Quest™

LiteSpeed® for SQL Server 8.6

Security and Compliance Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

LiteSpeedSecurity and Compliance Guide
Updated - September 2017
Version - 8.6

Contents

1

Introduction

About This Document

This document discusses data encryption, user authentication, data logging, and other LiteSpeed's security features and describes how to evaluate LiteSpeed’s security features in connection with the NIST’s recommended federal information security standards promulgated under the Federal Information Security Management Act (FISMA).

About LiteSpeed

LiteSpeed® for SQL Server, or LiteSpeed, is a fast and flexible backup and recovery solution that allows database administrators to easily maintain complete control over the backup and recovery process. LiteSpeed's low-impact, high-performance compression and encryption technology helps reduce storage costs and protect data, while maintaining a high level of recoverability.

While providing robust encryption and compression functionality, this cutting-edge database backup solution profoundly reduces the time needed to execute database backups. It supports the use of the FIPS 140-2 compliant encryption algorithms AES and 3DES for encrypting database backup files. LiteSpeed installs extended stored procedures on the SQL Server which it uses during backups and restores.

Security Features in LiteSpeed

Below follows a set of security features provided by LiteSpeed for SQL Server.

Data Encryption

A backup of a database will include all sensitive information stored in the original, and it is therefore prudent to offer a level of protection of the backup. LiteSpeed supports concurrent encryption during the creation of database backups and supports the following symmetric key encryption algorithms and key sizes:

Encryption Algorithm	Key Sizes (in bits)	FIPS 140-2 Approved
AES	128, 196, 256	Yes
3DES	168	Yes
RC2	40, 56, 112, 128	No
RC4	128	No

LiteSpeed uses Microsoft's Cryptographic API (CAPI) to provide the 3DES, RC2 and RC4 algorithms, and the LibTomCrypt library for AES. The reason for choosing LibTomCrypt over CAPI to support AES is that the encryption algorithm is not supported by the Microsoft Cryptographic Service Providers in Windows 2000.

The customer has the choice of only using FIPS 140-2 approved algorithms. The choice of encryption is specified through the backup wizard in the LiteSpeed UI Console. The user chooses the specific encryption algorithm and the corresponding key size. These parameters can also be included as part of script files.

Encryption Key

When choosing to enable encryption of backup files, the LiteSpeed user is prompted to enter a password. This password gets converted into a cryptographic key (password based encryption). Since the security of the key relies upon the password, the user should choose a strong password. The user is prompted to re-enter the password upon restore of an encrypted backup. Neither the key nor password are persisted with the backup file.

User Authentication

LiteSpeed relies upon SQL Server for user authentication and access control.

Privileges

During installation, LiteSpeed requires the user to have Administrator rights on the local machine and SYSDBA access on the SQL Server. Only SYSDBA access is required during operation of LiteSpeed.

Logging

LiteSpeed users can enable the Activity Logging feature causing activity data to be logged to a Local Repository database on each server instance on which Activity Logging is enabled.

Network Connectivity

LiteSpeed does not require any network connectivity during installation or operation. Backup files can be stored on local disks. Therefore, no network ports are required to be opened for LiteSpeed to work, meaning that the server's firewall settings can remain unchanged.

It is possible to initiate backups from the LiteSpeed UI Console by connecting to a database on a remote machine, assuming that LiteSpeed has been installed on it. When initiating encrypted backups from the console, we recommend that the SQL Server administrator enforces secure communication on the SQL Server, as doing so would prevent sending the encryption password in the clear over the network. The database backup files are created on the machine hosting the SQL Server. LiteSpeed uses tabular data stream packets (TDS) to communicate with the remote SQL Server.

Note: TSM backups conducted through LiteSpeed are transferred to and then stored in and/or managed by the Tivoli Storage Manager. The TSM handles the backup file from then on, managing expiration date, storage location, etc. Please refer to the TSM product documentation for further details.

Integrity of Backup Files

Cyclic Redundancy Checks (CRC) can be used to ensure the integrity of the backup files. CRC is used for detecting corruption during the file copy operation. LiteSpeed uses the Adler-32 checksum algorithm.

Verification of User Input

The LiteSpeed UI Console validates user input by checking for matching data type (no characters in a numeric only field) and length of inputs, such as to prevent against users attempting to enter malicious commands.

Configuration Parameters

LiteSpeed's configuration parameters are stored in the LiteSpeedSettings.ini file and are configurable through the LiteSpeed UI Console. Other parameters specific to backup files such as those required during restores are stored in the files themselves.

Daylight Savings Time Compliance

LiteSpeed will not be affected by the changes introduced by the Daylight Savings Time (DST) Extension (U.S. Energy Policy Act of 2005). It relies upon the Operating System for time management and does not implement any special logic around DST settings. Therefore, if the Operating System is DST compliant then so is LiteSpeed.

3

LiteSpeed for SQL Server and FISMA Compliance

The Federal Information Security Management Act (FISMA) was passed by the U.S. Congress and signed by the U.S. President, and is part of the Electronic Government Act of 2002. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information system that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. See http://csrc.nist.gov/groups/SMA/fisma/overview.html for more information.

A major component of FISMA implementation is the publication by the National Institute of Standards and Technology (NIST), entitled “Recommended Security Controls for Federal Information Systems”, listed as NIST Special Publication 800-53. It lists 17 general security categories against which an information security control program should be evaluated, so as to measure its level of compliance with an agency’s obligations under FISMA. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf for more information. Under 800-53, these seventeen listed categories define general security control “families” (e.g., “AC”), and that each family in turn contains several subcategories (e.g., “AC-1”, “AC-2”, “AC-3”, etc.) that further detail related aspects of information security and assurance. Consult Appendix F of 800-53 for further information.

