Luminex®

complexity simplified.

xMAP INTELLIFLEX® 2.1 System Administrator Guide

RUO   For Research Use Only.

Not for use in diagnostic procedures.

89-00002-00-828 Rev. A

11/2023

Luminex Corporation

12212 Technology Blvd.

Austin, Texas 78727

U.S.A.

Table of Contents

OVERVIEW

The xMAP INTELLIFLEX® System includes a custom integrated computer running Microsoft® Windows® 10 Internet of Things (IoT) Enterprise Long-Term Servicing Channel (LTSC, v1809) in kiosk mode. No external PC is required. Prior to installation, Luminex® asks that customers identify on-site users who will be responsible for the system at a privileged operating system (OS) administrator level. Luminex will supply the identified users with administrator-level access to the underlying OS. This access level is intended to support performing the configuration necessary for security and domain integration. Day-to-day instrument usage does not require ongoing access to the underlying OS. Use accounts that do not provide OS administrator access to perform instrument maintenance and operational tasks.

This document is intended to provide xMAP INTELLIFLEX OS administrators responsible for system security and configuration with a comprehensive informational resource, including:

- Guidance on accessing the underlying operating system
- Best-practices and recommendations
- Cautions and warnings about potentially harmful configurations
- General performance and security information additional to the computing elements of the xMAP INTELLIFLEX instrument
- Links to supplementary content

Where relevant, this document will indicate to which xMAP INTELLIFLEX Software version(s) the guidance applies. A list of released software versions, including support status and changes, is available at: http://www.luminexcorp.com/intelliflex/changes

This document may be updated without notice. For the latest version of this document and for questions not answered here, please contact Luminex Technical Support (*support@luminexcorp.com*) or by the methods listed on the last page of this document).

Additional administrator documents are available upon request from Luminex Technical Support:

- **MDS²** – standard-format Manufacturer Disclosure Statement for Medical Device Security documentation.
- **xMAP INTELLIFLEX Network Connection and Data Flow** – simple diagram overview of system connectivity.

End-user documentation is available online using the following links.

U.S. documentation: https://us.diasorin.com/en/product-documents-manuals

International documentation: https://int.diasorin.com/en/product-documents-manuals

> ⚠ This document is unable to provide a comprehensive list of all configuration elements that may adversely affect the system. Administrators are provided with **full** control over the OS. **Any changes made outside of the guidance in this document may lead to adverse effects**.

Users who elect to make changes outside of the intended use should be advised of the following:

- Luminex strongly recommends users independently validate that the system continues to conform to their needs following any changes.

- Changes outside of those described here may render the system inoperable or cause other abnormal behavior.

- If post-installation changes to the PC render the instrument inoperable, it may be necessary for Luminex Support or Service personnel to revert the system to its initial system state via re-imaging or hard drive replacement in order to properly support the system. **Such methods may lead to the loss of acquired data**. Administrators are strongly advised to export any critical data from the xMAP INTELLIFLEX system before making operating system changes and to be prepared to roll-back changes if necessary.

> This document assumes that administrators have basic functional familiarity with system administration concepts and methods, such as command-line usage. If you are uncertain how to apply the guidance defined in this document, contact Luminex Technical Support before proceeding.

This document uses a grey background format where command-line usage is indicated. The placeholder values to be provided by the administrator are shown in italics; non-italicized text must be entered exactly as shown. For example:

C:\Windows\system32\lmnx action –password *password*

> Luminex strongly recommends that users to refrain from using lmnx commands outside of the lmnx commands that Luminex recommends in this guide. Usage of a non-approved command may render the system inoperable or cause other abnormal behavior.

USER INFORMATION AND ACCESSING WINDOWS®

⚠️ To comply with cybersecurity best practices, Luminex® does not retain administrator-level access to the xMAP INTELLIFLEX® Instrument. Accordingly, Luminex cannot provide a method to reset the system. If the administrator password is lost, the only recovery method will be to revert the instrument to its initial factory state. A factory reset will permanently remove all data and settings present on the instrument. Users must take into consideration that the default password for admin expires 90 days after the instrument is manufactured. Therefore, it is the user's responsibility to create and maintain an admin password before the default password expires.

Pre-defined User accounts

The instrument is configured with four* predefined local Microsoft® Windows® accounts:

1. User: **LuminexFieldService**

   - A dedicated account for use only by Luminex Field Service Engineers to perform required system maintenance
   - May not be modified by the administrator, although administrators are provided with optional methods to restrict access
   - See Luminex Service Access for more details
   - The LuminexFieldService account signs into Windows with standard user permissions and is able to access a user-level Windows desktop.

