be included as part of a larger Local Area Network:



- PC 1a and 1b are servers. The UNICORN database and the UNICORN license server are installed separately on each of the respective two PCs.
- PCs 2 and 3 are *local stations*: they have UNICORN installed and are directly connected to instruments 4 and 5 as *instrument servers*.
- The UNICORN network is connected to the larger LAN, which serves the entire organization and provides access to the Internet, other network resources (i.e. printers, office application servers etc.) and other client computers. The connection between the UNICORN network and the larger LAN is through a router and protected by a firewall.

- PCs 6 and 7 are connected to the larger LAN and not directly to the UNICORN LAN. Provided the units have UNICORN client software installed and are allowed access by the firewall, they can operate UNICORN remotely and have access to the common database on the UNICORN database server.

Use different options from the ***Custom Installation*** alternative for each of the client stations and the server in this scenario. The client installation is described in *Section 2.4.1 Install the UNICORN 7.5 software - Custom installation, on page 55*. The server installation is described in *Section 2.4.2 Install the UNICORN database, on page 60*.

1.5 Associated documentation

Introduction

This section describes the user documentation that is delivered with UNICORN.

User documentation

The user documentation listed in the table below is available from the ***Help*** menu in UNICORN and as printed books.

Document	Main contents
UNICORN Method Manual	Overview and detailed descriptions of the method creation features in UNICORN. Instructions on how to use the software. Workflow descriptions for common operations.
UNICORN Evaluation Manual	Overview and detailed descriptions of the Evaluation Classic module. Workflow descriptions for common operations. Description of the evaluation algorithms used in UNICORN.
UNICORN Administration and Technical Manual	Overview and detailed description of network setup and complete software installation. Administration of UNICORN and the UNICORN database.
UNICORN System Control Manual	Overview and detailed description of the system control features in UNICORN. Includes general operation, system settings and instructions on how to perform a run.
UNICORN Online Help	Dialog box descriptions for UNICORN (from the ***Help*** menu).

2 Installation and configurations

About this chapter

This chapter describes how to

- install a complete UNICORN 7.5 installation on a stand-alone workstation (Full installation)
- install a UNICORN database (Custom installation)
- install a license server (Custom installation)

  and

- install UNICORN software client and instrument server software on a network client station (Custom installation).

It also describes how to

- define a system as part of the installation
- configure e-licenses
- configure Windows settings necessary for the UNICORN process pictures in a network deployment
- configure firewall settings, when necessary
- upgrade previously installed UNICORN versions (6.0 or later) to UNICORN 7.5
- remove UNICORN installations

  and

- set up a system printer.

Finally, the chapter also includes listings and descriptions of other software that are installed as prerequisites for the UNICORN 7.5 installation.

In this chapter

This chapter contains these sections:

2.1 Installation overviews

Introduction

This section provides overviews for UNICORN 7.5 installations and configurations either as stand-alone workstations or in a small, dedicated network.

Default installation folders

In this document, "Program Files Path" is used to represent the default path for the program files installation folder, depending on the Windows version. For example, the default path to the program files folder where UNICORN is installed in a 64-bit installation of Windows 10 is `C:\Program Files (x86)`.

For example, if the path is written as below you have to replace Program Files Path with the correct path for your version of Windows:

Program Files Path`\GE Healthcare\UNICORN\`.

Installation summary - stand-alone workstation installation

The table below is an overview of the complete stages in the UNICORN 7.5 installation procedure and the related actions required to set up a UNICORN stand-alone workstation. This installation option is called a ***Full Installation*** in the installation program.

Stage	Description
1	Install prerequisite software applications necessary to run the UNICORN software. *Reference* See *Section 2.2 Other software installed by UNICORN 7.5, on page 28*.
2	Install the UNICORN 7.5 software. *Reference* See *Section 2.3.1 Install the UNICORN software - Full installation, on page 33*.
3	Configure an e-license. *Reference:* See *Section 2.3.2 Configure an e-license, on page 39*.
4	Define a system. *Reference:* See *Section 3.1.3 Define a new system, on page 115*.

Stage	Description
5	Define a user profile and an access group for the user. ***Note:*** *Choose between defining UNICORN users or Network users* *Reference*: See *Section 3.2.1 Create a new user, on page 129*.
6	Check the system settings for the attached instrument. *Reference*: See System Settings in *UNICORN System Control Manual* .

Installation summary - network installation

The table below is an overview of the complete stages in the UNICORN 7.5 installation procedure and the related actions required to set up a complete working environment for UNICORN in a network.

Stage	Description
1	Install prerequisite software applications necessary to run the UNICORN software on the *Database* computer and the *License server* computer. ***Note:*** *The Database and the License server can be on the same computer.* ***Note:*** *Prerequisite software is already installed on computers delivered by GE Healthcare.* *Reference* See *Section 2.2 Other software installed by UNICORN 7.5, on page 28*.
2	Install the UNICORN 7.5 software on the *Database* computer. *Reference*: See *Section 2.4.2 Install the UNICORN database, on page 60*.
3	Install the UNICORN 7.5 software on the *License server* computer. *Reference*: See *Section 2.4.3 Install the Software Licensing Server and configure an e-license, on page 69*.
4	Configure e-licenses. *Reference:* See *Section 2.3.2 Configure an e-license, on page 39*.

Stage	Description
5	If necessary, prepare the *Instrument Server* computers. *Reference*: See *Section 2.4.5 Configure and set up the client computers, on page 73*. ***Note:*** *Previous UNICORN installations must be removed if the Instrument Server computers have been used as stand-alone units.*
6	Install prerequisite software applications necessary to run the UNICORN software on the *Instrument Server* computers. *Reference* See *Section 2.2 Other software installed by UNICORN 7.5, on page 28*.
7	Install the UNICORN 7.5 software on *Instrument Server* computers in the network. *Reference*: See *Section 2.4.1 Install the UNICORN 7.5 software - Custom installation, on page 55*.
8	Define systems. *Reference:* See *Section 3.1.3 Define a new system, on page 115*.
9	Check the system settings for the attached instrument. *Reference*: See System Settings in *UNICORN System Control Manual* .
10	If desired, install UNICORN 7.5 software on *Remote station* computers in the network, after installing any prerequisite software.
11	If desired, set up a default printer for system generated prints. *Reference:* See *Section 2.9 Printers, on page 91*.
12	Set up user access rights and profiles Define access levels for the installation. *Reference*: See *Section 3.3 Access groups and network users, on page 143* and *Section 3.3.3 Access items, on page 152*.
13	Define users. ***Note:*** *Choose between defining UNICORN users or Network users* *Reference*: See *Section 3.2.1 Create a new user, on page 129*.

Note: *This overview includes all the necessary actions for a network environment with several users and different work descriptions. Some of the stages are applicable for the organization. Perform the actions in a different order and for a single client computer or user at a time if that is preferable.*

Custom installation options

Using the Custom UNICORN 7.5 installation, select the software component parts that are needed for the workstation and server.

The Custom installation options are described in the following table:

Software components	Characteristics
UNICORN Software Client	The UNICORN software is used to control and manage an instrument that is connected to the station. Select this option if the station is used as a remote station only. This option does not include the necessary server components to control a locally connected instrument.
Database server	This option installs the server software necessary to operate the database where all UNICORN data is stored. In a network environment, the database is installed on a dedicated server computer.
License server	This option installs the license server software which is used to authenticate that all UNICORN software clients with access to the network are properly licensed. In a network environment, the license server is installed on a dedicated server computer.

Installation prerequisites

Before UNICORN installation, see the UNICORN compatibility matrix at http://www.gelifesciences.com/UNICORNcompatibility for UNICORN versions and the supported operating systems and database versions.

Do not copy the DVD-ROM or decompress the files

UNICORN 7.5 is supplied on a DVD-ROM. Files on the DVD-ROM are compressed and the installation cannot be performed by simply copying the files onto the hard disk. However, the installation files can be copied to a hard drive and the installation can be run from the hard drive instead. Do not run the installation from a network drive.

Upgrade old UNICORN version

UNICORN 6.2 and later can be upgraded from the installation program.

To upgrade UNICORN 6.0 or 6.1 installations to UNICORN 7.5 you must back up the database, uninstall the old UNICORN version, install UNICORN 7.5, restore the backup and convert the database to UNICORN 7.5 standard. This is described in *Section 2.7 Upgrade UNICORN 6.0 or later to UNICORN 7.5, on page 85*.

Replacing a UNICORN installation older than UNICORN 6.0 (e.g. UNICORN 5.2 and older) with the UNICORN 7.5 version of the software is not possible, since the data was stored as files in a folder structure and not in a database in these versions.

You can import methods and result data from a UNICORN 5.x run with some control unit (CU) based systems, for example, ÄKTApilot™ and ÄKTAprocess™, into the UNICORN 7.5 database. The import is described further in *Section 4.2.6 Import data from UNICORN 5, on page 187*.

Note: *In some cases the PC operating system must be changed when upgrading to new UNICORN versions.*

Changing the installation type

To merge several independent stand-alone workstations into a network with a common database, follow the procedure described below. It is recommended to store the largest database on the new database server.

Note: *The e-licenses for the stand-alone workstations need to be rehosted to the common e-license server if the license server is moved. Contact GE Healthcare for information and assistance.*

Step	Action
1	Create a backup of the database from the workstation that has the largest database, and save it outside the regular backup folder. ***Note:*** *This workstation is the new database server.* Then follow step 2-6 for each workstation that shall be connected to the new database server.
2	Perform database backup and save it outside the regular backup folder on each workstation.
3	Export and save the log files from each workstations. (These logs cannot be imported into the new database, but must be saved to provide a history of usage for the workstations before the database merge)
4	Export all results and methods you wish to move from the workstations.
5	On each workstation: • Remove the UNICORN installation and reinstall the UNICORN software. • Connect UNICORN to the new database server.
6	Redefine the systems.
7	Import results and methods as needed.

2.2 Other software installed by UNICORN 7.5

Required software applications

The following software applications are required by the UNICORN software to function properly. The installation can be initiated automatically by the UNICORN 7.5 installation program. If any of the listed applications is already installed, it is not included in this installation step. It is necessary to restart the computer several times to proceed from one application installation to the next.

- Microsoft® .NET® Framework 4.7.2 Full
- Microsoft Core XML Services (MSXML) 6.0
- Microsoft Visual C++® 2008 Redistributable Package SP1
- Microsoft Visual C++ 2010 Redistributable Package SP1
- Microsoft Visual C++ 2012 Redistributable Package
- Microsoft Visual C++ 2013 Redistributable Package
- Microsoft Visual C++ 2015 Redistributable Package
- Microsoft Visual C++ 2017 Redistributable Package
- Microsoft SQL Server® 2017 Express (Only if the database is selected for installation)
- OPC Core Components Redistributable 106.0

Note: *This process can take up to one hour to complete if all the applications are installed.*

Note: *By default, the applications listed above are installed on the C: drive. If the available space on this drive is insufficient, the installation fails and the installation program attempts to repeat the installation after each restart. Make sure that enough space is available on the C: drive before starting the installation. The required space varies depending on what is previously installed on the computer (e.g. applications listed above), and subsequent selections in the UNICORN installation. However, the installation program requires at least 11 GB of free space to initiate the installation.*

The help viewer application

As part of the UNICORN software installation, a special viewer for the online help is installed. This application, the ***MadCap™ Help Viewer***, is accessed from the UNICORN user interface either by clicking help buttons in dialog boxes, by pressing the **F1** key or by clicking ***Help*** menu items.

By default, this application creates a shortcut icon on the desktop. If logon to UNICORN fails, the online help can be opened using this shortcut.

To start the UNICORN online help:

Step	Action
1	Double-click the shortcut icon on your desktop. 
2	On the ***File*** menu, click ***Open***.
3	Browse to any of the folders: • Program Files Path`\GE Healthcare\UNICORN\UNICORN 7.5\Documentation\Help\Chromatography` for a Chromatography installation. or • Program Files Path`\GE Healthcare\UNICORN\UNICORN 7.5\Documentation\Help\Bioreactor` for a Cell Cultivation installation. or • Program Files Path`\GE Healthcare\UNICORN\UNICORN 7.5\Documentation\Help\Filtration` for a Filtration installation.
4	Select the file `Manual.mchelp`.
5	Click ***Open***. *Result:* The online help portal page opens.

Note: *Sometimes Windows needs to register the MadCap Help Viewer as the application for files of the type .mchelp before it recognizes calls from help buttons in UNICORN 7.5. If that happens, open the viewer manually as described above. It can be necessary to do this once for a new Windows user profile.*

The UNICORN Service Tool

The UNICORN Service Tool is installed by the UNICORN installation program. It is used to troubleshoot and set parameters in an existing UNICORN installation.

With the software you can:

- See a list of installed UNICORN components.
- Configure IP addresses of the *Real-Time Unit* (RTU).
- Test connection to a database server
- Test connection to a license server
- Manage processes needed by UNICORN
- Test communication ports
- Check if the computer and operating system settings fulfills the UNICORN specifications
- See a log of all events registered by the UNICORN Service Tool.

For more information see *UNICORN Service Tool User Manual*.

Start the UNICORN Service Tool

Step	Action
1	Click the Windows ***Start*** button.
2	Type `UNICORN Service Tool` in the ***Start*** menu search field.
3	Click the ***UNICORN Service Tool*** item that is displayed as the search result to start the program.

Installation of Griffin Launcher

On computers delivered and/or installed by GE Healthcare, service staff installs a software tool which is used for diagnostic, testing, and quality control. This tool can only be used by GE Healthcare service staff, for quality control, to optimize system performance and as an aid in troubleshooting.

2.3 Stand-alone workstation installation and configuration

About this section

The UNICORN 7.5 software is normally installed by a GE Healthcare representative. Follow the instructions in this section to install the program yourself if your system is not preinstalled.

In this section

This section contains these subsections:

2.3.1 Install the UNICORN software - Full installation

Introduction

The full UNICORN installation includes all software component parts necessary to operate UNICORN and a connected local instrument.

The installation includes the components described in the table below.

Software component	Characteristics
UNICORN software	The UNICORN software is used to control and manage an instrument that is connected to the workstation.
Database server	The server software necessary to operate the database where all UNICORN data is stored. Microsoft SQL Server® Express Edition is used for this.
License server	The license server software is used to authorize that the UNICORN software installation is properly licensed.

Step 1 - Start installation

Follow the instructions to begin the installation:

Step	Action
1	Start UNICORN installation program. The program can be found in the UNICORN installation DVD. *Result:* The UNICORN Installation wizard opens with a welcome dialog box. ***Tip:*** *If the DVD drive is not set up to allow automatic start, browse the DVD contents and double-click the file **Setup.exe** in the UNICORN folder to initiate the installation.*
2	Click ***Next***.
3	The UNICORN Installation Program is launched. Continue the installation as described below.

Tip: *It is possible to exit the installation by clicking **Cancel**. However, the installation remains incomplete and the software cannot be used. It is possible to go **Back** in some installation steps, to return to a previous step to change selections.*

Step 2 - License agreement

The next installation step shows the UNICORN 7.5 License Agreement text.

Step	Action
1	Read the license agreement carefully.
2	Click ***I accept the terms in the license agreement***.
3	Click ***Next*** to proceed.

Step 3 - Select type of installation

In this step of the installation you decide what kind of installation you want to make.

Step	Action
1	Select the installation type: • ***Full installation*** which includes all the UNICORN software necessary for stand-alone operation. or • ***Custom installation*** which allows you to install selected components. (This installation option is described in *Section 2.4.1 Install the UNICORN 7.5 software - Custom installation, on page 55*).
2	Click ***Full installation*** to proceed with this option, for a stand-alone workstation installation.
3	Click ***Next*** to proceed.

Step 4 - Select installation folder

Select the installation folder for UNICORN.

Step	Action
1	For Windows 10, by default, UNICORN suggests the following installation folder: `C:\Program Files(x86)\GE Healthcare\UNICORN\` Either • accept this installation folder or • click ***Change*** and select a folder for UNICORN installation. ***Note:*** *UNICORN calculates the available diskspace for the selected installation folder. The space required for the installation is also shown.* ***Note:*** *UNICORN 7.5 cannot be installed on a compressed disk.*
2	Click ***Next*** to proceed.

Note: *The general UNICORN installation folder structure is saved in the folder selected in this step. However, the SQL Server software and e-license server software are installed on the C drive by default. If the available space for this is insufficient, the installation can fail. The required space varies depending on what is installed on the computer but at least 2 GB must be available to complete the installation.*

Step 5 - Specify data storage

Specify storage folders for database backups and for archived database items.

Step	Action
1	Click ***Browse*** next to the ***Backup files folder*** field and navigate to a suitable folder to save the database backups. ***Note:*** *By default UNICORN suggests a backup folder in the selected installation folder. However, if possible it is recommended that the backups are saved on another physical drive than where the active database is stored. This physical drive must be installed on the same computer as where the database is installed. Network folders cannot be used for this purpose.* ***Note:*** *Make sure that the user `SYSTEM` has access rights to the selected folder*[1].
2	Click ***Browse*** next to the ***Archive files folder*** field and navigate to a suitable folder archive the data. ***Note:*** *By default UNICORN suggests an archive folder in the selected installation folder. However, if possible it is recommended that the archives are saved on another physical drive than where the active database is stored. This physical drive must be installed on the same computer as where the database is installed. Network folders cannot be used for this purpose.* ***Note:*** *Make sure that the user `SYSTEM` has access rights to the selected folder.*
3	Click ***Next*** to proceed.

Note: *To ensure data safety, it is recommended that the backup and the archive folders are copied or moved at regular intervals to another server computer or some other storage media.*

Tip: *The **UNICORN Configuration Manager** tool can be used to change data storage folders after the installation.*

- *Type `UNICORN Configuration Manager` in the Windows Start menu search field, click the **UNICORN Configuration Manager** item that is displayed as the search result.*

1 *The access rights are shown in the **Security** tab of the folder **Properties**.*

Step 6 - Password settings

Choose the password settings you wish to apply for UNICORN.

Step	Action
1	By default, the ***Require passwords*** check box is selected. • If you do not want to use passwords at log on or for electronic signatures, clear this check box.
2	Click ***Next*** to proceed.

Tip: *The **UNICORN Configuration Manager** tool can be used to change the password settings after the installation.*

- *Type `UNICORN Configuration Manager` in the Windows Start menu search field, click the **UNICORN Configuration Manager** item that is displayed as the search result.*

Step 7- Column logbook

The ***Column Logbook*** enables the recording of usage and performance history for individual columns.

Step	Action
1	Select the ***Enable Column Logbook*** check box to set up the logbook. (This is selected by default)
2	Click ***Install***. *Result:* The UNICORN 7.5 installation begins.

Tip: *The **UNICORN Configuration Manager** tool can be used to enable or disable Column LogBook after the installation.*

- *Type `UNICORN Configuration Manager` in the Windows Start menu search field, click the **UNICORN Configuration Manager** item that is displayed as the search result.*

Step 8 - Installation completed

The final wizard dialog box opens when the installation is complete and the UNICORN 7.5 database, elicense server and software are all installed on the workstation computer.

At this point:

- click ***Configure eLicense***

Result: The ***Configure eLicense*** dialog box opens.

- click ***Define System***

  Result: The ***Define System*** dialog box opens.

  and/or

- view an installation summary report by clicking ***Show Report***.

  These dialog boxes are described in subsequent sections in this chapter

Tip: *It is possible to configure an e-license and define a system later if required. The e-license configuration is described in Add more e-licenses to the license server, on page 159, and how to define a system is described in Section 3.1.3 Define a new system, on page 115.*

Installation summary report

When the installation is completed, open an installation report in text format. This report contains a list of all installed files, including size, version and date of creation. The report can be used to verify that the installation is complete and that the correct files are included.

Note: *During the UNICORN installation some of the default Windows firewall settings and local security policies are modified to enable communication between the workstation computer, the instrument and the database server. The modified settings are listed at the end of the report.*

2.3.2 Configure an e-license

Introduction

This section describes how to configure an e-license as part of a UNICORN 7.5 installation. A block of e-licenses can be retrieved using the procedure described in this section for configuring e-licenses for a common license server in a network.

It is possible to access the configuration program at any time. To start the program, type `Configure e-License` in the Windows Start menu search field, click the ***Configure e-License*** item that is displayed as the search result.

Before you start

Activation ID

An activation ID is required to retrieve an e-license from the GE Healthcare software e-licensing web site. The activation ID together with the software is sent via e-mail. Contact the GE Healthcare representative if the activation ID is not received.

Internet connection

To activate the e-license, you must have access to the Internet. If you are configuring the e-license for a stand-alone workstation with no external network access, retrieve the e-license file using another computer and then move the file to the workstation computer using, for example, a USB memory stick.

Computer Ethernet address

The Ethernet address for the computer where the license server is installed (i.e. either a stand-alone workstation or a database and license server) is required when performing the actions described in this section. This address is shown in the ***Configure e-License*** dialog box.

Note: *The displayed address is the Ethernet address for the Network Interface Card (NIC) which is used for the communication with the instrument, and not the address for a second interface card used for network communication. If the computer is equipped with two interface cards, it is recommended to verify the Ethernet address.*

Verify Ethernet address

Step	Action
1	• Open a ***Command Prompt*** window[2] and • type `ipconfig /all`, and press `Enter` to display the Ethernet addresses.
2	Locate the Network Interface Card (also called Ethernet adapter) with the IP address used to connect to the instrument. This is the Network Interface Card which is used for instrument communication.
3	The Ethernet address for this card is listed as the ***Physical Address***. Verify that this is the address shown in the ***Configure e-License*** dialog box.

Different types of e-licenses

The following table provides an overview of the different types of e-licenses available for UNICORN 7.5.

Floating license can be used on any workstation in a network, but there can only be as many simultaneous users as there are valid licenses. UNICORN 7.5 can be installed on more workstations than the number of valid licenses, but all these workstations cannot be used simultaneously. A node locked license can be used on one workstation only.

The table is not complete, refer to a GE Healthcare representative for more information on available e-licenses.

Type	Description
Workstation license	The workstation license is a node locked license that is used for one computer only.
Remote license	The remote license is a floating license that can be used on any workstation in a network.
Dry license	The dry license is a floating license that can be used for all functionality except System Control, Evaluation Classic, Design of Experiments (DoE) and Column Logbook.
Evaluation Classic license	The Evaluation Classic license is a floating license used for the Evaluation Classic module.

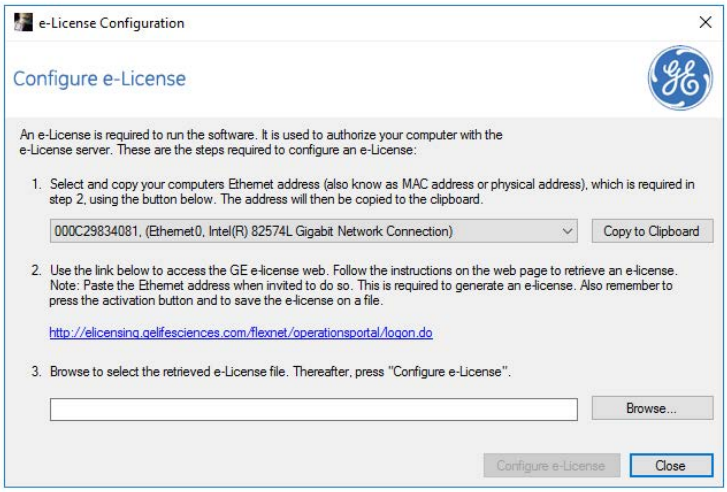
2 Type `Command Prompt` in the Windows Start menu search field, then click the ***Command Prompt*** item that is displayed as the search result.

Type	Description
Design of Experiment license	The Design of Experiment license is a floating license used for Design of Experiment.
Column logbook license	The Column logbook license is a floating license used for Column logbook.

Initiate the e-license configuration

After completing a UNICORN installation, you can choose to proceed to configure e-licenses for the installation. Follow the instructions to perform the final installation step and initiate the e-license configuration.

Step	Action
1	In the ***Configure e-License*** dialog box:



- Click ***Copy to Clipboard*** to copy the Ethernet address.

If the Network Interface Card name has been changed, the ***Configure E-License*** program fails to find the address. If this is the case:

- change the name of the Network Interface Card so that it starts with ***Local Area Connection***

  or

- find the MAC address as described in *Computer Ethernet address, on page 39*. Copy the address into the ***Configure E-License*** dialog box.

2	Click the hyperlink in the dialog box to proceed to access the e-licensing web site.

Note: *When activating additional licenses, it is essential to always use the Ethernet address for the computer where the license server software is installed. It is not recommended to use the Ethernet addresses for the additional client computers.*

Access the e-licensing web site

The e-license must be retrieved from the GE Healthcare e-licensing web site. Follow the instructions to access the site from the configuration dialog box.

Step	Action
1	Click ***Copy to Clipboard*** in the ***e-License Configuration*** dialog box. • This copies the Ethernet address from the computer (shown in the adjacent field), which is be used in subsequent steps.
2	Click the hyperlink in the configuration dialog box. *Result:* The ***GE Healthcare software elicensing web site*** opens in your web browser.

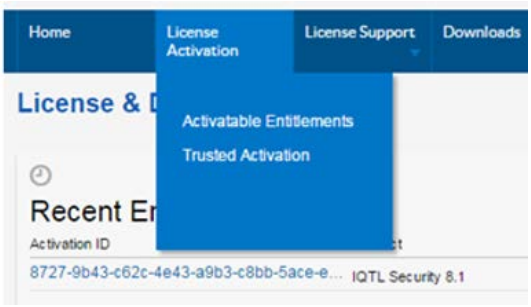
3	Type the ***Activation ID*** and click ***Log in***. *Result:* The ***License & Delivery Portal*** opens.

Retrieve the e-license

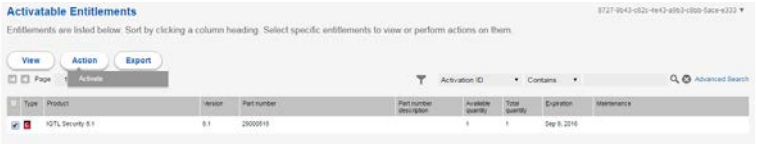
Go to www.gelifesciences.com/eDelivery and log in using Activation ID that you have received via E-mail during your purchase.

Follow the instructions to retrieve the e-license from the web site.

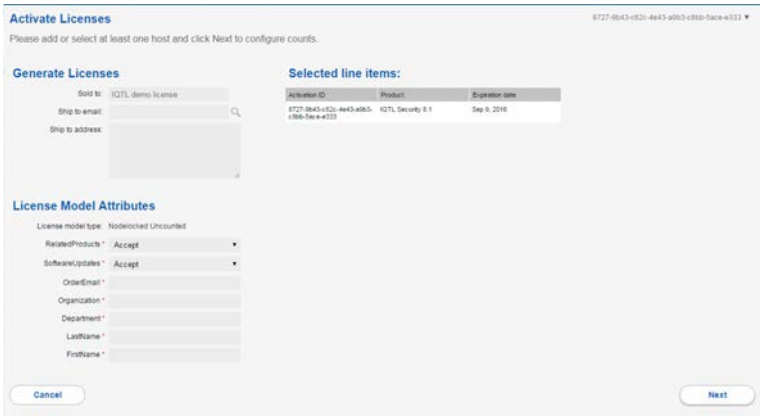
Step	Action
1	From ***License Activation*** menu choose ***Activatable Entitlements***.

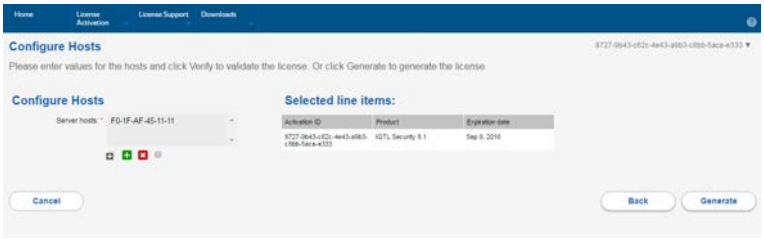
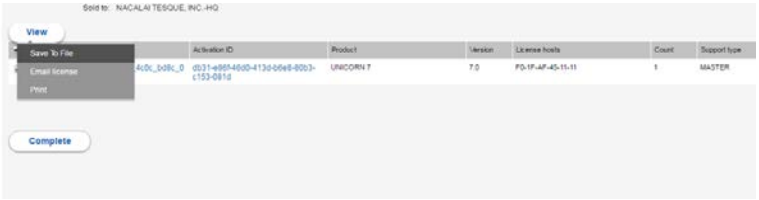


2	Select your entitlement from the list and choose ***Action > Activate***.



3	Fill in the appropriate information under ***License Model Attributes*** and click ***Next***. All items marked with red dots are mandatory.



Step	Action
4	Click the add button under ***Configure Hosts*** and in the empty ***Server Hosts*** field press the **Ctrl** and **V** keys simultaneously to paste your Ethernet address from the clipboard into this field. ***Note:*** *If you use another computer to retrieve the e-license, you must write down the Ethernet address from the computer you are installing the license server on and type this address in the* ***Server Hosts*** *field.* *Also, if UNICORN identified the wrong Ethernet address (e.g. from a second network interface card) in the* ***Configure e-License*** *dialog box, you must find the correct address and type it in manually.* *This is described in Computer Ethernet Address above.* 
5	Select your product in the list and click ***Save To File***. 
6	Click ***Save*** in the confirmation dialog that opens. *Result:* A download dialog box opens. Save the license file in a temporary folder or on your Windows desktop.
7	Click ***Logout*** to complete the procedure and log out from the ***License & Delivery Portal*** software e-licensing web site.

Locate and connect the e-license

Follow the instructions to connect and confirm the e-license in the UNICORN ***e-License Configuration*** dialog box.

Step	Action
1	• Click ***Browse*** to locate the license file and • click ***Open*** to add the search path to the file in the ***e-License Configuration*** dialog box.
2	Click ***Configure e-License***. *Result:* A message box opens, showing that the configuration has been successful.
3	Click ***OK*** in the message box, and then click ***Close*** to complete the process.

2.3.3 Define a system

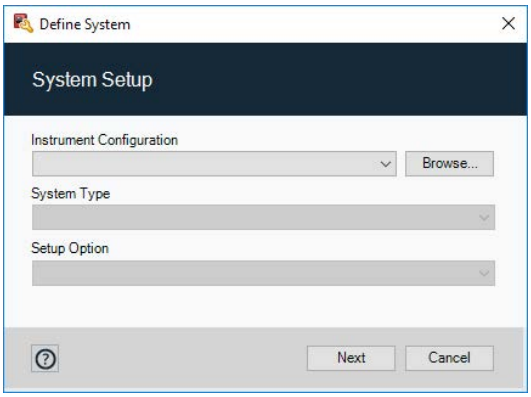
Introduction

In the UNICORN installation program, define a system if the computer is to be used as an instrument server for a locally connected instrument.

Note: *To enable connection tests, make sure that the instrument is turned on during the system definition.*

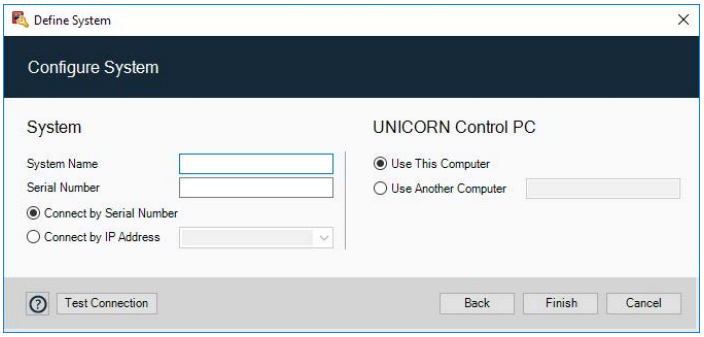
Tip: *It is possible to define a system at a later stage. This is described in Section 3.1.3 Define a new system, on page 115.*

Step	Action
1	Click ***Define System***. Result: The ***Define System*** dialog box opens.

Step	Action
2	 In the ***Define System*** dialog box: Select the appropriate instrument configuration in the ***Instrument Configuration*** list. ***Note:*** *For information about compatibility between UNICORN versions and the supported instrument configurations, see the UNICORN compatibility matrix at http://www.gelifesciences.com/UNICORNcompatibility.* ***Tip:*** *The list includes all instrument configurations currently in the UNICORN database. To select a new instrument configuration:* • *Click **Browse** and navigate to the configuration file.* • *Select and import the appropriate configuration file.* Result: The ***System Type*** field is populated with available System and the ***Setup Option*** field is populated with related Communication setup options.
3	Select the appropriate System from the ***System Type*** field.
4	Select the appropriate Communication setup from the ***Setup Option*** field and click ***Next***. Result: The ***Configure System*** dialog box opens. ***Note:*** *The **Configure System** dialog box differs depending on the selections in the previous steps.*
5	Follow the related instructions in the following sections:

System with UNICORN Control PC

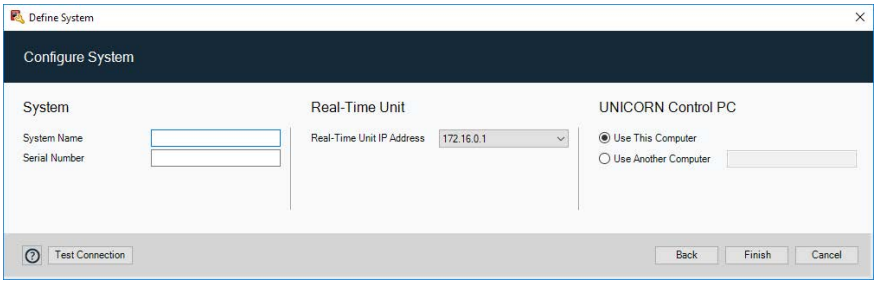
Follow these instructions if ***System with UNICORN Control PC*** is selected from the ***Setup Option*** field.



Step	Action
1	Enter a name in the ***System Name*** field. ***Note:*** *The system name cannot be changed once the system is defined.*
2	Enter the serial number for the instrument in the ***Serial Number*** field.
3	Select either ***Connect by Serial Number*** or ***Connect by IP Address***. If ***Connected by IP Address*** is selected, select the IP address from the list or enter the IP address manually.
4	Specify which computer to use as ***UNICORN Control PC***. To use as the ***UNICORN Control PC***, select either: • ***Use This Computer*** or • ***Use Another Computer*** and specify the name of that computer in the empty filed.
5	Click ***Finish*** to save and close the dialog box.

System with UNICORN Control PC and external Real-Time Unit

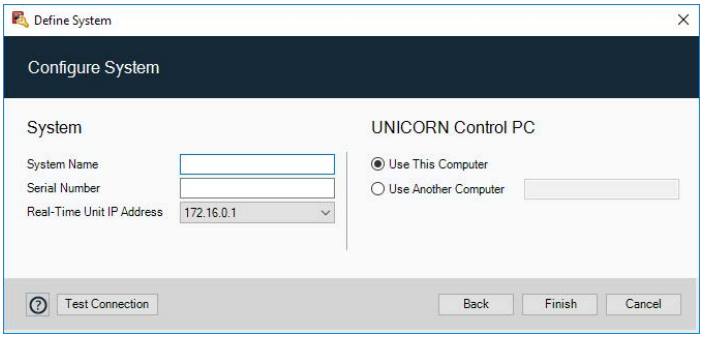
Follow these instruction if ***System with UNICORN Control PC and external Real-Time Unit*** is selected from the ***Setup Option*** field.



Step	Action
1	Enter a name in the ***System Name*** field. ***Note:*** *The system name cannot be changed once the system is defined.*
2	Enter the serial number for the instrument in the ***Serial Number*** field.
3	Select the ***Real-Time Unit IP Address*** from the list.
4	Specify which computer to use as ***UNICORN Control PC***. To use as the ***UNICORN Control PC***, select either: • ***Use This Computer*** or • ***Use Another Computer*** and specify the name in that computer in the empty filed.
5	Click ***Finish*** to save and close the dialog box.

System with UNICORN Control PC and internal Real-Time Unit

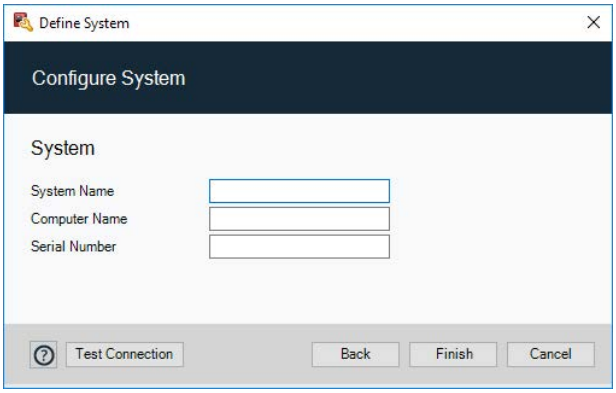
Follow these instructions if ***System with UNICORN Control PC and internal Real-Time Unit*** is selected from the ***Setup Option*** field.



Step	Action
1	Enter a name in the ***System Name*** field. ***Note:*** *The system name cannot be changed once the system is defined.*
2	Enter ***Serial Number*** .
3	Select ***Real-Time Unit IP Address*** from the drop-down list.
4 5	Specify which computer to use as *Instrument Server* under ***UNICORN Control PC***. To use as the *Instrument Server*, select either: • ***Use This Computer*** or • ***Use Another Computer*** and specify the name in that computer in the ***Name*** filed.
6	Click ***Finish*** to save and close the dialog box.

System with built-in UNICORN Instrument Server

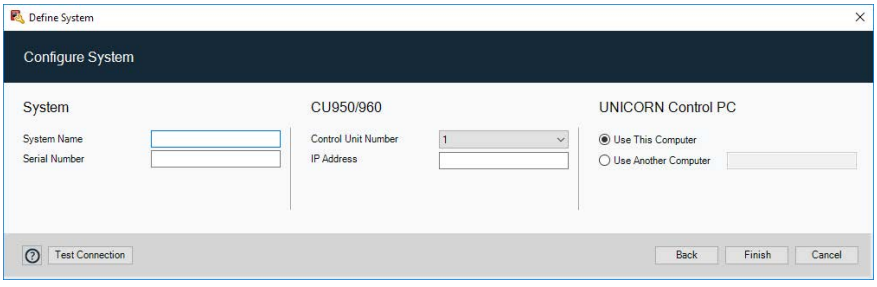
Follow these instructions if ***System with built-in UNICORN Instrument Server*** is selected from the ***Setup Option*** field.



