Inova Solutions
A Geomant Company

LightLink Symantec Endpoint Protection Solution Guide

LightLink Symantec Endpoint Protection

Solution Guide

October 9, 2013

NOTICE OF TRADEMARK:

Inova LightLink and its components are trademarks of Inova Solutions.

Symantec and its components are registered trademarks of Symantec Corporation.

While reasonable efforts have been taken in the preparation of this document to ensure its accuracy, Inova Solutions, Inc. assumes no liability resulting from any errors or omissions in this manual, or from the use of the information contained herein.

971 2nd ST S.E.
Charlottesville, VA 22902
434.817.8000
www.inovasolutions.com

Table of Contents

1. Introduction

Inova Solutions® understands that both LightLink® Client and Server computers need to be protected from external and internal threats, and that many customers deploy Symantec Endpoint Protection as an antivirus and Intrusion Detection system.

1.1. Challenge

Antivirus tools act generally in the same manner on Client and Server PCs; these antivirus tools scan processes and files for viruses both in real time and in accordance with a schedule.

- **Real time scans** act on files as they are accessed or modified and on emails as they are sent or received in real time. Real time scans are intended to have only a small performance impact on running applications.
- **Scheduled scans** are much deeper, and typically review every file and process in the system. Scheduled scans typically cause significant performance impact on running applications.

Antivirus tools such as Symantec Endpoint Protection are highly configurable so that users can balance necessary security against any negative performance impact.

For Client PCs, the effect on LightLink applications is generally limited to user frustration with slow response, particularly during a scheduled scan. However, on the Server PC, antivirus tools can have a more significant centralized impact on LightLink processes, depriving all users of LightLink functionality. For this reason, this document refers to Symantec and LightLink compatibility on server machines.

1.2. Solution

The Symantec Endpoint Protection product can be configured to modify the impact on running applications by tuning aspects of the product to balance the need for antivirus and intrusion detection with the need for operable applications.

Configuration action in these three areas will alleviate most problems:

- Controlling the frequency and intensity of scans.
- Excepting certain files and processes.
- Disabling heuristic scanning.
- Following best practices from Symantec.

2. Technical Details

2.1. Controlling the Frequency and Intensity of Scheduled Scans

Scheduled scans are intrusive and consume significant server resources. Follow these guidelines to ensure the continued protection of scheduled scans without impacting contact center operations:

- Schedule full scans to occur during off hours at a consistent time and day of the week or date of each month.
- Advise LightLink system administrators of the configured scan timing so that they can advise of call center activity in those times, and correlate performance problems or malfunctions with the antivirus activity if such problems occur.
- To avoid completely blocking LightLink processes and possibly disconnecting the clients from the servers, select the Symantec option for 'Best Application Performance' when available.

2.2. Excepting Certain Files and Processes

The Symantec system provides a Centralized Exception List, which includes the processes that support critical operations. The antivirus system has components that actively scan running programs outside of the scheduled scan. Programs placed in the exception list will not be scanned every time they are used.

Since the LightLink system consists of a number of program files which need to run without interference to provide the best service to contact center operations, all of the LightLink processes and files that need to be excepted from scans are listed in the Appendices. There is a separate Appendix for each LightLink release because the files vary from release to release. Please add these files to the Centralized Exception List.

2.3. Heuristic Scanning

Heuristic scanning looks for patterns of activities that viruses typically cause. This type of scanning is intended to provide 'zero day' detection, meaning a virus could be detected before Symantec has identified a specific pattern definition. There are many good places for such systems, but server applications such as LightLink frequently involve processes launching other processes and modifying files. For these reasons, Symantec's Heuristic scanning tools such as TruScan and Bloodhound should be disabled.

2.4. Following Best Practices from Symantec

Following the best practices listed below will help modify the impact of antivirus tools on contact center applications:

- Ensure that none of the following are in the scan path:
    - Network drives.
    - Compressed files.
    - Virtual disk file types (VMware specific).
- Randomize distribution of antivirus updates to virtual servers so that virtual servers running on the same hardware do not simultaneously receive updates.

3. Conclusion

It is important to note that development of antivirus and intrusion detections systems is a highly active area and is driven by infestations and attacks that occur daily. Inova Solutions has seen customers with active LightLink systems protected by antivirus software experience failures when a new antivirus update is issued, or a configuration is changed. For this reason, it is critical that customers be open to reviewing and tuning their antivirus configuration on machines running LightLink to maximize both protection and the operational capability of the LightLink system.

Appendix A – LightLink Version 5.10: Excluding LightLink Applications and Databases

Table 1 lists all applications associated with the LightLink system, version 5.10. The processes are segmented by LightLink component for reference only; all processes should be added the centralized exception list.