2. User: **admin**

   - Default password: admin (expires 90 days after instrument manufacture)
   - The admin account is intended for infrequent configuration tasks within the xMAP INTELLIFLEX Software interface or within the underlying OS, including configuring users and administering the Global settings page of the xMAP INTELLIFLEX interface.
   - After performing actions as the administrator, restart the instrument to properly continue use under an xMAP INTELLIFLEX user account.
   - The admin account signs into Windows with administrator permissions and is able to access an administrator-level Windows desktop.

3. User: **lablead**

   - Default password: password (expires 90 days after instrument manufacture)
   - The lablead account is intended for day-to-day instrument use operations, including operations that define the parameters of instrument acquisitions.
   - The lablead account signs into Windows with standard user permissions and has no direct access to the underlying OS, only to the xMAP INTELLIFLEX Software running in kiosk mode.

4. User: **operator**

    - Default password: password (expires 90 days after instrument manufacture)
    - The operator account is intended for day-to-day instrument use operations, including operations required to maintain the instrument.
    - The operator account signs into Windows with standard user permissions and has no direct access to the underlying OS, only to the xMAP INTELLIFLEX Software running in kiosk mode.

Refer to the *xMAP INTELLIFLEX System User Manual* and the Authorizations page of the xMAP INTELLIFLEX Software interface for additional details regarding pre-defined accounts.

*Instruments that were originally installed with software version 1.0 will include an additional predefined account. The 'INTELLIFLEX User' (password: user) account previously present in xMAP INTELLIFLEX v1.0 will remain present and active with operator-level permissions. Administrators may delete this user account at their discretion.

> The default built-in accounts can be disabled or removed.
>
> **NOTE:** At least one administrator account for the instrument must exist at all times.

> Field service engineers cannot service the Instrument without access to the software. If the LuminexFieldService default account is disabled or if the password for the account is changed, an administrator will need to be re-enable the account or set a temporary password when a Luminex Field Service Engineer is on-site to service the Instrument.

Manage User Accounts

The xMAP INTELLIFLEX® user permissions are managed via membership in four pre-defined Windows® groups:

1. **Administrators** (grants administrator-level access to both Windows and the xMAP INTELLIFLEX Software interface).
2. **Luminex Lab Leads** (grants lab lead-level access to the xMAP INTELLIFLEX Software interface).
3. **Users** (grants operator-level access to the xMAP INTELLIFLEX Software interface).
4. **Luminex Field Technicians** (grants user-level access to Windows and access to the Service sections of the xMAP INTELLIFLEX interface software).

Administrators can create and manage users either locally (local to the Instrument) or through a connected domain. Only assign users membership in one of the pre-defined groups. If users are assigned membership in multiple groups, they will receive the highest permission level of the groups that they are a member of.

The xMAP INTELLIFLEX Software interface provides methods to force users to change their passwords, to configure user lockout variables, etc. See the *xMAP INTELLIFLEX System User Manual* for more information on managing users through the xMAP INTELLIFLEX Software interface. Administrators can create users via standard Windows user management tools and can manage permissions by assigning users to the Administrators group or Luminex Lab Lead group; all other users receive the default operator permissions.

⚠️ Administrators should not assign users to the Luminex Field Technicians group. Access to the Service sections of the xMAP INTELLIFLEX Software interface requires authentication from Luminex via an offline challenge/response mechanism, so users assigned to the Luminex Field Technicians group will be unable to log-in to the xMAP INTELLIFLEX Software.

The xMAP INTELLIFLEX Software does not provide a method to modify the individual permissions granted to each user group within the xMAP INTELLIFLEX Software.

Sign in to the Admin Account

Sign in as a user with administrator credentials via the same method as standard user sign in: enter a username and password in the sign in prompt.

Auto Sign-In

Optionally, an administrator may provide a username, password, and domain (or leave blank to use a local user) for an auto sign-in user. The software does not specify an auto sign-in user by default. If no auto sign-in user is specified, the system will boot to a sign in prompt.

Refer to the *xMAP INTELLIFLEX System User Manual* for more information.

Auto-Lock

Administrators may configure the xMAP INTELLIFLEX® system to lock after a defined number of minutes. Administrators may also define a second inactivity interval, after which the system will transition from the sign in page to the system-status page.

These methods use underlying Windows® features related to custom sign in pages and screensaver time-outs. Domain or local policy restrictions may adversely affect these methods. Refer to policy information in *Domain Integration* for further details.