Step	Action
1	Enter a name in the ***System Name*** field. ***Note:*** *The system name cannot be changed once the system is defined.*
2	Enter ***Computer Name*** .
3	Enter ***Serial Number***.
4	Click ***Finish*** to save and close the dialog box.

CU950/960

Follow these instructions if ***CU950/960*** is selected from the ***Setup Option*** field.



Step	Action
1	Enter a name in the ***System Name*** field. ***Note:*** *The system name cannot be changed once the system is defined.*
2	Enter ***Serial Number***.
3	Select the ***Control Unit Number***.
4	Enter the IP Address of the Control Unit.
5	Specify which computer to use as ***UNICORN Control PC***. To use as the ***UNICORN Control PC***, select either: • ***Use This Computer*** or • ***Use Another Computer*** and specify the name in that computer in the empty filed.

2.4 Network installation and configuration

About this section

This section describes how to install the UNICORN 7.5 for server and client computers in a network deployment. It also describes basic configuration of the server and client computers.

In this section

This section contains these subsections:

2.4.1 Install the UNICORN 7.5 software - Custom installation

Introduction

The UNICORN 7.5 software is installed using the Custom installation option. The installation that is described in this section assumes that a database and license server is already installed and accessible on a network where the client station resides.

Step 1 - Start the installation

Follow the instructions to begin the installation:

Step	Action
1	Insert the installation DVD in your DVD drive. *Result:* The UNICORN Installation wizard opens with a welcome dialog box. ***Tip:*** *If the DVD drive is not set up to allow automatic start, browse the DVD contents and double-click the file* ***Setup.exe*** *to initiate the installation.*
2	Click ***Next***.
3	The UNICORN Installation Wizard is launched. Continue the installation below.

Tip: *It is possible to exit the installation at any point by clicking* ***Cancel****. However, the installation remains incomplete and the software cannot be used. It is also possible to go* ***Back*** *in any installation step to return to a previous step to change selections.*

Step 2 - License agreement

The next installation step shows the UNICORN 7.5 License Agreement text.

Step	Action
1	Read the license agreement carefully.
2	Click ***I accept the terms in the license agreement***.
3	Click ***Next*** to proceed.

Step 3 - Select type of installation

In this installation step you decide what kind of installation you want to make:

Step	Action
1	Select the installation type: • ***Full installation*** which includes all the UNICORN software necessary for stand-alone operation. (This installation option is described in *Section 2.3.1 Install the UNICORN software - Full installation, on page 33*) or • ***Custom installation*** which allows you to install selected components.
2	Select ***Custom installation*** and click ***Next*** to proceed with the network installation.

Step 4 - Select System Type

Select the application area that UNICORN is mainly used for:

Note: *UNICORN for Cell Cultivation provides tools for planning, controlling, and analyzing purification or cell culture runs and results.*

Step	Action
1	Either • click ***Chromatography*** or • click ***Cell Cultivation*** or • click ***Filtration***.
2	Click ***Next*** to proceed.

Step 5 - Select software components

Choose the software components to install:

Step	Action
1	Click ***Install*** for one of the following options • ***UNICORN Database*** (This installation option is described in *Section 2.4.2 Install the UNICORN database, on page 60*). The ***UNICORN Database*** must be installed before installing the ***UNICORN Software***. • ***UNICORN Software*** (The installation option described in this section) • ***Software Licensing Server***
2	Follow the installation steps of the chosen compontent. You can then proceed to install other components in the same way.

Step 6 - Select installation folder

- Click ***Next*** on the start page.
- Select the destination folder for UNICORN:

Step	Action
1	For Windows 10, by default, UNICORN suggests the following installation folder: `C:\Program Files (x86)\GE Healthcare\UNICORN\UNICORN 7.5\` Either • accept this installation folder or • ***Change*** to the folder for UNICORN installation. ***Note:*** *UNICORN calculates the available diskspace for the selected installation folder. The space required for the installation is also shown.* ***Note:*** *UNICORN 7.5 cannot be installed on a compressed disk.*
3	Click ***Next*** to proceed.

Step 7 - Locate database and install

Locate and select the UNICORN database.

Note: *This installation step assumes that you have already installed a database server in the network, according to the instructions in* *Section 2.4.2 Install the UNICORN database, on page 60*.

Step	Action
1	1 Enter the database server computer name and (where applicable) the folder where the database is located in the ***Database location*** field. 2 Enter the database name in the ***Database Name*** field. ***Note:*** *UNICORN can identify the database location and enter this by default. Sometimes the name of the database server computer cannot be provided by DNS/WINS. If that is the case, enter the IP address of the database host computer.*
2	Click ***Test connection*** to verify that the communication between the client station and the database is established.
3	Click ***Next***.

Step 8 - Locate Software Licensing Server

Step	Action
1	If the ***Software Licensing Server*** is located on the same computer as the UNICORN database, select the check box ***Use same computer as UNICORN Database computer***. If the ***Software Licensing Server*** is located on a computer other than the UNICORN database, clear the ***Use same computer as UNICORN Database computer*** check box and type the license server computer name in the ***Enter Software Licensing Server computer name:*** box.
2	If the ***Test connection*** button is available, click it to verify that the communication between the client station and the license server is established.
3	• Click ***Next***. *Result:* The wizard is ready to begin the software installation. • Click ***Install*** to initiate the installation with the settings selected so far.

Step 9 - Installation completed

The final wizard dialog box shown below opens when the installation is complete and the UNICORN Software is fully installed on the client computer.

At this point

- click ***Finish*** to exit the wizard

  and/or

- view an installation report.

Installation summary report

When the installation is completed you can open an installation report in text format. This report contains a list of all installed files, including size, version and date of creation. This report can be used to verify that the installation is complete and that the correct files are included.

Note: *During the UNICORN installation some of the default Windows firewall settings and local security policies are modified to enable communication between the client computer, the instrument and the database server. The modified settings are listed at the end of the report.*

Define a system

If the computer is to be used as an instrument server for a locally connected instrument, choose to define a system. See *Section 2.3.3 Define a system, on page 47* for how to define a system.

Tip: *If you want to define a system at a later time it is possible to do so. How to define a system later on is described in Section 3.1.3 Define a new system, on page 115.*

2.4.2 Install the UNICORN database

Introduction

The ***Custom Installation*** option is used to install a UNICORN 7.5 database necessary to host data for a number of UNICORN client stations in a network deployment.

The database is a Microsoft SQL Server database. The standard database software supplied with the UNICORN 7.5 installation is Microsoft SQL Server Express. This server software is suitable for small workgroups consisting of two to three client stations. Contact your GE Healthcare representative to discuss other options if you need a larger installation.

The database installation is the first part of the set up of a UNICORN 7.5 network.

Step 1 - Install UNICORN Common Components

Follow the instructions to begin the installation:

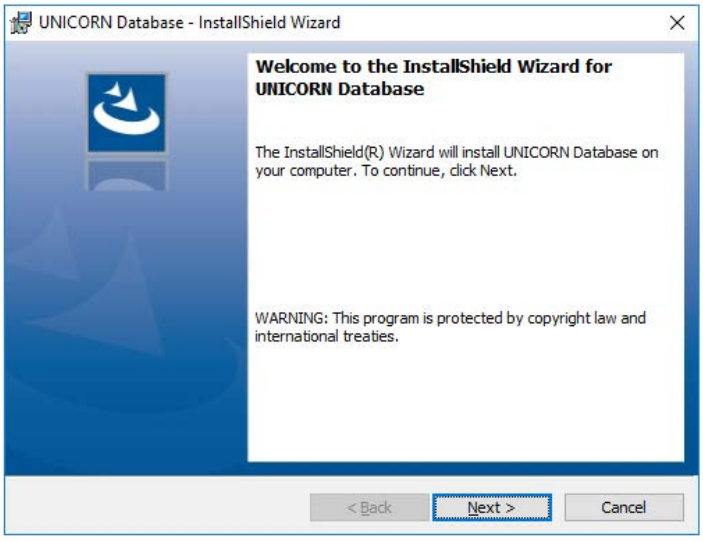
Step	Action
1	In the ***Custom Installation*** dialog box, click ***Install*** next to ***UNICORN Database*** *Result:* The ***UNICORN Common Components Installation Wizard*** opens .
2	Click ***Next***.
3	Select the installation folder for UNICORN Common Components. Either • accept the installation folder shown or • browse to the folder you want to install in. Click ***Next*** to proceed.
4	Click ***Install*** to begin the installation.

Step	Action
5	The final wizard dialog box opens when the installation is complete and the UNICORN Common Components is fully installed on the client computer. At this point • click ***Finish*** to exit the wizard and/or • view an installation report. Proceed with the database installation below.

Step 2 - Install UNICORN database

Follow the instructions to proceed with the database installation:

Step	Action
1	The UNICORN Database wizard opens.

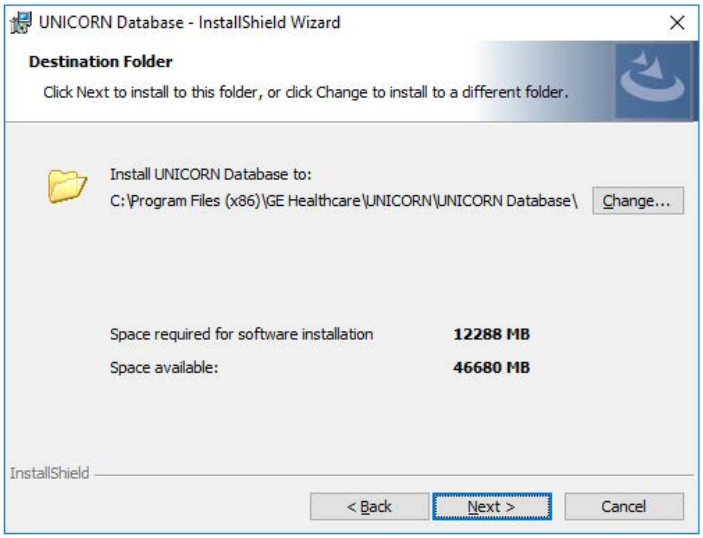


Click ***Next***.

Step	Action
2	The UNICORN Database installation continues. Proceed with the installation. ***Tip:*** *It is possible to exit the installation at any point by clicking **Cancel**. However, the installation remains incomplete and the software cannot be used. It is also possible to go **Back** in any installation step to return to a previous step to change selections.*

Step 3 - Destination folder

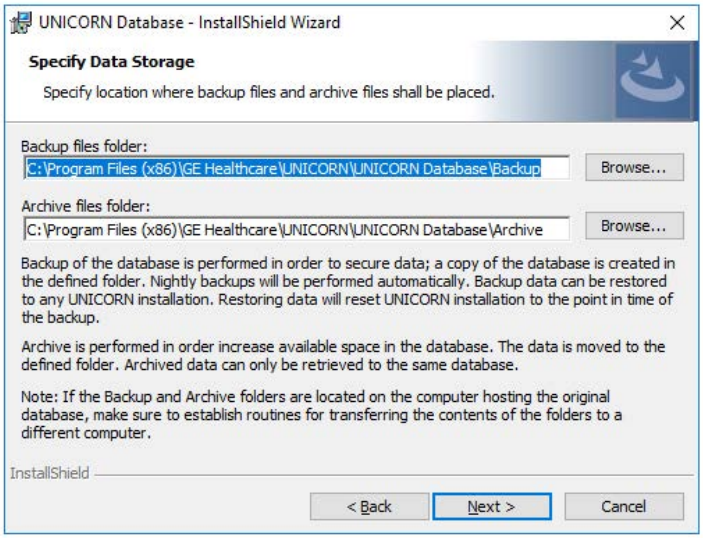
Select the installation folder for the UNICORN database:

Step	Action
1	The ***Destination Folder*** dialog box opens.  • Accept the installation folder shown or • Click ***Change*** to browse to the folder you want to install in.
2	Click ***Next***.

Step 4 - Specify data storage

Specify storage folders for database backups and for archived database items:

Step	Action
1	The ***Specify Data Storage*** dialog box opens.



Step	Action
2	• Click ***Browse*** adjacent to the ***Backup files folder*** field and navigate to a suitable folder to save the database backups. ***Note:*** *By default, UNICORN suggests a backup folder in the selected installation folder. However, if possible it is recommended that the backups are saved on another physical drive than where the active database is stored. This physical drive must be installed on the database server. Network folders cannot be used for this purpose.* ***Note:*** *Ensure that the user `SYSTEM` has access rights to the selected backup folder. This can be verified in the **Security** tab of the **Properties** dialog box for the folder.* • Click ***Browse*** adjacent to the ***Archive files folder*** field and navigate to a suitable folder to archive the data. ***Note:*** *By default, UNICORN suggests an archive folder in the selected installation folder. However, if possible it is recommended that the archives are saved on another physical drive than where the active database is stored. This physical drive must be installed on the database server. Network folders cannot be used for this purpose.* ***Note:*** *Make sure that the user `SYSTEM` has access rights to the selected archive folder. Right-click the folder, then click **Properties** and then click **Security** to verify this.* • Click ***Next*** to proceed.
3	Click ***Next***.

Note: *To ensure data safety, it is recommended that the backup and the archive folders are copied or moved at regular intervals to another server computer or some other storage media.*

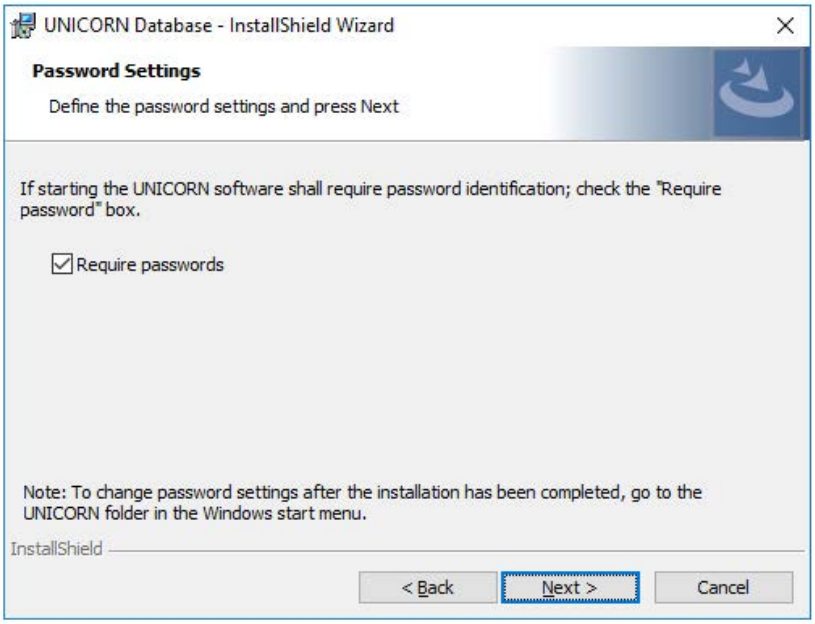
Tip: *The **UNICORN Configuration Manager** tool can be used to change data storage folders after the installation.*

- *Type `UNICORN Configuration Manager` in the Windows Start menu search field, click the **UNICORN Configuration Manager** item that is displayed as the search result.*

Step 5 - Password settings

Choose if password shall be required for log on to the UNICORN 7.5 network.

Note: *These settings are applied to all client stations sharing this database server.*



Step	Action
1	By default, the ***Require passwords*** check box is selected. If you do not want to use passwords at log on or for electronic signatures, clear the check box.
2	Click ***Next***.

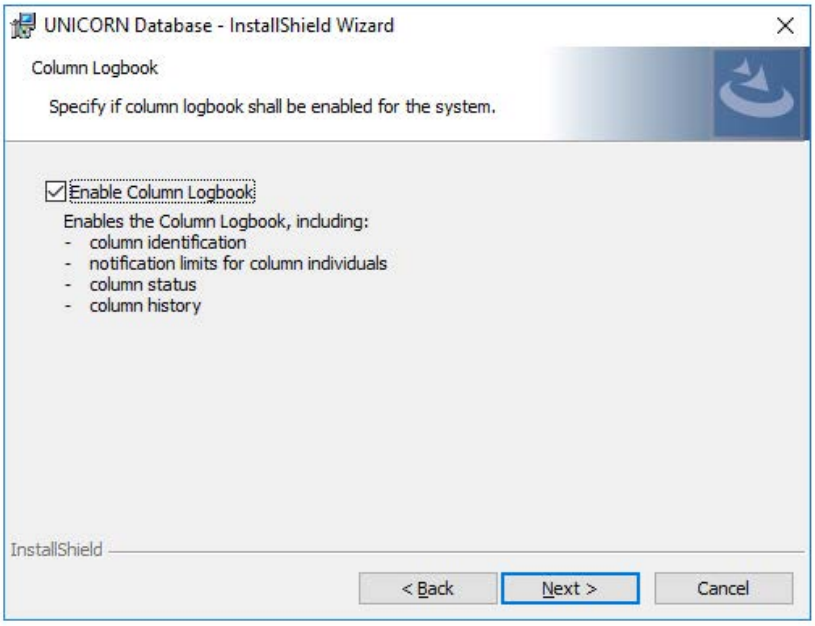
Tip: *The **UNICORN Configuration Manager** tool can be used to change the password settings after the installation.*

- *Type `UNICORN Configuration Manager` in the Windows Start menu search field, click the **UNICORN Configuration Manager** item that is displayed as the search result.*

Step 6 - Column logbook

The ***Column Logbook*** enables the recording of usage and performance history of individual columns. Follow the instructions to enable ***Column Logbook***.

Note: *A **Column Logbook** license named Site Wide is required to enable **Column Logbook**.*



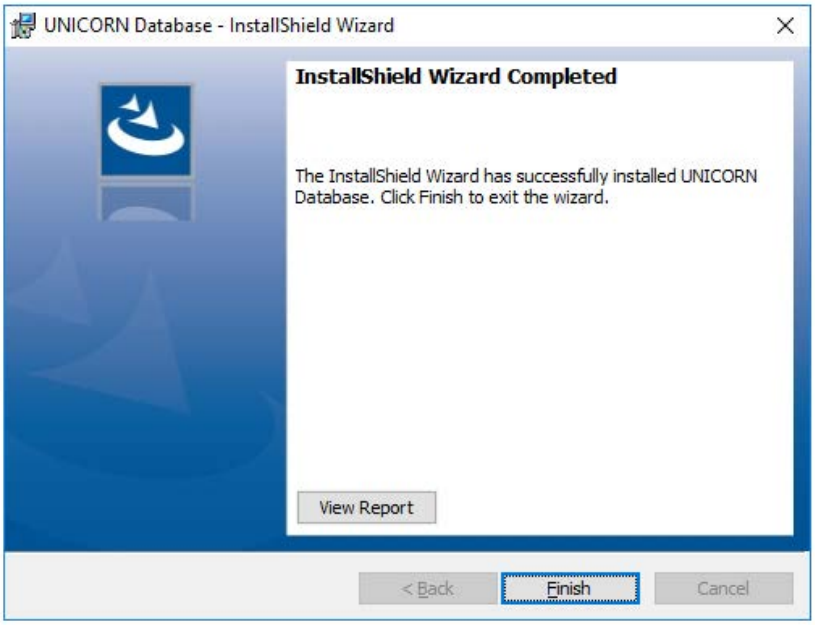
Step	Action
1	• Select the ***Enable Column Logbook*** check box to set up the logbook. This is selected by default. • Click ***Next***.
2	*Result:* The wizard is ready to install the UNICORN 7.5 Database and the ***Ready to Install the Program dialog*** opens. Click ***Install*** to begin the database installation.

Tip: *The **UNICORN Configuration Manager** tool can be used to enable or disable Column LogBook after the installation.*

- *Type `UNICORN Configuration Manager` in the Windows Start menu search field, click the **UNICORN Configuration Manager** item that is displayed as the search result.*

Step 7 - Installation completed

The final wizard dialog box shown below opens when the installation is complete and the UNICORN 7.5 database is fully installed on the server computer.



At this point

- click ***Finish*** to close the wizard

  and/or

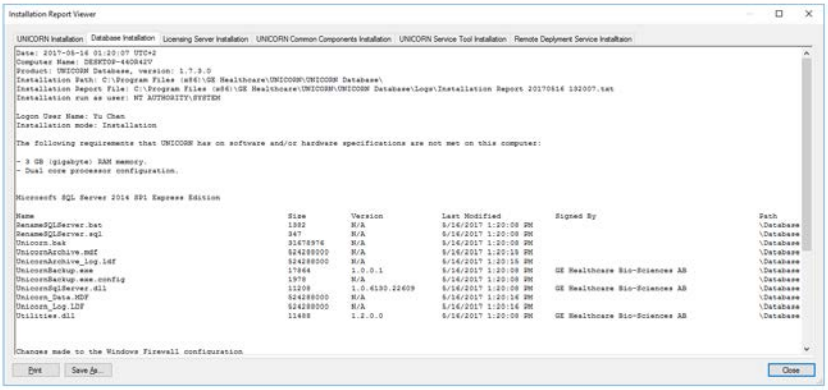
- view an installation report.

  Note: *The report can only be displayed at this point.*

Installation summary report

When the installation is completed, Optionally open an installation report in text format. This report contains a summary of the installation.

Note: *During the UNICORN installation some of the default Windows firewall settings and local security policies are modified to enable communication between client computers, instruments and the database server. The modified settings are listed at the end of the report.*


Installation Report Viewer
UNICORN Installation
Database Installation
Licensing Server Installation
UNICORN Common Components Installation
UNICORN Service Tool Installation
Remote Deployment Service Installation
Date: 2017-05-16 01:20:07 UTC+2
Computer Name: DESKTOP-44OB42V
Product: UNICORN Database, version: 1.7.3.0
Installation Path: C:\Program Files (x64)\GE Healthcare\UNICORN\UNICORN Database\
Installation Report File: C:\Program Files (x86)\GE Healthcare\UNICORN\UNICORN Database\Logs\Installation Report 20170516 192007.txt
Installation run as user: NT AUTHORITY\SYSTEM
Logon User Name: Yu Chen
Installation mode: Installation
The following requirements that UNICORN has on software and/or hardware specifications are not met on this computer:
- 3 GB (gigabyte) RAM memory.
- Dual core processor configuration.
Microsoft SQL Server 2014 SP1 Express Edition
Name
Size
Version
Last Modified
Signed By
Path
RenameSQLServer.bat 1382 N/A 5/16/2017 1:20:08 PM \Database
RenameSQLServer.sql 347 N/A 5/16/2017 1:20:08 PM \Database
Unicorn.bak 31478976 N/A 5/16/2017 1:20:08 PM \Database
UnicornArchive.mdf 524288000 N/A 5/16/2017 1:20:15 PM \Database
UnicornArchive_log.ldf 524288000 N/A 5/16/2017 1:20:15 PM \Database
UnicornBackup.exe 17864 1.0.0.1 5/16/2017 1:20:08 PM GE Healthcare Bio-Sciences AB \Database
UnicornBackup.exe.config 1978 N/A 5/16/2017 1:20:08 PM \Database
UnicornSqlServer.dll 11208 1.0.6130.22609 5/16/2017 1:20:08 PM GE Healthcare Bio-Sciences AB \Database
Unicorn_Data.MDF 524288000 N/A 5/16/2017 1:20:16 PM \Database
Unicorn_Log.LDF 524288000 N/A 5/16/2017 1:20:16 PM \Database
Utilities.dll 11488 1.2.0.0 5/16/2017 1:20:08 PM GE Healthcare Bio-Sciences AB \Database
Changes made to the Windows Firewall configuration
Print
Save As...
Close

2.4.3 Install the Software Licensing Server and configure an e-license

Introduction

The ***Custom Installation*** option is used to install the Software Licensing Server application necessary to authenticate licenses.

When the Software Licensing Server instrument server has been installed, it is possible to configure an e-license.

Instruction

Follow the instructions to install the Software Licensing Server:

Step	Action
1	In the ***Custom Installation*** dialog box, click ***Install*** next to ***Software Licensing Server***. *Result:* The ***Software Licensing Server*** is installed.
2	Click ***Configure eLicense***. *Result:* The ***Configure eLicense*** dialog box opens. Proceed to configure an e-license as described in *Section 2.3.2 Configure an e-license, on page 39*.

2.4.4 Configure the network

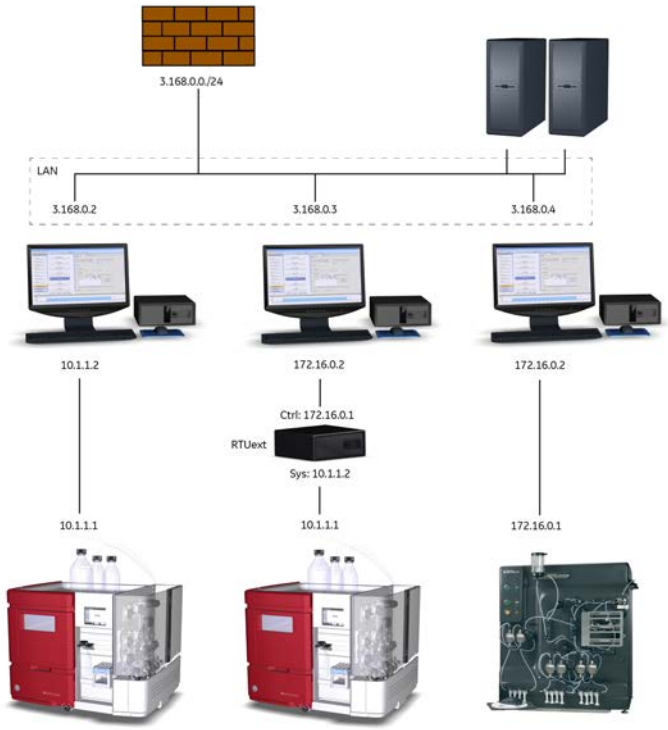
Introduction

The network environment for UNICORN 7.5 can be set up in many different ways, from a very simple solution for two to three simultaneous users to large scale operations where up to 20 instrument servers share a common database instance. In a larger installation the network can be set up either as Workgroups or Domains. Since the requirements for large scale installations inevitably are different and must be solved on a case by case basis, a model solution cannot be presented in this manual. Additional information necessary for larger installations is available on request from GE Healthcare.

This section describes a very simple solution for a small network, suitable for the number of clients that SQL Server Express is intended for.

Network illustration

The illustration below shows a small network example:



- In this example, the UNICORN network resides on a router, protected from the larger LAN by a firewall. The router address range is defined as 192.168.0.0 - 192.168.0.24.
- The Database server and the License server is set up with an IP address that is system dependent.
- Each client station is also an *Instrument server*.
- The *Network Interface Card 2* (NIC 2) for each *Instrument Server* is connected to the router for network communication. The IP addresses are allocated dynamically.
- The *Network Interface Card 1* (NIC 1) for each *Instrument server* is set with the static IP address 10.1.1.2. This card is connected to the instrument in a peer-to-peer connection.
- For systems where it is applicable, the IP addresses for the instruments are set with the static IP address 10.1.1.1.

(For some systems this adress is set on delivery, by default)

Firewall settings

The UNICORN 7.5 installation configures the Windows Firewall to allow all the network traffic necessary for the communication between the database server and client computers, and for the license authentication. However, if another firewall is used, the ports used by UNICORN must be set to allow traffic. See *Appendix C Firewall settings, on page 253*.

2.4.5 Configure and set up the client computers

Introduction

UNICORN 7.5 client computers delivered from GE Healthcare are set up with dual Network Interface Cards and configured for use as instrument servers in a network environment by default. These computers are ready to be installed following the instructions in the instrument's User Manual and require no additional configurations.

If other computers are used in a network, an extra Network Interface Card must be installed and configured. This is described here.

This section also briefly describes the connections between the client computer and other units. This is explained and illustrated in detail in the instrument's User Manual.

Additional information about the client computer configuration and set up is available in *Appendix B.1 User, client computer and database server set up, on page 237*, *Appendix C Firewall settings, on page 253* and in *Appendix D Post-installation settings, on page 260*.

Client computer prerequisites

Computers used for UNICORN 7.5 must fulfill the following prerequisites:

- Screen resolution 1280x1024 or higher
- Standard Windows default font (text size set to 100%)
- It is recommended to update windows manually or postpone windows update to a suitable time when UNICORN is not in use. This is because, windows update can interfere with UNICORN and interrupt ongoing runs.
- All Windows power save features must be turned off

  (using power save can interfere with the instrument server operation during active runs)

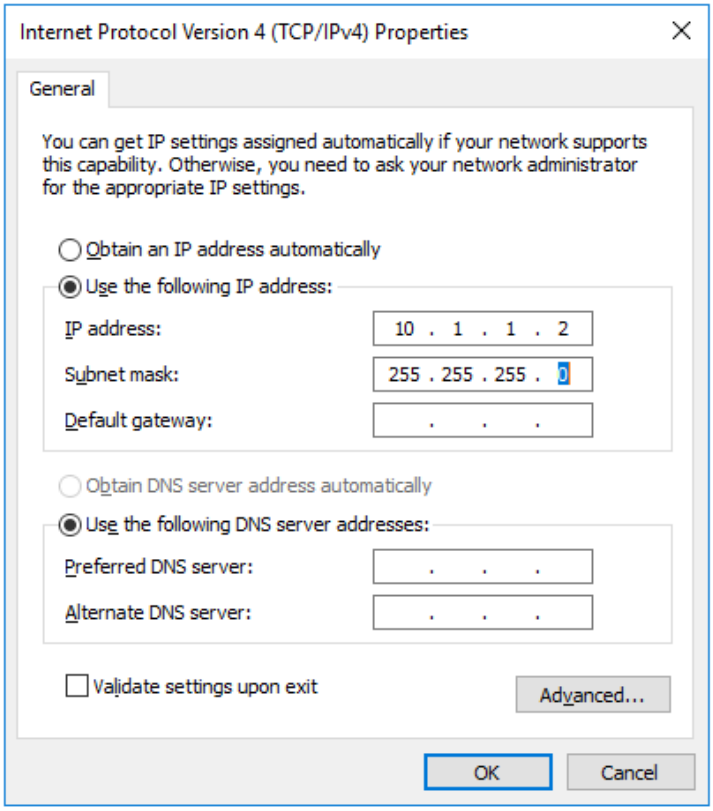
Other computer hardware recommendations are listed in *Appendix A.1 Computer recommendations, on page 232*.

Note: *Make sure that instrument server computers are not included in automatic software updates (for example of Anti-Virus or other security applications) requiring system restart. A scheduled update with a restart can collide with a method run in progress. For some systems, a restart can cause the run to stop.*

Configure the instrument server Network Interface Card

Step	Action
1	Install the Network Interface Card according to the installation instructions provided by the manufacturer.
2	Open the ***Network Connections*** window. Type `ncpa.cpl` in Windows Start menu search field, click the ***ncpa.cpl*** item that is displayed as the search result. *Result:* The ***Network Connections*** window opens.
3	• Right-click the network connection icon for the Network Interface Card to be used for the instrument communication, and then click ***Rename***. • Rename the network connection to ***AKTA***. (This enables GE Healthcare field service staff to easily identify the dedicated instrument communication card)
4	On the ***Advanced*** menu, click ***Advanced Settings***. *Result:* The ***Advanced Settings*** dialog box opens. If no menu is visible, press the ***Alt*** key.
5	• Select the network connection for the Network Interface Card in the ***Connections*** list in the ***Adapters and Bindings*** tab. • Click the up arrow button to move this network connection to the top of the list.  • Click ***OK*** to apply the settings and close the ***Advanced Settings*** dialog box.
6	• Double-click the instrument network connection. *Result:* The ***Status*** dialog box opens. • Click ***Properties***. *Result:* The ***Properties*** dialog box opens.
7	Select the ***Internet Protocol Version 4 (TCP/IPv4)*** item and click ***Properties***. *Result:* The ***Internet Protocol Version 4 (TCP/IPv4) Properties*** dialog box opens.

Step	Action
8	Click ***Use the following IP address*** and enter the following if no RTU is used: • IP address: 10.1.1.2 • Subnet mask: 255.255.255.0



Note:

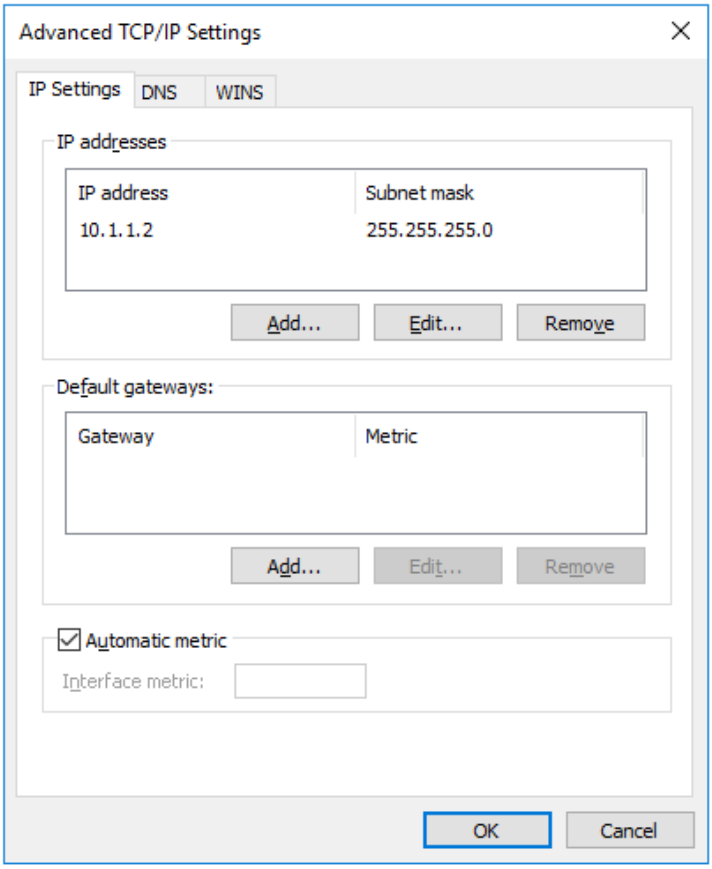
- *Do not enter a **Default gateway** in this dialog box.*
- *If two or more network adapters are in use, make sure that the configured IP address is not within the subnet of the other adapters. Recommended IP address to use is 10.1.1.X where X is 2 to 254.*

Or

Click ***Use the following IP address*** and enter the following if an RTU is used:

Step	Action
	• IP address: 172.16.0.2 • Subnet mask: 255.255.255.0 ***Note:*** • *Do not enter a **Default gateway** in this dialog box.* • *If two or more network adapters are in use, make sure that the configured IP address is not within the subnet of the other adapters. Recommended IP address to use is either 172.16.0.X or 10.0.0.X where X is 2 to 254.*
9	Click ***Advanced***. *Result:* The ***Advanced TCP/IP Settings*** dialog box opens.

Step	Action
10	Clear the ***Automatic metric*** check box and enter `25` in the ***Interface metric*** box:



11	• Click ***OK*** to apply the settings and close the ***Advanced TCP/IP Settings*** dialog box. • Click ***OK*** to close the ***Internet Protocol Version 4 (TCP/IPv4) Properties*** dialog box. • Click ***OK*** to close the ***Properties*** dialog box. • Click ***Close*** to close the ***Status*** dialog box.

Step	Action
12	• Right-click the network connection icon for the Network Interface Card to be used for the instrument communication, and then click ***Properties***. • Click ***Configure***. • Click the ***Advanced*** tab. • Under ***Property***, select ***Speed & Duplex***. • Select a suitable ***Value*** from the drop-down list under ***Value***. ***Note:*** *Make sure that the chosen **Value** is same on both sides. CU based systems (ÄKTA, Espresso etc.) support **10mbps Half Duplex** and NextÄKTA supports **Auto Negotiation** as **Value**.* • Click ***OK***.
13	Close the ***Network Connections*** window.

Firewall settings

The UNICORN 7.5 installation configures the Windows Firewall to allow all the network traffic necessary for the communication between the database server and client computers, and for the license authentication. However, if another firewall is used, the ports used by UNICORN must be set to allow traffic. See *Appendix C Firewall settings, on page 253*.

2.5 Control unit installation

CU-950 and CU-960

Control unit installation is system specific. UNICORN 7.5 supports Ethernet connected external control units of two types:

- CU-950

  and

- CU-960

Note: *Control unit installation is only necessary for a PC which is directly connected to a system. Whether this PC is connected to a network or not (stand-alone installation) does not matter. If your system is not pre-installed and the computer is directly connected to a chromatography system, you must install hardware.*

The installation of control units are made in the ***Define System*** dialog box if applicable, during or after the UNICORN installation. See *Section 3.1.3 Define a new system, on page 115*.

For information regarding CU-950 and CU-960 port numbers, see *CU-950 and CU-960 TCP ports, on page 256*.

2.6 OPC settings for UNICORN

Introduction

The information in this chapter is valid when using the industry standard OPC. This standard is based on DCOM (or Distributed COM) as the underlaying communication layer between the OPC client and the OPC server.

There are differences in how to configure the computer depending on if the computer is within a Windows workgroup or a Windows domain.

For detailed information about how to enable DCOM, see *Component services, on page 239*.

Prerequisite installation

OPC Core Components are installed as part of the UNICORN 7.5 installation of prerequisite software applications. The following instructions assume that the installation was completed as intended.

Windows user names and passwords

Unless a domain controller is used, all users must have exactly the same user name and password on all computers running UNICORN. If a domain controller is used, the users are created at the domain controller and not on each computer. This eliminates the need for synchronized user names and passwords.

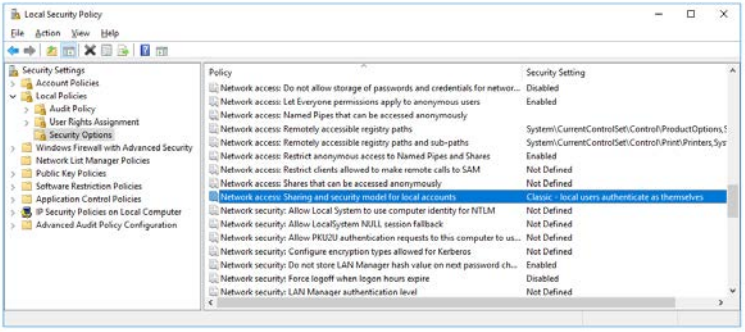
Additional configuration

When running UNICORN on Windows 10 computers with restrictions applied on DCOM, the User Account Control (UAC) feature in Windows 10 makes additional changes to the configuration. These settings can be applied to Windows 10 both in workgroups and domains.

