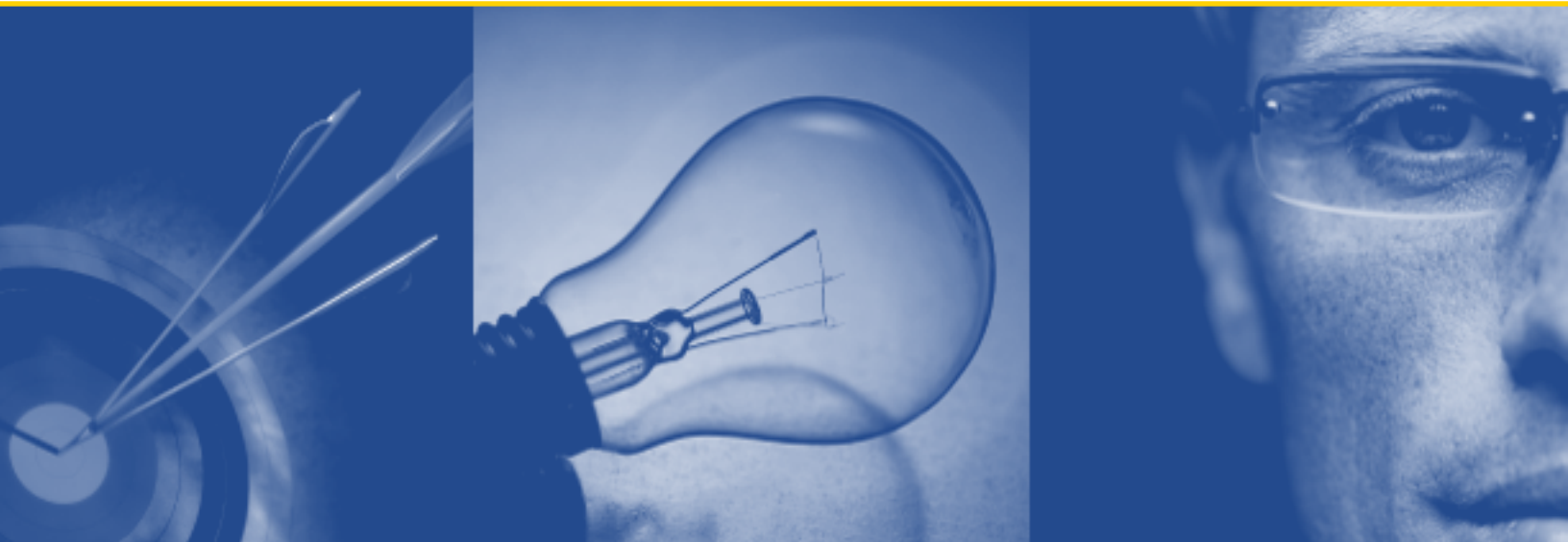


Quest[®] Enterprise Single Sign-On 8.0.2

What's New

Enterprise SSO and Data Privacy



**Copyright © Quest Software, Inc. (and / or its licensors), 2008.
ALL RIGHTS RESERVED.**

This publication contains proprietary information protected by copyright. The software described in this publication is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical or otherwise without the prior written permission of the publisher.

DISCLAIMER

The information in this publication is provided in connection with Quest branded products from Evidian. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this publication. EXCEPT AS OTHERWISE SPECIFIED IN THE END USER LICENSE AGREEMENT FOR THIS PRODUCT, EVIDIAN AND QUEST ASSUME NO LIABILITY WHATSOEVER AND DISCLAIM ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO THIS PRODUCT, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL EVIDIAN OR QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS PUBLICATION, EVEN IF EVIDIAN OR QUEST HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Evidian and Quest make no representations or warranties with respect to the accuracy or completeness of the contents of this publication and reserve the right to make changes to specifications and product descriptions at any time without notice. Evidian and Quest do not make any commitment to update the information contained in this publication. The information and specifications in this publication are subject to change without notice.

Trademarks

Quest, Quest Software, the Quest Software logo, Aelita, AppAssure, Benchmark Factory, Big Brother, DataFactory, DeployDirector, ERDisk, Foglight, Funnel Web, I/Watch, Imceda, InLook, IntelliProfile, InTrust, IT Dad, I/Watch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, NBSpool, NetBase, Npulse, PerformaSure, PL/Vision, Quest Central, RAPS, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL LiteSpeed, SQL Navigator, SQL Watch, SQLab, Stat, Stat!, StealthCollect, Tag and Follow, Toad, T.O.A.D., Toad World, Vintela, Virtual DBA, Xaffire, and XRT are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. The terms Evidian, AccessMaster, SafeKit, OpenMaster, SSOWatch, WiseGuard, Enatel and CertiPass are trademarks registered by Evidian. All other trademarks mentioned in this document are the property of their respective owners.