Access the Windows® Desktop

When signed in to the xMAP INTELLIFLEX® Software as an administrator, the Windows desktop is accessible from the xMAP INTELLIFLEX Software interface:

1. Select the **Main Navigation** button at the top-left corner of the interface.
2. Select the **Desktop** button at the bottom-left of the **Main Navigation** menu, immediately above the red **Switch Users** button.

Open an Administrator-Level Command Prompt

1. From the Windows® Desktop (refer to *Access the Windows® Desktop* for more details) press **Windows+R** on the keyboard to open the **Run** dialog box.
2. Enter **cmd** in the **Open** field.
3. Press **Ctrl+Shift+Enter** on the keyboard.
4. Select **Yes** to allow the app to make changes to the device, if necessary.

Change the Admin Password

Administrators may use the xMAP INTELLIFLEX® Software interface to require other administrators to change their password upon next sign in. Refer to the *xMAP INTELLIFLEX System User Manual* for guidance on administering users through the software interface

Administrators may change their own password from Windows®: Settings > Accounts > Sign-in Options.

Luminex Field Service Access

Luminex Field Service access uses a dedicated LuminexFieldService user account. This account is inaccessible to the OS administrator and does not provide Luminex Field Service Engineers (FSEs) with access to Windows® at the administrator-level.

Access to this account is controlled by a two-password system:

1. A password controlled by the OS administrator. OS administrators may change this password to prevent Luminex FSEs from accessing the instrument without direct approval from the administrator.

   > ⚠️ Changing LuminexFieldService password may delay instrument service. Luminex FSEs will be unable to access required software components without administrator approval. Administrators who choose to change this password for security reasons must be prepared to provide system access when needed by FSEs. Luminex is not responsible for servicing delays caused by changes to this password.

2. A challenge-response key. Upon sign in with the OS password, the Luminex FSE will receive a daily challenge code, which is unique to that instrument. Offline Luminex methods will provide a response. A correct response will provide the FSE with access to the xMAP INTELLIFLEX Software, including Service portions of the software. Non-Luminex users, including the OS administrator, do not have access to the challenge/response system or to the service software.

Authentication Logging

Sign in activity is recorded in Windows® security logs, available to the end-user through standard Windows methods. If Electronic Record Compliance is licensed and enabled, sign in activity is also recorded in xMAP INTELLIFLEX® System logs, which are viewable and exportable from the xMAP INTELLIFLEX Software interface.

Account Lockout

The xMAP INTELLIFLEX® System uses the Windows® default Account Lockout Policies. Optionally, the user may configure the lockout settings on a non-domain instrument.

To configure:

1. Sign in to the xMAP INTELLIFLEX System with the Admin account
2. Select ☰ in the upper left-hand corner of the screen and navigate to **CONFIGURATION** > **GLOBAL**.
3. Enter values in the **LOCKOUT DURATION**, **LOCKOUT THRESHOLD**, and **LOCKOUT OBSERVATION** window.

NOTE: Domain policies will override local account lockout policies.

CONFIGURATION RECOMMENDATIONS

Network Configuration

OS administrators may use standard Microsoft® Windows® tools to configure the network interface (DHCP, DNS, etc.). DHCP server is responsible for assigning a dynamic TCP/IP configuration, but administrators can set the instrument to use a static IP address using Settings app or commands.

Barcode Scanner, Keyboard, Mouse, or Other Ancillary Hardware Additions

OS administrators may use standard Windows® methods to add USB or network printers to the system.

NOTE: Luminex does not test or validate the system for use with any specific ancillary hardware and the possibility exists that specific drivers may result in conflicts. While no specific problems are anticipated, Luminex recommends that users validate that the system continues to conform to their needs after installing any additional devices. Luminex recommends using peripherals that can operate as standard HID devices and that do not require installation of additional drivers.

Regionalization

The xMAP INTELLIFLEX® System does not support regionalization and requires a regionalization setting of US English. Luminex strongly recommends against altering any Windows® regionalization settings as doing so may render the xMAP INTELLIFLEX software unusable.

The xMAP INTELLIFLEX interface (SETTINGS > CONFIGURATION > GLOBAL) provides methods to customize the decimal- and field-separator delimiters used in output data. These methods may be used to configure output data for compatibility with regionalized external applications.

These configurations only affect output data; imported data must be provided using US English conventions:

- Period character (".") for decimal separator
- Comma character (",") for field separator

Date/Time Configuration

OS administrators may use standard Windows® methods to configure the system date, time, and time zone.

⚠️ Luminex recommends against changing the date, time, and time zone settings while the system is actively acquiring data or undergoing calibration or performance verification.