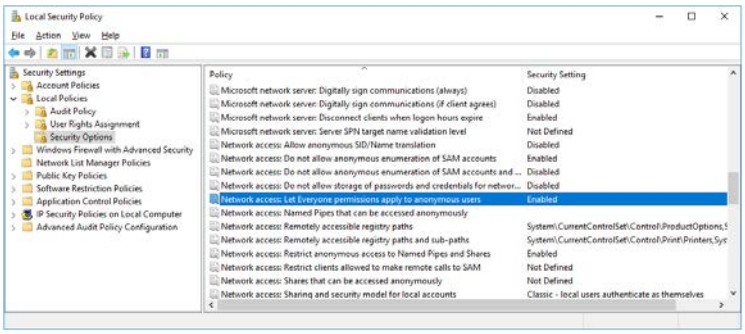
Step	Action
1	If there is a third party firewall [3] enabled on the instrument server, see *OPC settings, on page 256*.

3 Exceptions for the Windows firewall are added by the UNICORN 7.5 installation program.

Step	Action
2	Make sure that the OPC client and the instrument server are using the same subnet mask for the computer IP addresses. Also, the computer IP addresses shall be within the same subnet.
3	Set the ***Local Policies:Security Options*** setting ***Network access: Sharing and security module for local accounts*** to ***Classic - Local users authenticate as themselves***. 1 Type `Local Security Policy` in the Windows ***Start*** menu search box 2 Click the ***Local Security Policy*** item that is displayed as the search result. 3 Expand ***Security Settings:Local Policies:Security Options*** 4 Locate ***Network access: Sharing and security module for local accounts*** in the ***Policy*** list and change the setting if necessary



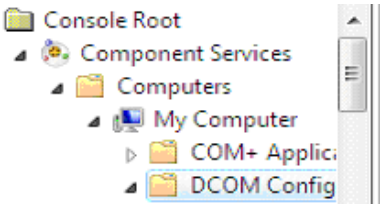
4	In the same dialog: • Make sure that the setting ***Network access: Let Everyone permissions apply to anonymous users*** is enabled.



Step	Action
5	Make sure that the user account which is running the OPC client has an equivalent account (using the same name and password) on the instrument server computer. A password is required and cannot be omitted. ***Note:*** *This is necessary only when the UNICORN computer is used in a workgroup, not when it is used in a domain.*

Instrument server settings

The following settings apply to the instrument server computers using the ***Component Services***:

Step	Action
1	Start the ***Component Services***: 1 Type `Component Services` in the Windows ***Start*** menu search field. 2 Click the ***Component Services*** item that is displayed as the search result.
2	Open the ***UNICORN Instrument Server.exe Properties*** dialog box: 1 Click the ▷ beside the ***Component Services*** object 2 Click the ▷ beside the ***Computers*** object 3 Click the ▷ beside ***My Computer***. 4 Click the ▷ beside the ***DCOM Config***.  5 Locate ***UNICORN Instrument Server.exe*** in the list, right-click the item and click ***Properties***. ***Note:*** *One or several DCOM configuration warnings can be displayed. Click **Yes** to acknowledge each one.*

Step	Action
3	Add the built-in group ***Users*** (or ***Authenticated Users*** if the computer is used in a domain) and set ***Launch and Activation Permissions*** for the group: 1 Click the ***Security*** tab. 2 Click ***Customize*** in the ***Launch and Activation Permissions*** field. 3 Click ***Edit*** in the ***Launch and Activation Permissions*** field. 4 Click ***Add*** in the ***Launch and Activation Permissions*** dialog box. 5 Enter the group ***Users*** (or ***Authenticated Users*** if the computer is used in a domain) in the ***Select Users, Computers, or Groups*** dialog box and click ***OK***.
4	Set the permissions for the new group ***Users*** (or ***Authenticated Users***) in the ***Launch and Activation Permissions*** dialog box. Select the group and select the check boxes to ***Allow*** • ***Local Launch*** • ***Remote Launch*** • ***Local Activation*** and • ***Remote Activation*** Click ***OK*** to apply and close the ***Launch and Activation Permissions*** dialog box.
5	Add the built-in group ***Users*** (or ***Authenticated Users*** if the computer is used in a domain) and set ***Access Permissions*** for the group: 1 Click ***Customize*** in the ***Access Permissions*** field. 2 Click ***Edit*** in the ***Access Permissions*** field. 3 Click ***Add*** in the ***Launch and Activation Permissions*** dialog box. 4 Enter the group ***Users*** (or ***Authenticated Users*** if the computer is used in a domain) in the ***Select Users, Computers, or Groups*** dialog box and click ***OK***.

Step	Action
6	Set the permissions for the new group ***Users*** (or ***Authenticated Users***) in the ***Access Permission*** dialog box. Select the group and select the check boxes to ***Allow*** • ***Local Access*** • ***Remote Access*** Click ***OK*** to apply and close the ***Access Permission*** dialog box. Click ***OK*** to close the ***UNICORN Instrument Server Properties*** dialog box.
7	Adjust the limits globally on the instrument server computer: 1 Right-click on ***My Computer*** in the tree view in the left panel of the ***Component Services*** dialog box, and click ***Properties***. 2 Click the ***COM Security*** tab. 3 Click ***Edit Limits*** in the ***Access Permissions*** field and allow ***Users*** (or ***Authenticated Users***) to have ***Local Access*** and ***Remote Access*** permissions. ***Note:*** *The group* ***Users*** *(or* ***Authenticated Users*** *if the computer is used in a domain) must be added if it is not already present*. Click ***OK***. 4 Click ***Edit Limits*** in the ***Launch and Activation Permissions*** field and allow ***Users*** (or ***Authenticated Users***) to have ***Local Launch***, ***Remote Launch***, ***Local Activation*** and ***Remote Activation*** permissions. Click ***OK***.
8	Click ***OK*** to close the ***My Computer Properties*** dialog box.
9	Close the ***Component Services*** dialog box and restart the computer.

2.7 Upgrade UNICORN 6.0 or later to UNICORN 7.5

Introduction

The UNICORN 7.5 installation program automatically identifies if an old UNICORN installation is present on the computer when installing UNICORN 7.5.

Follow the procedure described below to handle users, back up data, uninstall the old UNICORN version, install UNICORN 7.5 and restore the backup.

In a network deployment it is essential that all installations sharing data are upgraded, including all database servers, instrument servers and network clients.

Users and access groups

From UNICORN 6.2 and later, users and groups are handled differently compared to earlier versions of UNICORN.

All users with the same access and the same home folder after the upgrade must be placed in the same group. After the upgrade to UNICORN 7.5 these users belong to the same access group. The new access group can have the lowest common denominator of accesses that the users had before the upgrade.

Note: *If the home folders differ between the users in the group, a new home folder must be set for the new access group in UNICORN 7.5.*

Upgrade from UNICORN 6.0 or 6.1

Follow the instructions to perform the upgrade from UNICORN 6.0 or 6.1:

Step	Action
1	Backup the database as described in *Manual backups, on page 171*.
2	Insert the UNICORN 6.0 or UNICORN 6.1 installation DVD in your DVD drive. *Result:* The UNICORN Installation wizard opens with a welcome dialog box. ***Tip:*** *If the DVD drive is not set up to allow automatic start, browse the DVD contents and double-click the file* ***Setup.exe*** *in the UNICORN folder to initiate the installation.*
3	Click ***Remove Installation*** and proceed to uninstall the old UNICORN version.

Step	Action
4	Install UNICORN 7.5 as described in *Section 2.3.1 Install the UNICORN software - Full installation, on page 33*, but do not define a system or import any column lists, report formats, or recipes since the backup performed in Step 1 is restored later on.
5	Install the workstation e-license on the instrument server computer as described in *Locate and connect the e-license, on page 46*.
6	Uninstall the oldest version of OPC Core Components from the Windows ***Uninstall or change a program*** dialog box and repair the latest version. To open the ***Uninstall or change a program*** dialog box: • In ***Control Panel***, in the ***Programs*** group, click ***Uninstall a program***.
7	Restore the database backup as described in *Section 4.2.2 Restore backup data, on page 173*. ***Note:*** *The default backup location has changed since the old UNICORN version so the old database backup might have to be moved into the new backup location. Run a manual backup as described in Section 4.2.1 Database backup, on page 168 to create this location.*
8	Upgrade the database as described in *Section 4.2.7 Upgrade database, on page 188*.

Upgrade from UNICORN 6.2 or later

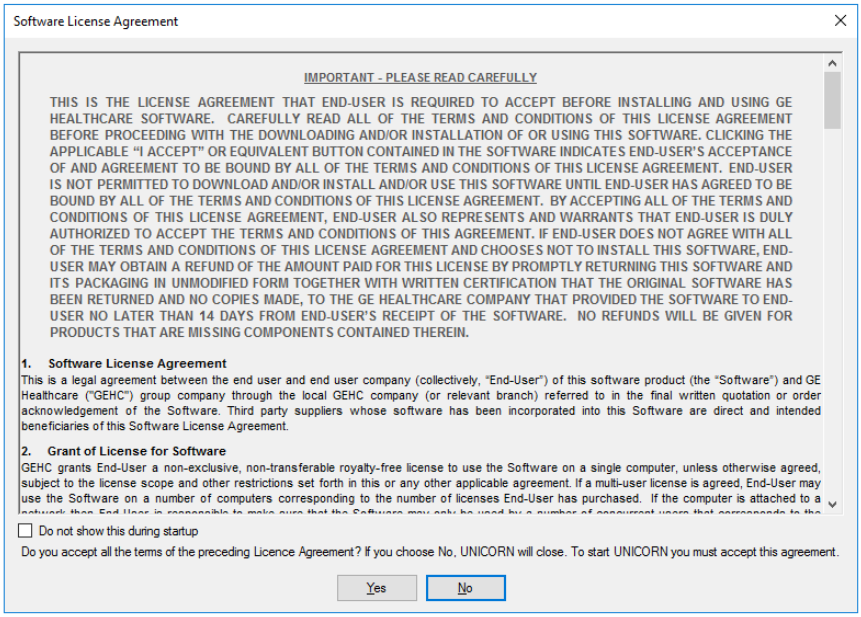
Follow the instructions to perform a upgrade from UNICORN 6.2 or later.

Step	Action
1	Insert the installation DVD in your DVD drive. *Result:* The UNICORN 7.5 Installation wizard opens with a welcome dialog box. ***Tip:*** *If the DVD drive is not set up to allow automatic start, browse the DVD contents and double-click the file `Setup.exe` in the UNICORN folder to initiate the installation.*
2	Click ***Upgrade Installation*** and proceed to upgrade UNICORN 6.2 or later to UNICORN 7.5.

Step	Action
3	Upgrade the database as described in *Section 4.2.7 Upgrade database, on page 188* if updating from UNICORN 6.X

License Agreement

The ***Software License Agreement*** dialog box appears during the start of the UNICORN 7.5 after the upgrade. The agreement must be accepted at least at the first logon for UNICORN 7.5 to start. Select the ***Do not show this during startup*** check box so that the license agreement is not displayed every time UNICORN 7.5 is started.



Update instrument configurations

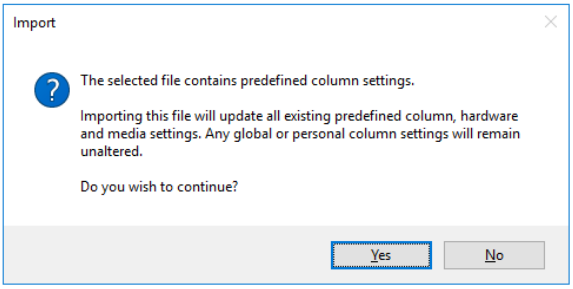
After the upgrade, import new, compatible instrument configurations for the systems. Contact the GE Healthcare representative for the most recent available instrument configuration CD.

Import new column list

The import of a new column list updates the column hardware list and the approved media list.

After upgrading to UNICORN 7.5, a new list of predefined Column types must also be imported. This list can be found in the `UNICORN Database\Misc` folder of the UNICORN 7.5 installation DVD.

Follow the instructions to import a new column list into the database:

Step	Action
1	In the ***Column Type Parameters*** tab in the ***Column Handling*** dialog box, click ***Import***. *Result:* The ***Import*** dialog box opens.
2	Locate the zip file with the column list to be imported and click ***Open***. *Result:* The ***Import*** message box opens, explaining what happens when the zip file is imported. 
3	Click ***Yes***. *Result:* The new list of predefined Column types is imported into the database.

2.8 Repair a UNICORN 7.5 installation

Introduction

This section describes how to repair a UNICORN 7.5 installation using the installation programs.

Note: *When repairing a UNICORN installation with a local database, it is irecommended to always take a backup of the database and save the backup somewhere else than in the regular backup folder.*

Repair the installation

Follow the instructions to repair the UNICORN 7.5 client, the UNICORN Common Components, and the UNICORN Database installations:

If you want to repair...	Then...
UNICORN 7.5 Client	1 Start UNICORN installation program. The program can be found in the UNICORN installation DVD. 2 *Result:* The UNICORN 7.5 Installation wizard opens with a welcome dialog box. 3 ***Tip:*** *If the DVD drive is not set up to allow automatic start, browse the DVD contents and double-click the file* ***Setup.exe*** *in the UNICORN folder to initiate the installation.* 4 Select ***Repair*** and click ***Next***. *Result:* The UNICORN client is repaired.
UNICORN 7.5 Common Components	1 Open the `UNICORN Common Components` folder on the UNICORN 7.5 installation DVD and double-click the file ***Setup.exe***. *Result:* The UNICORN Common Components InstallShield wizard opens. 2 Select ***Repair*** and click ***Next***. *Result:* The UNICORN Common Components software is repaired.

If you want to repair...	Then...
UNICORN 7.5 Database	1 Open the `UNICORN Database` folder on the UNICORN 7.5 installation DVD and double-click the file ***Setup.exe***. *Result:* The UNICORN 7.5 Database InstallShield wizard opens. 2 Select ***Repair*** and click ***Next***. *Result:* The UNICORN Database is repaired.

2.9 Printers

Printer for PDF

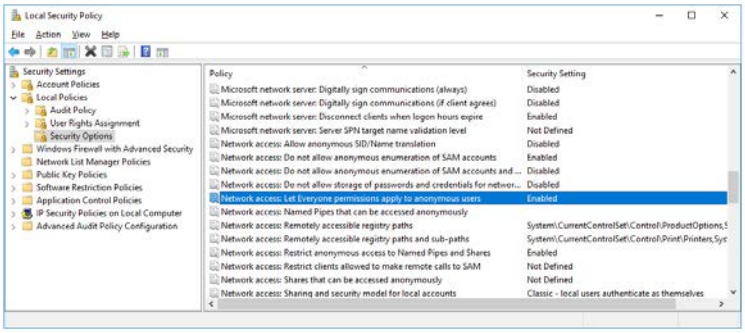
When printing reports, lists, and other items in UNICORN, use the printers that are defined in Windows for the client computer. The default Windows printer is always be shown as the first choice in the ***Print*** dialog boxes.

To save reports as PDF you must have a PDF printer installed on the computer where the report is printed. For this you need a full installation of Adobe™ Acrobat™ or a similar software.

Set up a system printer

For system generated prints you must define a default printer specifically for the instrument server computer. The table below describes how to do this.

Step	Action
1	Find the name of a suitable network printer that is accessible for the instrument server client station. • The name is available in the ***General*** tab of the printer properties. You can open the properties by right-clicking the printer in the ***Devices and Printers*** dialog box. This dialog box opens from the ***Control Panel*** in Windows. ***Note:*** *The printer must be a proper network printer with access for the **SYSTEM** user. All printers that are shared over the network are not necessarily work. Verify the status of the selected printer with the network administrator before you proceed with this instruction.*
2	Copy the printer name to the clipboard.

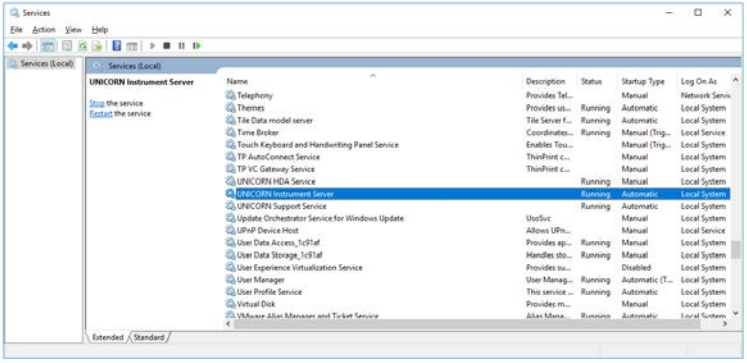
Step	Action
3	The printer setting is edited in the file `UNICORN Instrument Server.exe.config` located in the folder `\Program Files (x86)\GE Healthcare\UNICORN\UNICORN 7.5\bin`. ***Note:*** *The exact search path depends on the location of the UNICORN installation folder.* Locate the configuration file and open it in a text editor (e.g., Notepad). 
4	Locate the entry `<add key="SystemPrinterName" value="" />`
5	Place the mouse pointer between the last quotes in the line and paste the printer name there: • `<add key="SystemPrinterName" value="`**`Printer Name`**`" />`
6	Save the configuration file.
7	Restart the computer.

Note: *Do not make any other changes in this configuration file as this can cause severe performance problems for UNICORN. Errors in this file can make it impossible to run UNICORN at all.*

Set up a printer when running instrument server as non local system account

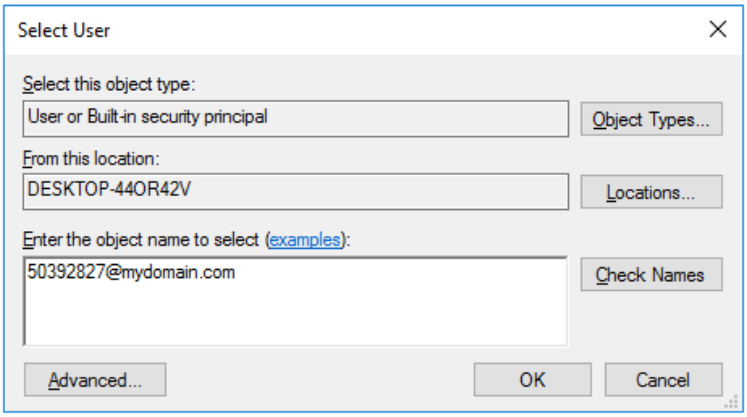
By default, the UNICORN instrument server runs as the local system account. The local system account does not have any access to network resources, i.e. printers. By having the UNICORN instrument server running as a Windows user with local administrative privileges it is possible to gain access to printers. Use an account with local administrative privileges when following the instructions below.

Step	Action
1	Type `Services` in Windows Start menu search field, click the ***Services*** item that is displayed as the search result. *Result:* ***Services*** opens.

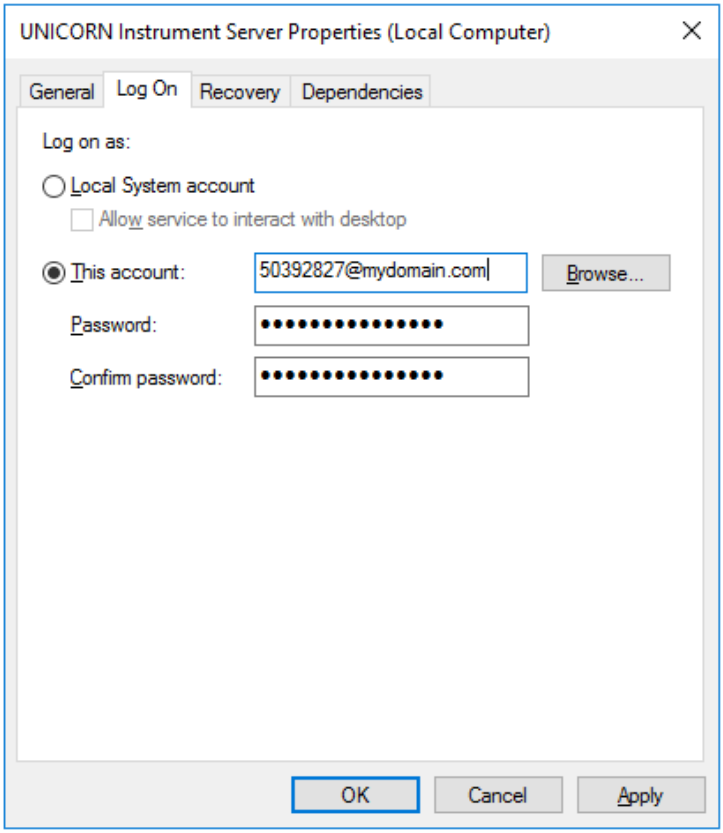


2	• Select ***UNICORN Instrument Server*** from the list. • Right-click and click ***Properties***. *Result:* The ***UNICORN Instrument Server Properties*** dialog box opens.
3	• Click the ***Log On*** tab. • Click ***This account***. • Click ***Browse***. *Result:* The ***Select User*** dialog box opens.

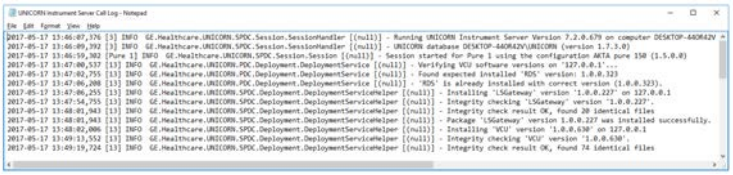
Step	Action
4	• Type in the Windows user name in the ***Enter the object name to select*** field. • Click ***Check Names*** to confirm that the user name is valid. • Click ***OK***.



Step	Action
5	In the ***Log On*** tab: • Enter the Windows user name password in the ***Password*** box. • Re-enter the password in the ***Confirm password*** box. • Click ***OK***. ***Note:*** *If the password is changed for the account running the UNICORN Instrument Server the password must be reset in this dialog box.*



6	Restart the computer.

Step	Action
7	• Open the file `UNICORN Instrument Server Call Log.txt` located in the folder `\Program Files (x86)\GE Healthcare\UNICORN\UNICORN 7.5\Logs\` • Locate the entry corresponding to `GE.Healthcare.UNICORN.SPDC.Session.SessionHandler [(null)] - Setting printer to HP Color LaserJet CP1215` as shown in the example below. 

2.10 Remove a UNICORN 7.5 installation

Introduction

This section describes how to remove a UNICORN 7.5 installation using the installation program. UNICORN can also be removed using the ***Uninstall a program*** Control panel item.

Note: *When removing a UNICORN installation with a local database, you are recommended to always take a backup of the database and save the backup safely, somewhere else than in the regular backup folder.*

Remove the installation

Follow the instructions to remove the UNICORN 7.5 software installation using the installation program:

Step	Action
1	Double-click the file ***Setup.exe*** in the UNICORN folder on the UNICORN DVD. *Result:* The UNICORN InstallShield wizard opens. Click ***Next***.
2	Click the ***Uninstallation*** tab in the ***UNICORN 7.5 Installer***. *Result:* The installed UNICORN software components are listed.
3	Select the check boxes of all the software components you want to remove and click ***Uninstall Selected Products***. *Result:* The ***UNICORN*** components are uninstalled.
4	When all components have been uninstalled the ***Restart computer*** dialog box opens. Click ***Yes*** to restart the computer and complete the uninstallation.

Note: *If the removal procedure is unable to access the database, an error message appears but it is still possible to proceed with the removal. Delete the remaining database components manually.*

Note: *The removal can fail in Windows due to insufficient privileges. In that case it can be helpful to turn off UAC temporarily.*

Remaining UNICORN objects after the installation is removed

After removing a UNICORN installation, some parts can still remain in the installation folder, for example logs. Database backups are also saved and not removed. These objects can be removed manually.

Removing additional software components

Some software components required to operate UNICORN cannot be removed automatically by the installation wizard. This is because the same components can be used for other purposes as well as for UNICORN. The components can also have been updated after the original installation, and UNICORN can no longer determine that they were part of the installation package. If needed, the components listed below must be removed manually:

- Microsoft® .NET® Framework 4.7.2 Full
- Microsoft Core XML Services (MSXML) 6.0
- Microsoft Visual C++® 2008 Redistributable Package SP1
- Microsoft Visual C++ 2010 Redistributable Package SP1
- Microsoft Visual C++ 2012 Redistributable Package
- Microsoft Visual C++ 2013 Redistributable Package
- Microsoft Visual C++ 2015 Redistributable Package
- Microsoft Visual C++ 2017 Redistributable Package
- Microsoft SQL Server® 2017 Express (Only if the database is selected for installation)
- OPC Core Components Redistributable 106.0

Follow the instructions to remove the components manually.

Step	Action
1	Open the ***Windows Control Panel***.
2	Double-click the ***Programs and Features*** icon. Result: The ***Uninstall or change a program*** dialog box opens. All programs installed on the client computer are listed.
3	Select the software component from the list and click ***Uninstall***.
4	Follow the instructions on the appearing dialog boxes, until the software is removed.

3 Configure systems and set up users and licenses

About this chapter

This chapter describes the administration aspects of a UNICORN 7.5 installation, for example how to define systems and how to assign different access levels to the users. Finally, some administrative operations for the license server are described.

In this chapter

This chapter contains these sections:

3.1 System administration

About this section

This section describes mainly

- how to edit system properties
- how to maintain the ***Instrument Configurations***
- how to define systems (after installation)
- how to view, edit and export log files of the UNICORN system activity and
- how to edit the default system settings for selected instruments.

In this section

This section contains these subsections:

3.1.1 System properties

General guidelines

- System properties are used to define the instruments in a UNICORN installation. The system properties must be defined for each new instrument that is connected.
- The system properties depend on the Instrument Configuration that is used. The Instrument Configuration defines the instrument components that are available for selection in UNICORN.
- In a network installation, the system properties must be defined for each instrument in the network.
- It is possible to define the computer names that can make a system connection.

Note: *Access rights to a system are controlled at the user administration level, see* *Section 3.3.3 Access items, on page 152*.

The UNICORN computer name

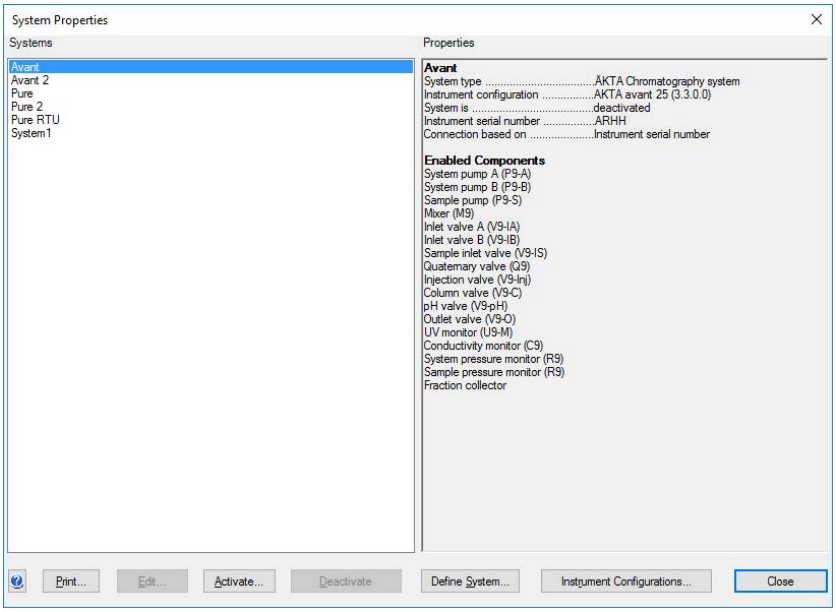
- The computer name in the UNICORN software *must* be the same as the Windows computer name. The Windows computer name is therefore automatically filled in as the UNICORN instrument server name when you define a new system.

  Note: *Not applicable for ReadyToProcess WAVE™ instruments.*
- Only common alphabetical letters (a-z) and numbers can be used for computer names.
- If an instrument server computer is changed for some reason, edit the corresponding system properties and change the computer name.

The System Properties dialog

System properties are shown in the ***System Properties*** dialog in the ***Administration*** module.

- Click ***System Properties*** on the ***Tools*** menu or click ***System Properties*** to open the dialog. See the following illustration:



Note: *To access this dialog, you must belong to an* ***Access Group*** *with* ***System Properties*** *access, see* *Section 3.3.3 Access items, on page 152*.

Possible actions

The following table describes the possible actions in the ***System Properties*** dialog.

If you want to...	then click
print the system properties for the selected system (described later in this topic)	***Print***
activate an inactivated system (described later in this topic)	***Activate***
deactivate a system (described later in this topic)	***Deactivate***

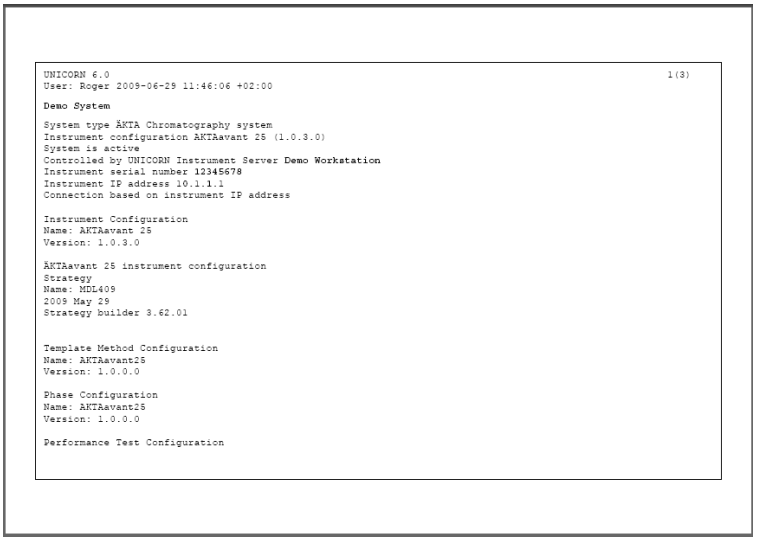
If you want to...	then click
edit system properties (see *Section 3.1.1.1 Edit System properties, on page 107* for details)	***Edit***
define a new system (see *Section 3.1.3 Define a new system, on page 115* for details)	***Define System***
view, import or delete instrument configurations (see *Section 3.1.2 Instrument Configurations, on page 112* for details)	***Instrument Configurations***

Print a system summary

It is possible to print a total summary of a selected system from the ***System Properties*** dialog.

Step	Action
1	• Select the system in the ***Systems*** list and • click ***Print***. *Result*: The ***Print*** dialog is displayed.

Step	Action
2	• Click a printer in the ***Printer*** list and • click ***OK***. *Result*: A summary report similar to the example below is printed by the selected printer:



```
UNICORN 6.0                                                    1(3)
User: Roger 2009-06-29 11:46:06 +02:00

Demo System

System type ÄKTA Chromatography system
Instrument configuration AKTAavant 25 (1.0.3.0)
System is active
Controlled by UNICORN Instrument Server Demo Workstation
Instrument serial number 12345678
Instrument IP address 10.1.1.1
Connection based on instrument IP address

Instrument Configuration
Name: AKTAavant 25
Version: 1.0.3.0

ÄKTAavant 25 instrument configuration
Strategy
Name: MDL409
2009 May 29
Strategy builder 3.62.01


Template Method Configuration
Name: AKTAavant25
Version: 1.0.0.0

Phase Configuration
Name: AKTAavant25
Version: 1.0.0.0

Performance Test Configuration
```

Tip:

Print the report in landscape format. Some parts of the report can be missing if the report is printed in portrait format.

Activate or deactivate systems

Once a system is defined in a UNICORN 7.5 database, it remains there and cannot be deleted or removed. However, the system can either be activated or deactivated.

Activated systems

A system must be activated to be available for use. To be activated, the system must include an assigned instrument server computer as well as the instrument.

When an instrument server is assigned to a system, it cannot be used to define another active system. The instrument server can only be connected to one instrument at a time. When activating a system, only unused instrument servers are available for selection.

Note: *If several database instances are in use, a system shall never be defined in more than one database instance. Doing so would make the system logs incomplete and might cause unresolvable conflicts.*

Note: *It is possible to define a deactivated system for an instrument server which already has an assigned, active system. This option is suggested if you try to define a new system when an active system is already defined. A new, inactivated system can be used for example when converting and scaling methods for use with another database than the one that it originally was created for. This is described in the UNICORN Method Manual.*

Deactivated systems

When an instrument is taken out of use, for example for maintenance or repair, the corresponding system must be deactivated in the ***System Properties*** dialog. The system remains in the list and it is connected to the identity of the instrument. It does longer have an assigned instrument server and is not available for use.

If an instrument server computer is taken out of use, the system can be edited and the instrument server computer name changed.

If an instrument is permanently taken out of use, the corresponding system must be deactivated. The system cannot be used for a replacement instrument.

The following steps describes how to deactivate and activate systems:

If you want to...	Then...
deactivate a system	• select the system in the ***Systems*** list • click ***Deactivate*** and • confirm that you want to deactivate the system. ***Result:*** A confirmation message is shown. You can now turn off the power to the instrument safely.

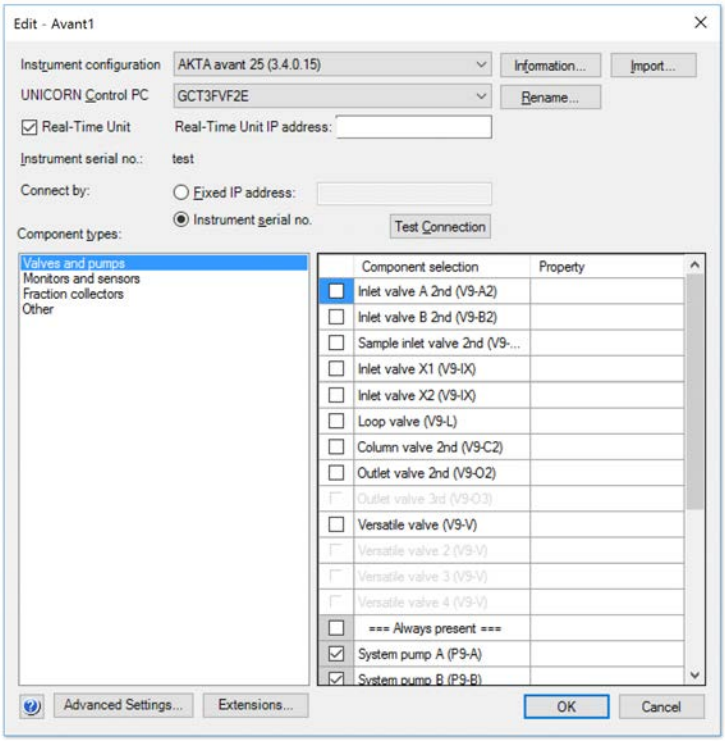
If you want to...	Then...
activate a system	• select the system in the ***Systems*** list and • click ***Activate***. *Result:* The ***Activate*** dialog opens. • Select the desired instrument configuration from the ***Instrument configuration*** list. • Select the desired server computer from the ***Instrument server*** list. and • click ***OK***. ***Result:*** A confirmation message is shown and the system is now activated.

3.1.1.1 Edit System properties

The Edit dialog

Follow the steps to open the Edit dialog where you can change the properties of a system:

Step	Action
1	Select a system in the ***System Properties*** dialog. ***Note:*** *Only active systems can be edited.*

Step	Action
2	Click ***Edit***. *Result*: The ***Edit*** dialog is displayed. This dialog is system specific. 

Set up instrument configuration and server connection

Step	Action
1	Click the desired instrument configuration in the ***Instrument configuration*** list. ***Tip:*** *Click **Information** for details about the configuration. Click **Import** to import a new configuration. This is described in Section 3.1.2 Instrument Configurations, on page 112.*

Step	Action
2	Click the desired server computer in the ***Instrument server*** list. Choose the connection type: • Click ***Fixed IP address*** or • Click ***Instrument serial no*** (This is explained in *Section 3.1.3 Define a new system, on page 115*)

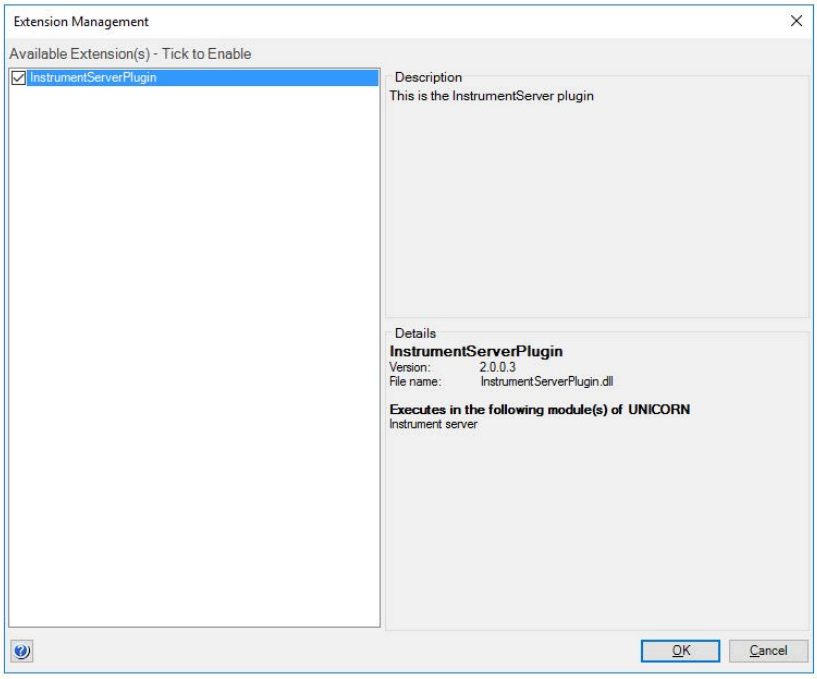
Set up instrument components

Step	Action
1	Click a ***Component type*** in the list. *Result:* All available components of this type are shown in the ***Component selection*** list.
2	• Select and clear the check boxes to select or de-select components. • When applicable, click the appropriate ***Property*** for a selected component. (e.g. position ***Before sample pump*** or ***After injection valve*** for ***Air sensor ext***)

Instrument server extension management

It is possible to enable and disable Instrument Server and UNICORN Support Service extensions for the selected instrument server. Extensions for other UNICORN modules are not listed here. Refer to *Chapter 6 Extension management, on page 197* for an introduction to UNICORN extensions.