World Headquarters, 5 Polaris Way, Aliso Viejo, CA 92656

Website: www.quest.com

Please refer to our website for regional and international office information.

Quest Enterprise SSO

Updated – November 2008

Software version – 8.0.2

CONTENTS

ABOUT THIS GUIDE.....	3
ABOUT THIS DOCUMENT	4
CONVENTIONS	4
ABOUT QUEST SOFTWARE, INC.....	5
CONTACTING QUEST SOFTWARE.....	5
CONTACTING QUEST SUPPORT.....	5
CHAPTER 1	
WHAT IS NEW IN ENTERPRISE SSO 8.0 EVOLUTION 2.....	6
1.1 NEW INSTALLATION MODES	7
1.2 ADAM IMPROVEMENTS.....	7
1.3 AUDIT IMPROVEMENTS	7
1.4 NEW E-SSO CONSOLE FEATURES	7
1.5 EMERGENCY ACCESS IMPROVEMENT	7
1.6 INTEGRATION WITH GEMALTO SA SERVER.....	7
CHAPTER 2	
TECHNICAL DETAILS.....	9
2.1 CLIENT ENVIRONMENT.....	10
2.1.1 OPERATING SYSTEM PREREQUISITES	10
2.1.2 HARDWARE PREREQUISITES.....	10
2.2 LDAP DIRECTORIES AND DATABASES VERSIONS	11
2.2.1 LDAP DIRECTORY VERSIONS	11
2.2.2 DATABASE VERSIONS	12
2.2.3 LINK WITH USER PROVISIONING	12
2.3 SUPPORTED AUTHENTICATION DEVICES.....	12
2.3.1 SMART CARDS AND USB TOKENS.....	12
2.3.2 BIOMETRIC DEVICES	13
2.4 SSOWATCH PLUG-IN REQUIREMENTS.....	14
2.4.1 GENERAL REQUIREMENTS	14
2.4.2 SSOWATCH SAP R/3 PLUG-IN REQUIREMENTS	14
2.5 SUPPORTED HTTP SERVER	14
2.6 CONFIGURING THE HLLAPI PLUG-IN.....	15
2.7 WARNINGS.....	15
2.7.1 UPDATING ENTERPRISE SSO MODULES	15
2.7.2 DO NOT USE ENTERPRISE SSO CONSOLE ON CITRIX OR TERMINAL SERVICES SERVERS.	15
2.7.3 SSOWATCH AND ADVANCED LOGIN POCs CAN BE DONE WITHOUT SMART CARDS ..	16
2.7.4 ADVANCED LOGIN: RDP CONNECTIONS ON WINDOWS XP.....	16
2.7.5 DO NOT USE SSOWATCH 8.0 WITH ACCESSMASTER	16
2.7.6 INTEGRATING AN APPLICATION WITH THE HLLAPI PLUG-IN DEPENDS ON MANY FACTORS.....	16
2.7.7 INTEGRATING A THIRD-PARTY CARD MANAGEMENT SYSTEM (CMS) IS NOT POSSIBLE IN ALL CASES	17

2.7.8 WHEN SSOWATCH IS USED WITH NOVELL NETWARE, THE NETWARE PASSWORD MUST BE THE SAME AS THE WINDOWS PASSWORD	17
2.7.9 ENTERPRISE SSO ONLY SUPPORTS THE DEFAULT VERSIONS OF CRYPTOFLEX CARDS	17
2.7.10 EVALUATE THE DATABASE SPACE REQUIRED TO LOG EVENTS FOR AUDIT	17
2.7.11 SSOWATCH INTERNET EXPLORER PLUG-IN WARNINGS	17
2.7.12 DO NOT INSTALL ENTERPRISE SSO SERVERS ON ACTIVE DIRECTORY CONTROLLERS	18
2.7.13 SOME FEATURES ARE AVAILABLE IN ENGLISH LANGUAGE ONLY	18
2.8 RESTRICTIONS.....	18
2.8.1 WINDOWS ACTIVE DIRECTORY INTER-DOMAIN SUPPORT WITH ENTERPRISE SSO CONSOLE IN TEMPORARY RESTRICTION	18
2.8.2 ACTIVE DIRECTORY MULTI-DOMAIN AND MULTI-FOREST	18
2.8.3 NOT YET AVAILABLE: MULTI-ACCOUNT MODE IN THE USER PROVISIONING LINK	18
2.8.4 LDAP ACCOUNTS USED BY ENTERPRISE SSO SERVERS MUST NOT EXPIRE	18
CHAPTER 3	
DOCUMENTATION.....	19