NOTE: After making any changes to the system clock or calendar, restart the xMAP INTELLIFLEX Instrument.

Email Configuration

The xMAP INTELLIFLEX® Software includes a feature that allows standard users to export system log data as a .ZIP file for troubleshooting purposes. Optionally, the user may configure SMTP information to enable sending this file directly to Luminex Technical Support via email.

To configure the functionality to email a .ZIP log file directly to Luminex Technical Support:

1. Sign in to the xMAP INTELLIFLEX System with an administrator account.
2. Select ☰ in the upper left-hand corner of the screen and navigate to **CONFIGURATION** > **GLOBAL**.
3. Enter a value in the **SmtpServerName**, **Username**, and **Password** fields.

Changing the PC Name

OS administrators may use standard Windows® methods to change the name of the xMAP INTELLIFLEX® PC at their discretion. The PC Name is referred to as the Machine Name or Instrument Name within the software and reports.

NOTE: If the customer has more than one xMAP INTELLIFLEX instrument, the instruments should all be given unique network names. Failure to do so may cause the software to fail to start on some of the network attached instruments.

Windows® Restore Points

The xMAP INTELLIFLEX® System does not enable Windows® restore points by default. Administrators may enable and use Windows restore points at their discretion.

⚠	Restore operations may permanently delete data acquired after the restore point is used.

Domain Integration

Administrators may add the xMAP INTELLIFLEX® System to a network domain at their discretion.

NOTE: When the System is added to a domain, in order to sign in to the Instrument with a Local Machine account, the user must precede their username with ".\". As an example, assuming the username is "localAdmin", to sign in, the user would put ".\localAdmin" for the username.

Luminex recommends refraining from applying Group Policies to the xMAP INTELLIFLEX instrument directly or via policy related registries unless explicitly permitted by this guide. Setting such policies may impact the behavior, look, and feel of the instrument. The following policies are known to impact the operation of the instrument:

Windows Updates/Drivers:

- *Computer Configuration > Administrative Templates > Windows Components > Configure automatic Windows Updates*
- *Computer Configuration > Administrative Templates > Windows Components > Do not include Drivers with Windows Updates*
- *Computer Configuration > Administrative Templates > System > Device Installation > Prevent*

device metadata retrieval from the Internet

- *Computer Configuration > Administrative Templates > System > Device Installation > Specify search order for device driver source locations*

Lockout Policies:

- *Computer Configuration > Windows Settings > Security Settings > Account Lockout Policy > Account lockout duration*
- *Computer Configuration > Windows Settings > Security Settings > Account Lockout Policy > Account lockout threshold*
- *Computer Configuration > Windows Settings > Security Settings > Account Lockout Policy > Reset account lockout counter after*

Screen Saver:

- *User Configuration > Administrative Templates > Control Panel > Personalization > Enable screen saver*
- *User Configuration > Administrative Templates > Control Panel > Personalization > Force specific screen saver*
- *User Configuration > Administrative Templates > Control Panel > Personalization > Screen saver timeout*

Login Screen/ Desktop Background:

- *Computer Configuration > Administrative Templates > Control Panel > Personalization> Force a specific default lock screen and logon image*
- *Computer Configuration > Administrative Templates > Control Panel > Personalization> Do not display the lock screen*
- *Computer Configuration > Administrative Templates > Control Panel > User Accounts> Apply the default account picture to all users*
- *Computer Configuration > Administrative Templates > Personalization> Prevent changing start menu background*

User Account Audit:

- *Security Settings > Local Policies > Audit policy > Audit account management*
- *Security Settings > Local Policies > Audit Logon events*

Domain policies may be used to map network drives for xMAP INTELLIFLEX users.

Windows® Server Update Services (WSUS) Integration

Administrators may configure the xMAP INTELLIFLEX System to receive updates from the WSUS server. To configure the xMAP INTELLIFLEX System to connect to the WSUS server:

1. Open the **Group Policy Editor**.

2. Expand **Computer Configuration > Administrative Templates > Windows Components**, and select **Windows Update**.

3. Select **Specify intranet Microsoft update service location** and enable the policy.

    a. Under **Set the intranet update service for detecting updates**, enter the URL for the WSUS server: *http://wsusServer[:port]*, where *wsusServer* is the name of WSUS server

and *port* is the port number.

    b.   Under **Set the intranet statistics server**, enter the same URL.