- Click ***Extensions*** to open the instrument server ***Extension Management*** dialog.



Command or field	Description
Available extensions	The left pane lists installed instrument server or support service extensions. A selected check box before the extension name means that it is enabled for use on the selected instrument server. The upper right pane gives a short description of the selected extension. The lower right pane provides details about the extension, for example, name, version number and a list of UNICORN modules where the extension executes. This information is primarily intended for the local administrator of extensions.

Command or field	Description
Cancel	Click ***Cancel*** to close the dialog without saving changes to enabled or disabled extensions. ***Note:*** *Installation and uninstallation of extensions can not be cancelled by clicking* ***Cancel****.*
OK	Click ***OK*** to save changes to enabled or disabled extensions and close the dialog. ***Note:*** *You must restart the Instrument Server for your changes to UNICORN Instrument Server or Support Service extensions to take effect.*

Restrict system access

It is possible to restrict system access, and only allow connection from specified computers.

Step	Action
1	Click ***Advanced Settings*** in the ***System Properties*** dialog. *Result*: The ***Advanced Settings*** dialog is displayed.
2	• Click the ***Restrict System Access*** tab • Click ***Allow connections to the system only from the following computer(s)*** and • select computers to allow system access in the ***Computers:*** field. • Click ***OK***.

3.1.2 Instrument Configurations

Introduction

This section explains some of the concepts where the UNICORN 7.5 ***Instrument configurations*** differ from corresponding configurations used in UNICORN 5.

The section also describes how to import new ***Instrument Configurations***, with updated or customized instructions and phase libraries. Finally, it describes how to delete ***Instrument Configurations*** that are no longer in use and which are obsolete.

About Instrument Configurations

UNICORN is a common software platform for a number of different instrument types and configuration. In previous versions, the system-specific parts of the software were referred to as the ***Strategy***. The ***Strategy*** contains the definitions for all the instructions, settings and options relevant for a specific instrument version. For information about compatibility between UNICORN versions and the supported instrument configurations, see the UNICORN compatibility matrix at http://www.gelifesciences.com/UNICORNcompatibility.

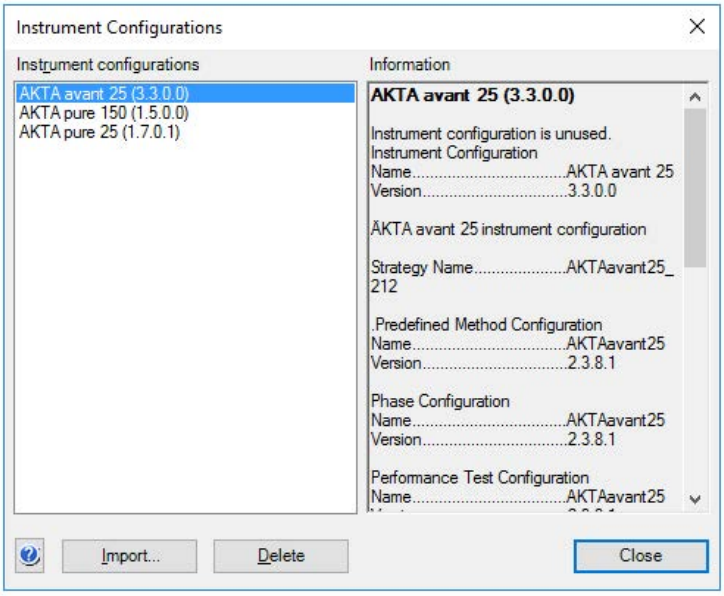
As a further development, UNICORN 6.0 introduced the ***Instrument Configuration***. This configuration includes a strategy but also other elements which are listed in the following able table:

Previous UNICORN instrument configurations	Instrument configuration for UNICORN 6.0	Description
Strategy	***Strategy***	The software instruction set which controls the instrument.
Process Picture	***Process Picture***	The graphic elements which are used to build the process pictures in the ***Method Editor*** and ***System Control*** modules.
	Phase Library	The phase library contains predefined phases and methods adapted to the available options for the specific instrument configuration.

Import an Instrument Configuration

The table below describes how to import an ***Instrument Configuration***

Step	Action
1	Click ***Instrument Configurations*** in the ***System Properties*** dialog. *Result:* The ***Instrument Configurations*** dialog opens.
2	Click ***Import***. *Result:* The ***Select Instrument Configuration Import Files*** dialog opens.
3	• Locate and select the import files (the files are stored in a .zip archive) • Click ***Open***. *Result:* The new configuration files are uploaded into the database and the configuration is available for selection. A progress dialog is displayed during this process.
4	Close the ***Instrument Configurations*** dialog and then click ***Edit*** in the ***System Properties*** dialog. *Result:* The ***Edit*** dialog opens.



Step	Action
5	Click the new configuration in the ***Instrument configuration*** list.
6	Click ***OK*** to apply the change and close the dialog.

Note: *Before using the new configuration, edit the system properties for each system and select the new instrument configuration.*

Delete an Instrument Configuration

The table below describes how to delete an obsolete ***Instrument Configuration***.

Note: *You cannot delete an* ***Instrument Configuration*** *that is in use.*

Step	Action
1	Click ***Instrument Configurations*** in the ***System Properties*** dialog. *Result:* The ***Instrument Configurations*** dialog opens.
2	• Select the obsolete ***Instrument Configuration*** and • click ***Delete***. ***Result:*** After you confirm the operation, the obsolete configuration is deleted from the database.

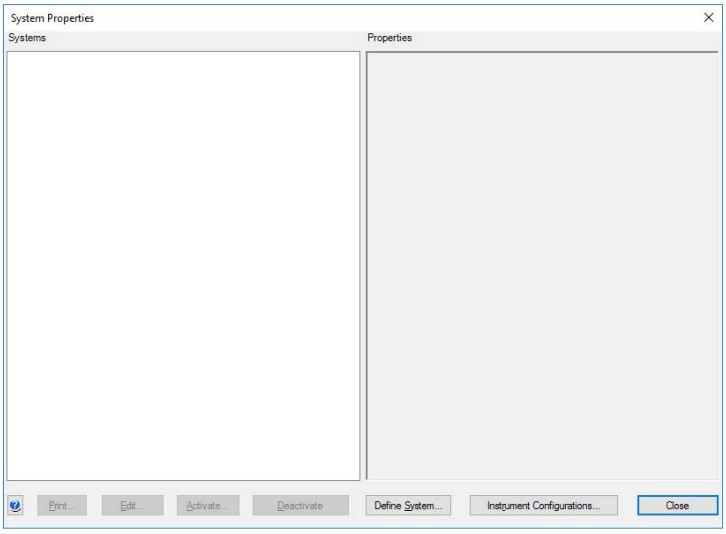
3.1.3 Define a new system

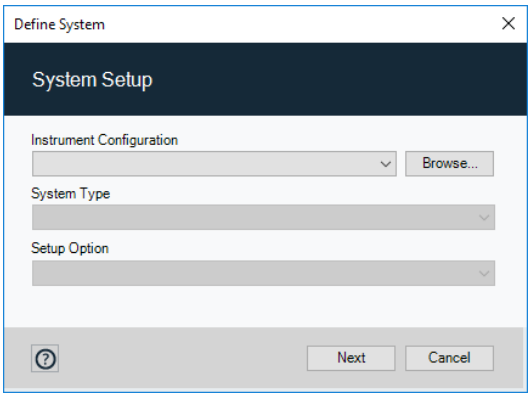
Introduction

If the system is not defined during the UNICORN installation, it is possible to define it from the ***System Properties*** dialog in the ***Administration*** module.

Note: *Only define one active system for each instrument server. If an instrument is replaced, the system must be deactivate in* ***System Properties*** *as described in* *Activate or deactivate systems, on page 105*.

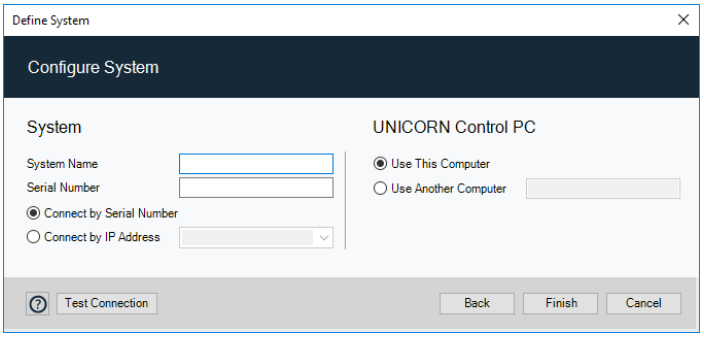
It is possible to define a deactivated system for an instrument server which has an assigned, active system. This option is suggested while defining a new system if there is an active defined system. A new, inactivated system can be used as an example when converting and scaling methods to use with another database. This is described in the UNICORN Method Manual.

Step	Action
1	 Click ***Define System***. Result: The ***Define System*** dialog box opens.

Step	Action
2	 In the ***Define System*** dialog box: Select the appropriate instrument configuration in the ***Instrument Configuration*** list. ***Note:*** *For information about compatibility between UNICORN versions and the supported instrument configurations, see the UNICORN compatibility matrix at http://www.gelifesciences.com/UNICORNcompatibility.* ***Tip:*** *The list includes all instrument configurations currently in the UNICORN database. To select a new instrument configuration:* • *Click **Browse** and navigate to the configuration file.* • *Select and import the appropriate configuration file.* Result: The ***System Type*** field is populated with available System and the ***Setup Option*** field is populated with related Communication setup options.
3	Select the appropriate System from the ***System Type*** field.
4	Select the appropriate Communication setup from the ***Setup Option*** field and click ***Next***. Result: The ***Configure System*** dialog box opens. ***Note:*** *The **Configure System** dialog box differs depending on the selections in the previous steps.*
5	Follow the related instructions in the following sections:

System with UNICORN Control PC

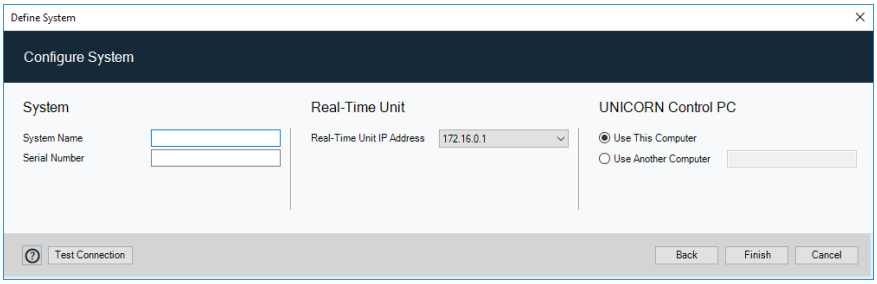
Follow these instructions if ***System with UNICORN Control PC*** is selected from the ***Setup Option*** field.



Step	Action
1	Enter a name in the ***System Name*** field. ***Note:*** *The system name cannot be changed once the system is defined.*
2	Enter the serial number for the instrument in the ***Serial Number*** field.
3	Select either ***Connect by Serial Number*** or ***Connect by IP Address***. If ***Connected by IP Address*** is selected, select the IP address from the list or enter the IP address manually.
4	Specify which computer to use as ***UNICORN Control PC***. To use as the ***UNICORN Control PC***, select either: • ***Use This Computer*** or • ***Use Another Computer*** and specify the name of that computer in the empty filed.
5	Click ***Finish*** to save and close the dialog box.

System with UNICORN Control PC and external Real-Time Unit

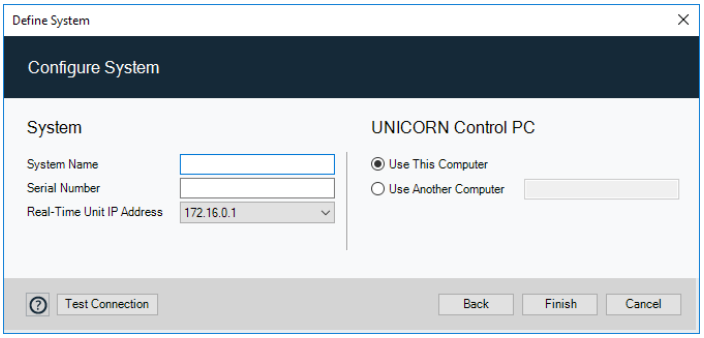
Follow these instruction if ***System with UNICORN Control PC and external Real-Time Unit*** is selected from the ***Setup Option*** field.



Step	Action
1	Enter a name in the ***System Name*** field. ***Note:*** *The system name cannot be changed once the system is defined.*
2	Enter the serial number for the instrument in the ***Serial Number*** field.
3	Select the ***Real-Time Unit IP Address*** from the drop-down list.
4	Specify which computer to use as ***UNICORN Control PC***. To use as the ***UNICORN Control PC***, select either: • ***Use This Computer*** or • ***Use Another Computer*** and specify the name in that computer in the empty filed.
5	Click ***Finish*** to save and close the dialog box.

System with UNICORN Control PC and internal Real-Time Unit

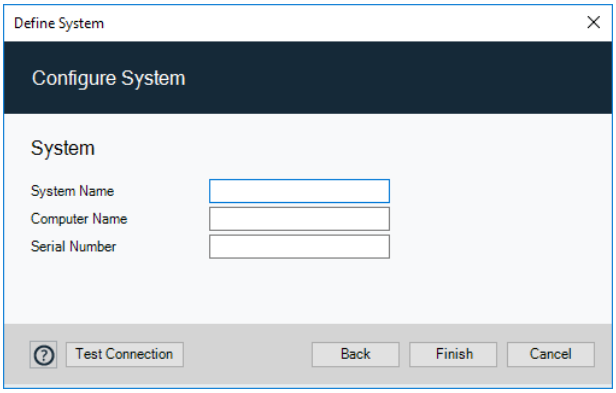
Follow these instructions if ***System with UNICORN Control PC and internal Real-Time Unit*** is selected from the ***Setup Option*** field.



Step	Action
1	Enter a name in the ***System Name*** field. ***Note:*** *The system name cannot be changed once the system is defined.*
2	Enter ***Serial Number*** .
3	Select ***Real-Time Unit IP Address*** from the drop-down list.
4 5	Specify which computer to use as *Instrument Server* under ***UNICORN Control PC***. To use as the *Instrument Server*, select either: • ***Use This Computer*** or • ***Use Another Computer*** and specify the name in that computer in the ***Name*** filed.
6	Click ***Finish*** to save and close the dialog box.

System with built-in UNICORN Instrument Server

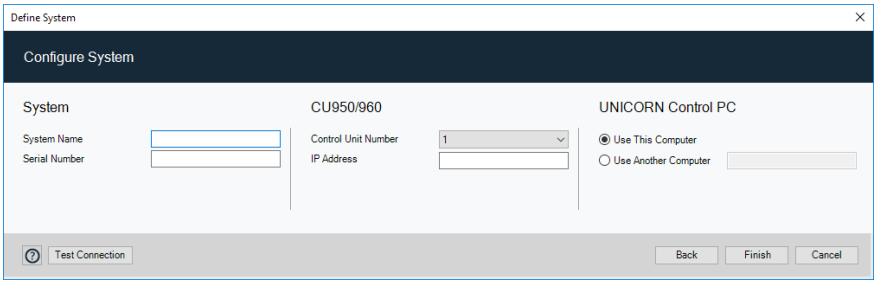
Follow these instructions if ***System with built-in UNICORN Instrument Server*** is selected from the ***Setup Option*** field.



Step	Action
1	Enter a name in the ***System Name*** field. ***Note:*** *The system name cannot be changed once the system is defined.*
2	Enter ***Computer Name*** .
3	Enter ***Serial Number***.
4	Click ***Finish*** to save and close the dialog box.

CU950/960

Follow these instructions if ***CU950/960*** is selected from the ***Setup Option*** field.



Step	Action
1	Enter a name in the ***System Name*** field. ***Note:*** *The system name cannot be changed once the system is defined.*
2	Enter ***Serial Number***.
3	Select the ***Control Unit Number***.
4	Enter the IP Address of the Control Unit.
5	Specify which computer to use as ***UNICORN Control PC***. To use as the ***UNICORN Control PC***, select either: • ***Use This Computer*** or • ***Use Another Computer*** and specify the name in that computer in the empty filed.

3.1.4 UNICORN and System logs

Purpose

The UNICORN, system, run and result related logs provide the system administrator with a full record of UNICORN usage and system activity.

The different types of logs

There are three types of logs:

- ***UNICORN logs***

  which record all system independent events,

- ***System logs***

  which record events related to specific systems

  and

- ***Run*** and ***Evaluation*** logs

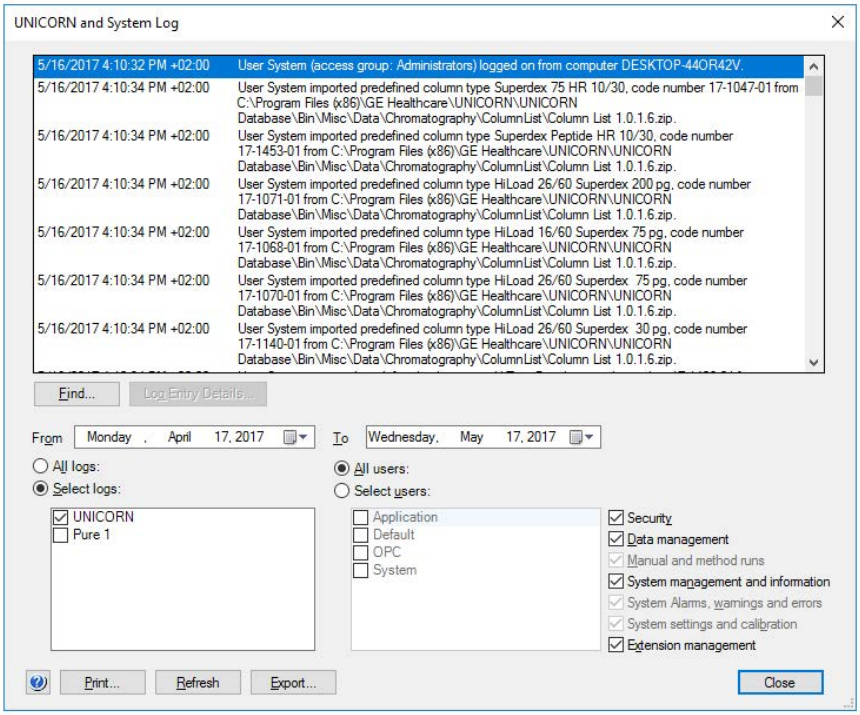
  which record events related to specific results. The ***Run*** log shows events from the run connected to the result, and the ***Evaluation*** log shows the evaluation actions that have been applied to the result.

The UNICORN and system logs are available in the UNICORN ***Administration*** module, by clicking the ***UNICORN and System Log*** icon.

The ***Run*** and ***Evaluation*** logs are available in the ***Documentation*** dialog. This dialog is opened from the ***Evaluation*** module.

UNICORN and System Log dialog

The ***UNICORN and System Log*** dialog is illustrated below.



Tip: *Click **Refresh** to update the displayed events to the latest records.*

View selected log entries

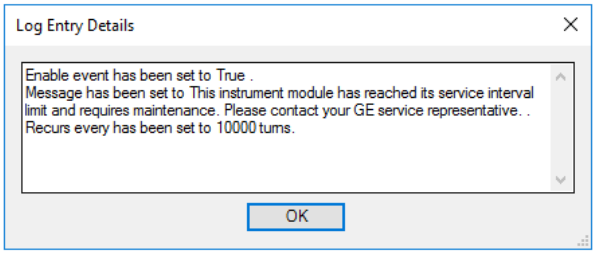
By default, the ***UNICORN and System Log*** dialog shows all log entries, for UNICORN, all systems and all users for a month before today's date. You can select specific log entries for display, to be able to view only the items of interest. You can also combine selections to narrow down the displayed items, for example to the log entries for a specific user at a specific system on a specific date.

The following table describes how to select specific log entries for display:

If you want to view log entries...	Then...
from a specific time period	• click the down arrow by the ***From*** field and select the starting date for the time period in the calender and • click the down arrow by the ***To*** field and select the ending date.
for specific systems	• click ***Select logs*** and • select one or several systems from the list below.
from the UNICORN log	• click ***Select logs*** and • select UNICORN from the list below.
for specific users	• click ***Select users*** and • select one or several users from the list below.
generated by the system	• click ***Select users*** and • select ***System*** from the list below.

If you want to view log entries...	Then...
for specific events	select one or several of the items below: • ***Security*** (log on/log off entries, password changes etc.) • ***Data management*** (folder, method and result activities, for example create, copy, changes etc.) • ***Manual and method runs*** (run start and end, created results etc.) • ***System management and information*** (connections, session start end end, create new, activate or deactivate systems etc.) • ***System Alarms, warnings and errors*** (alarm and error descriptions, acknowledgement and action records etc.) • ***System settings and calibration*** (changed settings and calibration actions) • ***Extension management*** (Extension related events)

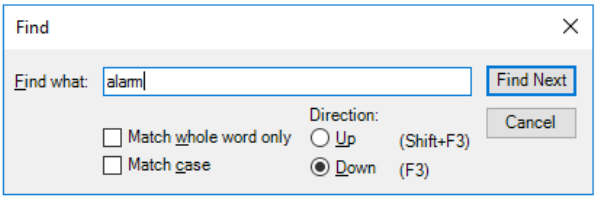
Long entries in the logs can sometimes be shown only in part, ending the entry with four period characters (i.e., ...). Select the entry and click ***Log Entry Details*** to view the remaining information. This button is enabled when the log entry is selected. The detail information is shown in a separate dialog:



Tip: *The complete entries are included in printed logs.*

Find specific log entries

You can search for specific log entry text by clicking the ***Find*** button and entering text to search for in the ***Find what*** field of the ***Find*** dialog:



Export logs

You can export the selected log entries to an XML file by clicking ***Export***. Using the XML file format, the log entries can be imported into XML-based reporting systems.

Archive logs

To reduce the size of the logs, you can choose to archive older records. The archiving procedure is part of the ***Database Management*** routines, and it is described in *Section 4.2.3 Archive data, on page 177*. If needed, retrieve the archived logs by using the ***Database Management*** retrieval procedure.

Note: *You can only retrieve logs to the same database that they were originally archived from. That is, you cannot use the retrieval procedure to import logs from one database to another.*

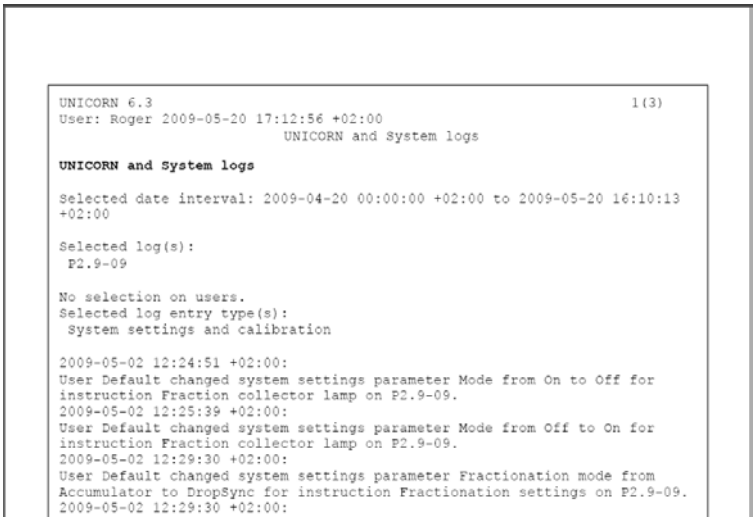
Note: *It is a recommendation that all archived logs are saved on a different hard drive than where the active database is stored.*

Print the logs

The following table describes how to print selected log entries:

Step	Action
1	Select the log entries you want to include in the print.
2	Click ***Print***. *Result*: The ***Print*** dialog opens

Step	Action
3	• Click a printer in the ***Printer*** list • If desired, click ***Properties*** and select printer settings and • Click ***OK***. *Result:* The selected log entries are printed.



```
UNICORN 6.3                                                    1(3)
User: Roger 2009-05-20 17:12:56 +02:00
                          UNICORN and System logs

UNICORN and System logs

Selected date interval: 2009-04-20 00:00:00 +02:00 to 2009-05-20 16:10:13
+02:00

Selected log(s):
 P2.9-09

No selection on users.
Selected log entry type(s):
 System settings and calibration

2009-05-02 12:24:51 +02:00:
User Default changed system settings parameter Mode from On to Off for
instruction Fraction collector lamp on P2.9-09.
2009-05-02 12:25:39 +02:00:
User Default changed system settings parameter Mode from Off to On for
instruction Fraction collector lamp on P2.9-09.
2009-05-02 12:29:30 +02:00:
User Default changed system settings parameter Fractionation mode from
Accumulator to DropSync for instruction Fractionation settings on P2.9-09.
2009-05-02 12:29:30 +02:00:
```

3.2 UNICORN User setup

About this section

Access to the UNICORN software is controlled by username and password authorization. This is done from within UNICORN, where each authorized user is assigned to an access group that determines which functions the user can perform. There are two types of users. The UNICORN users that are described in this section, and the network users that are described in *Section 3.3.2 Network users as members, on page 148*.

In this section

This section contains these subsections:

3.2.1 Create a new user

Introduction

This section describes how to create a new UNICORN user and assign user properties.

The Default user

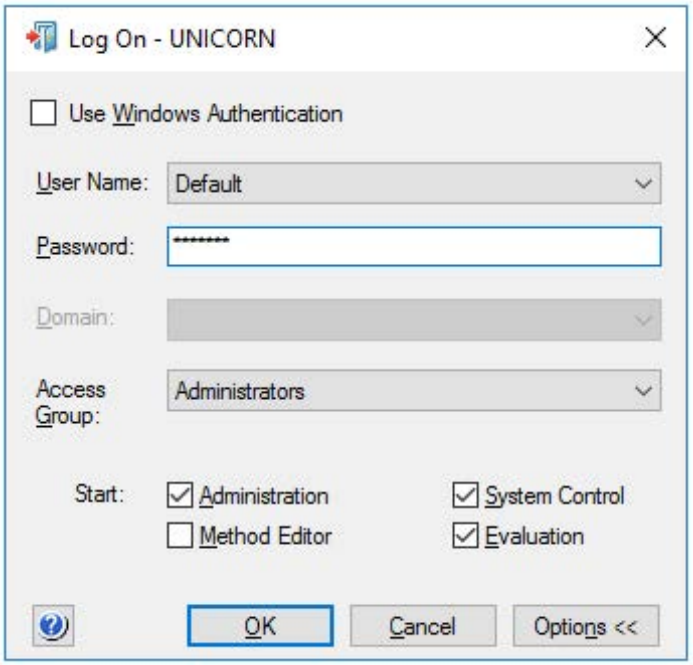
A ***Default*** user is created when the system is installed. The ***Default*** user is assigned to the ***Administrators*** access group with unrestricted access to all UNICORN functions. Log on with this profile to access a newly installed system.

Note: *The **Default** user must be deleted when regular user profiles have been created.*

The following table describes how to log on as the default user:

Step	Action
1	Start UNICORN.

Step	Action
2	• Click ***Default*** in the ***User name*** list.



- Type the password default.
- Click ***OK***.

Note:
*The **Default** user is the only user where the user name and the password can be identical.*

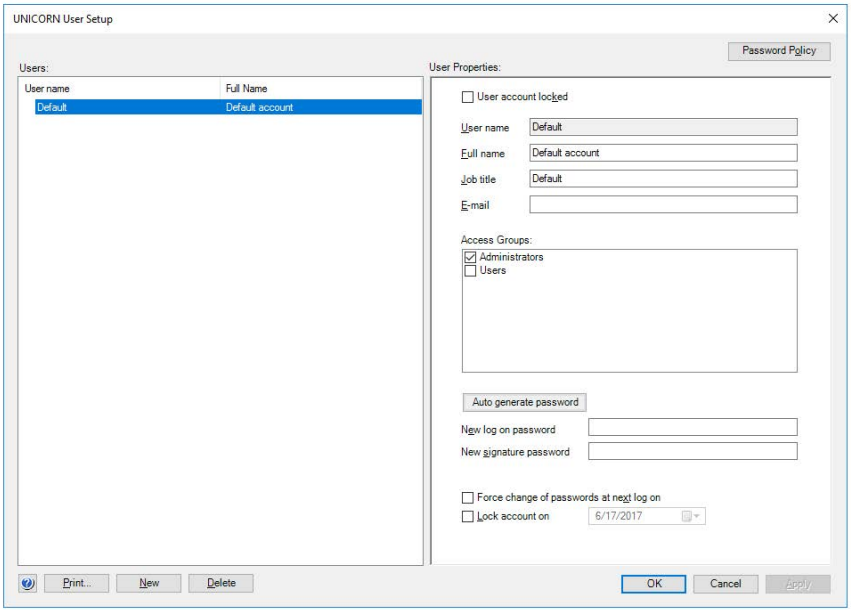
The User Setup dialog

All user administration is performed in the ***User Setup*** dialog in the ***Administration*** module. It is accessible only to authorized users (and the default user).

- On the ***Tools*** menu, click ***UNICORN User Setup***

  or

- click the ***UNICORN User Setup*** button in the ***Administration*** module to display the ***UNICORN User Setup*** dialog.



Instruction

The table below describes how to create a new user:

Step	Action
1	Click ***New*** in the ***User Setup*** dialog. *Result*: A ***New User*** is added to the ***Users*** list:
2	Enter information about the new user in the ***User Properties*** pane: • Type a user name in the ***User name*** field. • Type the full name of the user in the ***Full name*** field. • Type the job title of the user in the ***Job title*** field. • Type the e-mail address of the user in the ***E-mail*** field.
3	Select the ***Access Groups*** for the user. Refer to *Section 3.3 Access groups and network users, on page 143* for more information on how to set up access groups.

Step	Action
4	• Enter a ***New log on password*** *and* • To authorize an user to sign electronically, enter a ***New signature password*** Use the ***Auto generate password*** button to generate two passwords automatically. ***Note:*** *These password are used only the first time the user logs on. The user is asked to enter new passwords at that time.* ***Note:*** *The passwords are sent to the e-mail address set in a previous step.*
5	If desired, select the option to have the account locked on a certain date.

Save the new user entry

After all user settings are completed, you can either

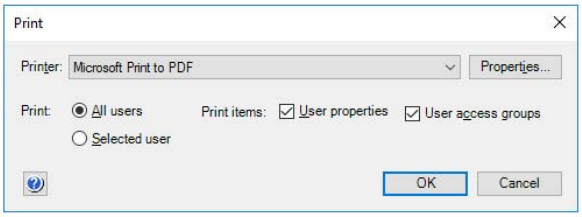
- Click ***Apply*** to save the entered settings and continue working in the ***User Setup*** dialog

  or

- Click ***OK*** to save the entered settings and close the dialog.

Print user settings

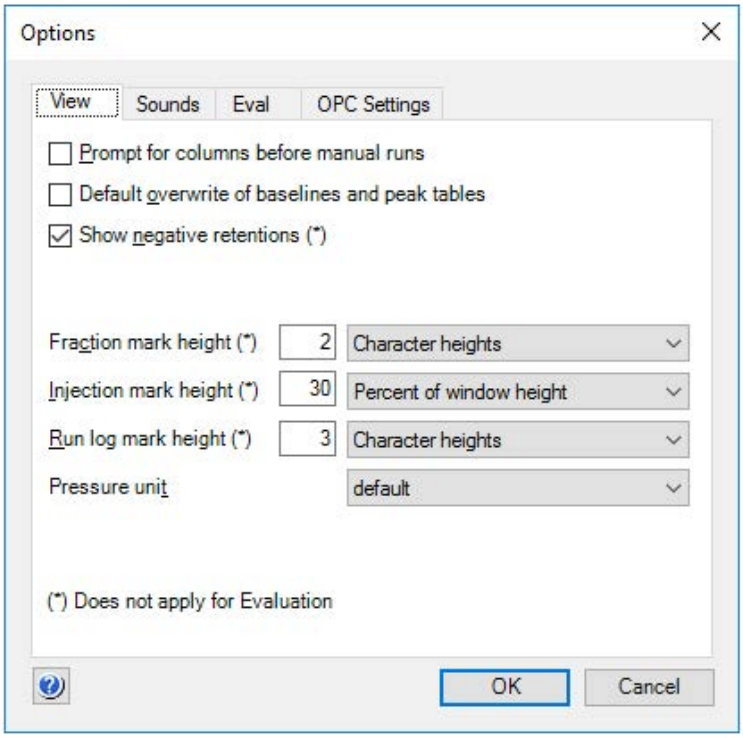
Click ***Print*** in the ***User Setup*** dialog to print a summary of the settings for a selected user or for all users. The items included in the summary can be selected in the Print dialog:



3.2.2 User options

Introduction

In the ***Options*** dialog, each logged in user can select preferred individual ***View***, ***Sound***, and ***Evaluation*** settings. The ***Options*** dialog is available under the ***Tools*** menu (where applicable). The changes are applied when the user logs on next time.



View options

The following table describes the ***View*** tab settings:

Command	Description
Default overwrite of baselines and peak tables	If this check box is selected, new baselines and peak tables are overwritten and the older baselines and peak tables are replaced. ***Note:*** *This only applies as default and the user can override this selection as needed.*
Show negative retentions	If this check box is selected, negative retentions are shown in the ***Evaluation Classic*** and ***System Control*** modules. This means that curve data before the injection point is displayed, that is before time or volume is zero. Clear this check box to hide curve data before the injection point. ***Note:*** *The data is still recorded although it is not shown when the result is displayed. The selection only applies as default and the user can change this selection as needed.*
Fraction mark height	The value in this field determines the height of the fraction marks in the ***Evaluation Classic*** and ***System Control*** modules. The height can be expressed as • ***Character heights*** • ***Percent of window height*** (This option allows to rescale the mark height when the window is resized) • ***Pixels*** ***Note:*** *The value in this field is not recalculated the expression is changed. For example, if it is changed from* ***Character heights*** *to* ***Percent of window height****, the value must be increased substantially to avoid that the marks are extremely small.*
Injection mark height	The value in this field determines the height of the injection marks in the ***Evaluation Classic*** and ***System Control*** modules. It is entered in the same manner as the ***Fraction mark height***.
Run log mark height	The value in this field determines the height of the run log marks in the ***Evaluation Classic*** and ***System Control*** modules. It is entered in the same manner as the ***Fraction mark height***.

Command	Description
Pressure unit	The selection determines the pressure unit thatis used in the results. The value can either be the default value determined by UNICORN or set to: • ***MPa*** • ***bar*** • ***psi***
OK	Click ***OK*** to apply the changes and close the dialog box.
Cancel	Click ***Cancel*** to close the dialog box without any changes.

Sounds options

The following table describes the ***Sounds*** tab settings:

Command	Description
System	Click the system you want to change sounds for in the list.
Play sound for	Click a sound in the corresponding list, to be played for • ***Alarms*** • ***Warnings*** • ***Errors*** • ***End of method*** ***Note:*** *The default settings for each instrument is **Classic**, which is the sound scheme used for older versions of UNICORN.*
OK	Click ***OK*** to apply the changes and close the dialog box.
Cancel	Click ***Cancel*** to close the dialog box without any changes.

Note: *The workstation computer must be equipped with a soundcard and suitable speakers to play the system sounds.*

Evaluation options

The following table describes the ***Evaluation*** tab settings:

Command	Description
Asymmetry Ratio at	Set the peak height value (in percent of the total peak height) where the ***Asymmetry Ratio*** is calculated.
Resolution Algorithm	There are three different algorithms available to determine the peak resolution. Click the algorithm you want to use in the list. By default, algorithm three is selected. ***Note:*** *Refer to the UNICORN Evaluation Manual for information about the* ***Resolution Algorithms***.
OK	Click ***OK*** to apply the changes and close the dialog box.
Cancel	Click ***Cancel*** to close the dialog box without any changes.
Show system default curves	Select this check box to show all system default curves when opening results in the ***Evaluation*** module.
Auto-integrate result	Select this check box to automatically integrate curves when opening results in the ***Evaluation*** module. ***Note:*** *This check box in selected by default*.

Default Layout

Some systems have the tab ***Default view*** in the ***Options*** dialog box. The table below describes the ***Default Layout*** tab settings:

Command	Description
Default Layout	Select a type of system to adapt the default view.
OK	Click ***OK*** to apply the changes and close the dialog box.
Cancel	Click ***Cancel*** to close the dialog box without any changes.

OPC Settings options

The table below describes the ***OPC Settings*** tab settings:

Command	Description
Logon required for HDA clients	Select this check box to set login requirement for OPC-HDA clients. ***Note:*** *An HDA client is used to access archived data.*
OK	Click ***OK*** to apply the changes and close the dialog box.
Cancel	Click ***Cancel*** to close the dialog box without any changes.

3.2.3 User passwords and account access limitations

Introduction

User password authentication for log on and electronic signatures is an important feature to ensure the security and integrity of the system. The general password policy is determined at the installation of the UNICORN server (or at a ***Full Installation*** of a stand-alone workstation).

This section describes

- how to change the password for a selected user
- how users change their own passwords
- how to lock accounts and limit user log on access to UNICORN
- how to set up administrator e-mail notifications for system messages.

The section also includes general rules and recommendations for UNICORN passwords.

Tip: *The use of passwords can be enabled or disabled after the installation by using the **UNICORN Configuration Manager** tool. This tool is installed on the server computer.*

- *Type `UNICORN Configuration Manager` in the **Start** menu search field. Click the **UNICORN Configuration Manager** item that is displayed as the search result to start the tool.*

Note: *All password related features and settings are only applicable for UNICORN users, and not for Network users.*

Rules and recommendations for UNICORN passwords

The list below summarizes rules and recommendations for UNICORN passwords.