About This Guide




- About This Document
- Conventions
- About Quest Software
- Contacting Quest Software
- Contacting Quest Support

About This Document

Subject	This document provides information relating to release 8.0 Evolution 2 of Quest Enterprise SSO.
Intended Readers	<ul style="list-style-type: none"> • System integrators • Administrators
Software/Hardware Required	IAM Suite 8 and later versions.

Conventions

In order to help you get the most out of this guide, we have used specific formatting conventions. These conventions apply to procedures, icons, keystrokes and cross-references.

ELEMENT	CONVENTION
Select	This word refers to actions such as choosing or highlighting various interface elements, such as files and radio buttons.
Bolded text	Interface elements that appear in Quest products, such as menus and commands.
<i>Italic text</i>	Used for comments.
<i>Bold Italic text</i>	Introduces a series of procedures.
Blue text	Indicates a cross-reference. When viewed in Adobe® Acrobat®, this format can be used as a hyperlink.
	Used to highlight additional information pertinent to the process being described.
	Used to provide Best Practice information. A best practice details the recommended course of action for the best result.
	Used to highlight processes that should be performed with care.
+	A plus sign between two keystrokes means that you must press them at the same time.
	A pipe sign between elements means that you must select the elements in that particular sequence.

About Quest Software, Inc.

Quest Software, Inc., Microsoft's 2007 Global Independent Software Vendor Partner of the Year, delivers innovative products that help organizations get more performance and productivity from their applications, databases Windows infrastructure and virtual environments. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 90,000 customers worldwide meet higher expectations for enterprise IT. Quest's Windows Management solutions simplify, automate secure and extend Active Directory, Exchange Server, SharePoint, SQL Server, .NET and Windows Server as well as integrating Unix, Linux and Java into the managed environment. Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

Email: info@quest.com
Mail: Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA
Web site: www.quest.com

Refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at <http://support.quest.com>

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the **Global Support Guide** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: [http://support.quest.com/pdfs/Global Support Guide.pdf](http://support.quest.com/pdfs/Global%20Support%20Guide.pdf)

1

What is New in Enterprise SSO 8.0 Evolution 2

- New Installation Modes
- ADAM Improvements
- Audit Improvements
- New E-SSO Console Features
- Emergency Access Improvement
- Integration with Gemalto SA Server

With E-SSO 8.0 Evolution 2 version, the new functionalities/improvements are:

- New installation modes,
- ADAM improvements,
- Audit improvements,
- New E-SSO Console features,
- Emergency access improvements,
- Integration with Gemalto SA Server.

1.1 New Installation Modes

The new version improves ease of use for small installations, and does not require any new hardware. It uses existing infrastructure so SSO can be deployed gradually.

This version can be installed:

- Without security module: you can choose to use software protection (PassPhrase) to protect your data. All E-SSO features are available in this mode.
- Without managing Access Point: you can choose to manage Access Point or not.



When the Access point management is deactivated the audit origin is no more certified.

1.2 ADAM Improvements

ADAM servers can now be used in multi-domain configuration, therefore fast deployments can be done without modifying the Active Directory schema.

1.3 Audit Improvements

Administrators can now define which audit events must be generated.

1.4 New E-SSO Console Features

There are two improvements:

- The administration rights can manage individual rights.
- The search method has been replaced.

1.5 Emergency Access Improvement

Emergency access questions can be translated and the questions asked to users can be a sub set of the supplied ones.

1.6 Integration with Gemalto SA Server

Drawing on its partnership with Gemalto, Quest includes the management of Gemalto SA Server® in Enterprise SSO 8 evolution 2. Organizations can harmonize card assignment procedures for combined local/remote access.