4.   Select **Allow signed updates from an intranet Microsoft® update service location** and enable the policy.

5.   Select **Do not allow update deferral polices to cause scans against Windows Update** and then enable the policy.

MANAGING DATA AND FILE-SHARING

Shared Network Folder Access

The xMAP INTELLIFLEX® Software does not provide a method to map network drives for lab lead- or operator-level users. Network data export may be managed in a variety of ways:

- Users may manually enter a UNC path for manual export operations. If needed, the user will be prompted for access credentials.

NOTE: Users must confirm the correct folder is selected when manually entering a UNC path.

Domain-connected instruments:

- The domain administrator may give the xMAP INTELLIFLEX PC write access to a network location. The xMAP INTELLIFLEX administrator or lab lead may configure the xMAP INTELLIFLEX software to automatically export data to this UNC path.

- Domain policy may map one or more network drives for users. Users may manually export data to mapped network drives, or the administrator may configure xMAP INTELLIFLEX software to automatically export data to a single mapped drive letter.

Data Storage

Data acquired on the instrument is retained in various formats:

- In an internal, unencrypted SQL Server database

  - Users are not provided with methods to access the database directly.

  - The database is an integral part of the application architecture and may not be moved to an off-instrument location.

  - Data is written to the database at the time of acquisition and is not modified by subsequent operations.

  - Administrators are authorized to Read/Write access of the SQL database. However, the only supported access to the data is using the installed xMAP INTELLIFLEX software.

  - ODBC connections are not supported.

- Raw fluorescence data is stored on the file system as .LXB files. Such files are non-human readable, are inaccessible to the end user, and are intermediary files; they are not considered the final result of an acquisition.

- Acquisition data may be manually or automatically exported from the instrument as human-readable CSV files in two file formats. This data is considered the final, calculated result from acquisition. Refer to the *xMAP INTELLIFLEX System User Manual* for more information on file formats.

- XLS files, containing both acquisition data and configuration/logging data associated with the acquisition.

Data Export

The xMAP INTELLIFLEX® Software supports data output in three file formats:

1. xPONENT CSV format – where possible, retains compatibility with the existing xPONENT file specification for use in existing applications compatible with this format.

2. INTELLIFLEX CSV format – a streamlined and customizable file format. The user may optionally configure the statistical and metadata values to be included in an exported file. Exporting to the INTELLIFLEX file format with all optional values selected is the most complete backup method available to the end user.

3. INTELLIFLEX XLSX format – a comprehensive data format with the same customizability of the INTELLIFLEX format (a user may define which metadata and statistical content to include), with additional log data and a comprehensive record of configuration events leading to acquisition and creation of the data.

   NOTE: xMAP INTELLIFLEX Software does not provide methods to restore data from exported CSV or XLSX. Results deleted from the instrument are permanently deleted. Administrators should use caution to ensure that comprehensive data is exported before deleting results from xMAP INTELLIFLEX Software.

Data Capacity

There is no fixed limit to the number of plates the instrument can store. The amount of data allocated per plate varies based on multiplex and other factors but is approximately 5-50mb per 96-well plate. The xMAP INTELLIFLEX® PC contains a 512GB hard drive, though a fraction of this capacity is consumed by the application, OS, and system configuration. Generally, the xMAP INTELLIFLEX system's data storage capacity is expected to exceed 1 year under common usage conditions. The software will notify the user when the storage capacity approaches a database or file-system limit. Refer to the *Archive Results* section in the *xMAP INTELLIFLEX System User Manual* for information on archiving results to increase available storage.

Database Security

Only the Local System Account and any users in the local administrators group have direct access to the local SQL Server database. The Administrator is responsible for maintaining the security of these accounts and, thus, of the onboard database.

SYSTEM BACKUP AND RESTORE

Starting with INTELLIFLEX version v2.0, a full system backup may be initiated from both the command line and INTELLIFLEX user interface. All backups are full system backups that include both the OS state and application data created with the Windows® wbadmin utility. The backup creates a folder within the specified path to store the image. The name of the folder is based on the date and time the image was created, using the following format: yyyy-MM-dd-T-HH-mm-ss. For example, if a backup image was created on April 28, 2022 at 18:28.27, the folder would be named 2022-04-28-T-18-28-27. The time required to back-up a system varies depending on several factors. However, a typical backup will require several minutes to complete.

These instructions assume you are familiar with using the Windows® backup tool and the command line.

A reciprocal command is available to restore the instrument to the backup state of the instrument. The restore feature is only available as a command-line function. The restore feature relies on the lmnx.exe application. The lmnx.exe file is copied to the target backup folder when the backup is created via the user interface. If the backup is created by other means, such as the command-line, the lmnx.exe file may not be readily available. In these instances, you can copy the lmnx.exe file from the instrument. The file can be found on the INTELLIFLEX instrument in the path "**C:\Program Files\Luminex\lmnx X.X.XXX.X**," where X.X.XXX.X is the version of the lmnx.exe tool.