- The system can be set up to operate without required passwords.
- The following rules can be configured in ***Password Policy*** in ***UNICORN User Setup***:
  - minimum number of password characters,
  - upper case or lower case letter requirement,
  - one or two digits requirement,
  - allowed special characters,
  - begin and end with letter requirement.
- Passwords can be any combination of letters and digits conforming to the configured rules.

- Passwords are case sensitive.
- Avoid using obvious passwords.
- You cannot use the user name as password (except for the ***Default*** user).
- Expiration time for passwords is set in ***Password Policy*** in ***UNICORN User Setup***. However, it is recommended to change password regularly even if no password expiration time is set.

Change passwords for a selected user

A user who is in the ***Administrator*** access group (usually a system administrator) can change the passwords for any user.

The following table describes how to change the passwords for a selected user:

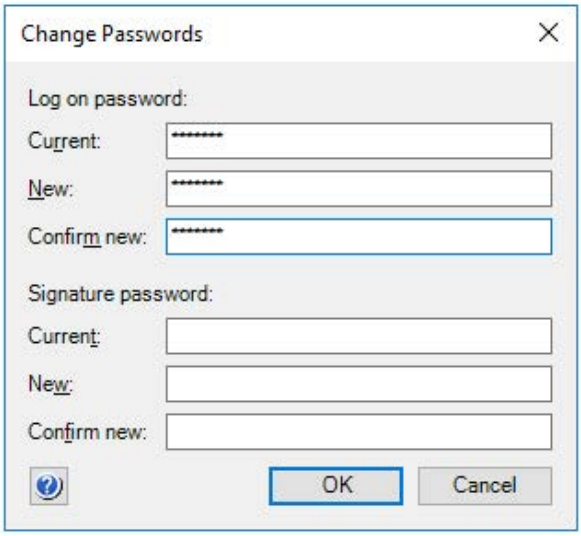
Step	Action
1	• On the ***Tools*** menu, click ***User Setup*** or • click the ***User Setup*** button in the ***Administration*** module. *Result*: The ***User Setup*** dialog is displayed.
2	Click the user in the list. *Result*: The ***User Properties*** tab is displayed for the selected user.
3	Type the new log on password in the ***New log on password*** and ***Confirm log on password*** fields. If desired, repeat this for the signature password. ***Note:*** *It is possible to auto generate passwords by pressing the* ***Auto generate password*** *button.*
4	• Click ***OK***. *Result:* At the next log on, the user must enter the log on password and then change to a new password.

Note: *If the general password settings are changed, for example if the required minimum password length is increased, it is important to set up a mandatory password change at the next log on for all users.*

How users change their own passwords

When passwords have expired, the user is required to enter new passwords during logon. The user can also choose to change passwords at other times. The following table describes how users can do this. This procedure is similar to how to change expired passwords during logon.

Step	Action
1	In any UNICORN module, on the ***Tools*** menu, click ***Change Passwords***. *Result*: The ***Change Passwords*** dialog box opens.



2	• Type the old log on password in the ***Current*** box under the ***Log on password*** heading. ***Note:*** *The passwords are only shown as asterisks.* • Type a new password in the ***New*** box. • Repeat the new password exactly in the ***Confirm new*** box.
3	To define a electronic signature password, repeat step 2 under the ***Signature password*** heading. ***Note:*** *The signature password cannot be the same as the log on password.*

Step	Action
4	Click ***OK***.

Locking user accounts

A user account can be locked for log on either by UNICORN based on a set expiration time, or manually by the system administrator. The user with a locked account does not have access to UNICORN until another user unlocks the account. This user must be assigned to an ***Access Group*** with ***User Setup*** access.

Note: *It is recommended that **User Setup** access is limited to administrators and similar user groups only, to avoid unauthorized user property changes, including the unlocking of locked accounts.*

The following table describes how to lock a user account from access.

If...	Then...
to lock the user account manually	select the ***User account locked*** check box in the ***User Properties*** for the user in question. *Result:* The user is unable to access UNICORN at the next logon.
to lock the account after a set time	• select the check box for ***Lock account on*** • click the down arrow by the date field and click a date in the pop-up calender. *Result:* The account is locked on the chosen date.

Tip: *It is possible to select a check box to have UNICORN generate an e-mail to a specified administrator mail address whenever a user account is locked. This check box is available only if a receiving mail address has been set up. See* *Section 3.5 E-mail Setup, on page 162*.

3.2.4 Delete users

Introduction

This section describes how to delete a user account.

Delete a user

The following table describes how to delete a user:

Step	Action
1	• On the ***Tools*** menu, click ***User Setup*** or • click the ***User Setup*** icon in the ***Administration*** module. *Result*: The ***User Setup*** dialog is displayed.
2	• Select the user from the ***Users*** list and click ***Delete***. *Result*: A confirmation dialog is displayed, asking you to verify that the user has no active runs, or no runs placed in a system queue, before the user account is deleted. • Click ***OK*** in the confirmation dialog, to confirm that the user can be deleted. ***Note:*** *You can delete all users except the last user with* ***User Setup*** *access. This ensures that at least one user has the right to perform administration functions.*
3	Click ***OK*** to close the ***User Setup*** dialog.

Note: *When you delete a user, the user's method and result files are not deleted.*

3.3 Access groups and network users

About this section

This section describes

- the purpose of access groups and access items
- how to view and edit access groups
- the purpose and setup of network users

In this section

This section contains these subsections:

Access group types

A UNICORN installation has different access groups with different rights to perform actions in the UNICORN system. Some access groups are predefined, for example the ***Administrators*** group. New access groups can be created as needed, and the access rights for each group can be edited to suit the duties for each user group.

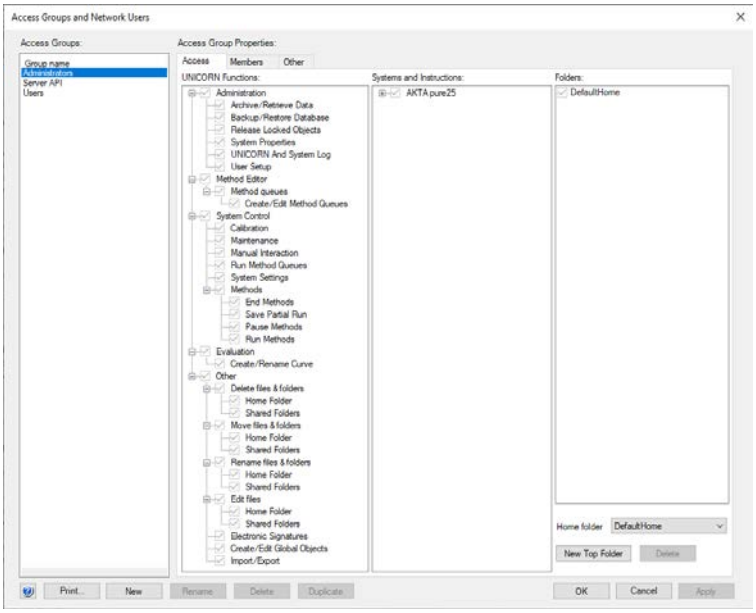
3.3.1 Access group setup and network users dialog

To view the access groups, you must have ***Administration*** module and ***User Setup*** access.

Access group properties

The following table describes how to view the properties of an access group:

Step	Action
1	On the ***Tools*** menu, click ***Access Groups and Network Users*** or click the ***Access Groups and Network Users*** button in the ***Administration*** module. *Result*: The ***Access Groups and Network Users*** dialog box is displayed.



2	Click a group in the ***Access Groups*** field to view the access items, the systems and instructions and the folders available to the selected access group on the ***Access*** tab. ***Note:*** *The access items that are valid for the group have selected checkboxes.*
3	Click the ***Members*** tab. All members that belong to the selected access group are listed in this tab.

Step	Action
4	Click the ***Other*** tab. The check boxes for ***Automatic UNICORN log off*** and ***Column protect mode*** are shown on this tab. Enter the number of minutes a user in the access group can stay inactive before being automatically logged off from UNICORN. Also, choose whether to activate the column protection mode. ***Note:*** • *If column protect mode is activated, a dialog opens before you start a manual run, requesting you to select the column pressure limits to be used for the run. This can be done either manually or by selecting the column type. If the column type is selected, the maximum values for pre-column pressure and Delta column pressure for that column type are set automatically.* • *If any method is open when being automatically logged off from UNICORN, the method is locked for editing by other users until it is released by a user with access item* ***Release Locked Objects*** *privileges. See* *Description of the access items, on page 152* *and* *Release locked objects, on page 186**.*

Edit or create new access groups

With UNICORN, you can create any number of access groups, all assigned to different levels of access to UNICORN. For practical reasons, it is recommended to only use a limited number of groups that correspond to the different job descriptions in your organization.

The following table describes how to create new or edit existing access groups:

Step	Action
1	On the ***Tools*** menu, click ***Access Groups and Network Users*** or click the ***Access Groups and Network Users*** button in the ***Administration*** module. *Result*: The ***Access Groups and Network Users*** dialog is displayed.

Step	Action
2	In the ***Access Groups and Network Users*** dialog you can perform the following actions:

Create a new group

- Click ***New***.

  Result: A group is added to the list, with the name `New user group`.

- Enter a new name and choose access items as described below.

Change the name of a group

- Select the group in the ***Access groups*** field of the dialog.
- Click ***Rename***.
- Type the new name over the original name.

  Note:

  You cannot change the name of a predefined access group.

Choose access items for a group

- Select the group in the ***Access groups*** field of the dialog.
- Select the checkboxes in the ***Access*** tab, to choose access items. See *Section 3.3.3 Access items, on page 152* for an explanation of the access items.

  Note:

  If the definition of an access group is edited, the changes apply to all users in the group.

Add members to a group

- Select the group in the ***Access groups*** field of the dialog.
- Click the ***Members*** tab.
- Click ***Add Members*** and add UNICORN users created in ***UNICORN User setup*** or network users (see *Section 3.3.2 Network users as members, on page 148*).

Choose folders for a group

- Select the group in the ***Access groups*** field of the dialog.
- Click the ***Access*** tab. Select the checkboxes of the folders that you want the selected access group to be able to use.
- In the list, click the folder to be the home folder for the access group.

Step	Action
	Delete a group • Select the group in the ***Access groups*** field of the dialog. • Click ***Delete***. • Confirm that you want to delete the group in the dialog that opens. ***Note:*** *You cannot delete the* ***Administrator*** *group.* **Duplicate a group** • Select the group in the ***Access groups*** field of the dialog. • Click ***Duplicate***. *Result:* A group is added to the list, with the name "New user group". • Enter a new name and choose access items as described above.
3	Click ***OK*** to apply the changes. ***Note:*** *Changes made to any currently logged on user, are applied after next logon to UNICORN.*

3.3.2 Network users as members

Introduction

UNICORN can be accessed by a user created in ***UNICORN User Setup***. It is also possible to give access to users in the network using LDAP (Lightweight Directory Access Protocol). By using Windows Authentication, a network user of an Access group can have the same username and password for UNICORN as for the network.

Add a new network user

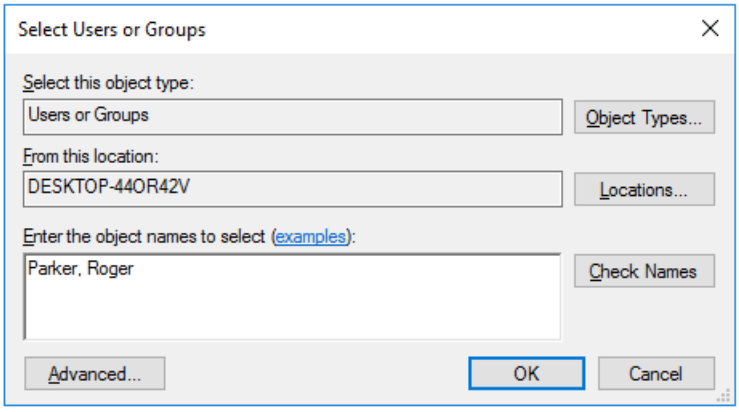
A network user added to an access group has the same available options as a user created in ***UNICORN User Setup***. It is possible to log in to UNICORN and to sign electronically with the network user ID and password.

The following table describes how to add a network user as a member to an access group:

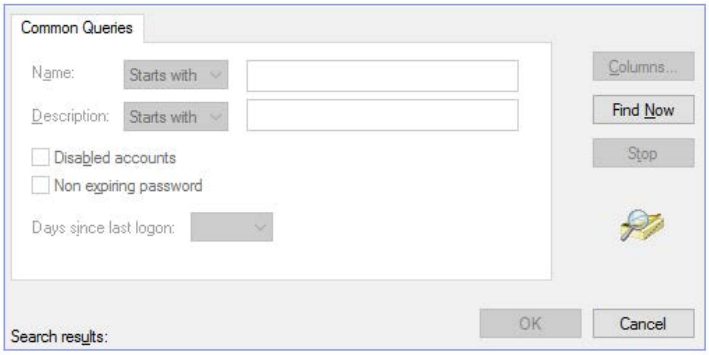
Step	Action
1	On the ***Tools*** menu, click ***Access Groups and Network Users*** or click the ***Access Groups and Network Users*** button in the ***Administration*** module. *Result*: The ***Access Groups and Network Users*** dialog is displayed.
2	In the left field, click the group to which the network user members shall be added and click the ***Members*** tab.

Step	Action
3	Click ***Add Members***, then click ***Network Members***.

Result: The ***Select Users or Groups*** dialog is displayed.

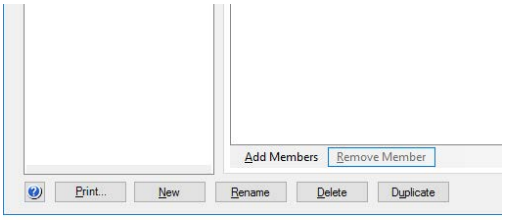
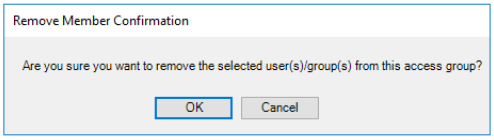


Step	Action
4	• Click ***Object Types*** to search for Groups or Users. • Click ***Locations*** to select which network location to search in. • Type in a user name or a user ID of the authorized network user you want to add as a member and click ***Check Names***. ***Note:*** *The name structure depends on how it is registered on the network. For example it can be Lastname, Firstname or Firstname Lastname. Contact the local IT department for support*. • To see more advanced search options, click ***Advanced***. Type, for example the name, in the search field and click ***Find Now***
5	When the correct user has been found, click ***OK***. ***Note:*** *If more than one user is found, select the correct one in the list*. *Result*: The selected user has now been added to the list of members in ***Access Groups and Network Users*** dialog.



Remove a network user

The following table describes how to remove a network user from an access group:

Step	Action
1	On the ***Tools*** menu, click ***Access Groups and Network Users*** or click the ***Access Groups and Network Users*** button in the ***Administration*** module. *Result*: The ***Access Groups and Network Users*** dialog is displayed.
2	Select the group in the left field from which the network user member shall be removed and select the ***Members*** tab.
3	• Click the member in the ***Members*** list. • Click ***Remove Member***.  *Result*: The ***Remove Member Confirmation*** dialog opens.  • Click ***OK*** to remove the member.

3.3.3 Access items

What is an access item?

An access item specifies an action that the user is allowed to perform in the UNICORN system. The access items are assigned to the user access groups in the ***Access Groups and Network Users*** dialog, see *Section 3.3 Access groups and network users, on page 143*.

To view the access items in the ***Administration*** module:

- On the ***Tools*** menu, click ***Access Groups and Network Users***
- or click the ***Access Groups and Network Users*** button in the ***Administration*** module.

  Result: The access items are listed in the ***Access*** tab.

Description of the access items

The following table describes each access item:

Access area	Access items in this area allow the user to
Administration	• archive and to retrieve archive data • backup a database and to restore backups • release data objects that have been locked by a user • edit system properties • access UNICORN and system logs • perform user setup
Method Editor	• create and edit method queues

Access area	Access items in this area allow the user to
System Control	• calibrate monitor settings • perform maintenance operations • run the system manually • run method queues • edit system settings • perform actions during method runs: - end methods - save partial runs [4] - pause methods - run methods
Evaluation	***Note:*** *This information only applies to the Evaluation Classic module.* • create and rename curves

4 By default, partial runs are saved. This access item allows the user to choose not to save a partial run if desired.

Access area	Access items in this area allow the user to
Other (general)	• Delete files and folders - in the user's own Home folder - in shared folders • Move files and folders - in the user's own Home folder - in shared folders • Rename files and folders - in the user's own Home folder - in shared folders • Edit files and folders - in the user's own Home folder - in shared folders • sign methods and results electronically • create and edit objects that are available to all users • import and export items, for example methods or results

Note: *A user group can have access to all items in any area, or only selected items. User groups with specific duties can only have access to a certain area and are unable to open or access the other UNICORN software modules.*

3.3.4 Folder access

An Access group must have access to a folder, for the users in the group to be able to copy, move, save or delete files in the folder. The Access group must also have read and write rights to shared folders, for the users to be able to perform these operations.

Home folders

General

Each Access group must be assigned to a home folder. This folder is a virtual storage for methods and results created for the group and not accessible for example by browsing the Windows folder structure. The home folder is valid only within the framework of the UNICORN database.

The home folder is always a ***Top Folder***. However, there can be any number of top folders that are for common use and not assigned as home folders for specific Access groups.

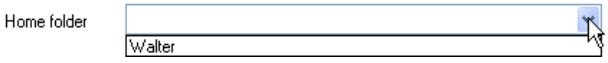
Top folders can only be created or deleted in the ***Access Groups and Network Users*** dialog box.

Subfolders to the home folder

Each Access group can have a number of subfolders within the home folder (and any other top folder to which the group has access) to arrange methods and results in a preferred, logical folder structure. This can be done by the user in ***Navigator*** panes in all UNICORN modules except the ***Administration*** module.

Select a Home folder

- Select the ***Access*** tab in the ***Access Groups and Network Users*** dialog.
- Click the droplist arrow in the ***Folders*** field to display a list of the folders that the group has access to:



- Select the home folder for the Access group.

Create a Home folder

- Select the ***Access*** tab in the ***Access Groups and Network Users*** dialog.
- Click ***New Top Folder*** in the ***Folders*** field.

Result: A folder called ***New Folder*** is added to the list.

- Type a new name over the ***New Folder*** text, for example the name of the Access group.
- Select the check box for the folder to make it accessible for the selected Access group.

Delete special folders

Any user with ***User Setup*** access can delete top folders. However, a home folder cannot be deleted if it is assigned to an active user. The conditions for deleting top folders are described below:

A common top folder which is not an assigned home folder.

To delete a top folder that is not a home folder

- ensure that the folder does not contain any object (deleting a folder with content is not allowed)
- select the folder in the ***Access*** tab of the ***Access Groups and Network Users*** dialog and
- click ***Delete***.

Note: *The **Delete** button is not available if the folder is assigned as home folder for an active user. It is not possible to delete an assigned home folder by mistake.*

A home folder to which an Access group is assigned

To delete a home folder to which an Access group is assigned

- re-assign another home folder to the group

  or

- delete the Access group first if this is the reason why the home folder is deleted.

See Edit Access Group for further information.

You can then proceed to delete the folder as any other top folder.

3.4 License server administration

Introduction

Access to UNICORN 7.5 is regulated by the number of valid e-licenses. A license is either node locked or floating. A node locked license can be used on one workstation only and a floating license can be used on any workstation in a network, however only on one workstation at the time.

The e-licenses are handled by the Software Licensing Server. Normally, the license authentication operates without any user interaction. However, in some cases it can be necessary to use the License Server Admin tool as described below.

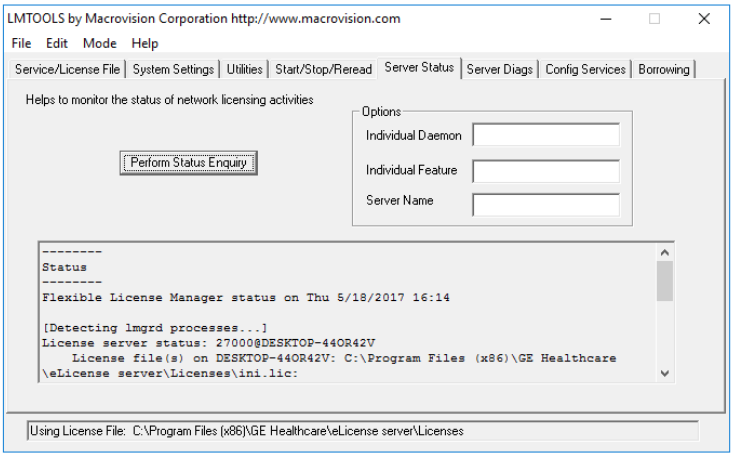
Note: *The Software Licensing Server is common for several e-licensed products from GE Healthcare. If other e-licensed products (for example DeCyder™) are already installed, the UNICORN 7.5 licenses are added to the previous installation*

Verify the number of active and available e-licenses

Follow the instruction to use the ***License Server Admin*** tool to identify the number of available licenses and determine how many that are in use.

Step	Action
1	Start the License ***Server Admin*** tool: enter `License server admin` in the ***Start*** menu search field, then Click the ***License Server Admin*** item that is displayed as the search result.
2	Click the ***Server Status*** tab.

Step	Action
3	Click ***Perform Status Enquiry***. *Result:* A status report similar to the illustration below is displayed:

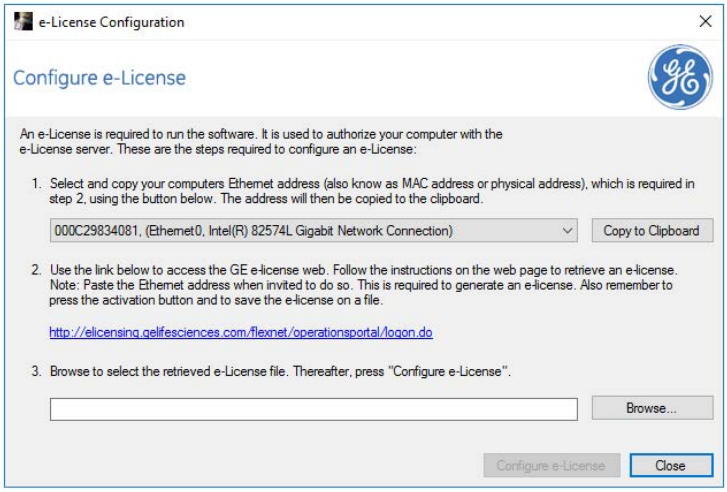


4	Read the total number of issued licenses and the number currently in use (in this case 20 licenses issued and 3 in use).

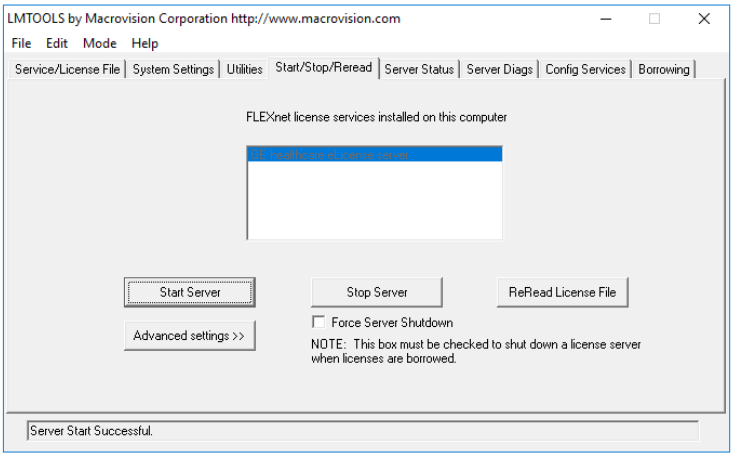
Note: *If several license servers are in use, you can enter the server name to view only the licenses for a specific server. If you want to view the information for a specific application only, you can enter that in the* ***Individual Feature*** *field.*

Add more e-licenses to the license server

The following table describes how to add more licenses to the license server.

Step	Action
1	Type `Configure e-License` in the ***Start*** menu search field, then click the ***Configure e-License*** item displayed as search result. *Result:* The ***e-License Configuration*** dialog box opens: 
2	Proceed to retrieve the added e-licenses as described in *Section 2.3.2 Configure an e-license, on page 39*. ***Note:*** *It is important that the Ethernet address of the license server computer is used, when the additional e-licenses are retrieved.*
3	Once the retrieval procedure is finished. Start the ***License Server Admin tool***: enter `License Server Admin` in the ***Start*** menu search field, then Click the ***License Server Admin*** item that is displayed as the search result.

Step	Action
4	Click the ***Start/Stop/Reread*** tab.



5	Click ***Stop Server***.
6	Click ***Start Server***. *Result:* The added licenses are registered and available for use.

Tip: *Restart the license server if no license is available. Restarting the sever enables the server to register the licenses again.*

Troubleshoot licensing problems

The table below describes how to use the Admin tool for a diagnosis when a license cannot be obtained.

Step	Action
1	Click the ***Server Diags*** tab.
2	Enter the feature name, eg. ***UNICORN_Login***, in the ***Feature Name*** field.
3	Click ***Perform Diagnostics***. *Result:* A list of the license files is displayed, showing the status and if the license(s) can be checked out.

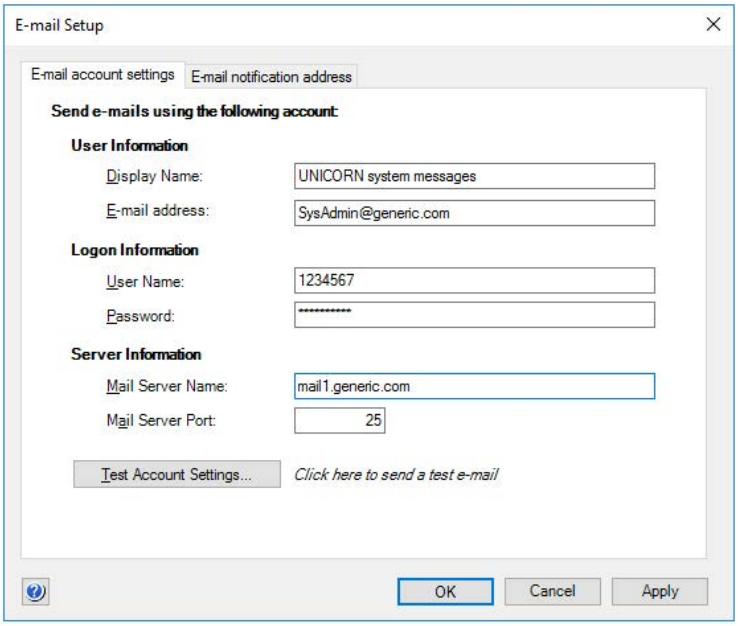
View license server debug logs

In case of problems when obtaining licenses, a debug log can be viewed by clicking the ***View Log*** button in the ***Config Services*** tab. This information can provide useful input to the GE Healthcare support staff.

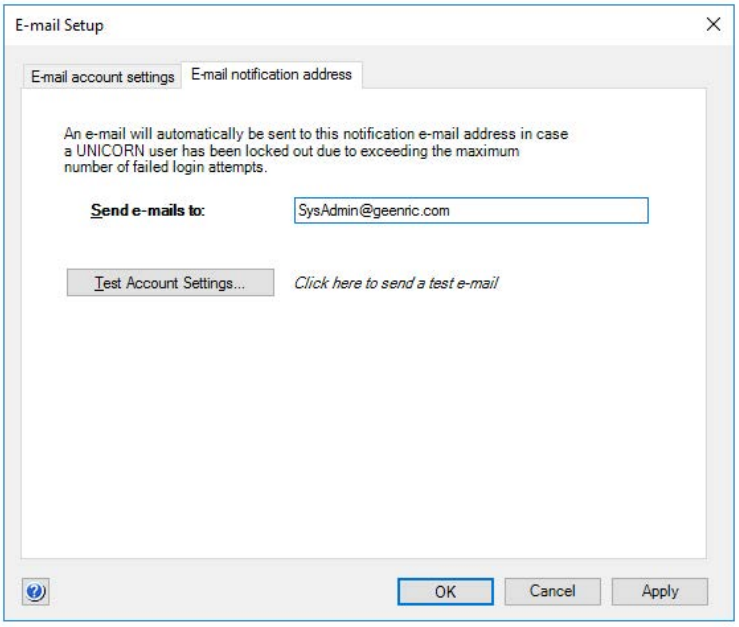
3.5 E-mail Setup

The following instruction describes how to set up an e-mail account for automated system messages.

Step	Action
1	• On the ***Tools*** menu, click ***E-mail Setup*** or • click the ***E-mail Setup*** button in the ***Administration*** module. *Result*: The ***E-mail Setup*** dialog box opens.
2	Click the ***E-mail account settings*** tab.



Step	Action
3	Enter the account settings for the e-mail account to be used to send the generated system messages. ***Note:*** *This is the e-mail address that for example sends an e-mail to a user when the password has been changed.* ***Tip:*** *Since the same account is used for all system messages regardless of the individual user, the most convenient solution can be to set up a common, specific account for this purpose.*
4	Click ***Test Account Settings*** to test the settings. *Result:* A test message is generated and sent. An error message is displayed if the settings are incorrect.
5	Click the ***E-mail notification address*** tab. Enter the e-mail address for the mailbox that is monitored by the responsible system administrator in the ***Send e-mails to*** field. ***Note:*** *This is the e-mail address that receives an e-mail when a user account has been locked.*



Step	Action
6	Click ***Test Account Settings*** to test the settings. *Result:* A test message is generated and sent. An error message is displayed if the settings are incorrect.
7	Click ***OK*** to save changes and close the dialog box.

4 Database management

About this chapter

This chapter describes the standard database solution used for data storage and the maintenance procedures required to operate the database.

In this chapter

This chapter contains these sections.

4.1 Database overview

About the UNICORN 7.5 database

Data storage in UNICORN 7.5 is handled by a database. The database is a relational database and the querying language used for the retrieval, insertion, updating, deleting and general managing of the data is SQL (Structured Query Language).

The standard UNICORN 7.5 database server installation, both for a dedicated server in a network environment and a stand-alone workstation, includes the distributable version of Microsoft SQL Server 2017 Express. It is described in *SQL Server 2017 Express, on page 166*.

The installation and basic set up of the database is an integrated part of the installation sequence for the options including the database server functions. It does not require any user settings other than the initial selection of the option and selection of destination folders for backup and archives.

Normally, the database maintenance functions offered by UNICORN is sufficient for the UNICORN administrator. Using management tools such as SQL Server Management Studio is not necessary and also not recommended as any invalid change can corrupt the database.

It is also possible to use other existing databases. Ask your GE Healthcare representative for information regarding use of enterprise server databases with UNICORN.

SQL Server 2017 Express

The following list includes some facts about Microsoft SQL Server 2017 Express:

- Primarily suited for smaller-scale applications
- Up to 1 GB of server RAM can be utilized
- Utilizes one single physical CPU
- Operates databases up to 10 GB, excluding log files

4.2 Database maintenance

About this section

Once the database is installed and systems are running and producing data, it is essential that routines and schedules for the back up and archiving of data are established. This section describes how to perform these routines, and also how to import data from earlier UNICORN versions.

In this section

This section contains these subsections:

4.2.1 Database backup

Introduction

At the database server installation a target folder for the regular, scheduled backup was set up. By default, backups were also scheduled at the installation. The default backup settings are

- daily backup
- at 03:00 local time
- in the selected target folder
- with the last 14 recent backup files kept.

  (when additional files are saved, the oldest backup is deleted)

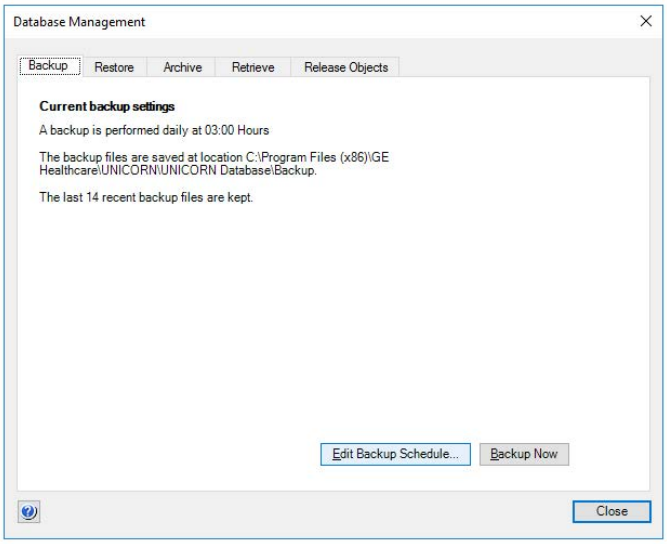
This section describes how to verify or edit the current backup schedule settings. It also describes how to perform manual backups between the scheduled backups.

Note: *It is recommended that the scheduled backups are stored on another physical drive than where the active database is stored. If this is not possible, it is recommended that the backup files are copied to another physical drive or storage media at regular intervals.*

Verify or edit the database backup schedule

The following table describes how to schedule the database backup:

Step	Action
1	Click the ***Database Management*** button in the ***Administration*** module. *Result:* The ***Database Management*** dialog opens.

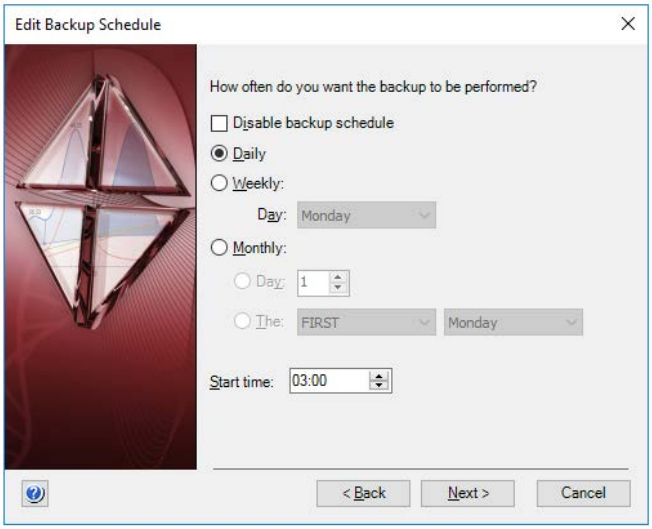


Tip:

*The **Backup** tab shows the current schedule. If the settings are suitable you can click **Close** at this point.*

2	Click ***Edit Backup Schedule***. *Result:* The ***Edit Backup Schedule Wizard*** opens.

Step	Action
3	Click ***Next*** to open the next wizard dialog:



4	Select the frequency and the start time for the scheduled backups. ***Note:*** *It is also possible to select **Disable backup schedule** at this point. For example, this is a necessary step before changing the SQL Server installation. After a new SQL Server edition is installed, the scheduled backups can be restored.* Click ***Next*** to proceed.
5	Choose the number of backup files to keep. ***Note:*** *It is possible to choose to keep all files. However, depending on the number of users and results that are created, this can cause uncontrolled disk space problems.* Click ***Next*** to proceed.
6	The final wizard page shows a summary of the selected settings. Click ***Finish*** to accept and apply the schedule. ***Note:*** *By default, he backup files are named as:* `UNICORN_SCHEDULED_BACKUP_<Date>_<Time>.BAK`.

Note: *It is recommended that another physical drive than where the active database is stored is selected for the scheduled backups at the installation of the UNICORN software. If this is not possible, it is recommended that the backup files are copied to another physical drive or storage media at regular intervals.*

Note: *Ensure that the database server computer is turned on at the time when the scheduled backup occurs. Otherwise, the backup fails and is not postponed. This is specially important for stand-alone workstations, which are generally turned off when not in use.*

Manual backups

If necessary, you can make extra backups manually between the scheduled backups. This is described in the following table.

Step	Action
1	Click the ***Database Management*** button in the ***Administration*** module. *Result:* The ***Database Management*** dialog opens.
2	Click the ***Backup*** tab, then click ***Backup Now***. *Result:* A ***Backup Now*** confirmation dialog opens.
3	Click ***OK*** to start the backup. ***Note:*** *This process can take several minutes. A progress dialog is displayed while the backup is performed.* *Result:* A ***Backup*** confirmation dialog opens when the backup is completed. By default, the backup file is named as: `UNICORN_MANUAL_BACKUP_<Date>_<Time>.BAK`.
4	Verify that the backup has been performed in the default folder and then either • click ***Close*** or • click ***Go To Backup File*** to open the backup folder and access the files. ***Note:*** *The backup folder is created by the program when performing a backup for the first time.*

Tip: *It is recommended that to either copy or move the backup files to an external storage device to minimize the risk for loss of data. The backup includes the UNICORN database content and a log report about the backup action.*

4.2.2 Restore backup data

Introduction

If necessary, restore data from a backup. The restored data replaces all the current data in the database with the data generated up to the point of time when the backup was made. All changes performed after the time of the backup are lost.

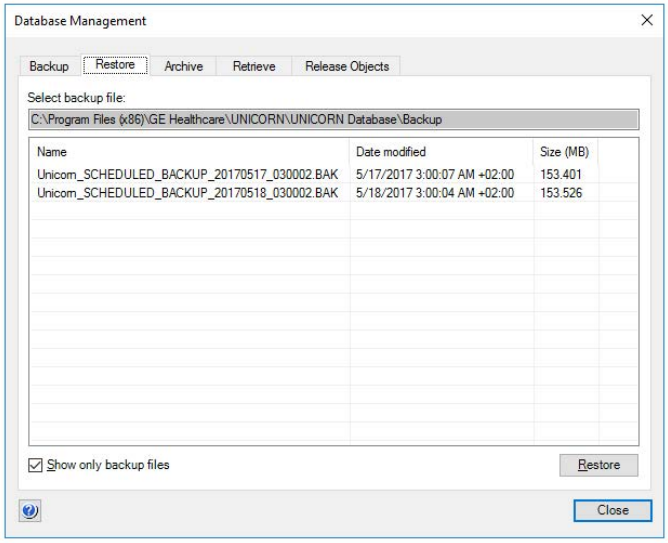
Perform this procedure to move data from one database instance to another but all data in the database instance where the backup is restored are overwritten.

Note: *A database backup from UNICORN versions earlier than UNICORN 7.5 can be restored and used in UNICORN 7.5. After the restoration, the database must be upgraded as described in* *Section 4.2.7 Upgrade database, on page 188**.*

Restore backup data

The following table describes how to restore backup data.