Technical Details

- Client Environment
- LDAP Directories and Databases Versions
- Supported Authentication Devices
- SSOWatch Plug-in Requirements
- Supported HTTP Server
- Configuring the HLLAPI Plug-in
- Warnings
- Restrictions

2.1 Client Environment

2.1.1 Operating System Prerequisites

Enterprise SSO 8.0 modules can be installed on the OS platforms detailed in the table below. This concerns the following modules:

- SSOWatch
- Advanced Login
- Enterprise Console
- Token Manager

OPERATING SYSTEM	SERVICE PACKS	MANDATORY MODULES
Windows 2000	SP2, SP3 or SP4	Internet Explorer 5.5 or 6.0
Windows XP (Home or Professional Edition)	SP1 or SP2	Internet Explorer 6.0 or 7.0
Vista (all editions)		Internet Explorer 6.0 or 7.0
Windows 2000 Server	SP2, SP3 or SP4	Internet Explorer 5.5 or 6.0
Windows 2003 Server	Original, SP1, R1 and R2	Internet Explorer 6.0 or 7.0
Windows 2008 Server	Original	Internet Explorer 7.0
Citrix MetaFrame	1.8 SP3	Internet Explorer 5.5 or 6.0
Citrix MetaFrame XP	SP3	Internet Explorer 5.5 or 6.0



On Windows 2008 Server, the MSDE audit database natively provided cannot be used.

Quest Data Privacy modules (Enterprise SSO Mobile Protect and Enterprise SSO File Encryption) can be installed on the following operating systems:

- Windows 2000 SP 4
- Windows XP (Home or Professional Edition) SP2

Please note that Enterprise SSO has **not** been validated with the following:

- Any 64-bit version of Windows, such as Windows XP Professional x64 Edition or Windows Server 2003 x64 Editions
- Any virtualization software such as VMware Workstation or Microsoft Virtual PC.

2.1.2 Hardware Prerequisites

- SSOWatch, Advanced Login and Token Manager

The Enterprise SSO client does not require significant resources on modern computers. The recommended minimal configuration on Windows XP is the following:

- 1 GHz Intel processor
- 256 MB RAM
- Enterprise SSO Console

The Enterprise SSO Console must run on a recent configuration in order to access the audit base with satisfactory performance. The recommended minimal configuration is the following:

- Intel Core 2 Duo processor
- 2 GB RAM

The size of the hard drive hosting the audit base depends on how long you want to keep the log on-line before archiving it. (The audit base does not need to reside on the Enterprise SSO server itself.). For a rough estimate use the following:

- One log entry = 1000 bytes (including database index and other overhead),
- Typical log activity = 20 log entries per user per day.

2.2 LDAP Directories and Databases Versions

2.2.1 LDAP Directory Versions

Enterprise SSO can access user information located in LDAP directories and use these directories to store SSO and security data. The directories supported by Enterprise SSO are:

DIRECTORIES	OPERATING SYSTEMS AND/OR DIRECTORY VERSIONS
Active Directory	<ul style="list-style-type: none"> • Windows 2000 Server SP4 • Windows Server 2003 SP1 & SP2 • Windows 2008
Sun Java System Directory Server	Sun Java System Directory Server 5.2
Fedora Directory Server	Fedora Directory Server 1.0.1 on Red Hat Linux
OpenLDAP	OpenLDAP Directory 2.2.29 <i>Use the latest stable version from the OpenLDAP Foundation or your OS manufacturer.</i>
Novell eDirectory	Version 8.7.3 minimum
IBM Tivoli Directory Server	Version 5.2 with Fix Pack 003

Enterprise SSO can use Microsoft Active Directory Application Mode (ADAM) to store SSO and security data. In that case, Enterprise SSO requires ADAM version 1.1 (SP1) or later.



Don't find the version you're using? To obtain an up-to-date list of supported LDAP directories versions, please contact your Quest representative.

Using Enterprise SSO with Samba

Enterprise SSO can be installed in an environment where Samba is used as an authentication server and domain controller. The prerequisites are:

- Samba must be in version 3.0.x
- Samba must use OpenLDAP (see version above)

2.2.2 Database Versions

Enterprise SSO server can store a “master” audit base on a relational database. Enterprise SSO has been validated with the following database versions running on Windows 2003 Server Enterprise Edition:

- Oracle 8.1.7.4
- IBM DB2 version 9.0
- MySQL Server 5.0
- PostgreSQL 8.1
- Microsoft SQL Server 2000 and 2005

The audit cache base can also be one of the database types listed here.