NOTE: Backups include all OS and applications settings, including settings established by the Field Service Engineers. It is recommended to take a backup image prior to performing any software or system upgrade.

NOTE: The USB or external SSD drive must be in NTFS format.

Backup System from User Interface

Create a backup via the user interface:

1. Connect the USB or external SSD drive if necessary.

   NOTE: The USB or external SSD drive must be in NTFS format.

2. Sign in to the xMAP INTELLIFLEX System with an administrator account.

3. Select ☰ in the upper left-hand corner of the screen and navigate to **SETTINGS** > **ABOUT**.

4. Select the **Create Windows Backup Image** button.

5. Select the appropriate USB, external SSD or network drive, and the desired folder for the backup.

6. Press the **Select** button to start the backup process. A message displays indicating the backup is in progress.

   a. Select **Yes** in the **User Account Control** dialog if necessary.

   NOTE: Backup process runs in background in command window. Closing the command window prematurely will show INTELLIFLEX notification error: *Failed to create windows backup image, error code: -1073741510*. However, the backup process is still running and visible in task manager.

   A message is recorded in the Notification center when the backup is complete.

7. If applicable, once the backup is created, remove the USB drive and store it in a safe place.

Backup System from Command-Line

Create a backup via the command line:

1. Open an administrator-level command prompt (refer to *Open an Administrator-Level Command Prompt* for details).

2. Enter lmnx backup –p *BackupDesiredFolder* in the administrator command prompt, where *BackupDesiredFolder* is the folder path where the backup file should be placed (for example, "D:\MyBackups"). Press Enter.

    NOTE: The default path is D:\ when the –p parameter is not included. The path may be either an attached USB, external SSD or Network drive. If the path contains spaces, it must be quoted. For example:
    lmnx backup -p "D:\Backup Directory"

System Restore

Restore a system backup**:**

1. Enter the Windows Recovery Environment:

    a. Select the **Windows Start Menu**.

    b. Select the **Power** button.

    c. Press and hold the Shift button (on the keyboard) and select **Restart**.

2. Select **Troubleshoot**.

3. Select **Advanced Options**, then select **Command Prompt** on the next page that pop ups. The system will restart.

4. Sign in as an administrator user. A command prompt at the root directory of X should now be showing.

5. Locate the drive letter where the Windows folder resides. This is the *TargetDrive*.

    NOTE: Change the directory by entering the drive name followed by colon (for example E:)

6. Find the path to the *SourceBackupPath* directory.

    This is the folder named as a timestamp that was created by the backup. For example, if the system backup targeted the "**\MyBackups**" folder on a USB drive and the USB drive is now drive E:\, the path would be "**E:\MyBackups\{timestampFolder}**".

7. Change directory to the root of the *SourceBackupPath* drive (E:\ in the example).

    NOTE: lmnx.exe will be in this directory.

8. Type .\lmnx.exe restore –p *SourceBackupPath* –t *TargetDrive* (where *SourceBackupPath* is the path from Step 6 and *TargetDrive* is the drive from step 5), then press Enter.

    For example: .\lmnx.exe restore –p E:\MyBackups\2022-04-28-T-18-28-27 –t C: will restore a backup taken at 7:28:27 on 4/28/202 to the E:\MyBackups folder. The leading **.** is important because it tells Windows to run lmnx.exe from your current directory.

    NOTE: The lmnx restore function is not compatible with mapped drives. Use the UNC path when restoring from a network drive. For example: lmnx.exe restore –p \\MyServer\MyBackups\2022-04-28-T-18-28-27 –t C:

9.   Type **Exit**.

10. Select **Continue to Windows 10**.

GENERAL SYSTEM INFORMATION AND CAUTIONS

Ports

Luminex® does not specifically disable unused ports. No specific ports are required for standard operation, and operating system (OS) administrators may disable ports at their discretion.

Services

The xMAP INTELLIFLEX System requires the following services to be running and configured for automatic start up:

- Luminex INTELLIFLEX Services
- Luminex INTELLIFLEX IC Services
- SQL Server (INTELLIFLEXSQL)

Disabled Windows® Tools

Telnet and FTP are disabled by default.