Step	Action
1	Click the ***Database Management*** button in the ***Administration*** module. *Result:* The ***Database Management*** dialog opens.
2	Click the ***Restore*** tab. All the available backup files are shown in the displayed list.



Note:

It is possible to select to show only backup files in the list. If this option is not selected, the backup log files are also become visible.

3	Select the backup file to restore and click ***Restore***. *Result:* A warning dialog opens. This dialog suggests to backup the database before restoring the previous backup. This ensures that all essential data is saved before it is replaced with the data from the backup.

Step	Action
4	Either • click ***Yes*** to backup before restoring or • click ***No*** to proceed without making a new backup. *Result:* A second warning dialog opens. This dialog shows the backup file to be restored and explains the implications for the current data. All other UNICORN modules are closed and no other actions can be performed during the restoration. ***Note:*** *All other client computers connected to this database instance must be logged off from UNICORN during the restoration.*
5	Click ***OK*** to proceed. *Result:* A progress dialog is displayed while the restoration is performed. The process is completed when the dialog closes.

Note: *The **Restore** operation resets the user **Default** in the **Administrator** user group, with the password* `default`*. To ensure access security, the user **Default** must be deleted again, after each restoration of backup data.*

Restore backup data to a new UNICORN installation

This scenario applies when trying to restore a UNICORN database in a new UNICORN installation. As part of moving data from one database instance to another, it is necessary to manually copy the database backup file to the new UNICORN installation backup folder.

Step	Action
1	Make a manual backup of the new database (even if the UNICORN database is empty) as described in *Manual backups, on page 171* *Result:* The target backup folder set at the database installation is created and a new backup file is created in the folder. ***Note:*** *The backup folder is created by the program when performing a backup for the first time.* ***Note:*** *A target folder for the regular, scheduled backup was set up at the database server installation. This can be changed later with the* ***UNICORN Configuration Manager*** *tool.*
2	Copy the database backup file you want to restore to the backup folder of the new UNICORN installation.
3	Restore the database as described in *Restore backup data, on page 174*

4.2.3 Archive data

Introduction

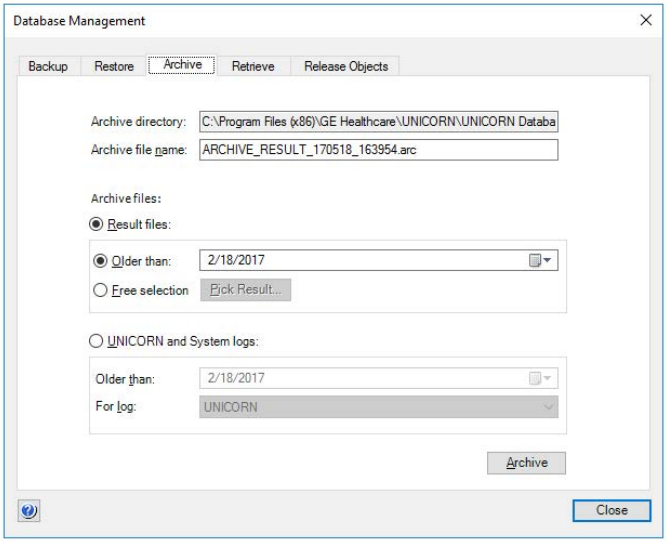
When your database size reaches a level where performance is affected and the remaining space is not enough for the immediate storage needs, you can archive selected parts of the result data. This can either be the entire result contents from before a specified date, or selected results. You can also archive logs. It is normally a good idea to archive data that is not immediately needed at regular intervals.

Archiving reduces the size of the database. It is not the same as exporting result data, which creates copies of the results but does not reduce the size of the database.

Archive data

The following table describes how to archive complete result data or logs:

Step	Action
1	Click the ***Database Management*** button in the ***Administration*** module. *Result:* The ***Database Management*** dialog opens.

Step	Action
2	Click the ***Archive*** tab. ***Note:*** *The **Archive** tab is hidden if the check box **Enable Archiving** is cleared in the **UNICORN Configuration Manager** tool. See Change installation settings, on page 267.*  The archive directory and a suggested archive file name are shown in the dialog. The directory was selected at the installation and cannot be edited here. The file name can be changed. The default name suggested by UNICORN includes the date of the archiving, and reflect if the selected contents are results or logs.

Step	Action
3	Choose the data to be archived: • If you click ***Result files*** - then click a date in the ***Older than*** list or - click ***Free selection*** and then click ***Pick Result***. (The ***Pick Result*** dialog is described in *Archive selected results, on page 179*) If you click ***UNICORN and System logs*** • click a date in the ***Older than*** list and then, • click the log to archive - UNICORN or a system log - in the ***For log*** list.
4	Click ***Archive***. *Result:* A warning dialog opens. This dialog suggest that you backup the database before archiving the selected data. ***Note:*** *It is recommended to always perform a backup before archiving.*
5	Either • click ***Yes*** to backup before restoring or • click ***No*** to proceed without making a new backup. *Result:* A progress dialog opens while the data is archived. Depending on the selections above, this can take several minutes. When the archiving is completed, a confirmation dialog opens.
6	Click ***Close*** to close the confirmation dialog.

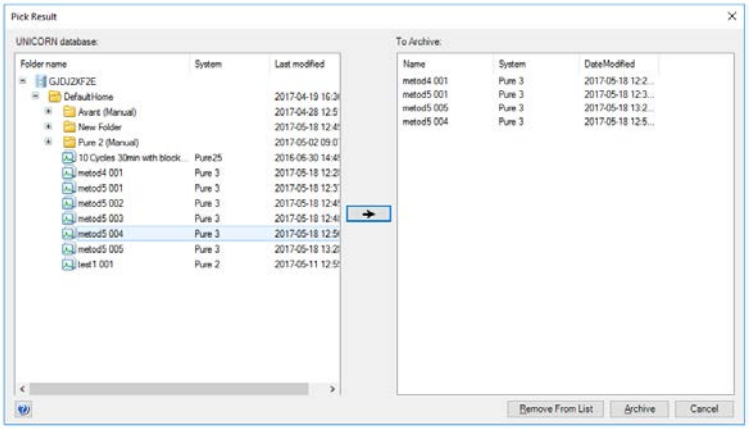
Note: *It is recommended to save the archived data on another storage media than where the active database is stored.*

Archive selected results

The following table describes how to select individual results for archiving:

Step	Action
1	In the ***Database Management*** dialog, click the ***Archive*** tab.

Step	Action
4	• Click ***Result files*** • Click ***Free selection*** and then • Click ***Pick Result***. *Result:* The ***Pick Result*** dialog opens.
5	In the ***Pick Result*** dialog: • Locate and select the result you want archive and • click the arrow button to add it to the ***To Archive*** list.
6	Repeat step 2 until you have added all results you wish to archive to the list. • You can remove results from the list by selecting them and clicking ***Remove From List*** button.
7	Click ***Archive***. *Result:* A warning dialog opens. This dialog suggest that you backup the database before archiving the selected data.



Step	Action
8	Either • click ***Yes*** to backup before restoring or • click ***No*** to proceed without making a new backup. *Result:* A progress dialog opens while the data is archived. Depending on the selections above, this can take several minutes. When the archiving is completed, a confirmation dialog opens.
9	Click ***Close*** to close the confirmation dialog.

4.2.4 Retrieve archived data

Introduction

Archived results and logs can be retrieved from the archive and be included in the active database. Individual results are selected from the archive directory, but not the entire archive. However when logs are retrieved, the entire log is restored.

Note: *This procedure can not be used to migrate data from one database to another. It is only possible to retrieve archived results and logs into the same database they are archived from.*

Tip: *In the new **Evaluation** module, the archived results are always listed under the **Results** tab.*

*In the **Evaluation Classic** module, the archived results can be shown in the **Result Navigator** by selecting the **Show All** option. This can help to locate the archived results. Archived results are represented by a special icon:*

*Right-click the archived result and click **Properties**.*

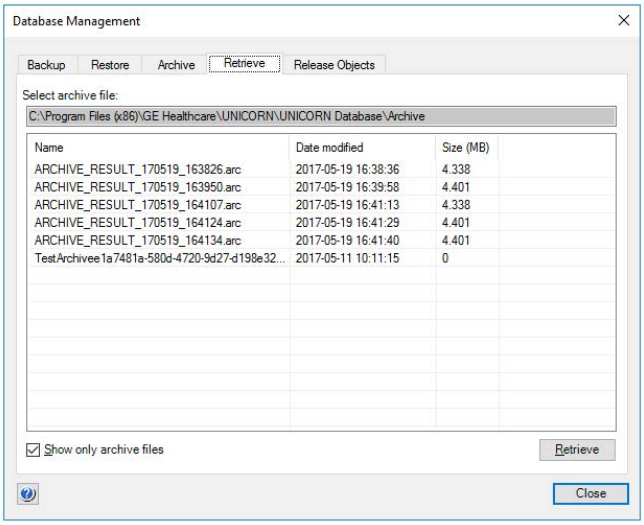
*Click the **Result** tab.*

*The **File Name** shown here is the name of the archive directory where you can find the archived result.*

Retrieve archived results or logs

The following table describes how to retrieve archived data:

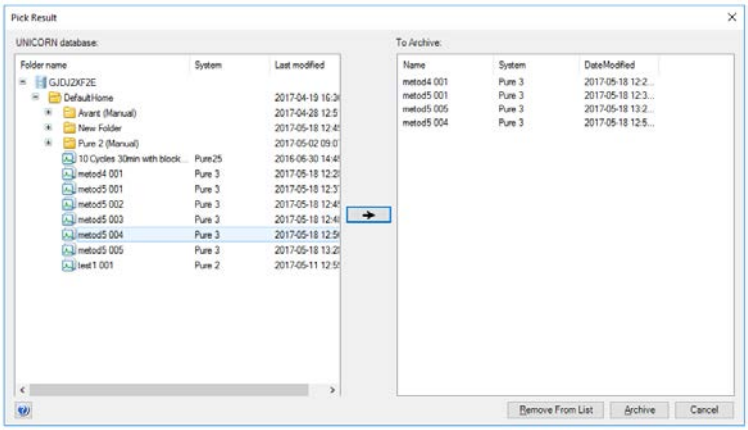
Step	Action
1	Click the ***Database Management*** button in the ***Administration*** module. *Result:* The ***Database Management*** dialog opens.
2	Click the ***Retrieve*** tab. ***Note:*** *The **Retrieve** tab is hidden if the check box **Enable Archiving** is cleared in the **UNICORN Configuration Manager** tool. See Change installation settings, on page 267.*



Note:

It is possible to retrieve either archived results or logs. All archived files have `.arc` format. These log files record the archiving operations and are not connected to the actual UNICORN results or logs.

Step	Action
3	Select the archive file you want to retrieve and click ***Retrieve***. If a log file is selected: • The log is restored to the active database and a confirmation dialog is shown. (This completes the retrieving process) If archived results are selected: • The ***Pick Result*** dialog opens.



4	Select an archived result in the ***Archive file*** list and click the right arrow button. *Result:* The result is moved to the ***UNICORN database*** list. The destination folder search path is shown in the list. You can remove selected results from the ***UNICORN database*** list by clicking the left arrow button.
5	Click ***Retrieve*** in the ***Pick Result*** dialog. *Result:* The results are restored to the active database and a confirmation dialog is shown.

Note: *The retrieved results are restored to the folder where they are originally archived from. All archived materials are saved in the archive.*

4.2.5 Release locked database objects

Introduction

Whenever a database object is opened in UNICORN, it is automatically locked by tge user and write protected from all other users. This applies to all objects such as methods, results, Design of Experiments etc. The automatic locking ensures that conflicting editing cannot be performed and saved simultaneously by several users.

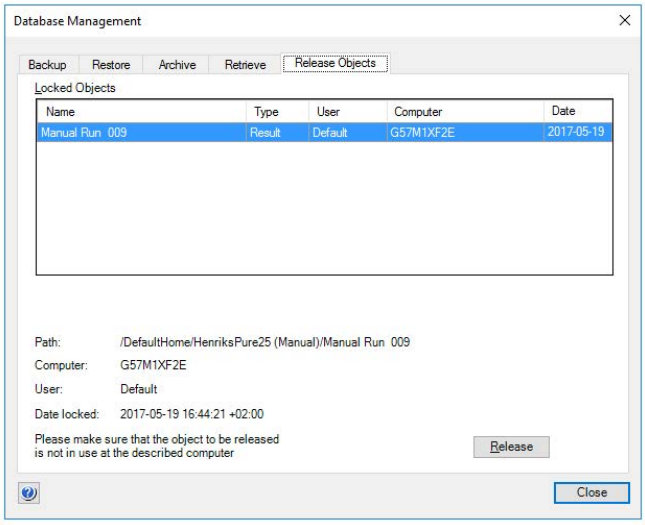
However, if objects are not closed and UNICORN is logged off in an improper manner, the locking can not be released. This can happen if UNICORN shuts down due to an error. In such cases, release the locked objects manually. This is described below.

Note: *Make sure that the released object is not in use at the computer listed in the dialog. Releasing an object that is actually in use can cause unexpected results.*

Release locked objects

The following table describes how to release locked database objects:

Step	Action
1	Click the ***Database Management*** button in the ***Administration*** module. *Result:* The ***Database Management*** dialog opens.
2	Click ***Release Objects***.



3	Select the object you want to release and click ***Release***. *Result:* The ***Release Objects*** warning dialog opens, asking if you have verified that the object is no longer in use by the listed user at the listed computer.
4	Click ***Yes*** to confirm. *Result:*The lock is released and a confirmation dialog opens.
5	Click ***OK*** to close the dialog.

4.2.6 Import data from UNICORN 5

Introduction

It is possible to import results and methods from UNICORN 5.11 and later.

Import from UNICORN 5 is available for results created with some CU based systems, for example, ÄKTApilot and ÄKTAprocess.

In versions of UNICORN earlier than 6.0, data was stored in a file structure and not in a database. Due to the differences in format, results and methods from these earlier versions cannot be used directly in UNICORN 7.5. When importing old methods and results, they are subsequently converted to the database format automatically.

Data migration from UNICORN 5

In order for the import to work the results must be valid for UNICORN 5. That is, the result must have been created in UNICORN 5.11 or subsequent versions and be able to be opened without errors.

It can be possible to import results from earlier versions if they are opened and saved in UNICORN 5 before the import. However, it is likely that more data is excluded than if the result was originally generated in UNICORN 5.

How to import results from UNICORN 5 is described in *UNICORN Evaluation Manual*.

How to import methods from UNICORN 5 is described in *UNICORN Method Manual*.

4.2.7 Upgrade database

Introduction

After an upgrade from UNICORN versions earlier than UNICORN 7.5 the UNICORN database instance must be upgraded to UNICORN 7.5 standard.

Database upgrade to UNICORN 7.5

Follow the instructions in the table to upgrade the database.

Step	Action
1	Start ***UNICORN Configuration Manager***: Click the ***Windows*** Start button, then type `UNICORN Configuration Manager` in the Start menu search field and then click the ***UNICORN Configuration Manager*** item that is displayed as the search result.
2	Log in with a user that belongs to the UNICORN administrators access group.
3	Click ***Yes*** to upgrade the database.
4	If you have upgraded from UNICORN 6.0 or 6.1 you must use ***UNICORN Configuration Manager*** to remove ***FILESTREAM*** and increase the size of the database to 10 GB.
5	When the database has been upgraded, close the ***UNICORN Configuration Manager***.

5 Security

About this chapter

This chapter presents the security concepts and features of a UNICORN installation. The concepts and features are good to know since they are also used in other parts of this manual.

In this chapter

This chapter contains these sections:

5.1 Access security

Purpose

The purpose of access security is to avoid unauthorized user access to the UNICORN system. UNICORN provides this functionality for local UNICORN users. For network users, the access security depends on the network.

Passwords to restrict access

User access is often restricted by means of a password. The following password rules apply:

- The password must have a minimum number of characters. The minimum length is set in UNICORN User Setup, see *Section 3.2.3 User passwords and account access limitations, on page 138*.
- The password must be changed regularly depending on the importance of the access security. See *Section 3.2.3 User passwords and account access limitations, on page 138*.

Access groups

Each user is assigned to an access group that defines the operations that the user can perform. The purpose of the access groups is to restrict access to sensitive functions in UNICORN for users without the necessary qualifications or areas of responsibility to operate these functions.

Access groups are described in *Section 3.3 Access groups and network users, on page 143*.

Delete default user

When you install UNICORN, a default user with full access rights is automatically created. For system security reasons the default user must be deleted when you have created the site-specific users.

Maintain system security

To maintain system security, it is recommended to allow only the system administrator to perform administrative routines such as user setup and system definitions.

5.2 Connection security

About this section

The purpose of connection security is to avoid conflicts regarding system control, so that only one user at a time controls the instrument.

Control mode and View mode connections

Two kinds of connection modes can be established with the UNICORN system:

- ***Control*** mode connection: The user has full system control, that is control of the instrument.
- ***View*** mode connection: The user can view the process but not control it.

To prevent conflicts, the system can have only one control mode connection at a time, that is only one user at a time can control the process.

Prevent unwanted system control

To prevent other users from establishing a control mode connection to the system, a user must establish a ***Control*** mode connection to the system.

Note: *If a user leaves the system in a **View** mode connection, any other user can establish a control mode connection to the system.*

It is also possible to define access rights, see *Section 3.3.1 Access group setup and network users dialog, on page 144*, and to enable system control from only one computer, see *Restrict system access, on page 111*.

When to maintain control over a system

It is recommended that control over systems are maintained when a user leaves the system temporarily. When the system is controlled, the responsible user is identified in the ***Connected Users*** dialog box. A system which is left with no ***Control*** mode connection has no identified responsible user.

5.3 Data security

About this section

Data security prevents the loss of results of a run due to failure in the network communication or the local station.

Network communication failure - remote station

If the network communication fails while a method is running, the remote station loses control of the system and the following happen:

- After 30 seconds, the remote station client is disconnected by the instrument server. The run continues under the control of the instrument server. No other connected client is affected.
- The remote station displays a message that it is disconnected. Try to reconnect after a minute and if that fails, check the condition of the general network connections.

Network communication failure - local station

The following table describes the scenarios when the network communication fails between a local station and the network.

Stage	Description
1	The local station is disconnected from the database server and other client stations, but the contact with the locally connected instrument is maintained. Any remote station that is connected to this instrument is disconnected automatically after 30 seconds.
2	The run on the connected instrument continues as normal. Result data is saved locally on the local station hard drive. If the local station tries to perform actions that require a database connection, an error message is displayed suggesting that UNICORN is restarted and a log on without database connection is performed.
3	If the network connection isn't restored when the run is completed, the result data is still saved locally pending a restored connection.

Stage	Description
4	When the network connection is restored and a user tries to assume control over the system, the user is asked if the temporarily stored result data should be uploaded into the database or discarded.

Local station failure

The table below describes what happens when the network communication fails between a local instrument server station and a non-CU based instrument, for example, ÄKTA avant.

Stage	Description
1	The run is terminated.
2	The result data is saved and the run log shows that the run was terminated before it was completed.
3	A message is displayed at all connected client stations requesting a restart of the instrument. ***Note:*** *You must be connected in control mode to be able to restart the system.*

Systems with CU-950/CU-960 Advanced controller

For a CU based system, for example, ÄKTApilot or ÄKTAprocess, the run continues and run data is stored in the CU memory until the connection is restored.

The list later in this topic describes what happens when all the following conditions are fulfilled:

- A CU-950/CU-960 Advanced controller (with a memory card) is used
- Data recovery = ***ON***
- Method behaviour = ***CONTINUE***
- The communication is lost between the local station and the CU-950/CU-960.

Stage	Description
1	• The run continues under the control of CU-950/CU-960 during the communication loss. • The run data is saved in the CU-950/CU-960 memory card.

Stage	Description
2	When the local station is up and running and the connection between the local station and the CU-950/CU-960 has been reestablished, • UNICORN uploads backup files from the hard drive of the local station • UNICORN requests the missing data from the CU-950/CU-960 • the missing data is uploaded to the local station • during the upload, a progress bar is shown in the ***System Control*** module. ***Note:*** *The **System Control** module is unresponsive until the upload is finished.*
3	The run continues as normal.

5.4 Prevent accidental shut-down

About this section

This section covers accidental shut-downs of instruments and built-in computers.

Accidental shut-down of an instrument

Instruments can be controlled without running the user interface modules. This is possible in the following cases:

- Network installation: If an instrument is controlled from a remote station without starting UNICORN on the local station.
- Stand-alone installation: If a user quits UNICORN after starting a run.

In both these cases, it is *not* apparent from the desktop that the UNICORN control software is actually running. Therefore there is a risk that someone shuts down the computer in the belief that it is not in use.

How to prevent accidental shut-down of an instrument

Make sure you follow the recommendations below to prevent an accidental shut-down of a control station (which controls an UNICORN run):

- Do not quit UNICORN if you are controlling a system.
- Do not turn off local station computers in a network installation.
- Start the UNICORN program on all local stations in a network installation, if possible, and establish a view mode connection as an indication that a connected system might be running.

Accidental shut-down of a built-in computer

Some instruments, for example, ÄKTAprocess and Customized BioProcess Solution systems, have built-in computers. The instrument power switch also cuts the power to the computer. Do not turn off the instrument power before shutting down the computer.

Following is the correct shutdown procedure.

Step	Action
1	In any UNICORN module, on the ***File*** menu click ***Exit UNICORN***.
2	Shut down the computer from the Windows ***Start*** menu.
3	When the computer screen has switched off, turn off the power switch on the instrument.

6 Extension management

About this chapter

This chapter presents UNICORN extensions and management of UNICORN extensions.

In this chapter

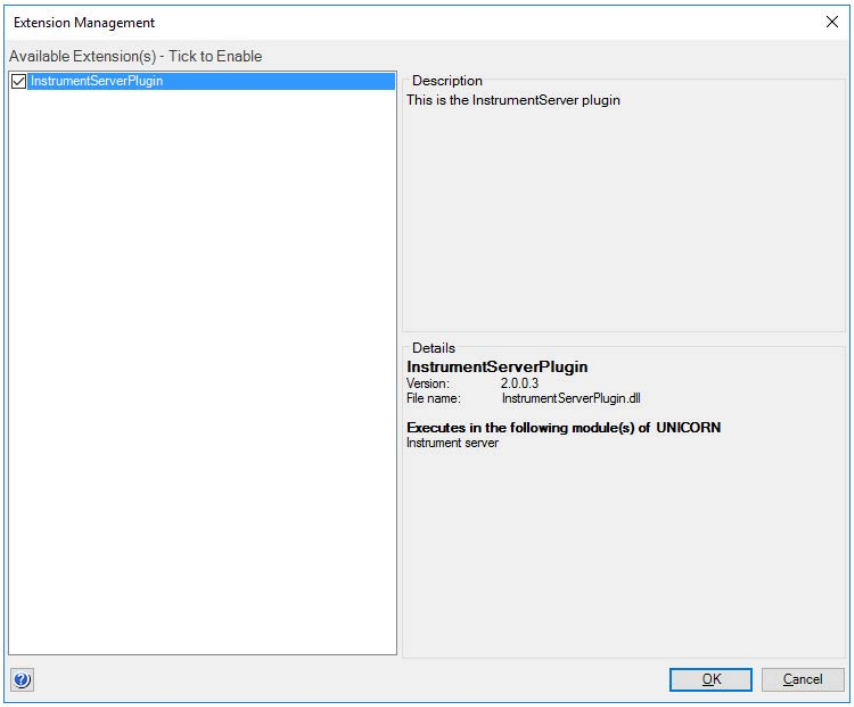
This chapter contains these sections:

6.1 Introduction to UNICORN extensions

UNICORN extensions are software packages that extends the capabilities of UNICORN. They are managed from the UNICORN ***Administration*** module. UNICORN Database extensions are installed in a UNICORN database and can be enabled or disabled for users of the local UNICORN client.

Extension Management dialog

In the ***Administration*** module, on the ***Tools*** menu, click ***Extension Management***.



Command or field	Description
Available extensions	The left pane lists installed database extensions. A selected check box before the extension name means that it is enabled for use on the local UNICORN client. The upper right pane gives a short description of the selected extension. The lower right pane provides details about the extension, for example, name, version number and a list of UNICORN modules where the extension executes. This information is primarily intended for the local administrator of extensions.
Install	Click ***Install*** to install an extension.
Uninstall	Click ***Uninstall*** to uninstall an extension.
Cancel	Click ***Cancel*** to close the dialog without saving changes to enabled or disabled extensions. ***Note:*** *Installation and uninstallation of extensions can not be cancelled by clicking* ***Cancel****.*
OK	Click ***OK*** to save changes to enabled or disabled extensions and close the dialog. ***Note:*** *You must logout from UNICORN and login again for your changes to UNICORN Database extensions to take effect.*

6.2 Installing and uninstalling UNICORN extensions

When installing a UNICORN extension, it is available for all users of the UNICORN database. Uninstalling a UNICORN extension makes it unavailable for all users of the UNICORN database.

Note: *The extension is disabled by default when installed. Select the check box in front of the extension name to enable the extension for users of the local UNICORN client.*

Tip: *If you want to disable an extension for users of the local UNICORN client only, clear the check box in front of the extension name.*

Installing an extension

The following steps describes how to install an extension in the UNICORN database.

Step	Action
1	In the ***Administration*** module, on the ***Tools*** menu, click ***Extension Management***. *Result:* The ***Extension Management*** dialog opens.
2	Click ***Install***. *Result:* The ***Install Extension*** dialog opens.
3	Browse to the location of the desired extension, select it and click ***Open***. *Result:* The ***Install Extension*** dialog closes and the extension is shown in the list of installed extensions. The UNICORN extension is now installed in the UNICORN database. ***Note:*** *The extension is disabled by default when installed. Tick the check box in front of the extension name to enable the extension for users of the local UNICORN client.*
4	Click ***OK*** to close the ***Extension Management*** dialog. ***Note:*** *You must logout from UNICORN and login again for the extension to be available in the corresponding UNICORN module(s).*

Uninstalling an extension

The following steps describes how to uninstall an extension.

Tip: *Uninstalling a UNICORN extension makes it unavailable for all users of the UNICORN database. If it is necessary to disable an extension for users of the local UNICORN client only, clear the check box in front of the extension name.*

Step	Action
1	In the ***Administration*** module, on the ***Tools*** menu, click ***Extension Management***. *Result:* The ***Extension Management*** dialog opens.
2	Select the extension you want to uninstall from the list of installed extensions, then click ***Uninstall***. *Result:* The ***Uninstall Extension*** dialog opens.
3	Click ***Yes*** to uninstall the extension from the UNICORN database. Click ***No*** to keep the extension in the list of installed extensions.
4	Click ***OK*** to close the ***Extension Management*** dialog. ***Note:*** *The extension is now uninstalled from the database and can not be used. However, you must logout from UNICORN and login again for the extension to be removed from the user interface of the corresponding UNICORN module(s).*

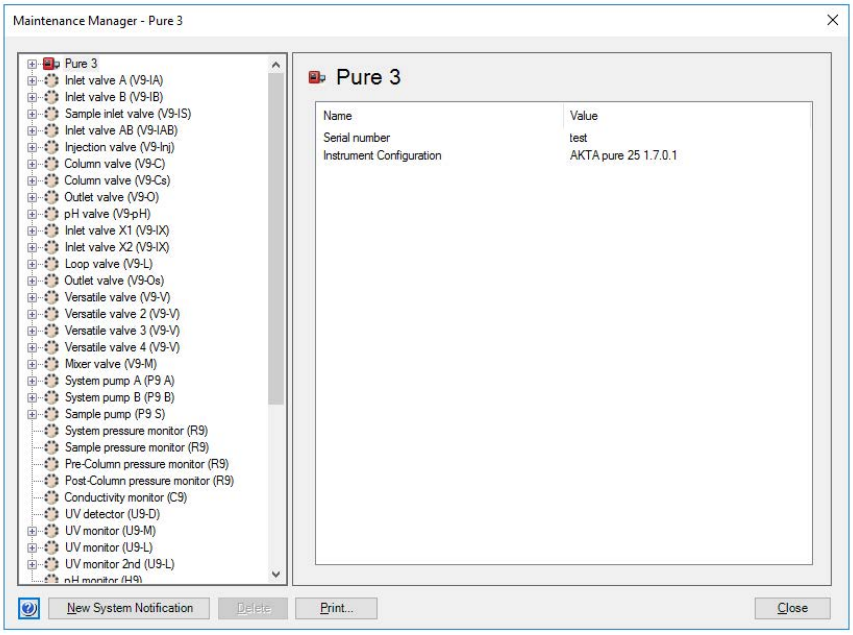
7 Maintenance Manager

Introduction

Maintenance Manager allows the user to display general information about the system and its modules, and also operational statistics of the modules. Notifications for maintenance actions of the system and its modules are predefined. The user can add automated maintenance notifications for the system. Maintenance notifications are based on calender periods of system use, and for some systems also on operational statistics for the modules.

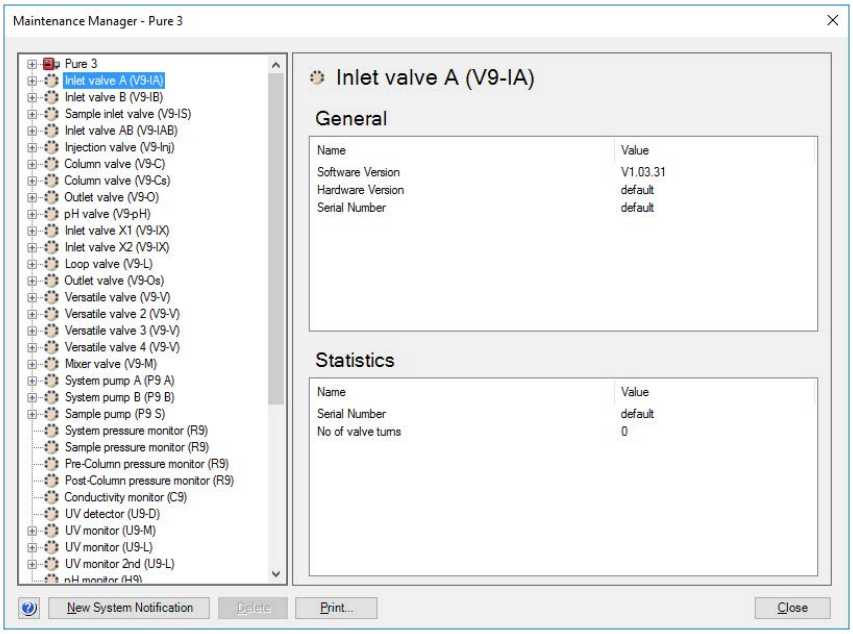
Open Maintenance Manager

In the ***System Control*** module, on the ***System*** menu, click ***Maintenance Manager*** to open the ***Maintenance Manager*** dialog box.



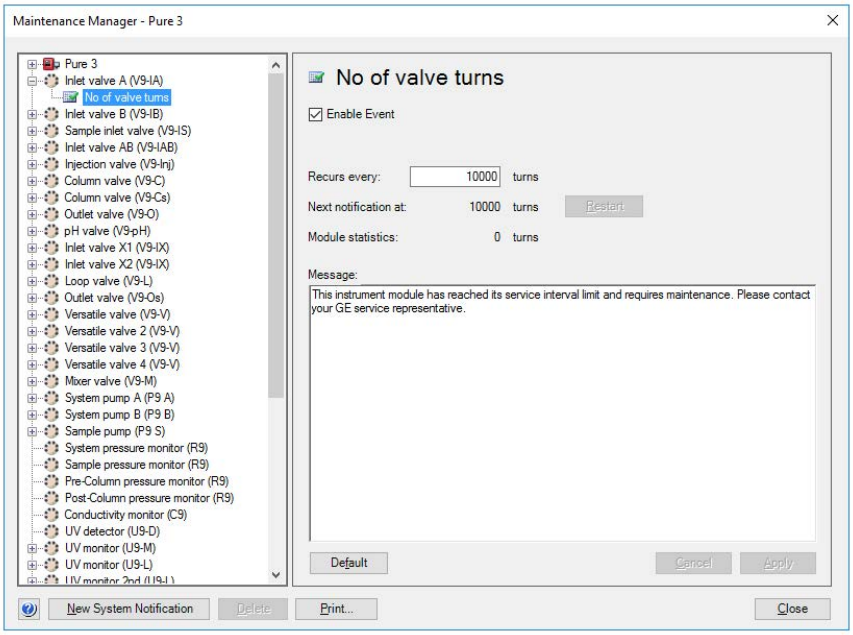
View general information and statistics

In the left pane of the ***Maintenance Manager*** dialog box, select the system of interest to view general information of the selected system. For some systems it is possible to view information for a module of interest. When modules are selected, operational statistics are also displayed.



View maintenance notifications

Click the plus symbol (**+**) of the system of interest to expand the list of related maintenance notifications. For some systems it is possible to view maintenance notifications for a module of interest. Select a notification to view notification details.

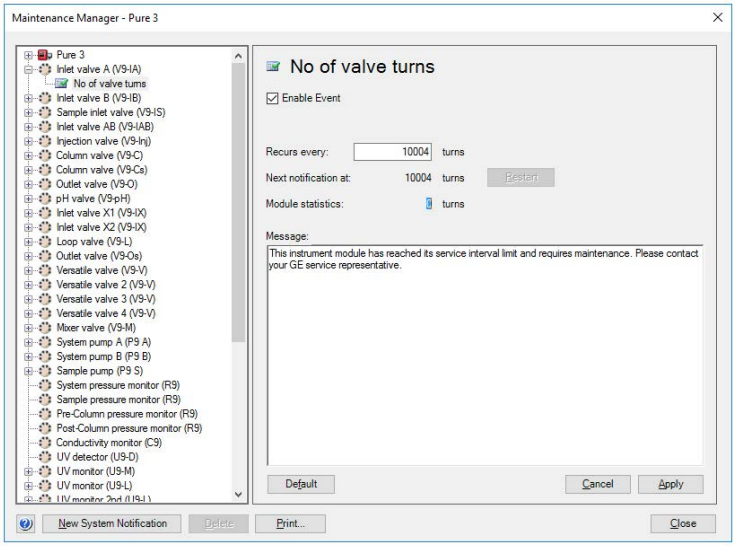


Note: *Modules with no plus symbol (**+**) have no related maintenance notifications.*

Edit a maintenance notification

Follow the instruction to edit a maintenance notification.

Step	Action
1	In the left pane of the ***Maintenance Manager*** dialog box, select a maintenance notification. *Result:* Details of the selected maintenance notification are displayed in the dialog box.



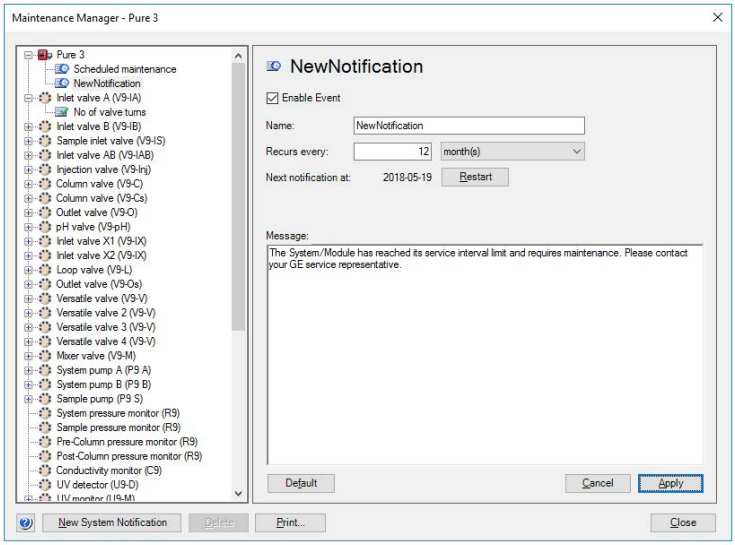
2	Edit the maintenance notification as desired: • Select the ***Enable Event*** check box to activate the notification. If the box is unchecked, the notification is not issued. • Enter a new interval after which the new notification is issued. • Click ***Restart*** to reset the counter and add a complete interval before the next notification. • Edit the message that is shown in the maintenance notification. • Click ***Default*** to restore the default settings for maintenance notifications.
3	Click ***Apply*** to save the changes.

Add a new system notification

The user can add new system notifications to the list of system events.

Follow the instructions to add a new system notification.

Step	Action
1	In the ***Maintenance Manager*** dialog box, click ***New System Notification***. *Result:* The ***NewNotification*** field appears in the ***Maintenance Manager*** dialog box.



2	In the ***NewNotification*** field: • Enter a name for the new notification. • Select a time interval after which the new notification is issued. • If desired, write a message that is shown for the maintenance notification.
3	Click ***Apply*** to save the changes and apply the notification settings.

Delete a user defined system notification

To delete a user defined system notification, select the notification in the ***Maintenance Manager*** dialog box and press the ***Delete*** button.

Note: *Module notifications are predefined and cannot be deleted. If desired, they can be disabled.*

Handle a maintenance notification

Each maintenance notification has a time interval after which the notification is issued. When this time interval has been reached, a ***Maintenance Notification*** dialog box appears.

Note: *The possibility to add maintenance notifications for modules is only available for some systems, but all systems can add maintenance notifications for the complete system.*

Follow the instruction to handle the notification.

Click...	to...
Acknowledge	reset the counter for a new maintenance notification period. ***Note:*** *Make sure that the maintenance action is performed as instructed after the notification is acknowledged, otherwise the system performance can deteriorate.*
Ignore	close the dialog box without action. ***Note:*** *The **Maintenance Notification** is displayed each time the **System Control** module is opened until the notification is acknowledged.*

Note: *The predefined maintenance notifcation periods use average values. The actual service interval for a specific module can be shorter or longer.*

8 Troubleshooting

About this chapter

This chapter describes different operational scenarios which can arise in UNICORN and their solutions or consequences.