If you want to use another type of relational database, please contact Quest for a feasibility and cost evaluation.

2.2.3 Link with User Provisioning

The link with the User Provisioning requires User Provisioning 8.0.

2.3 Supported Authentication Devices

2.3.1 Smart Cards and USB Tokens

The following middleware and authentication devices are compatible with these specific Enterprise SSO modules:

- **Advanced Login** can use the devices for user authentication
- **Token Manager** and **Enterprise SSO Console** can manage these devices.
- **Token Manager** and **Enterprise SSO Console** can use these devices for administrator authentication.

VENDOR	MIDDLEWARE	TOKENS
Gemalto	No middleware	Cryptoflex e-gate 32K NOTE: in this mode, only Enterprise SSO can use the authentication device.
Gemalto	ACS 5.2	Cryptoflex e-gate and e-gate 32K with USB connectors or PC/SC readers
Gemalto	ACS 5.2	Cyberflex 64K with PC/SC readers
ActivCard	ActivClient 5.3.1	Cyberflex and Oberthur smart cards
AET	SafeSign 2.2	Cyberflex smart cards and IKEY3000 tokens
Aladdin	eToken RTE 3.65	eToken PRO (USB and smart card)
Oberthur	AWP (Authentic Web Pack) 3.6.2.2	Cosmo 64 v5 + Option MiOption Hybride Mifare 1Kfare smart cards

To request validation with other types of middleware and devices, please contact Quest.

Please note that when using smart cards, you must use **PC/SC smart card readers** that are compatible with both the cards and the middleware detailed above.

The only Certification Authority that is supported at the moment is the Microsoft Windows 2000/2003 Certification Authority in an Active Directory configuration. Other Certification Authorities can be used via the PKCS import feature of the Enterprise SSO Console and Token Manager.

2.3.2 Biometric Devices

Biometrics support requires that you purchase from Precise Biometrics a license of **Precise BioMatch™ Pro Toolkit 2.3.0** for each workstation where biometric authentication will be performed.

The list of biometric devices supported by Precise BioMatch™ Pro Toolkit 2.3.0 is currently the following:



Some of these devices require a specific license of the Precise Biometrics software. Determine with the vendor which license is appropriate

- Precise 100 A/AX/SC/MC/XS/BioKeyboard/PC-Card
- Precise 200 MC
- Precise 250 MC
- IRIS BCR100T
- IRIS Mobile SmartTerm St4E
- AuthenTec AES4000 API-based readers
- AuthenTec AES2501 API-based readers
- Cherry FingerTIP Keyboards
- UPEK ST1
- UPEK ST2
- silex FUS-200N
- silex MUSB-200-COMBO
- silex COMBO-Mini

For an up-to-date list, contact Precise Biometrics (www.precisebiometrics.com).

2.4 SSOWatch Plug-in Requirements

2.4.1 General Requirements

Plug-ins are extensions of SSOEngine and SSOSTudio. They provide SSO authentication methods for specific types of applications.

These plug-ins are delivered with SSOWatch. Plug-ins are available for:

- Microsoft Internet Explorer (for Internet Explorer 5.5, 6.0 and 7.0)
- Firefox 1.5 and 2.0
- Sun Java SE Runtime Environment (JRE) 1.4. and 1.5
- Lotus Notes versions 4.x, 5.x and 6.5.
- Microsoft Telnet
- HLLAPI (see 2.6 "Configuring the HLLAPI plug-in" for supported emulators).
- SAP R/3 client version 6.20
- Script environment for Windows and HTML applications that are not covered by the standard Enterprise SSO process.

2.4.2 SSOWatch SAP R/3 Plug-in Requirements

The table below shows the supported versions of SAP R/3 components:

SSOWATCH WINDOW TYPE	SAP R/3 CLIENT VERSION	SAP R/3 SERVER VERSION (MINIMUM KERNEL PATCH LEVEL)
SAPGUI Scripting	SAP GUI 6.20	6.10 (360)
	SAP GUI 6.40	4.6D (948)
		4.5B (753)
		4.0B (903)
		3.1I (650)



The SAP web-based Start Center is compatible with Enterprise SSO, but you need to upgrade to SAPGUI Version 6.40 with Patchlevel 23.



The SAPLogin and SAPEXPIRED window types defined in version 3.71 of SSOWatch remain available to ensure the continuity of deployed configurations.