Non-Luminex Software Dependencies

- SQL Server 2016
- .NET Framework v4.8

Install Additional Software

Luminex does not test or validate the xMAP INTELLIFLEX® System with any third- party software. Using unauthorized third-party software with the xMAP INTELLIFLEX Software may result in corruption or failure of the xMAP INTELLIFLEX Software. Do not use third-party software on the xMAP INTELLIFLEX System. Administrators who choose to install any additional software are strongly advised to:

- Validate that system performance continues to conform to your needs, and be prepared to revalidate if such software is updated at a later date.
- Be prepared to rollback changes, if needed.

Software changes may render xMAP INTELLIFLEX Software inoperable. Restoration to working state may require a complete wipe of the internal hard drive, resulting in the loss of all acquired data. Ensure that all critical data is exported or recorded before applying any software changes.

Operating System Updates

The xMAP INTELLIFLEX® System is configured to disable automatic Windows® updates by default. Administrators may re-enable updates at their discretion, using either standard Windows methods or a dedicated option within the xMAP INTELLIFLEX Software (CONFIGURATION > GLOBAL).

The xMAP INTELLIFLEX Software is tested in a configuration that receives updates directly from Microsoft®. Luminex does not anticipate specific problems with deploying updates through WSUS or domain control, but has not validated or tested such methods.

Luminex does not test xMAP INTELLIFLEX software for compatibility with specific Windows updates. While Luminex does not anticipate problems, any changes to the tested configuration have the potential to cause performance problems or unexpected errors. Users who enable operating system updates are advised to perform their own validation testing to ensure that system performance continues to conform to their needs and to be prepared to roll-back updates as needed.

xMAP INTELLIFLEX® Software and Firmware Updates

Updates to the xMAP INTELLIFLEX® software are delivered by Luminex in the form of a digitally signed file. Installing xMAP INTELLIFLEX software and firmware updates requires OS administrator-level access.

Updates are provided on an as-needed schedule determined by Luminex, not at a fixed calendar interval.

Encryption At Rest

The file-system is not encrypted by default. As of xMAP INTELLIFLEX® Software v1.1, the TPM chip on the system will be enabled. Administrators may enable BitLocker at their discretion.

Encryption In-Transit

The xMAP INTELLIFLEX® System does not require any external network interface to operate. Administrators may optionally configure the system for flat-file transfer via standard Windows® methods.

TLS (Transport Layer Security)

The xMAP INTELLIFLEX® System uses an HTTPS interface for its Automation Clients. This interface is encrypted using TLS 1.2. TLS 1.0 & 1.1 are disabled system-wide via the registry settings under HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

Luminex recommends against enabling TLS 1.0 or TLS 1.1 through a Group Policy.

NOTE: The Automation API is accessed via port 443 over an SSL connection.

Electronic Certificates

Starting with v2.0, the xMAP INTELLIFLEX® Software uses x509 electronic certificates to identify the instrument when creating digital signatures and to verify the validity of license files using the instrument's serial number. To establish the instrument's identity, its certificate is signed by Luminex's private certificate authority.

Hardcoded Passwords

None.

Confidential Data

Proper use of the system does not require entry or storage of any confidential patient information. Various fields in the xMAP INTELLIFLEX® software accept free-text data. Data exported from the system or included in the exported Support Package for Luminex Technical Support may include the content of these fields. Luminex recommends that users incorporate administrative controls to prevent entry of any potentially confidential patient information into these free-text fields.

Windows® Power Settings

Administrators should not modify the Windows® power-management settings locally or via domain policy. The xMAP INTELLIFLEX® System should not be configured to enter any reduced state (e.g., the system should not be configured to drop to a reduced power consumption mode). Configuring the system to enter a reduced state will likely cause data loss if the system status changes during acquisition operations.

The xMAP INTELLIFLEX Software supports methods to automatically or manually sign out the active user at any time, including while an acquisition is in progress.

Anti-Virus/Malware Protection

Microsoft Defender® is enabled in its default configuration, with no Luminex-applied exclusions. Administrators may disable Microsoft Defender® at their discretion.

While Luminex does not anticipate any specific problems from the installation of third party antivirus or malware protection applications, Luminex does not test or validate the xMAP INTELLIFLEX® System with any specific third party tools. Administrators who choose to install and enable additional antivirus tools are advised:

- To validate that the system continues to conform to their needs.
- To be prepared to rollback changes if needed.
- Luminex recommends against performing scans during data-intensive operations, such as during data acquisition operations.

File/Folder Exclusion and Whitelisting Considerations

The following is a list of files and folders that should be considered for exclusion or whitelisting from any malware scanning software products.

- **C:\ProgramData\Luminex**

  Instrument software writes log files and data to this location. Scanning this folder may result in undue stress for resources.