LightLink Component	Process		
Core	await_app_exit.exe cefview.exe config_blurt.exe find_running.exe gag_launcher.exe gui_message.exe i_cefloon.exe i_launcher.exe i_sublauncher.exe	i_uls.exe ll_shutdown.exe l_controller.exe log_viewer.exe push_config.exe query_text.exe show_hostname.exe show_versions.exe	set_license_key.exe sleep_ms.exe test_bus.exe test_transport.exe ungag_launcher.exe version_reporter.exe zap_process.exe zing_window.exe
Desktop	datalink.exe drone_client.exe	marquee.exe	tasklinkapp.exe
Broadcaster	BroadcastClient.exe drone_client.exe	TextMessageWindow.exe	watchdog.exe
Server	autosim.exe BackupLightLinkDatabase.exe create_dsn.exe Datascope.exe display_monitor.exe ds_config_editor.exe DSMXServer.exe get_configured_servers.exe i_auditserver.exe i_bus_server.exe i_client_mgr.exe i_dbproxy.exe i_dsm.exe	i_exe_aspect.exe i_ext_inin.exe i_ext_genesys.exe i_ext_symposium.exe i_ext_im.exe i_inputmanager.exe i_odms.exe i_redisdb.exe i_site_monitor.exe launch_remote.exe LLAdmin.exe ll_exporter.exe msmtp.exe	OCMXServer.exe plink.exe python.exe redis-cli.exe redis-server.exe SecurityKey.exe SecurityManager.exe simswitch.exe smaddu.exe stdio_wrapper.exe t_data_set_contracts.exe zap_remote.exe
Supervisor	bitmap_editor.exe datalink.exe	display_monitor.exe display_sim.exe launch_remote.exe msgedit.exe	quicklaunch.exe SupervisorDBSetup.exe sysman.exe zap_remote.exe

Table 1

The LightLink Database folders and the files within those folders should also be excluded from antivirus scans. Refer to Table 2 for a list of these folders and files. Note that Table 2 includes the default location, but the actual location for the LightLink database files will be on the database host, as specified during the default or custom installation.

LightLink Component	Files
Server	[LightLink Path]\Server\srvcfg\datadir\lightlinkdb.mdf [LightLink Path]\Server\srvcfg\datadir\lightlinklog.ldf

Table 2

Appendix A – LightLink Version 5.9:
Excluding LightLink Applications and Databases

Table 3 lists all applications associated with the LightLink system, version 5.9. The processes are segmented by LightLink component for reference only; all processes should be added the centralized exception list.

LightLink Component	Process		
Core	await_app_exit.exe cefview.exe config_blurt.exe find_running.exe gag_launcher.exe gui_message.exe i_cefloon.exe i_launcher.exe i_sublauncher.exe	i_uls.exe ll_shutdown.exe l_controller.exe log_viewer.exe push_config.exe query_text.exe show_hostname.exe show_versions.exe	set_license_key.exe sleep_ms.exe test_bus.exe test_transport.exe ungag_launcher.exe version_reporter.exe zap_process.exe zing_window.exe
Desktop	datalink.exe drone_client.exe	marquee.exe	tasklinkapp.exe
Broadcaster	BroadcastClient.exe drone_client.exe	TextMessageWindow.exe	watchdog.exe
Server	autosim.exe BackupLightLinkDatabase.exe create_dsn.exe Datascope.exe display_monitor.exe ds_config_editor.exe DSMXServer.exe get_configured_servers.exe i_auditserver.exe i_bus_server.exe i_client_mgr.exe i_dbproxy.exe	i_exe_aspect.exe i_ext_inin.exe i_ext_genesys.exe i_ext_symposium.exe i_ext_im.exe i_inputmanager.exe i_odms.exe i_redisdb.exe i_site_monitor.exe launch_remote.exe LLAdmin.exe ll_exporter.exe msmtp.exe	OCMXServer.exe plink.exe python.exe redis-cli.exe redis-server.exe SecurityKey.exe SecurityManager.exe simswitch.exe smaddu.exe stdio_wrapper.exe t_data_set_contracts.exe zap_remote.exe
Supervisor	bitmap_editor.exe datalink.exe	display_monitor.exe display_sim.exe launch_remote.exe msgedit.exe	quicklaunch.exe SupervisorDBSetup.exe sysman.exe zap_remote.exe

Table 3

The LightLink Database folders and the files within those folders should also be excluded from antivirus scans. Refer to Table 4 for a list of these folders and files. Note that Table 4 includes the default location, but the actual location for the LightLink database files will be on the database host, as specified during the default or custom installation.

LightLink Component	Files
Server	[LightLink Path]\Server\srvcfg\datadir\lightlinkdb.mdf [LightLink Path]\Server\srvcfg\datadir\lightlinklog.ldf

Table 4

Appendix B – LightLink Version 5.8:
Excluding LightLink Applications and Databases

Table 5 lists all applications associated with the LightLink system version 5.8. The processes are segmented by LightLink component for reference only; all processes should be added the centralized exception list.