The following table describes how LiteSpeed addresses categories listed in NIST 800-53.

Category	Applicable	Description
Access Control (AC)	Yes	LiteSpeed relies upon SQL Server for user authentication and access control.
Awareness and Training (AT)	No	This category does not apply to LiteSpeed as it would be the responsibility of the customer who installs LiteSpeed on its systems to develop and review its own security awareness and training policy.
Audit and Accountability (AU)	Yes	LiteSpeed users can enable the Activity Logging feature causing activity data to be logged to a Local Repository database on each server instance on which Activity Logging is enabled.
Certification, Accreditation and	No	This category does not apply to LiteSpeed as it would be

Category	Applicable	Description
Assessments (CA)		the responsibility of the customer who installs LiteSpeed on its systems to develop and review its own security assessment, accreditation and certification policy.
Configuration Management (CM)	Yes	LiteSpeed's configuration can be modified through the LiteSpeed UI Console. For more information, see Configuration Parameters on page 7.
Contingency Planning (CP)	No	This category does not apply to LiteSpeed since it is the responsibility of the customer to design and implement their own contingency plans. As defined by NIST (publication 800-34), disruptive events to IT systems include power-outages, fire and equipment damage, and can be caused by natural disasters or terrorist actions.
Identification and Authentication (IA)	Yes	LiteSpeed relies upon SQL Server for authentication and identification of users. Only users with sufficient privileges are able to execute commands within LiteSpeed. For more information, see User Authentication on page 6.
Incident Response (IR)	No	This category does not apply to LiteSpeed since it is the responsibility of the customer who installs LiteSpeed on its systems to develop and review its own incident response policy and procedures.
Maintenance (MA)	Yes	Quest Software monitors developments and newly discovered security flaws in the software components and libraries used by ActiveRoles, and provides product and security patches to its customers when necessary.
Media Protection (MP)	No	This category does not apply to LiteSpeed since it is the responsibility of the customer who installs LiteSpeed on its systems to develop and review its own media protection policy.
Physical and Environmental Protection (PE)	No	This category does not apply to LiteSpeed since it is the responsibility of the customer who installs LiteSpeed on its systems to develop and review its own physical and environmental policy.
Planning (PL)	No	This category does not apply to LiteSpeed since it is the responsibility of the customer who installs LiteSpeed on its systems to develop and review its security planning policy.
Personnel Security (PS)	No	This category does not apply to LiteSpeed since it is the responsibility of the customer who installs LiteSpeed on its systems to enforce its personnel security policies.
Risk Assessment (RA)	No	This category does not apply to LiteSpeed since it is the responsibility of the customer who installs LiteSpeed on its

Category	Applicable	Description
		systems to develop and review its own risk assessment policy.
System and Services Acquisition (SA)	No	This category does not apply to LiteSpeed since it is the responsibility of the customer who installs LiteSpeed on its systems to develop and review its own system and services acquisition policy.
System and Communications Protection (SC)	Yes	LiteSpeed allows for encryption of the created backup files. The FIPS 140-2 approved AES and 3DES are amongst the supported encryption algorithms. For more information, see Data Encryption on page 5.
System and Information Integrity (SI)	Yes	LiteSpeed permits the user to create an integrity check of the backup files that can later be used to verify the integrity of the files, for example after a file transfer. For more information, see Integrity of Backup Files on page 6.

Note: A statement that a particular security category is applicable to LiteSpeed means only that LiteSpeed contains security features that are or may be relevant to some or all aspects of the security category in question. It does not necessarily mean that LiteSpeed fully meets all of the requirements described in that security category, or that the use of LiteSpeed by itself will guarantee compliance with any particular information security standards or control programs. Indeed, the selection, specification, and implementation of security controls in accordance with a customer-specific security program is ultimately dependent upon the manner in which the customer deploys, operates, and maintains all of its network and physical infrastructure, including LiteSpeed. For more information, see Customer Measures on page 11.

4

Customer Measures

The security features of LiteSpeed for SQL Server are only one part of a secure environment. The customer's operational and policy decisions will have a great influence upon the overall level of security achieved. In particular, the customer is responsible for the physical security of the appliance and the security of the network from which the appliance is accessible. Administrators should also change default passwords and replace them by strong passwords.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/company/contact-us.aspx or call +1 949 754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Third Party Contributions

This product contains some third-party components (listed below). Copies of their licenses may be found at referencing http://www.quest.com/legal/license-agreements.aspx. Source code for components marked with an asterisk (*) is available at http://opensource.quest.com.

Table 1: List of Third-Party Contributions

Component	License or Acknowledgement
ActiPro Syntax Editor (for Windows Forms) 4.0	ActiPro Syntax Editor (for Windows Forms) 4.0 license
Active Directory Common Dialogs .NET 2.5.0	Ms-PL
AWS SDK for .NET 3.1.3	This component is governed by the Apache 2.0 license.
CMarkup Developer 11.2	CMarkup Developer 1.0 license
Developer Express .NET (DXperience) 13.2	Developer Express .Net (DXperience) 13.2 license
LibTomCrypt 1.17	LibTomCrypt 1.17 license
LZMA 4.65	Public Domain
QuickLZ 1.5	QuickLZ Commercial License 1.0
SharpZipLib 0.85.5.452	SharpZipLib License
Task Scheduler Managed Wrapper 2.5.8	MIT
TimeSpan Helper Library 2.1.1	New BSD License (BSD)
Microsoft Windows Azure Storage 6.1.0	This component is governed by the Apache 2.0 license.
WinForms Group Controls 1.5.0	This component is governed by the Apache License 2.0 (Apache)
Wizard .NET Library 2.1.0	The MIT License (MIT)
zlib 1.2.8	zlib 1.2.8 License