Tip: *For additional advice concerning operational scenarios and possible solutions, refer to the UNICORN Information Letter. The UNICORN Information Letters are available at www.gelifesciences.com/unicorn.*

In this chapter

This chapter contains these sections:

8.1 Troubleshooting: User, function or system access

In this section

This section describes the following scenarios:

- Log on access problems
- Unable to access UNICORN functions
- Unable to connect or locate systems or computer stations

User Access

Problem description	Solution
Username and password not accepted	• The UNICORN administrator can check if the user account is locked. (for example after too many unsuccessful log on attempts) • The UNICORN administrator can try to set a new password. • If a password reset does not work, it is recommended to be delete the user profile and create new profile. • If it is a network user that cannot log in, verify that the network access works.
The log on dialog is inactive and a password cannot be entered	1 Verify that no UNICORN window or module is opened. 2 Restart Windows.
The license server cannot be contacted or no licenses are available	1 Verify that the available number of licenses have not been exceeded. Check the number of used licenses in the ***License Server Connection*** tab in the UNICORN Service Tool. See *UNICORN Service Tool User Manual*. 2 Restart the license server computer

Problem description	Solution
An error message is displayed, stating that a connection to the e-license server cannot be established.	• This can happen if an incorrect Ethernet address (MAC address) has been entered for the e-license, causing a mismatch. • 1 Verify that the e-license server is accessible from the network. 2 Contact GE Healthcare for assistance in verifying the validity of the e-license. • TCP ports in range 27000-27009 are closed in firewall. See *Appendix C Firewall settings, on page 253*.
The network and/or database is not available when a network user tries to login, and a network error message is displayed.	• Check that the network and the database is available and try to log in again. ***Tip:*** *If the network is unavailable, it is possible to log in with a local UNICORN user to terminate a run.* • TCP port 1433 and UDP port 1434 are closed in firewall. See *Appendix C Firewall settings, on page 253*.

Access to UNICORN functions

Problem description	Solution
UNICORN modules are not available for selection in the ***Log On*** dialog.	• Check that the modules in question are not open. • The UNICORN administrator can open the ***User Setup*** in the ***Administration*** module to verify that the user has access to the modules in question.
Functions to which you do not have access appear gray in the menus or cannot be accessed	In the ***Administration*** module, on the ***Tools*** menu, click ***User Setup*** to change the user profile access rights as needed.

Problem description	Solution
Methods or results cannot be edited even though they are not used by another user	Unlock the method or result using the ***Database Management Release Objects*** function in the ***Administration*** module. This is described in *Section 4.2.5 Release locked database objects, on page 185*.
The help viewer cannot be opened using help buttons or the **F1** key.	1 Double-click the shortcut icon on your desktop.  2 Try the help button or **F1** key again.
The Microsoft Office Document Image Writer causes UNICORN to terminate.	This writer application does not work. Choose another option, for example a PDF writer application.
When trying to edit the system properties for a system that has a method in queue, a message stating that the system is not in a ***Ready*** state and cannot be edited is received. However, the system queue can be waiting and the system can in fact be in a ***Ready*** state.	Wait until the system queue is completed and try again.
When viewing, printing or exporting "all logs", the logs for inactive systems are not included.	Select the logs for the inactive systems individually and perform the desired action for each system.

System connections

Problem description	Solution
The connections are not available, i.e., the selection check box appears dimmed	• Check if system has been deactivated. • Check that the power to the instrument is turned on. • Check the connection between the PC and the instrument.

Problem description	Solution
The connections are not available even though • the connection between the PC and instrument appears to be correct • the power is turned on	1 Switch off the instrument. 2 Quit UNICORN. 3 Shut down the instrument server computer. 4 Restart the instrument. 5 Restart the instrument server computer. 6 Log on to UNICORN.
A system is not available when you attempt to establish a connection	• Check that you have access rights to the system. Access rights are not automatically assigned for a newly defined system. • The system is not active. • Log off and log on again for access rights changes to be applied.
You receive the error message "`Cannot connect to system...`" in a network installation	• Check that the local computer, to which the system is connected, is turned on and logged on to the network. • Check that the computer from which you try to establish a connection is logged on to the network. • Check that the limit of five simultaneous connections to the system has not been exceeded.
You receive the error message "`Warning, system occupied`" when trying to connect	This error message is displayed if a system is defined and active in two different database instances and is already connected in the other instance. It is not recommended to have a system defined and active in more database instances than one.
You are connected to a system but have no contact with the instrument. The system hangs at initialization	• Check that the instrument is turned on. • Check that all cable connections are intact. • Check that the system is configured correctly, in ***System Properties*** and on the instrument display. • If the above actions do not help, restart both the instrument server computer, RTUext (if any), and the instrument.

Problem description	Solution
When without RTUext, the IP address 10.1.1.X is used in an internal network and connection problems are seen	Change the IP address of the instrument and the controlling network interface card to either 172.16.0.X or 192.168.0.X. The instrument and the controling network interface card must be on the same network.
When with RTUext, the IP address 172.16.0.X is used in an internal network and connection problems are seen	Change the IP address of the instrument and the controlling network interface card to either 192.168.0.X or 10.0.0.X. The instrument and the controling network interface card must be on the same network.
Connection to system failed after an upgrade from Windows 7 to Windows 10.	There is no specific support for upgrade from Windows 7 to Windows 10 with UNICORN installed. It is recommended to reinstall the UNICORN software.
Other reason for connection issues are:	
`AKTAconnection` NIC IP address and ICU/CU960 IP address is not in the same subnet	Subnet mask must be set to same for ÄKTA connection NIC and in CU960/ICU. Default is 255,255,255,0.
Ports that UNICORN uses are closed in the firewall	See *Appendix C Firewall settings, on page 253*.
Configuration files are not updated with correct `AKTAconnection` NIC IP address	Run the UNICORN Service Tool and edit the configuration files in the ***Instrument Connection*** tab. See *UNICORN Service Tool User Manual*.
CU960: UNICORN 5 is still installed on computer and occupies the CU-960	Uninstall UNICORN 5.
CU960: Node number must be correct set in system set-up/in CU960.	Check node number settings.
Computer name has been changed.	Change back to previous computer name.
The system disconnects irregularly	Check antivirus, computer hibernation, power management on computer and NICs.
System control: Connected but nothing is shown/layout looks strange	Use restore to default in “View”.

Problem description	Solution
System control: Connecting too fast after disconnect and vice versa can cause issues like Internal error or nothing is shown	Connect again (approximately 20 seconds wait is recommended).
System control: In connect box it seems that you are connected but you are not	Clear the ***Connect*** check box and disconnect by clicking ***OK***.Then try to connect again (reopen the connect dialog and check the system and click ***OK***).
Only possible to connect in view mode after an upgrade	Set home folders on all access groups.
When connecting to a system, the connection hangs during recovery of a terminated run	The recovery can take very long time (up to one hour). However if there is no progress anyway, on the computer controlling the instrument, delete all the contents of the folders: • Program Files Path`\GE Healthcare\UNICORN\UNICORN 7.5\Runtime Backup\AuditTrail` • Program Files Path`\GE Healthcare\UNICORN\UNICORN 7.5\Runtime Backup\Results` • Program Files Path`\GE Healthcare\UNICORN\UNICORN 7.5\Runtime Backup\Services` Restart the computer
The system backup could not be deleted and unable to start the System	Delete the file **`backup.sqlite`** located in `ProgramData\GE Healthcare\Virtual Control Unit\Adapters\InstrumentServerAdapter\` on the same computer as UNICORN Instrument server or on the RTU.
UNICORN Instrument Service does not register when defining system.	Run the UNICORN Service Tool and register the service in the ***Process Status*** tab. See *UNICORN Service Tool User Manual*.

Problem description	Solution
Failed to connect to system in view mode.	Make sure that the system is using a private network. If not then set the network as a private network and make sure that the following private network properties are turned on. For information on how to set a public network to a private network, see Post-installation settings. • File and Printer sharing • Network Discovery For information on how to change these settings, see Private network settings in section Post-installation settings.

Installation

Problem description	Solution
An error message stating that the access rights are insufficient appears when trying to uninstall UNICORN from the Windows 10 ***Programs and Features*** dialog.	This is caused by Windows UAC. Turning off UAC can solve this problem. If not, use the software removal procedure from the UNICORN 7.5 installation DVD.
When running a method or a manual run, a run log entry every 0.25 minutes appears: `User OPC <...> connected to system <...> in view mode.`	This is due to a corrupt OPC Core Components installation. Uninstall all versions of OPC Core Components and then install the latest by starting the UNICORN installation DVD and let the installation program install OPC Core Components which is a prerequisite to UNICORN.

Disable Power save

Problem description	Solution
Power save has been turned-off but the computer still goes into power save mode.	This is because the power save options are on a per user basis. Solve the problem by turning off power save for: • each user • the hard drive *and* • the network interface cards.

E-license

Problem description	Solution
E-license server does not find any licenses	Do not place a node-locked license in the Licenses folder of the e-license server installation, this prevents the e-license server software from running. Always let the software itself copy the e-license files into the proper location.
Can not find location of the node-locked e-license files	1 Type `Run` in the ***Start*** menu search field, then click the ***Run*** item displayed as search result. 2 Type `%programdata%\GE Healthcare\licenses` in the ***Open*** textbox, then press **Enter**.
Node-locked license installed but UNICORN is not able to find the license	This can happen if the license is deployed using a different Windows account than the Windows account running UNICORN, e.g., installing UNICORN and the node-locked license as a local administrator on the PC and then run UNICORN as a domain user can create this problem. This is likely a folder permission issue on the folder where the node-locked license is located. Update the permissions of the folder where the node-locked license is located to allow ***Everyone*** full control.
Location of e-license server is not set during installation	If the e-license server is not set to a network server during UNICORN installation, a manual update is required using the UNICORN Service Tool.

Problem description	Solution
Ports used by the e-license server	If not explicitly set, the e-license server communicates on one of the following ports 27000-27009 (TCP). Sometimes these must be made exceptions for in the firewall in order for the communication to function properly with the e-license server.

8.2 Troubleshooting: Network access

In this section

This section describes the following scenarios:

- A network drive is selected as backup and archive location of the database.
- A remote client is unable to connect to an instrument, or a local client is unable to connect to a CU-950 or CU-960 based system where the IP address of the CU- 950 or CU-960 differs from 10.1.1.1.

Problems with network drive as location for backup

Scenario	Solution
A network drive is selected as the location for backup and archive versions of the database. This can cause problems if the user "system" is not allowed write access to the drive.	It is not recommended to select network drives for backup and archive. If needed, backup and archive files can be copied from the database server to a network drive or other storage media as an extra precaution.

Instrument connection problem for remote or local client

Scenario	Solution
A remote or a local client is unable to connect to an instrument where the IP address differs from the default IP address.	Configure UNICORN in the ***Instrument Connection*** tab in UNICORN Service Tool. See *UNICORN Service Tool User Manual*. The IP addresses have to match the actual settings of the network interface card. If this fails, set the interface metric of the ÄKTAConnection NIC to 25 and the LAN NIC to 20.
Connection test from the Admin module fails despite being connected to the system in the System Control module.	Restart the UNICORN Control PC and RTUext (if used). If the problem is not solved, make sure that all the necessary services are started. This can be done using the UNICORN Service Tool.

Scenario	Solution
A local client is unable to connect to an instrument or RTUext.	Make sure that the network cable from the RTUext or the instrument is connected to the network card that is configured for instrument communication. If the network card has a label **AKTA**, make sure that the label is on the correct network card. The Network Connection AKTA must match the network card connected to the RTUext or the instrument. Disconnect the network cable and reconnect to the other network card if necessary.
Connection related issues after changing IP address for any of the network cards on the local computer or connected RTU/instrument.	Restart both computer and connected RTU/instrument.

8.3 Troubleshooting: Database functions

In this section

This section describes troubleshooting scenarios related to the database.

Database functions

Problem description	Solution
The database is not available at log on	• Wait a couple of minutes to allow the SQL Server services to start and try to log on again. (This can be necessary when logging on after a computer restart) • Verify in the ***Windows Services*** dialog that the ***SQL Server*** and ***SQL Server Browser*** services are running properly. • Verify that the firewall port settings are correct. See *Appendix C Firewall settings, on page 253* for port settings
The database cannot be located at the installation of a client/instrument server computer.	• Sometimes the computer name of the database server cannot be identified. In that case, enter the IP address instead. • Ensure that a static IP address is used.
The scheduled database backups are not performed	Reset the scheduled backup in the Database backup wizard. If another SQL Server edition than ***SQL Server Express*** is used, verify that the service ***SQLAgent*** has started.
The workstation computer is restarted and the user tries to log on to UNICORN immediately. The UNICORN client cannot connect to the database, which is a local database (Full installation).	Allow some time for the database to start before trying to log on.

Problem description	Solution
Not possible to use ***Database Management*** after restore of a database originated from a 32-bit operating system on a 64-bit operating system. In case of a computer upgrade from 32-bit Windows XP to 64-bit Windows 7 or Windows 10, it might happen that it is no longer possible to use ***Database Management***. You get an internal error when you open ***Database Management*** and you can no longer archive/retrieve or perform backups	Update the registry. Find the `HKEY_LOCAL_MACHINE\Software\Wow6432Node\GE Healthcare` and choose to ***Export*** this. Open the export file and do a ***Search/Replace*** for `Wow6432Node32\` and replace with blank. Double-click to run the registry export. This creates the necessary information in the registry to be able to use a former 32-bit database in 64-bit environment.
After computer startup on a standalone installation – a database connection error is shown when starting UNICORN.	The database server takes some time to start. Wait a minute and try again.

This computer already has an database installed named UNICORN

Problem description	Solution
Installation claims that the database already exists despite being installed on a brand new computer. Sometimes during installation of the database this error is displayed: "`The database cannot be installed. This computer already has an database installed named UNICORN. Either uninstall SQL Server, ensure that the database instance does not contain any user created databases or install the database on another computer`".	The error message is very likely erroneous. See the following table for possible solutions

If...	Then...
The operating system is still being updated The database installation has failed due to pending updates. This can be Windows updates or local IT software updates.	Make sure that Windows update and other IT software updates are turned-off during installation. If this error happens, it is advised to uninstall ***Microsoft SQL Server*** and repeat the installation with the software updates turned off.

If...	Then...
Loopback adapter security issue	In case the computer has a loopback adapter installed, its security settings need to be adjusted to include the ***Administrators group***. Also, adjust the loopback adapter check in the registry. In order to see if it indeed is a problem with the loopback adapter security settings, look in the ***Event log*** of the computer for an entry similar to this: `SSPI handshake failed with error code 0x8009030c, state 14 while establishing a connection with integrated security the connection has been closed. Reason: AcceptSecurityContext failed. The Windows error code indicates the cause of failure. [CLIENT: 127.0.0.1].` In order to fix this issue: • Open ***Local policies:User rights assignment:Access this computer from the network*** and add the ***Administrators group*** and in case it still fails, add ***Everyone*** as well. Second solution, disable the loopback adapter check by performing the following: 1 Edit the registry using ***regedit***. (***Start:Run:Regedit***). 2 Browse to : `HKLM\System\CurrentControlSet\Control\LSA`. 3 Add a ***DWORD*** value called `DisableLoopbackCheck`. 4 Set this value to 1. 5 Reboot computer and try to install again.
Installation fails due to Reporting services database exists	The UNICORN installer counts the number of existing databases and unfortunately it does not make an exception for the Reporting services databases, which leads to the above error message even if there is no UNICORN database installed, but only Reporting services.

8.4 Troubleshooting: Upgrade, restore, repair

In this section

This section describes troubleshooting scenarios related to

- upgrading UNICORN version from 6.0 or 6.1
- restoring UNICORN 6.0 or 6.1 database
- reparing a corrupt database

Upgrade UNICORN version from 6.0 or 6.1 to 6.2 or later

The following is an outlined process of how to upgrade from UNICORN 6.0 or 6.1:

Stage	Description
1	Backup database.
2	Uninstall UNICORN 6.1.
3	Uninstall OPC Core Components in the Windows ***Programs and Features*** dialog.
4	Install the new verision of UNICORN
5	Restore the backup from 6.1. ***Note:*** *If UNICORN 6.3 or later is installed using default locations, the backup location has changed since UNICORN 6.1 and thus you have to move the old database backup into the new backup location. Quickest way to create this location is to run a manual backup.*
6	Upgrade SQL Server to the version found on the UNICORN installation media.
7	Upgrade the restored database using ***UNICORN Configuration Manager***.
8	Drop FILESTREAM and increase the database size to 10GB.
9	Install new e-licenses.
10	Start UNICORN.
11	For all user groups, set a home folder from ***Administration : Access Groups*** and ***Network Users***.

Stage	Description
12	If the computer had an instrument server: start ***Administration : System Properties*** and select ***Edit System*** and click ***Test connection*** to register to UNICORN Instrument Server service.
13	Restart the computer.

Unable to restore a UNICORN 6.0 or 6.1 database

Restoring a 6.0 or 6.1 database on a UNICORN 6.2 or later version can sometimes fail if the backup is brought to a completely new installation of UNICORN 6.2 or later versions where no UNICORN installation has previously existed. This is due to a dependency on the paths. The old path to the `ResultData` folder must exist.

The default path is:

```
C:\Program Files (x86)\GE Healthcare\UNICORN\Database\ResultData
```

- Make sure that this folder exists prior to performing the RESTORE operation.
- However, if this still fails or you cannot create the folder required due to the drive needed does not exist on the target machine, you need to issue a "Restore with move" SQL command. Ask your GE Healthcare representative for more information.

Repair a corrupt database

It is often possible to repair a corrupt database. Follow the instructions below to find out a corrupt database:

1 Right-click on the ***Command prompt*** item in ***Start:All Apps:Windows System***.

2 Select ***Run as Administrator***.

3 Enter the following command:

```
sqlcmd -Slocalhost\UNICORN -Q"USE UNICORN;DBCC CHECKDB" >
C:\temp\dbcc.txt
```

This runs a check command and see if any tables or indexes in the database are corrupt and place the output into a file called `dbcc.txt` in the `C:\temp` folder.

If all is well, the text file `dbcc.txt`, shows the follwoing text at the bottom:

```
CHECKDB found 0 allocation errors and 0 consistency errors in
database 'UNICORN'. DBCC execution completed. If DBCC printed
error messages, contact your system administrator.
```

If on the other hand there are an indication of errors, like this:

```
CHECKDB found 0 allocation errors and 14 consistency errors in
database 'UNICORN. repair_rebuild is the minimum repair level for
the errors found by DBCC CHECKDB (UNICORN). DBCC execution com-
pleted. If DBCC printed error messages, contact your system admin-
istrator.
```

Examine the rest of the output in order to locate which tables are causing problems. A problematic entry looks similar to this:

```
Table error: table 'AuditTrailEntry' (ID 773577794). Index row
in index 'IX_AuditTrailEntry_AuditTrailID' (ID 2) does not match
any data row. Possible extra or invalid keys for: Msg 8956, Level
16, State 1, Server HCE-13B72Q1\UNICORN, Line 1
Index row (1:15445:151) with values (AuditTrailID = 1 and LogTime
= '2013-04-08 09:13:48.3371785 +05:30' and AuditTrailEntryID =
10698) pointing to the data row identified by (AuditTrailEntryID
= 10698).
```

Note that the table name is `AuditTrailEntry` and in order to possibly correct the problem, the following command shall be run for each table:

```
sqlcmd –Slocalhost\UNICORN –Q”USE UNICORN;DBCC DBREINDEX (Audit-
TrailEntry, ‘ ‘, 0)”
```

Once completed, keep checking by running ***DBCC CHECKDB*** until there are no further errors.

8.5 Troubleshooting: Additional information

In this section

This section describes various troubleshooting scenarios.

UNICORN dialog boxes not displaying properly

Problem description	Solution
Buttons and other interface items are not positioned correctly in the UNICORN dialog boxes.	The size of Windows interface text must be set 100% in Windows ***Control Panel***. 1 Click the Windows ***Start*** button. 2 Type `Display` in the Start menu search field. 3 Click ***Display settings*** (or ***Display*** in Windows 10) item that is displayed as the search result 4 Click 100% to set the size of text and other items on your screen. 5 Click ***Apply***.

UNICORN terminates unexpectedly

Problem description	Solution
UNICORN terminates unexpectedly each time the UNICORN instrument server is restarted	With an unexpected termination it means you get a message stating `UNICORN experienced a problem and had to close.` Sometimes IP v6 is prohibited in networks. In order to get IP v6 compatible computers to work on those LAN:s IP v6 has to disabled in the registry. Add ***DWORD*** value named `DisabledComponents` with the value `000000ff` to the registry entry: `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters]`

Firewall issues

If the client has connection problems the following can be used as a help to identify if it is the firewall that is the root cause:

- Add the following to the config file for UNICORN Instrument Server:

  ```
  <logger name=" GE.Healthcare.UNICORN.Common.Events">
  <level value="DEBUG"/>
  </logger>
  ```

  Add the above lines before the line:

  ```
  </log4net>
  ```

- Save the file and restart the ***UNICORN Instrument Server***.
- After the ***UNICORN Instrument Server*** has been restarted try to reconnect to the system. Wait until the client has been disconnected.
- Open the log file for ***UNICORN Instrument Server*** and search for the following text(s):

  ```
  System.Reflection.TargetInvocationException: Exception has been
  thrown by the target of an invocation. --->
  System.Net.Sockets.SocketException: A connection attempt failed
  because the connected party did not properly respond after a
  period of time, or established connection failed because
  connected host has failed to respond 10.9.216.80:51886
  ```

  ```
  System.Reflection.TargetInvocationException: Exception has been
  thrown by the target of an invocation. --->
  System.Net.Sockets.SocketException: A connection attempt failed
  because the connected party did not properly respond after a
  period of time, or established connection failed because
  connected host has failed to respond 10.9.216.80:9944
  ```

The ending number is the port number and the port 51886 can be something else since UNICORN is using so called ephemeral ports.

Entries like this indicates that the ***UNICORN Instrument Server*** has failed to send an event to the client. The port 9944 is used for an Alive event that must succeed; otherwise the client is disconnected.

To verify that it is the Windows firewall that blocks the traffic, open the Windows firewall log, see

http://technet.microsoft.com/en-us/library/cc736373(v=ws.10).aspx

The following entries corresponds to the entries from the log file for ***UNICORN Instrument Server*** above:

```
2013-09-10 12:05:04 DROP TCP 10.9.28.158 10.9.216.80 62442 51886
52 S 1034333319 0 8192 - - - RECEIVE
```

```
2013-09-10 12:05:46 DROP TCP 10.9.28.158 10.9.216.80 62456 9944
52 S 3482814844 0 8192 - - - RECEIVE
```

Not able to connect to a system after computer restart or change of a component

This can occur due to a problem with full log files (even though this is a unlikely since this works automatically). The log files are roughly 498 KB when full and usually new files are created automatically, but if UNICORN is terminated during the process of creating log files, this can cause such problem.

The solution is to rename the `UNICORN Client Log.txt`, `UNICORN Instrument Server Call Log.txt` and `UNICORN OPC Call Log.txt` to something else and restart the computer. Log files are found in the Logs folder of the installation.

A way to discover that it is this issue is by checking the ***Application Event Log*** for error entries similar to the following:

```
Event Type: Error
Event Source: .NET Runtime
Event Category: None
Event ID: 1026
Date: 1/11/2013
Time: 9:33:07 AM
User: N/A
Computer: SEHCUPM-0054899
Description:
Application: UNICORN Instrument Server.exe
Framework Version: v4.0.30319
Description: The process was terminated due to an unhandled excep-
tion.
Exception Info: System.ObjectDisposedException
Stack:
at
System.Threading.WaitHandle.WaitOneNative(System.Runtime.InteropSer-
vices.SafeHandle, UInt32, Boolean, Boolean)
at
System.Threading.WaitHandle.InternalWaitOne(System.Runtime.In-
teropSer vices.SafeHandle, Int64, Boolean, Boolean)
at System.Threading.WaitHandle.WaitOne(Int32, Boolean)
at System.Threading.WaitHandle.WaitOne()
at log4net.Appender.FileAppender+InterProcessLock.AcquireLock()
at log4net.Appender.FileAppender+LockingStream.AcquireLock()
```

```
at log4net.Appender.FileAppender.WriteFooter()
at log4net.Appender.TextWriterAppender.WriteFooterAndCloseWriter()
at log4net.Appender.FileAppender.Reset()
at log4net.Appender.TextWriterAppender.OnClose()
at log4net.Appender.AppenderSkeleton.Close()
at log4net.Appender.AppenderSkeleton.Finalize()
```

For more information, see *Microsoft Events and Errors Message Center* at http://www.microsoft.com/technet/support/ee/ee_basic.aspx

Appendix A
Technical specifications

Introduction

This appendix describes

- the UNICORN system recommendations
- UNICORN's capability to control instruments
- how UNICORN samples data from the instruments.

Contents

The table below describes the contents of this appendix:

A.1 Computer recommendations

Introduction

This section describes some general technical specifications for UNICORN 7.5 computers.

General computer specifications

For information on computer specifications, see http://www.gelifesciences.com/UNICORNPCspecifications.

For information about compatibility between UNICORN versions, the supported operating systems, database versions, and instrument configuration, see the UNICORN compatibility matrix at http://www.gelifesciences.com/UNICORNcompatibility.

The following applies:

- A screen resolution of 1280x1024 or higher is recommended. Parts of the UNICORN user interface can not be displayed properly using a lower resolution.
- Changing the default font and changing the font size from 100% in Windows can cause problems in the UNICORN user interface.
- Windows power save features must be turned off to avoid conflicts with system operations.
- UNICORN is not compatible with the Windows feature High DPI Awareness, which allows the graphic user interface to be scaled. The interface scale must remain at 100% to avoid issues with clipping and misaligning of parts of the UNICORN user interface. Normally, the scale is set at 100% by default.

A.2 UNICORN 7.5 control capacity

Introduction

This section describes the capability of UNICORN 7.5 to control systems in stand-alone installations and network installations.

Stand-alone installations

In a stand-alone installation the workstation computer can be connected to a single instrument.

Network installations

The list below describes some basic facts and recommendations about network installations:

- Instruments must be connected to the network through an instrument server. It is not recommended to connect the instruments directly to the network [1].

  Note: *This is not applicable for WAVE systems.*

- Each local station can be connected to a single instrument.
- A database server can support up to 32 clients [2]. This can be any combination of local stations with connected instruments, and remote stations in the network. The number of supported systems depend on the server solution and the network workload.
- A client computer can locally control one and remotely another two instruments. Alternatively, a client computer can control a total of three instruments remotely.
- Each instrument in UNICORN
  - can be *controlled* by only one active ***System Control*** module
  - can be *viewed* by four other ***System Control*** modules.

1 The instrument can also be connected to the network through RTU, CU950, or CU960. Although it is possible to connect instruments directly to a network, this is not recommended since it can have a negative impact on the communication between instrument and instrument server. With a peer-to-peer connection between each instrument server and instrument, the system operation is less vulnerable to network communication problems and the general network traffic load is reduced.

2 The SQL Server Express version distributed with the standard UNICORN 7.5 installation is suitable for up to three clients. For larger installations an upgrade of the SQL Server is recommended.

- a total of five ***System Control*** modules can be connected to a single system in *view* mode, provided that no one is connected in *control* mode.

A.3 Data sampling

Data storage

Result is saved when a running method or a manual run ends. Data is also saved in a runtime backup on the instrument server local hard drive during a run, thus minimizing data loss in the event of power or communication failure.

Data buffer capacity

The capacity of the data buffer is up to 180 000 data points for each curve. The maximum number of data points can be set either to 18 000, 54 000 or 180 000 data points. For most curves, the default setting is 54000 points. For common applications, the default setting produces a resolution that is more than adequate.

Note: *The data buffer capacity is listed in the **Data collection** group of **System:Settings** in the **System Control** module.*

Effective sampling frequency

If a buffer is filled during a run, i.e 54 000 points have been recorded, the number of points is halved by deleting every second point, leaving 27 000 data points of the curve data. For subsequent sample points, every second point is dropped, thus halving the effective sampling frequency. When the curve again reaches 54 000 points the process is repeated and the effective sampling frequency is halved once again. Now every fourth sampling point is recorded.

Note: *The real sampling frequency, i.e. the sampling frequency of the system, never changes.*

Ensure maximum resolution

To ensure maximum resolution for a crucial part of a run, issue a `New_Chromatogram` instruction at the beginning of the part. This empties the data buffers, which allows the selected maximum number of data points (e.g. 54000) to be recorded from this part of the run before the effective sampling frequency is reduced again.

Appendix B
Advanced system administration

Introduction

This appendix contains additional information that is relevant for UNICORN 7.5 network deployments and details about Windows settings. It describes software settings and selections necessary in order for the UNICORN client and server computers to operate as intended in a network environment. Issues addressed include

- Prerequisite application installations
- Windows user names and passwords
- Services and ports used

The appendix also includes instructions for how to uninstall UNICORN 7.5 and SQL Server Express manually if the installation has become corrupted and cannot be uninstalled using the normal procedures.

Contents

The table below describes the contents of this appendix:

B.1 User, client computer and database server set up

Introduction

This appendix provides information about the Windows user setup and computer settings necessary in network deployments. The appendix also contains information about basic computer configuration and prerequisite installations. These settings are normally performed as part of the normal installation procedure. Manual adjustments are not necessary.

Hard disk compression

It is not recommended to compress the hard disks of the computers where UNICORN 7.5 is installed.

Computer configuration with Windows 10

Follow the instructions to configure a Windows 10 computer before installing UNICORN:

Step	Action
1	Install Windows 10 Professional. • Select US or UK English as the Language Option. • Set the regional settings to use the US standard for decimal delimiter, which is a decimal point (".").
2	Install any additional hardware drivers that can be needed, for example network, graphics, sound or chipset drivers. See also RefToInstall extra network cards.
3	Since a computer with a musti-core processor is the recommended minimum for UNICORN 7.5, make sure that all cores of the processor are running.

Step	Action
4	Install the following prerequisite applications in the exact order listed below [1]: 1 Microsoft .NET Framework 4.7.2 ***NDP472-KB4054530-x86-x64-AllOS-ENU.exe*** 2 Microsoft Visual C++ 2008 Redistributable Package ***vcredist_x86_Studio_2008_SP1.exe*** 3 Microsoft Visual C++ 2010 Redistributable Package ***vcredist_x86_Studio_2010_SP1.exe*** 4 Microsoft Visual C++ 2012 Redistributable Package ***vcredist_x86_Studio_2012.exe*** ***vcredist_x86_studio_2013.exe*** ***vcredist_x64_studio_2013.exe*** ***vcredist_x86_studio_2015.exe*** ***vcredist_x86_studio_2017.exe*** 5 Microsoft Core XML Services (MSXML) 6.0 ***msxml6.msi*** 6 UNICORN Certificate Package 1.0.0 ***CertificateImporter.exe***
5	Enable high performance power plan: 1 Click ***Power Options*** in the ***Control Panel:Hardware and Sound***. *Result:* The ***Power Options*** dialog opens. 2 Expand ***Show additional plans***. 3 Select ***High performance***.
6	Disable all power save settings: Follow the instruction in Disable Power Save section in *Appendix D Post-installation settings, on page 260*

Step	Action
7	Turn off the Windows screen saver: 1 Click ***Start*** and then click ***Settings***. 2 Click ***Personalization***. 3 Select ***Lock Screen*** option, and then click ***Screen saver settings***. 4 Select ***[None]*** from the ***Screen Saver*** list, and then uncheck ***On resume, display logon screen***. 5 Click ***OK*** to apply the settings and close the dialog.

1 All listed prerequisites are available on the UNICORN 7.5 installation package in the `ISSetup-Prerequisites` folder.

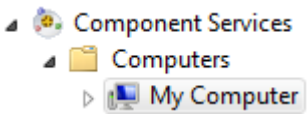
Windows user names and passwords

Unless a domain controller is used, all users must have exactly the same user name and password on all computers running UNICORN. If a domain controller is used, the users are created at the domain controller and not on each computer. This eliminates the need for synchronized user names and passwords.

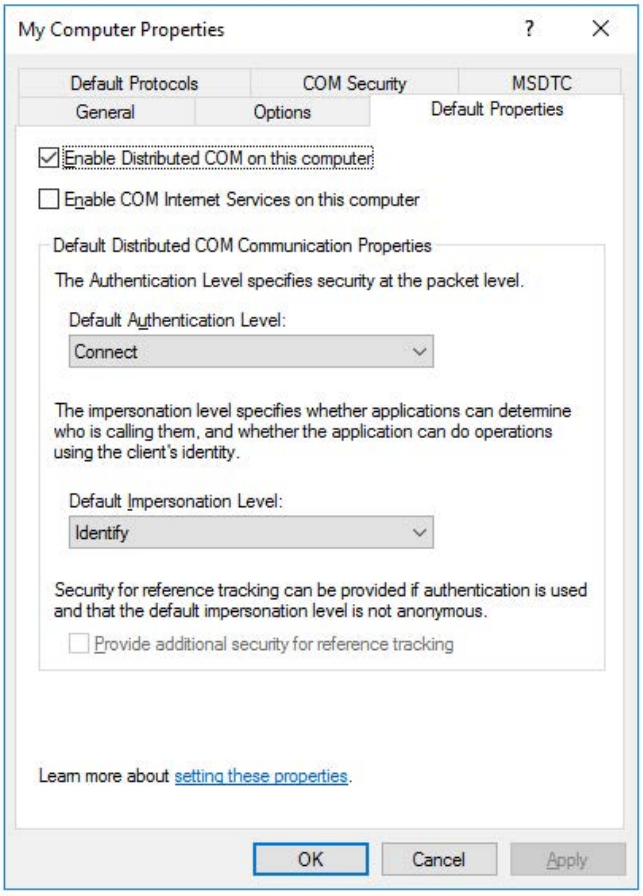
Component services

The table below describes the steps for how to set up the ***Component Services*** settings on a UNICORN computer.

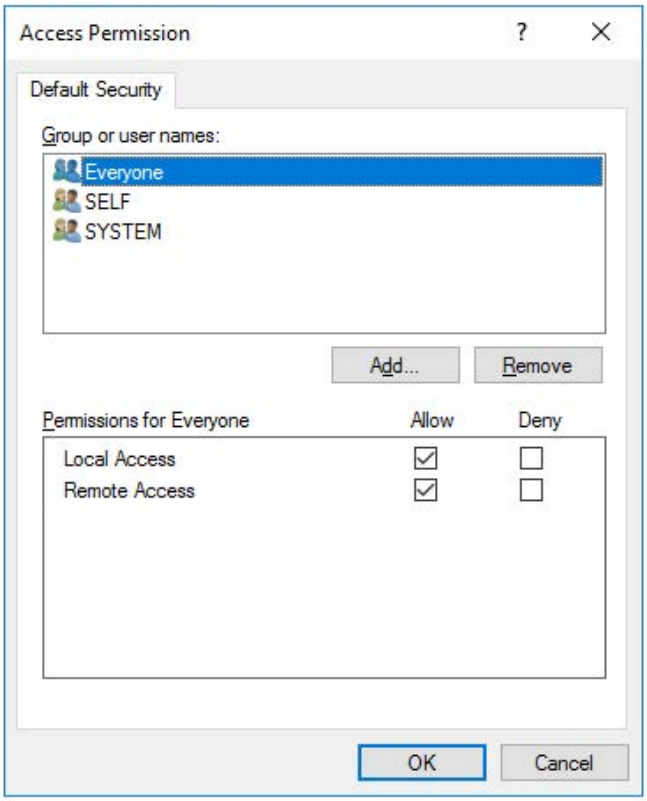
My Computer Properties

Step	Action
1	Start the ***Component Services***: 1 Type `Component Services` in the ***Start*** menu search field. 2 Click the ***Component Services*** item that is displayed as the search result.
2	Click the right arrows to expand the tree structure under ***Component Services*** to show ***My Computer***. 

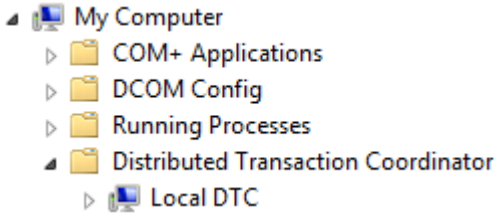
Step	Action
3	Right-click ***My Computer*** and click ***Properties*** to open the ***My Computer Properties*** dialog.
4	Click the ***Default Properties*** tab and • Select ***Enable Distributed COM on this computer***. • Click ***Connect*** in the ***Default Authentication Level*** list ***Note:*** *Client and server computers must have corresponding* ***Default Authentication Level*** *settings and be in the same domain.*



Step	Action
5	Click the ***COM Security*** tab and click ***Edit Default*** in the ***Access Permissions*** field, to open the ***Access Permission*** dialog. • Add the group ***Everyone*** with permissions for ***Local Access*** and ***Remote Access***. • Click ***OK*** to apply and close the dialog.

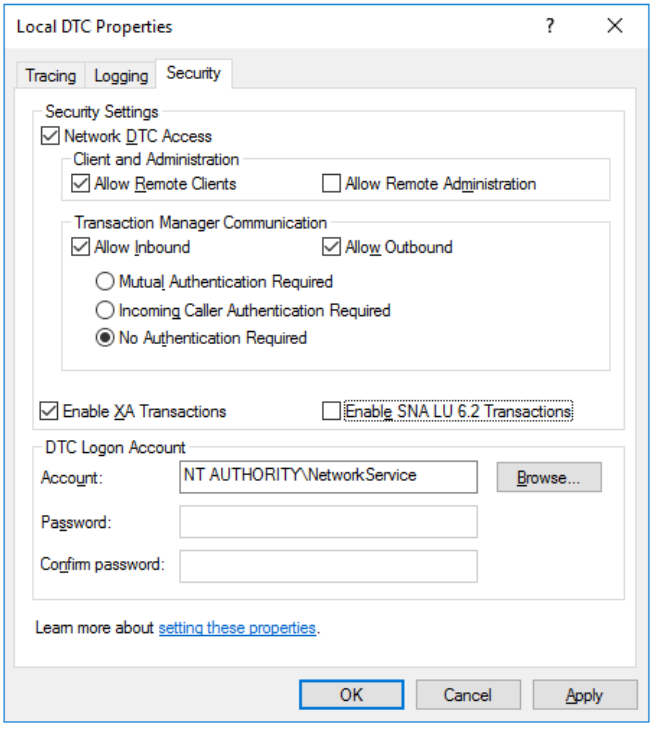


6	• Click the ***MSDTC*** tab and • verify that ***Use local coordinator*** is selected.
7	Click ***OK*** to close the ***My Computer Properties***.