We recommend not using them for new deployments. Existing windows should be ported to SAPGUI Scripting window types.

2.5 Supported HTTP Server

The following Enterprise SSO features require an HTTP server:

- Enterprise SSO Web Service administration API
- Enterprise SSO password reset feature

Quest delivers an HTTP server with the Enterprise SSO CD-ROM (based on Apache 2.0). This web server is the only server supported by Quest.

We strongly recommend you use the HTTP server delivered by Quest. Quest will not provide support for the above-mentioned features when used with any other server. As well, Quest will not support the bundled server for functions other than those that are strictly necessary for the above Enterprise SSO features.

The password reset feature requires you to use a certificate generated by a Certification Authority (CA) in order to activate HTTPS. Quest delivers a sample CA for testing purposes, but *does not provide support* for that CA. Please use a supported CA for actual deployments.

2.6 Configuring the HLLAPI Plug-In

The HLLAPI plug-in communicates with a terminal emulator through a DLL. Each emulator provides a different DLL for that purpose.

To tell SSOWatch how to communicate with your terminal emulator, you need to edit the Microsoft Windows Registry and enter three values located under HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\SSOWatch\HLLAPI

- *HllLibrary*—the name of the emulator’s DLL (file name or full path) that gives access to the HLLAPI feature.
- *HllEntryPoint*—the name of the relevant function in the DLL file.
- *HLLAPI-32bit*—indicates whether the HLLAPI is in 32-bit mode (value=1) or not (value=0)

	HLLIBRARY	HLENTRYPOINT	HLLAPI-32BIT
Attachmate EXTRA!® Enterprise 2000	ehlapi32.dll	hllapi	0
<i>Values used by the plug-in if the registry entries do not exist.</i>	<i>PCSHLL32.dll</i>	<i>hllapi</i>	<i>1</i>



The Registry entry and associated values are not created during installation. You need to manually create the Registry entry "HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\SSOWatch\HLLAPI" and the three values "HllLibrary", "HllEntryPoint" and "HLLAPI-32bit"

2.7 Warnings

2.7.1 Updating Enterprise SSO Modules

The Advanced Login, SSOWatch, File Encryption, Token Manager and Enterprise SSO Console modules may be installed on a same system. In this configuration, when you update these Enterprise SSO modules, please bear in mind that:

- If the Enterprise SSO server component is present, it must be updated before any other modules.
- Quest recommends that you update all the Enterprise SSO modules installed on this station to the latest patch level.

2.7.2 Do Not Use Enterprise SSO Console on Citrix or Terminal Services Servers.

Due to performances issues, we recommend not to install Enterprise SSO Console on Citrix or Windows Terminal Services servers

2.7.3 SSOWatch and Advanced Login POCs Can Be Done without Smart Cards

To facilitate LDAP-based Proof-of-Concept (POC), it is now possible to demonstrate SSOWatch without smart cards and readers (including, if required, SSOSTudio or Advanced Login features).

Please note that in this configuration, the following features are not available:

- *Primary passwords reset by the administrator.* The administrator cannot use Enterprise SSO to reinitialize the user's primary password. The administrator should not use the standard LDAP console to modify the primary password; otherwise SSOWatch will ask the user to provide his or her old password when connecting.
Users can still modify their primary password themselves using either the standard Windows interface or Advanced Login (if present).
- *Secondary password reset and modification by the administrator.* The administrator cannot force or reset any secondary password.
Users can still create and modify their secondary passwords themselves using SSOWatch.

2.7.4 Advanced Login: RDP Connections on Windows XP

On Windows XP, the Remote Desktop Protocol (RDP) connections with a smart card are supported on Windows XP SP2 only.

Please note that Quest only supports this feature for Microsoft's client portion of Remote Desktop. No other RDP clients are supported.

2.7.5 Do not Use SSOWatch 8.0 with AccessMaster

Please note that SSOWatch 4.5 must not be used with AccessMaster. You must use the version of SSOWatch that is delivered with your AccessMaster CDs.

2.7.6 Integrating an Application with the HLLAPI Plug-in Depends on Many Factors

Successful integrating a terminal application with the HLLAPI module depends on many parameters:

- Which terminal emulator is used
- Which terminal protocol is used
- The specific way in which the application implements login

The HLLAPI plug-in has been tested by Quest with the following emulators in **some** basic conditions:

- Attachmate EXTRA! Mainframe Server Edition 8.1
- Gallagher & Robertson Glink Professional Edition version 8.0.5
- NetManage RUMBA version 7.4
- Zephyr PASSPORT PC TO HOST (version 2004-3B30-4)
- Distinct IntelliTerm 8.1

However, this does not mean that integrating any application with any terminal protocol will always work with the above emulators. In some cases, the specificities of applications means that successfully integrating them may require paid services from Quest or Quest partners.