LightLink Component	Process		
Core	await_app_exit.exe cefview.exe config_blurt.exe find_running.exe gag_launcher.exe gui_message.exe i_cefloon.exe i_launcher.exe i_sublauncher.exe	i_uls.exe ll_shutdown.exe l_controller.exe log_viewer.exe push_config.exe query_text.exe show_hostname.exe show_versions.exe	set_license_key.exe sleep_ms.exe test_bus.exe test_transport.exe ungag_launcher.exe version_reporter.exe zap_process.exe zing_window.exe
Desktop	datalink.exe drone_client.exe	marquee.exe	tasklinkapp.exe
Broadcaster	BroadcastClient.exe drone_client.exe	TextMessageWindow.exe	watchdog.exe
Server	autosim.exe BackupLightLinkDatabase.exe create_dsn.exe Datascope.exe display_monitor.exe ds_config_editor.exe DSMXServer.exe get_configured_servers.exe i_auditserver.exe i_bus_server.exe i_client_mgr.exe i_dbproxy.exe	i_exe_aspect.exe i_ext_inin.exe i_ext_genesys.exe i_ext_symposium.exe i_ext_im.exe i_inputmanager.exe i_odms.exe i_redisdb.exe i_site_monitor.exe launch_remote.exe LLAdmin.exe ll_exporter.exe msmtp.exe	OCMXServer.exe plink.exe python.exe redis-cli.exe redis-server.exe SecurityKey.exe SecurityManager.exe simswitch.exe smaddu.exe stdio_wrapper.exe t_data_set_contracts.exe zap_remote.exe
Supervisor	bitmap_editor.exe BroadcastDesigner.exe BroadcasterTVRemote.exe datalink.exe	display_monitor.exe display_sim.exe launch_remote.exe msgedit.exe	quicklaunch.exe SupervisorDBSetup.exe sysman.exe zap_remote.exe

Table 5

The LightLink Database folders and the files within those folders should also be excluded from antivirus scans. Refer to Table 6 for a list of these folders and files. Note that Table 6 includes the default location, but the actual location for the LightLink database files will be on the database host, as specified during the default or custom installation.

LightLink Component	Files
Server	[LightLink Path]\Server\srvcfg\datadir\lightlinkdb.mdf [LightLink Path]\Server\srvcfg\datadir\lightlinklog.ldf

Table 6

Appendix B – LightLink Version 5.7:
Excluding LightLink Applications and Databases

Table 7 lists all applications associated with the LightLink system. The processes are segmented by LightLink component for reference only; all processes should be added the centralized exception list.

LightLink Component	Process		
Core	bus_config.exe cefview.exe config_blurt.exe find_running.exe gag_launcher.exe gui_message.exe i_bus_server.exe	i_cefloon.exe i_sublauncher.exe i_uls.exe log_viewer.exe push_config.exe query_text.exe	show_hostname.exe sleep_ms.exe test_bus.exe test_transport.exe version_reporter.exe zing_window.exe
Desktop	datalink.exe drone_client.exe	marquee.exe	tasklinkapp.exe
Broadcaster	BroadcastClient.exe drone_client.exe	TextMessageWindow.exe	watchdog.exe
Server	auditor_uninstall.exe BackupLightLinkDatabase.exe create_dsn.exe database_porter.exe dsms_setup.exe DSMXServer.exe EIM_uninstall.exe get_configured_servers.exe i_auditserver.exe i_client_mgr.exe	i_coalescer.exe i_ddsrv.exe i_ext_im.exe i_inputmanager.exe i_odms.exe i_site_monitor.exe i_streaming_channel.exe IM_uninstall.exe msmtp.exe	OCMXServer.exe odms_setup.exe odms_uninstall.exe RestoreLightLinkDatabase.exe smaddu.exe sminstall.exe stdio_wrapper.exe
Supervisor	auditorreport.exe autosim.exe bitmap_editor.exe BroadcastDesigner.exe BroadcasterTVRemote.exe CheckLightLinkConnection.exe client_simulator.exe cms_cleaner.exe cms_defaulter.exe ConfigEditor.exe connector_config.exe DataDirectorySetup.exe	Datalink.exe ddiag.exe display_monitor.exe display_sim.exe ds_config_editor.exe fontedit.exe i_ddproxy.exe import_config.exe launch_remote.exe ll_exporter.exe LLAdmin.exe msgedit.exe	multi_display_sim.exe plink.exe quicklaunch.exe SecurityManager.exe SetupLightLinkAccessPrivilege.exe simswitch.exe stdiosim.exe sysman.exe t_data_set_contracts.exe toollauncher.exe zap_remote.exe

Table 7

The LightLink Database folders and the files within those folders should also be excluded from antivirus scans. Refer to Table 8 for a list of these folders and files.

LightLink Component	Files
Server	[LightLink Path]\Server\srvcfg\datadir\lightlinkdb.mdf [LightLink Path]\Server\srvcfg\datadir\lightlinklog.ldf

Table 8