Luminex

Luminex xMAP Software Security Information and Recommendations

Overview

Luminex software is tested and validated as standalone software in a non-networked environment. Adding Luminex PCs to a domain, installing third-party software alongside Luminex software, or other various PC configuration changes may prevent Luminex software from installing or functioning properly, or may lead to other unexpected behaviors.

Luminex cannot provide comprehensive guidance to ensure that domain migration or other configuration-altering processes will be successful, but does provide the following information and general recommendations as guidance. This guidance pertains to all Luminex software packages unless specifically contraindicated.

Ports

Software	Version(s)	Port	Protocol	Description	Required?
xPONENT®	All	80	TCP & UDP	Instrument status web page	Optional
		1434	UDP	SQL Server browser	Optional
		11111	TCP	Automation interface	Optional
		11112	TCP	Remote monitoring	Optional
		11113	TCP	Data management	Optional
		11114	TCP	Remote analysis	Optional
		1433	TCP	SQL Server	Optional
SYNCT™	All	1433	TCP	Outbound SQL Server connection to ARIES® (no inbound required for SYNCT™)	Yes, if connecting to ARIES®

Services

Software	Version(s)	Service Notes
xPONENT®	All	Both the '**SQL Server**' and '**Distributed Transaction Coordinator**' services must be active for proper operation. Both services should be configured to set the Startup Type to 'Automatic.'
SYNCT™	All	SQL Server must be configured to set the Startup Type to 'Automatic.'

These services are configured to run under a network account. Altering this configuration may cause adverse effects.

Non-Luminex Software Dependencies

Software	Version(s)	Dependency	Version
xPONENT®	3.0.380–3.1.971	SQL Server Express	2005
	4.2.1441–4.2.1705		2008 R2
	4.3.229		2016
	All versions	.NET Framework	3.5
	4.2 or newer	.NET Framework	4.x
SYNCT™	1.1 u2 (v1.1.349)	.NET Framework	4.x
		SQL Server Express	2016

User Permissions and Account Settings

Luminex-provided PCs are configured with an account that maintains local administrator privileges. While users may choose to change the password for this account, Luminex discourages deleting this account, as doing so may adversely affect database configurations or other software elements.

Luminex software should only be installed using an account with full local administrator privileges. Subsequent troubleshooting, including patch updates, software repairs, or uninstall/reinstall operations, will also require an account with full local administrator privileges.

While an administrative account is necessary for system installation and configuration, the software may be used while logged in under an account with limited privileges. Limited accounts should be granted full read/write permissions to the following folders:

C:\Program Files\Luminex

C:\Program Files (x86)\Luminex

C:\ProgramData\Luminex

Anti-Virus Configuration

Luminex does not test or validate any specific anti-virus software for use with Luminex software, but recommends the following general configuration guidelines:

- Flag any Luminex or SQL Server software as 'safe' or 'trusted.'
- Flag the Distributed Transaction Coordinator (DTC) service as 'safe' or 'trusted' (xPONENT® only).
- Disable 'on-access' scans: anti-virus scans performed during data acquisition, data analysis, or other resource-intensive operations may cause performance problems.
- Exclude Luminex folders from scans, including:
  - **C:\Program Files\Luminex**
  - **C:\Program Files (x86)\Luminex**
  - **C:\ProgramData\Luminex**
  - Any folders used for data export

Operating System Updates

Luminex applications are tested and validated on a specific PC and operating system configuration; no additional testing is performed to validate compatibility with subsequent Windows feature or security updates.

Currently, xPONENT is available on Windows 10 LTSC, while SYNCT is available on Windows 10 Pro.

Windows 10 LTSC is configured to receive only security updates, not feature updates. Windows Pro is configured to disable the Windows Update service, though users are provided with Administrator credentials and may choose to re-enable at their discretion.

Administrators are advised that feature updates have the potential to cause unexpected errors. Luminex recommends that users who enable feature updates perform their own validation testing to ensure that the system's performance continues to conform to their needs.

PC Power and Sleep Settings

Luminex PCs are configured with the following power management settings:

- Hard disks are configured to never turn off.
  Altering this setting may cause data loss during acquisition or export.
- Windows is configured to never hibernate or sleep.
- The screen saver is disabled.
  Altering the hibernation, sleep, screen saver settings, or applying any configuration which leads to a lowered priority state may cause unexpected behavior during acquisition or analysis.

At application startup, xPONENT monitors the status of two registry keys for an expected value of '0.' Configurations which alter either of these values may cause xPONENT to display a warning notification, or prevent xPONENT from launching. These registry keys are:

- HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaveActive
- HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaveTimeOut

Additionally, the following features are recommended:

- USB Selective Suspend features are disabled.
  Altering this setting may cause instruments to disconnect from the PC during operation.
- PCI Express Link State Power Management set to off.
- Display is set to never power off.

Luminex recommends that users who elect to alter these settings perform their own validation testing to ensure that system performance continues to conform to their needs.

Confidential Data

Luminex systems do not use, transmit, retain, or host Protected Health Information (PHI). Luminex recommends using anonymous identifiers for Sample ID fields used within our software systems, as these ID fields may be transmitted when providing test results or other content to Technical Support for troubleshooting assistance.

Hardcoded Passwords

Administrators should be advised that xPONENT® and SYNCT™ systems may rely on hardcoded, unchangeable passwords, including those used for the SQL Server. These passwords may be visible in unencrypted files found on the system. Security policies which enforce minimum password complexity requirements may prevent proper installation or function.

Encryption

Luminex applications are not tested or validated for use with any specific encryption methods. While Luminex does not have reason to expect modern, full-disk encryption methods—intended to be fully transparent to the application—to cause any specific problems, users should be advised that such encryption methods are unsupported by Luminex and may cause aberrant behavior. Luminex strongly advises users who choose to enable disk encryption to independently validate that Luminex applications continue to perform as expected, particularly during resource-intensive operations, such as data acquisition or analysis.

Luminex®
A DiaSorin Company

For more information, please visit luminexcorp.com

For Informational Use Only.

luminexcorp.com

HEADQUARTERS
UNITED STATES
+1.512.219.8020
info@luminexcorp.com

EUROPE
+31.73.800.1900
europe@luminexcorp.com

CANADA
+1.416.593.4323
info@luminexcorp.com

CHINA
+86.21.8036.9888
infocn@luminexcorp.com

JAPAN
+81.3.5545.7440
infojp@luminexcorp.com

FL233961.0823