

Oracle® StorageTek Enterprise Library Software (ELS)

Security Guide

All ELS Releases

E36422-01

2012

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software

License (2012). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services

Contents

Contents.....	3
Product Overview.....	4
General Security Principles.....	5
Keep Software Up To Date.....	5
Restrict Network Access As Appropriate.....	5
Keep Up To Date on Latest Security Information.....	5
Part 2: Secure Installation and Configuration.....	6
Installation Overview.....	6
Installing NCS/ELS.....	6
Post-Installation Configuration.....	6
Part 3: Securing ELS with AT-TLS.....	7
Part 4: Security Considerations for Developers.....	8
Part 5: Appendices.....	9
Appendix A: Secure Deployment Checklist.....	9
References.....	10
ELS Documentation.....	10

This section gives an overview of the ELS software suite and explains the general principles of application security.

Product Overview

ELS provides tape automation support for Oracle StorageTek mainframe tape environments for the IBM z/OS platform. ELS supports a TCP/IP client/server tape automation architecture allowing the SMC client software running on one z/OS LPAR to communicate with the HSC/VTCS server software running on a different z/OS LPAR. ELS client/server communication is used to issue control path requests, primarily mount/dismount requests, for virtual and physical tape volumes. Information contained in these control path requests consists of TapePlex configuration and policy information, virtual/physical tape transport unit addresses and virtual/physical tape volume serial numbers. Most important, ELS client/server communication never contains any customer data, which always travels over IBM FICON/ESCON data path interfaces connecting host LPARs to Oracle StorageTek tape transports or VSM virtual tape devices.

The information in this Security Guide applies to all ELS releases. As discussed in Part 3 of this guide, it is possible to secure ELS client/server control path communications when such protection is desirable or is required. Additionally, this document discusses security aspects of various ELS installation and post-installation activities.

General Security Principles

The following principles are fundamental to using any application software securely.

Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. The latest ELS cumulative maintenance bundle, along with individual PTFs and HOLDDATA, are all available on My Oracle Support (MOS). Cumulative maintenance bundles are updated monthly to include all PTFs from the latest ELS monthly regression test cycle. All the PTFs in a cumulative bundle have been tested together as a complete package. HIPER PTF Email notification is available by subscribing to MOS Hot Topics Alert documents for the ELS products. Customers are encouraged to stay on current maintenance levels, keep HOLDDATA up-to-date and subscribe to Hot Topics Alerts for HIPER notifications.

Restrict Network Access As Appropriate

For performance and security, route ELS control path communications over an isolated network behind a firewall. Using a firewall provides assurance that access to ELS systems is limited to a known network, which can be monitored and restricted if necessary. Using a dedicated network for ELS client/server communications eliminates network contention with other applications and improves tape system performance.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check for revisions to this Security Guide and all other ELS product documentation on a regular basis. All of the ELS documentation referenced in this document is available on the Oracle Technical Network in the Tape Storage Products section.

Part 2: Secure Installation and Configuration

Installation Overview

The IBM z/OS System Authorization Facility (SAF) provides essential protection for most security aspects of ELS. SAF is typically implemented with the IBM RACF package or equivalent. This section outlines using a RACF-based SAF environment to install and configure a secure ELS installation.

Installing NCS/ELS

The Oracle document *StorageTek Enterprise Library Software: Installing ELS* describes how to install and configure your version of ELS using RACF protection. Refer to this document for more information on security-related installation topics:

- Installing the base software and the latest cumulative maintenance bundle
- ELS load library APF authorization
- HSC user exit library APF authorization
- SMC JES3 load library APF authorization.

Post-Installation Configuration

These Oracle documents describe post-installation configuration tasks for your version of ELS:

- *StorageTek Enterprise Library Software: Configuring HSC and VTCS*
- *StorageTek Enterprise Library Software: Configuring and Managing SMC*
- *StorageTek Enterprise Library Software: ELS Programming Reference.*

Refer to these documents for more information on security-related post-installation topics:

- Defining RACF protection for CDS data set security
- Defining command authority and programmatic interface authority using HSC user exit SLSUX15
- Defining volume access authority for mounting and ejecting volumes using HSC user exit SLSUX14
- Defining MVC pool and scratch subpool volser authority

- Defining an SMC OMVS RACF segment for communication with a remote HSC subsystem
- Defining an SMC OMVS RACF segment for communication with a VLE appliance

Part 3: Securing ELS with AT-TLS

The IBM z/OS Application Transparent Transport Layer Security (AT-TLS) facility uses SSL data encryption to secure z/OS TCP/IP applications. For more information on AT-TLS, refer to the IBM publication *z/OS Communications Server: IP Configuration Guide*, and see information on the AT-TLS Policy Agent information in the IBM publication *z/OS Communications Server: IP Configuration Reference*.

Securing ELS client/server communications between SMC and HSC/VTCS is described in the Oracle white paper *Using AT-TLS with HSC/SMC Client/Server z/OS Solution: Implementation Example*. This white paper is published on the Oracle Technical Network in the Tape Storage Products section. Refer to this publication for detailed configuration information.

To secure ELS with AT-TLS, Oracle recommends using any of these SSL cryptographic algorithms:

- SHA-2 family (SHA-256, SHA-384, SHA-512)
- AES \geq 128-bit
- RSA \geq 2048-bit
- Diffie-Hellman (DH) \geq 2048-bit
- ECC \geq 256-bit

Any other SSL cryptographic algorithms provide weaker protection and should not be used with ELS.

Note: The Oracle StorageTek Virtual Library Extension (VLE) appliance for VSM does not currently support ATTLS communications. Do not secure ELS VLE communications with ATTLS.

Part 4: Security Considerations for Developers

The Oracle document *StorageTek Enterprise Library Software: ELS Programming Reference* describes ELS APIs available to application developers. Programmatic interface to ELS uses the Unified User Interface (UUI), which uses the HSC command security exit SLSUX15 to manage access to its functions based on RACF authorization (or equivalent.) See p. 6, Post-Installation Configuration, for more information on securing SLSUX15 with RACF.

Part 5: Appendices

Appendix A: Secure Deployment Checklist

1. *Use RACF protection (or equivalent) as discussed in this Security Guide.*
2. *Restrict network access. ELS and the tape libraries it manages should be behind the corporate firewall.*
3. *Secure ELS network traffic with the IBM AT-TLS facility if required.*
4. *Apply all ELS PTFs and HOLDDATA.*
5. *Contact Oracle Support if you encounter vulnerability in Oracle ELS software.*

References

ELS Documentation

The ELS documentation is saved in libraries organized by ELS release. Access this from [Tape Storage Documentation page](#).