Step	Action
8	Click the right arrows to expand the tree structure under ***My Computer*** to show ***Local DTC***. 
9	Right-click ***Local DTC*** and click ***Properties*** to open the ***Local DTC Properties*** dialog.

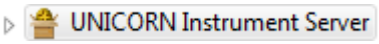
Step	Action

10	Click the ***Security*** tab and select the following options:
	• ***Network DTC Access***
	  - ***Allow Remote Clients***
	• ***Transaction Manager Communication***
	  - ***Allow Inbound***
	  and
	  - ***Allow Outbound***
	  - ***No Authentication Required***
	• ***Enable XA Transactions***

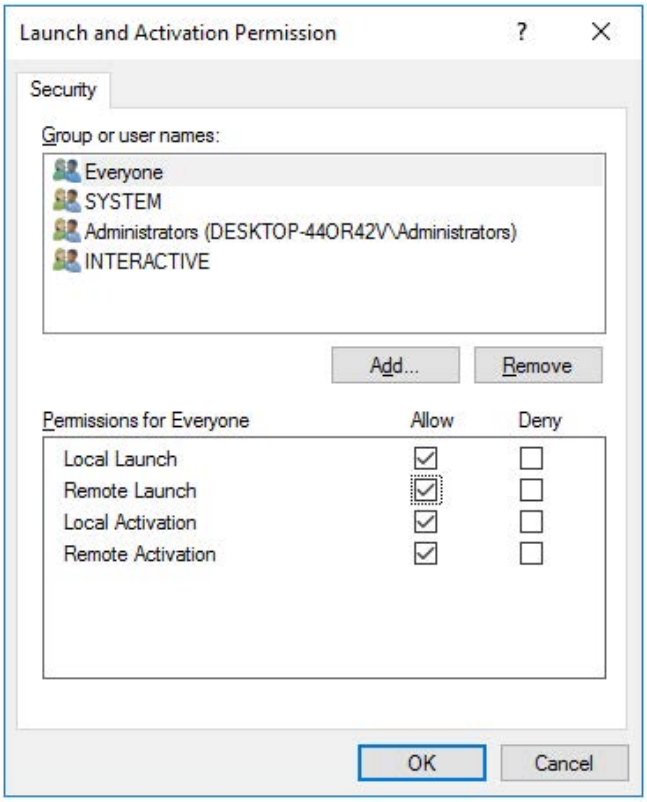


11	Click ***OK*** to apply the changes and close the ***Local DTC Properties*** dialog.
12	Proceed with the *UNICORN Instrument Server Properties, on page 244* .

UNICORN Instrument Server Properties

Step	Action
1	Click the right arrows to expand the tree structure under ***DCOM Config*** to show ***UNICORN Instrument Server***. 
2	Right-click ***UNICORN Instrument Server*** and click ***Properties*** to open the ***UNICORN Instrument Server Properties*** dialog.
3	• Click the ***Security*** tab • In the ***Launch and Activation Permissions*** field, click ***Customize*** and • click ***Edit*** to open the ***Launch and Activation Permission*** dialog.

Step	Action
4	Select the ***SYSTEM*** user and select ***Allow*** for all permissions.



Note:

*Only the **SYSTEM** user can have **Launch** permissions.*

5	Select the ***Administrators*** user and select ***Allow*** for the ***Local Activation*** and ***Remote Activation*** permissions.
6	Select the ***Everyone*** user and select ***Allow*** for the ***Local Activation*** and ***Remote Activation*** permissions.
7	• Click ***OK*** to apply the changes and close the ***Launch and Activation Permission*** dialog. • Click ***OK*** to close the ***UNICORN Instrument Server Properties*** dialog.

B.2 Manual uninstallation

Introduction

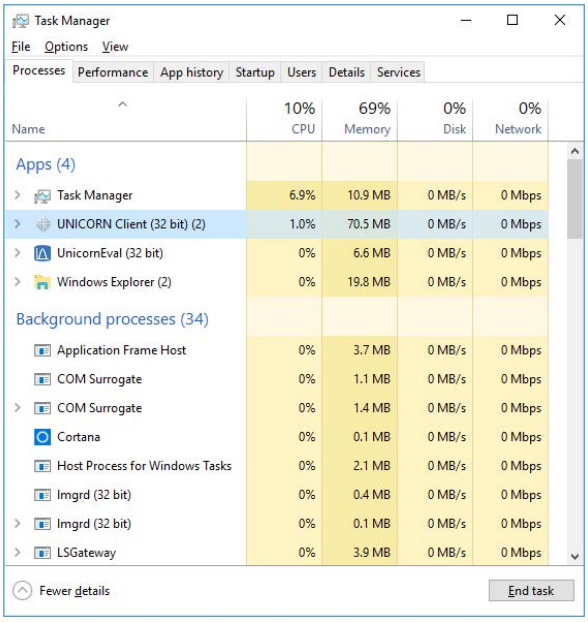
This appendix contains instructions for how to remove a UNICORN 7.5 and/or SQL Server installation manually in the event that the installation has become corrupt and cannot be removed in a regular manner.

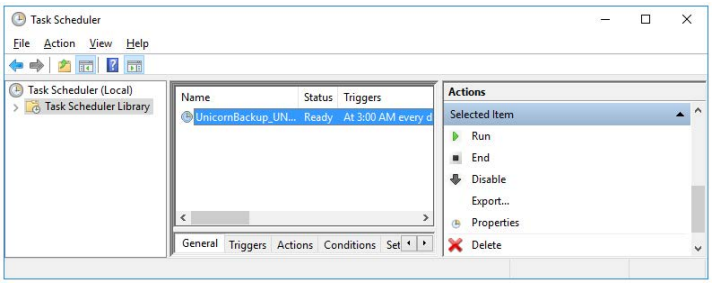
Note: *It is important to schedule backups of the database to prevent loss of data.*

Remove a UNICORN 7.5 installation

The instruction describes how to remove the UNICORN 7.5 installation:

Step	Action
1	Open the ***Windows Task Manager***, then click the ***Processes*** tab.



Step	Action
2	Select and end the following processes if applicable: • ***UNICORNClient.exe*** • ***UNICORN Instrument Server.exe*** • ***UNICORN Support Service.exe*** • ***NextCU.exe*** • ***VIDMain.exe*** • ***UNICORN HDA server.exe*** • ***UNICORNeval.exe*** • ***P950_DRV.exe*** • ***LSGateway.exe*** Close the ***Windows Task Manager***.
3	Remove the UNICORN backup task: 1 Open the ***Task Scheduler***. In the ***Start*** menu search field type `task scheduler`, then click the ***Task Scheduler*** item that is displayed as the search result.  2 Select the UNICORN backup task. 3 Click ***Delete*** in the ***Action*** menu. 4 Close the ***Scheduled Tasks*** dialog.

Step	Action
4	For client installations, remove the folder Program Files Path\GE Healthcare\UNICORN\UNICORN 7.5. For database and standalone installations, uninstall the SQL Server as described in *Remove the UNICORN database instance, on page 248*, before the UNICORN folder is removed. ***Note:*** *The actual search path to this folder depends on what was selected at the UNICORN installation.* *This folder can contain backup files, log files, and error reports that can be saved for future reference.*
5	Reboot the computer.

Remove the UNICORN database instance

This instruction describes how to remove the UNICORN database instance using Windows ***Programs and Features*** dialog.

Note: *Some of the images in the instruction have been cropped and do not show the available buttons on the bottom part of the dialog (**OK**, **Next**, **Back**, **Cancel**, **Help** etc.).*

NOTICE

If more than one database instance is installed on the computer you must ensure that only the UNICORN database instance is removed. Do not remove Setup Support Files, Native Client or any SQL Server files, to ensure that the other database instances remain operable.

Step	Action
1	Open the Windows ***Control Panel*** and click ***Programs:Programs and Features***.
2	Right-click ***Microsoft SQL Server 2017(64-bit)*** and click ***Uninstall/Change***.
3	The ***SQL Server*** dialog opens. Click ***Remove***.

Step	Action
4	A ***Setup Support Rules*** dialog opens and run a discovery operation to identify possible problems with the maintenance operation. • Click ***OK*** to proceed after this operation step is completed.
5	• Click ***UNICORN*** on the ***Instance to remove features from*** menu and • Click ***Next*** to proceed.
6	• Select ***Database Engine Services*** and ***SQL Server Replication*** and • Click ***Next*** to proceed.
7	Setup runs ***Removal Rules*** to identify possible problems with the removal. • Click ***Next*** to proceed after this operation step is completed.
8	A summary of the removal operation is shown. • Click ***Remove*** to proceed.
9	The progression of the removal operation is shown. • Click ***Next*** to proceed after this operation step is completed.
10	The ***Complete*** dialog opens. This dialog provides a link to a summary log file. • Read the information in the log file and on the ***Complete*** page. • Click ***Close*** to close the wizard dialog. • Close the ***Add or Remove Program*** dialog.

Uninstalling an existing instance of SQL Server

The instruction below describes how to uninstall SQL Server if the procedure described above cannot be used.

NOTICE

The uninstallation procedure below can only be used if the UNICORN database instance is the *only* database instance installed on the computer. The procedure described causes all Microsoft SQL Server-related entries to be completely deleted from the computer.

Step	Action
1	Perform a backup of the Windows Registry:
2	Delete the registry keys listed below: • `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server` • `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer`

Step	Action
3	• Locate and select the key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager` • If there is an entry (of the ***Type REG_MULTI_SZ***) named `PendingFileRenameOperations`: 1 Right-click the entry and click ***Modify***. *Result:* The ***Edit Multi-String*** dialog opens. 2 Clear the ***Value data***. 3 Click ***OK*** to close the dialog and update the ***Data*** column. • If there is a key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\FileRenameOperations`: 1 Right-click the key and click ***Rename***. 2 Change the name to `FileRenameOperations2` ***Note:*** *After a successful installation, restore the name of this key to* ***FileRename-Operations***.
4	Delete the SQL Server related services from • `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQL` For example - `MSSQL$UNICORN` - `MSSQLFDLauncher$UNICORN` - `MSSQLServerADHelper100` - `SQLAgent$UNICORN` - `SQLBrowser` - `SQLWriter`
5	Rename all folders on Microsoft SQL Server under `C:\Program Files (x86)` , and in any data drive.
6	Reboot the computer.

Tip: *For more information refer to:*
msdn.microsoft.com/en-us/library/ms143412.aspx

Appendix C
Firewall settings

Introduction

If third party firewalls are used within the UNICORN network, the exceptions described in this chapter must be set in order for UNICORN to operate properly. However, if the Windows firewall is used, the UNICORN installation configures the firewall settings.

Note: *Firewall settings which concern the OPC funcationality are listed in* *Section 2.6 OPC settings for UNICORN, on page 80**.*

Firewall program exceptions

Exceptions must be set for the following programs:

Program	Comment
gehealth.exe	Only available when the License server has been installed and is usually found in Program Files Path`\GE Healthcare\eLicense server`
lmgrd.exe	Only available when the License server has been installed and is usually found in Program Files Path`\GE Healthcare\eLicense server`
OPCEnum.exe	Usually found in `C:\WINDOWS\system32`
p950_drv.exe	Usually found in Program Files Path`\GE Healthcare\UNICORN\UNICORN 7.5\bin\Middleware\CU950`
SystemInstallation.exe	Usually found in Program Files Path`\GE Healthcare\UNICORN\UNICORN 7.5\bin`
Sqlservr.exe	Only available in a Database installation and is usually found in Program Files Path`\Microsoft SQL Server\MSSQL12.UNICORN\MSSQL\Bin`[1]
UNICORNClient.exe	Usually found in Program Files Path`\GE Healthcare\UNICORN\UNICORN 7.5\bin`
UNICORN Instrument Server.exe	Usually found in Program Files Path`\GE Healthcare\UNICORN\UNICORN 7.5\bin`
UNICORN Support Service.exe	Usually found in Program Files Path`\GE Healthcare\UNICORN\UNICORN 7.5\bin`
UNICORN User Server.exe	Usually found in Program Files Path`\GE Healthcare\UNICORN\UNICORN 7.5\bin`
RemoteDeploymentService.exe	Usually found in Program Files Path`\GE Healthcare\Remote Deployment Service\UNICORN 7.5\bin`

1 The path is dependent on SQL Server version and database instance name. E.g., `MSSQL12.UNICORN` is the folder name for SQL Server 2014 and the instance name UNICORN.

Firewall port exceptions

Firewall exceptions must be set for the following ports:

TCP port	UDP port	Comment
135		Firewall exception is needed for DCOM communication. Described in *OPC settings, on page 256*.
1433		For communication with SQL Server on the SQL Server computer.
	1434	For use of SQL Browser service in order to locate database instances.
9920		For communication between computers where different parts of UNICORN are deployed.
27000 to 27009		For communication with the License Server on the License Server computer.
40500		Used internally by UNICORN client.
40501 to 40502		For UNICORN client to UNICORN Instrument Server communications.
40503		For NextCU to VID communication. ***Note:*** *Not needed when RTUext is used.*
	40504 to 40510	For communication with instrument. ***Note:*** *Not needed when RTUext is used.*
	50000 to 50003	For communication with instrument. ***Note:*** *Not needed when RTUext is used.*
40511	40511	For RTU/RDS [1] communication.
40512		For RTU communication.
443		For UNICORN User Server communication.
40513		For UNICORN Instrument Server communication.
40514		For UNICORN Instrument Server communication.
40516		For UNICORN User Server communication.

1 Remote Deployment Service

CU-950 and CU-960 TCP ports

The TCP ports used by UNICORN for the CU-950 and the CU-960 (CU) with the listed numbers are shown in the following table. Only one CU per instrument server computer is supported. By default the CU is set to Control Unit number (CU #) 1 and uses the ports listed in the first column. Both inbound and outbound data communication must be allowed for the used ports.

Channel	CU #1	CU #2	CU #3	CU #4
Software & Data storage	60033	60133	60233	60333
Download & Manual	60032	60132	60232	60332
Trend & Event	60031	60131	60231	60331
Info	60030	60130	60230	60330

OPC settings

The User Account Control (UAC) feature in Windows, combined with restrictions applied on DCOM when running UNICORN on Windows computers, makes additional changes to the configuration necessary to allow other OPC clients to communicate with the OPC server. These settings can be applied to Windows both in workgroups and domains if needed.

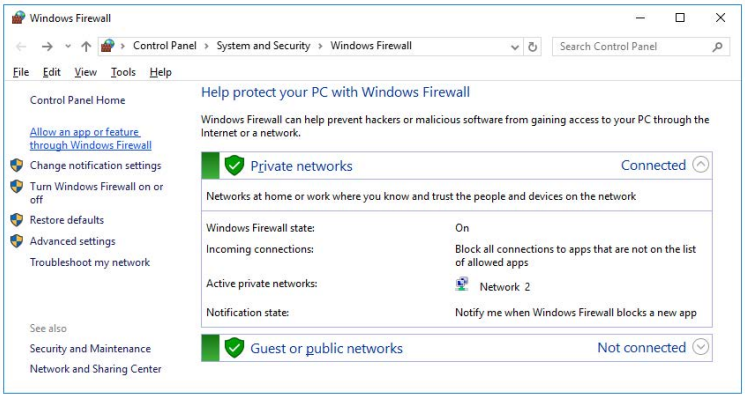
Step	Action
1	If there is a third party firewall[3] enabled on the instrument server: • Allow the ***OPCEnum*** service access (The executable file is located in the ***System32*** directory in the Windows installation directory, typically `c:\windows\system32`) • Allow ***DCOM*** (port 135) access.
2	Continue with the instructions in *Additional configuration, on page 80*.

3 Exceptions for the Windows firewall are added by the UNICORN 7.5 installation program.

Manually define firewall exceptions in Windows Firewall

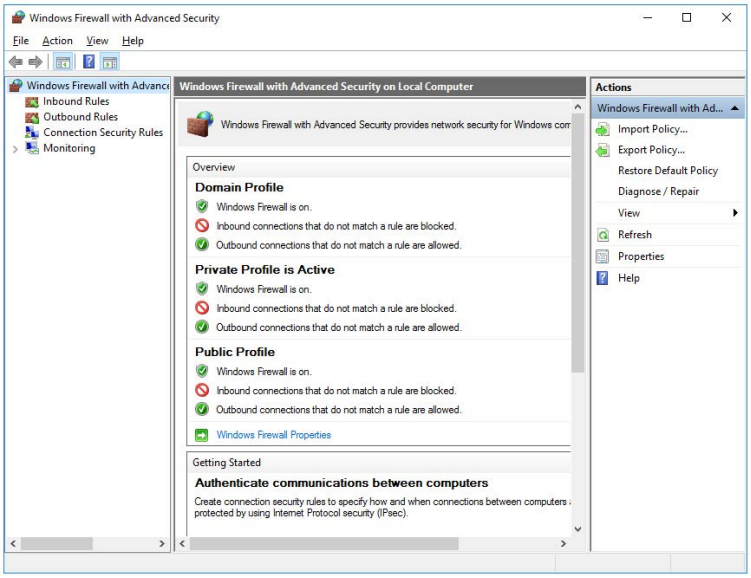
Follow the instructions to define firewall exceptions in the ***Windows Firewall***:

Step	Action
1	In the ***Control Panel*** (category view), click ***System and Security***, then click ***Windows Firewall*** and then click ***Allow an app or feature through Windows Firewall***.
2	Click ***Change Settings*** to make all buttons available, then click ***Allow another app*** to open the ***Add an app***dialog box:
3	• Click ***Browse*** to locate and select the program file you want to add or • select the program in the list and • click ***Add*** to add the program to the ***Allowed programs and features*** pane.
4	Redo step 2 and 3 for all the program files you want to add.
5	Click ***OK*** to close the ***Allow programs to communicate through Windows Firewall*** window and apply the changes.



Adding exceptions for specific ports

Step	Action
1	In the ***Start*** menu search box, type `Windows Firewall with Advanced Security`. Click the Windows ***Firewall with Advanced Security*** item that is displayed as the search result.



2	In the ***Windows Firewall with Advanced Security*** dialog box, in the left pane, click ***Inbound Rules***, and then, in the right pane, click ***New Rule*** to open the ***New Inbound Rule Wizard***.
3	Click ***Port***, then click ***Next***.
4	Click ***TCP***, then select ***Specific local ports***. Type `9920, 40500-40503, 40511, 40512` in the box, then click ***Next***.
5	Click ***Allow the connection***, then click ***Next***.
6	Select the ***Domain***, ***Private*** and ***Public*** check boxes, then click ***Next***
7	Type `UNICORN` in the ***Name*** box, then click ***Finish***.
8	Repeat step 2 to 7 to add an exception for TCP port 135. Name this rule `DCOM`.
9	Repeat step 2 to 7 to add an exception for TCP port 1433. Name this rule `SQL Server`.

Step	Action
10	Repeat step 2 to 7 to add an exception for all TCP ports from 27000 to 27009. Name this rule `License Server`.
11	Repeat step 2 to 7 to add exceptions for all UDP ports from 40504 to 40510, and from 50000 to 50003. Name this rule `UNICORN`

Appendix D
Post-installation settings

Introduction

This appendix describes various recommended post-installation procedures. These procedures ensure proper operation of UNICORN 7.5.

Disk space for a database server (standalone installation)

The free space of the disk or disk partition where the UNICORN archive and backup files are located must be at least 160 GB to avoid errors related to insufficient disk space.

A database for one, or for several, systems that has been in use for an extended period of time contains large amounts of data. Backups corresponding to two weeks and some archived data therefore require a large amount of disk space. For this reason, a minimum disk space of 160 GB must be reserved.

Windows update

Windows update can interfere with UNICORN and interrupt ongoing runs. To avoid this, It is recommended to update windows manually or postpone windows update to a suitable time when UNICORN is not in use.

Anti-virus software

Anti-virus software can interfere with the operation of UNICORN and must be regulated accordingly. It is necessary to avoid any virus scan while runs are in progress to avoid complications.

The following folders must not be scanned:

- Program Files Path`GE Healthcare\UNICORN\UNICORN 7.5\Logs`
- Program Files Path`GE Healthcare\UNICORN\UNICORN 7.5\Logs`
- Program Files Path`GE Healthcare\UNICORN\Runtime backup`
- Program Files Path`GE Healthcare\UNICORN\UNICORN Common Components 7.0\Logs`

- Program Files Path`GE Healthcare\UNICORN\UNICORN Database\Backup`
- Program Files Path`GE Healthcare\UNICORN\UNICORN Database\Logs`
- Program Files Path`GE Healthcare\UNICORN\UNICORN Database\Database`
- `ProgramData\GE Healthcare\LS Gateway`

  Note: *`ProgramData` is a hidden folder in the C: drive.*
- `ProgramData\GE Healthcare\Remote Deployment Service`
- `ProgramData\GE Healthcare\UNICORN`
- `ProgramData\GE Healthcare\Virtual Control Unit`

Disable Power Save

If the UNICORN computer enters standby or hibernation mode while a run is in progress, the run is interrupted for systems not using CU or RTU and the system is disconnected from UNICORN. To avoid this, disable any power save mode settings in Windows. This is done by adjusting the power save options in the Windows Control Panel.

For CU950/960 connected systems, for example, ÄKTApilot and ÄKTAprocess, the run continues and the information is stored on the CU until the memory card is full. For systems using RTU, the run continues and the information is stored locally on the RTU.

Power save must also be disabled for the Network Interface Cards. This is described below.

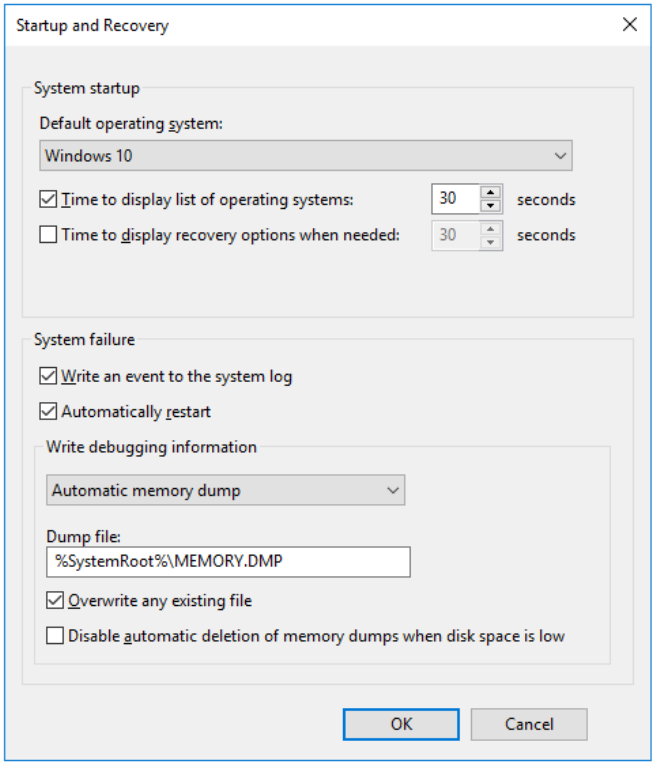
Note: *This process can differ slightly depending on the network card device driver.*

Step	Action
1	Open the Windows ***Control Panel***, and then click ***Network and Sharing Center***.
2	Click ***Change adapter settings*** in the left panel.
3	Right-click the network connection for the Network Interface Card, then click ***Properties***. *Result:* The ***Properties*** dialog box for the network connection opens.
4	Click ***Configure***. *Result:* The ***Properties*** dialog box for the card opens.
5	Click the ***Power Management*** tab, then clear the ***Allow the computer to turn off this device to save power*** check box.
6	Click ***OK*** to apply the changes.

Disable Automatic Restart

Serious errors in Windows can cause the operating system to halt, to prevent possible damage. This is usually caused by faulty drivers. When this occurs, a blue screen is displayed with technical information in white text. The default setting for Windows is to automatically restart after this blue screen is displayed. This is normally not the desired behavior, as the technical information is essential in order to diagnose the cause for the error. It is a recommendation to disable the automatic restart function so that crash codes can be saved. Follow the instructions below to disable the automatic restart function:

Step	Action
1	• Type `Advanced System Settings` in the ***Search Windows*** box, and then press ***Enter***. Result: The ***System Properties*** dialog opens.
2	• Click the ***Advanced*** tab, then click ***Settings*** in the ***Startup and Recovery*** field. *Result:* The ***Startup and Recovery*** dialog box opens.



Step	Action
3	Clear the ***Automatically restart*** check box.
4	Click ***OK*** in all open dialog boxes to apply the changes and close the dialog boxes.

Internet time synchronization

When UNICORN is run in a network environment there is a need to ensure that the time of the connected computers is synchronized. In order to be able to compare time and dates for items stored in the database, for example with timestamps in log files, all UNICORN computers in the network must be on synchronized time.

If the company has an available Internet Time Server, it is preferable that the UNICORN computers are set to automatically synchronize time using that server. If no company Internet Time Server is available, then `time.windows.com` can be used as an alternative.

Note: *Internet time can not be set if the computer is on a domain. If the computer is a member of a domain, then the domain controller handles the time synchronization. So internet time synchronization cannot be set*.

The instruction below describes how to set the Internet time synchronization option.

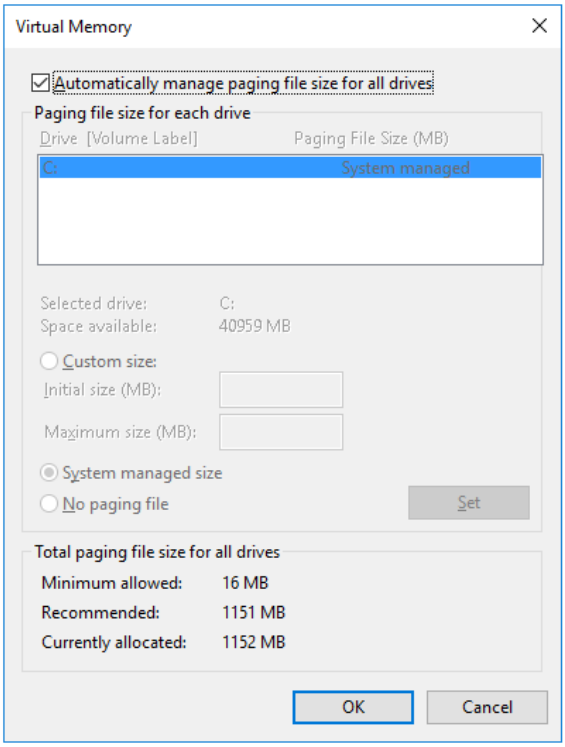
Step	Action
1	Type `Date and Time` in ***Windows Search*** and press ***Enter***. *Result:* The ***Date and Time*** dialog box opens.
2	Click the ***Internet Time*** tab. ***Note:*** *This tab is not shown, if it is disabled by Domain policies.*
3	Click Change settings, and then check the ***Synchronize with an Internet time server*** box.
4	Enter the Internet Time Server in the ***Server*** field.
5	Click ***OK*** to apply the changes and close the dialog box.

Note: *If the UNICORN computer is used for a standalone installation in a workgroup and there is no access to* ***time.windows.com****, clear the* ***Internet time server*** *check box.*

Update paging file size

It is recommended to let the operating system manage the paging file size for a UNICORN 7.5 computer. The following instruction describes the correct virtual memory settings:

Step	Action
1	• Type `Advanced System Settings` in the ***Search Window*** box and then press ***Enter***. Result: The ***System Properties*** dialog opens.
2	• Click the ***Advanced*** tab, then click ***Settings*** in the ***Performance*** field. *Result:* The ***Performance Options*** dialog box opens.
3	• Click the ***Advanced*** tab and click ***Change*** in the ***Virtual memory*** field. *Result:* The ***Virtual Memory*** dialog box opens.



Step	Action
4	• Select the drive where UNICORN 7.5 is installed or select ***Automatically manage paging file size for all drives*** check box. • Click ***System managed size*** ***Note:*** *The **System managed size** radio button is not available if **Automatically manage paging file size for all drives** is selected.*
5	Click ***OK*** in all open dialog boxes to apply the changes and close the dialog boxes.

Set a public network to a private network

Follow the instructions to change a public network to a private network:

Step	Action
1	Type `Local Security Policy` in the Windows search box.
2	Click the ***Local Security Policy*** item that is displayed as the search result. Result: The ***Local Security Policy*** window appears.
3	Click on ***Network List Manager Policies*** on the left. Result: The list of available networks appears.
4	Double-click on the network to be changed. Result: The window of the related network properties appears.
5	Select the ***Network Location*** tab.
6	Select ***Private*** as ***Location type***.
7	Click ***OK*** to save the settings.

Private network settings

Follow the instructions to change the private network settings:

Step	Action
1	Open the Windows ***Control Panel***, and then click ***Network and Sharing Center***.

Step	Action
2	Click ***Change advances sharing settings*** in the left panel.
3	Expand ***Private***.
4	Under ***Network discovery*** select ***Turn on network discovery***.
5	Under ***File and printer sharing*** select ***Turn on file and printer sharing***.
6	Click ***Save changes*** to apply the changes.

Appendix E
Additional computer setting changes

Introduction

This appendix contains instructions how to perform certain computer setting changes after installation.

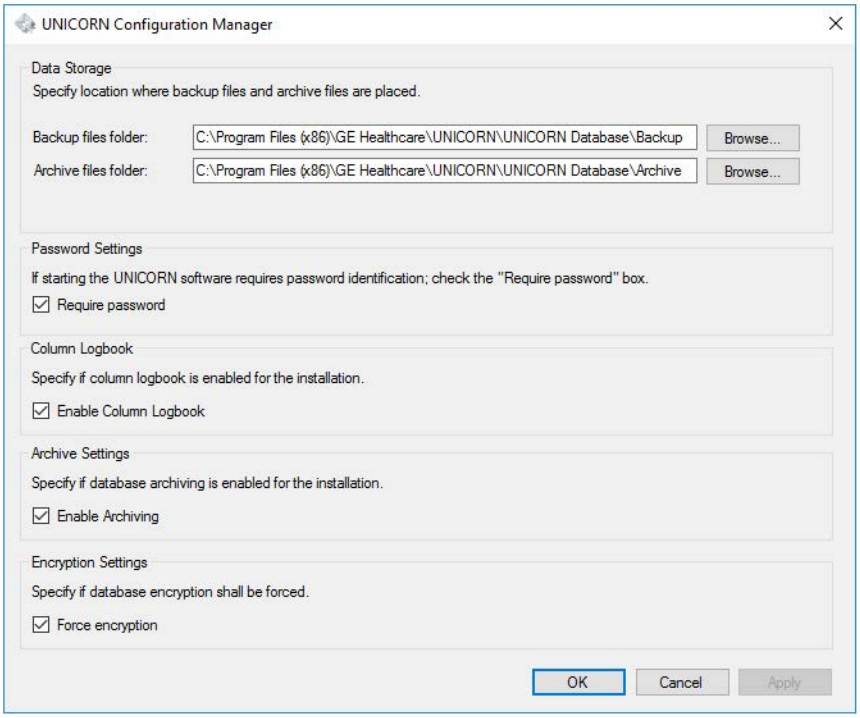
Change installation settings

Certain installation settings can be changed in the ***UNICORN Configuration Manager*** tool.

Note: *It is only possible to log in to the **UNICORN Configuration Manager** as a local UNICORN user or administrator (default). It is not possible for a network user.*

Note: *Only the settings of the local database can be updated in **UNICORN Configuration Manager** and only if the database is located on the SQL Server that is installed by the UNICORN installation program.*

- Start ***UNICORN Configuration Manager***: Click the ***Windows*** Start button, then type `UNICORN Configuration Manager` in the Start menu search field and then click the ***UNICORN Configuration Manager*** item that is displayed as the search result.



In this dialog box you can

- Change folders for backup and archiving.
- Change the settings for password requirements.
- Turn on or turn off the ***Column Logbook***.
- Turn on or turn off database archiving for the installation.
- Turn on or turn off forced database encryption.

Changing standalone or database server computer name

The following instruction describes the steps that must be completed to change the name of the computer which is used for a standalone or database server installation of UNICORN 7.5.

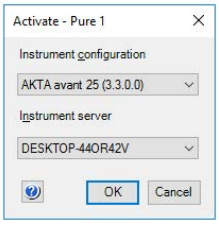
Step	Action
1	Deactivate the system.

Step	Action
2	• Type ***System*** in ***Windows Search*** box and then click ***System*** from the search result. *Result:* The ***System*** dialog opens. • Click ***Change settings*** in the ***Computer name, domain and workgroup settings*** field. *Result:* The ***System Properties*** dialog opens.
3	Click ***Change***.
4	• Enter the new name in the ***Computer name*** field, • click ***OK*** in the open dialog boxes to apply the change, and • restart the computer.
5	After the computer has restarted, open a ***Command Prompt*** window[4].

6	• Change to the database directory by typing the following in the ***Command Prompt***:
	Program Files Path`\GE Healthcare\UNICORN\UNICORN Database\Database`
	• Run the `RenameSQLServer.bat` script by typing the following in the ***Command Prompt***:
	`RenameSQLServer.bat "` old computer name"`\UNICORN` "new computer name"`\UNICORN`
	For example:
	`RenameSQLServer.bat HP14603418012\UNICORN GE145010\UNICORN`

7	Reboot the computer.
8	To verify the name change, open a command prompt window and type the following command: • `sqlcmd -Slocalhost\UNICORN -Q"select @@servername"` *Result:* The new name is shown as in the following example: **GE145010\UNICORN** **(1rows affected)**

4 Type `Command promt` in the ***Windows Search*** box, right-click on ***Command Prompt***, and then click ***Run as administrator***.

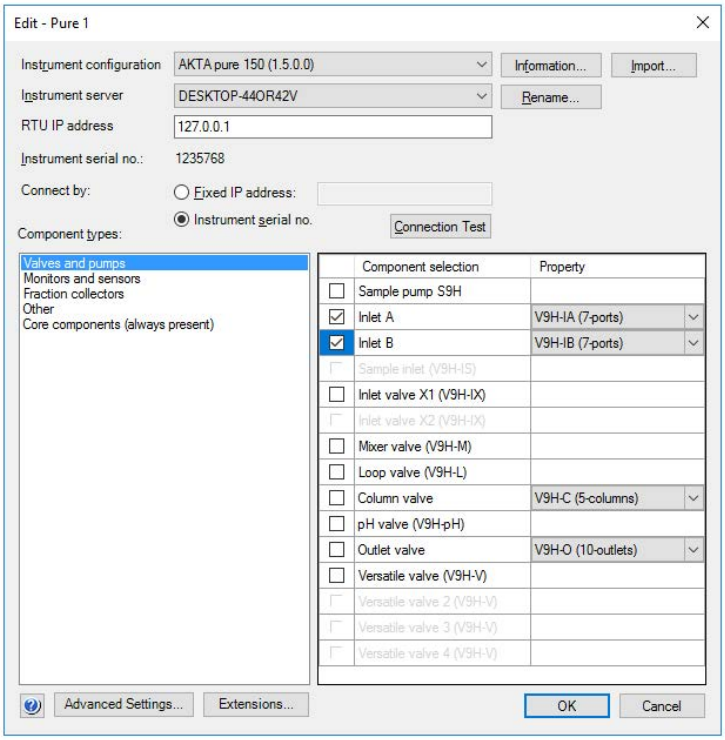
Step	Action
9	Start UNICORN and open the ***Administration*** module.
10	• Open the ***System Properties*** dialog box, • select the system and • click ***Activate***. *Result:* The ***Activate*** system dialog box opens.
11	Click the new server computer name from the ***Instrument server*** list: 
12	• Click ***OK*** to perform the change and • log off UNICORN.
13	Restart the computer.
14	• Start and log on to UNICORN and • connect to the instrument.

Changed name for a computer that serves as an instrument server only

The instruction describes the steps that must be completed if the name of a computer, which is used as an instrument server in a distributed installation, is changed.

Step	Action
1	• Change the name of the computer as described in *Changing standalone or database server computer name, on page 268*. and • reboot.
2	Start UNICORN and open the ***Administration*** module.
3	• Open the ***System Properties*** dialog box, • select the system and • click ***Edit***. *Result:* The ***Edit*** system dialog box opens.

Step	Action
4	Select the new server computer name from the ***Instrument server*** menu:



5	• Click ***OK*** to perform the change and • log off UNICORN.
6	Restart the computer.
7	• Start and log on to UNICORN and • connect to the instrument.

Changed computer names in a distributed environment

If the computer names in a network environment , i.e. not for a standalone system, are changed some configuration files must be updated on the UNICORN instrument server and UNICORN client computers.

Use the UNICORN Service Tool to update the configuration files. The UNICORN Service Tool can be used to update configuration files due to name changes of both the database server and license server computer. See *UNICORN Service Tool Instructions*.

Moving a Workgroup PC to a Domain after a UNICORN 7.5 installation

If a UNICORN computer has been moved from a Workgroup to a domain, make sure that the firewall has been set up to allow UNICORN communication, see *Appendix C Firewall settings, on page 253*.

You can test port communication in the ***Port check*** tab in UNICORN Service Tool. See *UNICORN Service Tool User Manual*.

Actions for cloned computers

If the Windows operating system for a UNICORN 7.5 computer is installed using a cloning mechanism, the cloning must follow the guidelines for disk duplications of Windows installations.

For more information see *The Microsoft policy for disk duplication of Windows installations*.

For more information about imaging and automated installations of different Windows versions, see *Microsoft Deployment Toolkit (MDT) 2012*.

General computer management

If the UNICORN computer is not supplied by GE Healthcare, it is a recommended practice to check the computer vendor website to see if there are any known issues with the computer, and that all computer drivers are up-to-date.

Start the UNICORN HDA Service

The UNICORN HDA service used for OPC browsing of historical data is only registered when a system is defined. To run the service on a PC without defining a system the service must be manually started. This can be done with the UNICORN Service Tool. See *UNICORN Service Tool User Manual*.

Unregister UNICORN HDA Service

Use the UNICORN Service Tool to unregister the ***UNICORN HDA Service***. See *UNICORN Service Tool User Manual*.

Index

T

U

For local office contact information, visit
www.gelifesciences.com/contact

GE Healthcare Bio-Sciences AB
Björkgatan 30
751 84 Uppsala
Sweden

www.gelifesciences.com/unicorn

29448356 AA 12/2019 a1355