- **C:\Program Files (x86)\Luminex\INTELLIFLEX\ICService.exe**

  A Windows® Service that runs under the SYSTEM account. This can be recognized as a threat by some Malware Scanners.

- **C:\Program Files\Luminex\Intelliflex Services\Luminex.Intelliflex.Service.exe**

  A Windows® Service that runs under the SYSTEM account. This can be recognized as a threat by some Malware Scanners.

- **C:\Program Files\Luminex\INTELLIFLEX Touchscreen\IntelliflexTouchscreen.exe**

- **C:\Program Files\Luminex\INTELLIFLEX Touchscreen\IntelliflexTouchscreen.dll**

    Application binaries that may be recognized as a threat by some Malware Scanners.

- **C:\Program Files\Luminex\lmnx 2.1.80.0\lmnx.exe**

    Application binary that may be recognized as a threat by some Malware Scanners.

Network Time/Date

Administrators may connect the xMAP INTELLIFLEX® System to a network-time server at their discretion. The xMAP INTELLIFLEX Software operations are logged in UTC+offset format.

USB

Users are expected to configure the system to either export to USB drive or to export to network, but USB data transfer is not required for system operation.

Remote Access

The xMAP INTELLIFLEX® System does not enable methods to remotely access the system.

Luminex personnel have no method to access the instrument remotely.

RDP is disabled by default. Luminex does not validate enabling and using RDP.

Digitally Signed Excel Reports

The xMAP INTELLIFLEX® digitally signed Excel (XLSX) reports cannot be viewed in a browser window.

MISCELLANEOUS NOTES FOR ADMINISTRATORS

Power Off the xMAP INTELLIFLEX® System

If the soft power button on the xMAP INTELLIFLEX® System is depressed while the xMAP INTELLIFLEX Software interface is not in the foreground, the xMAP INTELLIFLEX System will not power off. Return to the xMAP INTELLIFLEX Software interface and acknowledge the power off confirmation dialog to properly power off the xMAP INTELLIFLEX System.

Restart After Configuring Settings

Changes to the following settings available in the CONFIGURATION > GLOBAL page do not take effect until after the instrument has been restarted.

- Auto Sign-in User Name
- Auto Sign-in Password
- Auto Sign-in Domain
- Automatic Windows Update

Restart the xMAP INTELLIFLEX® System after modifying these system settings, as indicated by the notification message.

SCHEDULED TASKS

The xMAP INTELLIFLEX® Software creates several scheduled tasks. Tasks are configured to run based on system status, such as being idle for a pre-configured amount of time, on startup, sign on, sign off, or only for a specified time.

Check Databases Capacity

Checks the size of the databases on the system and rolls over specific databases when they meet a threshold. It runs at 12:00 AM every day.

Condense Results

Removes old result entries from the system after they have been archived. It runs at sign in of any user. After triggered, the task runs every day indefinitely.

Delete Temporary Files

Removes diagnostic logs. It runs at sign in of any user. After triggered, the task runs every day indefinitely.

Export Queued Files

Assists in moving auto-export files to their final destination. It runs at sign in of any user. After triggered, the task runs every minute indefinitely.

PurgeUserOnLogonTaskName

Purges inactive users. It runs at sign in of any user or after an account is unlocked.

ScreenSaverOnLockWorkstationTask

Sets screen saver timeout on workstation lock. It runs on workstation lock of any user.

ScreenSaverOnLogonTask

Configures screen saver settings on user sign in. It runs at sign in of any user.

ScreenSaverOnUnlockWorkstationTask

Sets screen saver timeout on workstation unlock. It runs on workstation unlock of any user.

Start Data Collector

Starts a Windows® Data Collector named INTELLIFLEX. This helps diagnose performance issues when they occur. It runs at sign in of any user. After triggered, the task runs every 4 hours indefinitely.

StartServiceOnStartUpTask

Starts the Luminex INTELLIFLEX Services. It runs at system startup and every 60 seconds after the initial trigger. This ensures that the service is promptly restarted should it ever fail.

LUMINEX TECHNICAL SUPPORT

Contact Luminex Technical Support by telephone in the U.S. and Canada by calling: 1-877-785-2323

Contact outside the U.S. and Canada by calling: +1 512-381-4397

International: + 800-2939-4959

Fax: 512-219-5114

Email: *support@luminexcorp.com*.

Additional information is available on the Luminex website. Search on the desired topic, navigate through menus. Also, review the website's FAQ section. Enter *http://www.luminexcorp.com* in your browser's address field.

This manual can be updated periodically. To ensure that you have a current version, contact Technical Support.