2.7.7 Integrating a Third-party Card Management System (CMS) is not Possible in all Cases

Quest can integrate a third-party CMS with Enterprise SSO on a service basis. This requires paid professional services from Quest.

Once integrated, the third-party system replaces the CMS features of Token Manager and Enterprise SSO Console.

Please be aware that, for this integration to be technically feasible, there are a number of technical prerequisites on the third-party CMS. Please contact Quest for a list of those prerequisites.

2.7.8 When SSOWatch is Used with Novell NetWare, the NetWare Password Must Be the Same as the Windows Password

When SSOWatch is used in Novell NetWare environments, please make sure that the NetWare password is always the same as the Windows password.

You must use a NetWare option to synchronize the Windows password with the NetWare password.

If this is not done, the user will need to perform a second authentication to Novell NetWare after his or her Windows authentication.

2.7.9 Enterprise SSO Only Supports the Default Versions of Cryptoflex Cards

Enterprise SSO only supports the default "answer to reset" (ATR) of Gemalto Cryptoflex cards:

- Cryptoflex 32K : 3b 95 XX 40 ff 64 02 01 XX XX
- Cryptoflex e-gate 32K : 3b 95 XX 40 ff 62 01 02 XX XX

Customized Cryptoflex cards are not supported.

2.7.10 Evaluate the Database Space Required to Log Events for Audit

The version of SQL Server that is bundled with Enterprise SSO is limited in storage space; it can only hold 2 gigabytes of data. This can be used up quickly for large numbers of users.

As each audit event occupies ca. 1 kilobyte, storing audit events for 250 users typically requires archiving every week.

To overcome this limitation, please use a "master" audit database (see 2.2.2 "Database versions").

2.7.11 SSOWatch Internet Explorer Plug-in Warnings

The following warnings apply to the new Internet Explorer 6.0 and 7.0 plug-in:

- Framesets are only managed on a single level.
- If a frameset contains a secure page that contains a combo box, SSOWatch cannot activate that combo box.

2.7.12 Do not Install Enterprise SSO Servers on Active Directory Controllers

It is not recommended to install Enterprise SSO servers on Active Directory controllers because of startup problems.

2.7.13 Some Features Are Available in English Language Only

The following will be displayed in English language only in localized versions:

- Detailed description of administration events (audit feature of Enterprise SSO).
- Java Virtual Machine (JVM) configuration program (Java plug-in feature of SSOWatch)

2.8 Restrictions

2.8.1 Windows Active Directory Inter-Domain Support with Enterprise SSO Console in Temporary Restriction

When a station is declared in several domains using Enterprise SSO Console, there are restrictions in access for users who do not belong to the same domains as the station.

	WITH ADVANCED LOGIN	WITHOUT ADVANCED LOGIN
Users who belong to the same domain as the station	Can authenticate SSO active	Can authenticate SSO active
Users who do not belong to the same domain as the station	<i>Cannot authenticate</i>	Can authenticate SSO not active

This restriction exists:

- In server mode, if the various domains the user belongs to are not located in the same Active Directory forest.
- In standalone mode, if the middleware does not have a user account. In that case, deploying a user account for the middleware will lift the restriction.

2.8.2 Active Directory Multi-Domain and Multi-Forest

The multi-domain functions are managed in one forest only.

2.8.3 Not yet Available: Multi-Account Mode in the User Provisioning Link

When the User Provisioning link is active, it is not possible for a user to have more than one account on the same application (e.g. user account and administrator account).

2.8.4 LDAP Accounts Used by Enterprise SSO Servers Must Not Expire

The LDAP accounts used by Enterprise SSO servers must not expire. This restriction will be lifted in the future.

Documentation

Quest Enterprise SSO

Documentation of Enterprise SSO can be found on the Evidian IAM suite documentation CDROM.

Available documents are:

DOCUMENT TITLE	DOCUMENT REFERENCE
Enterprise SSO—Getting Started with SSOWatch	39A243LU00
Enterprise SSO Installation and Configuration Guide—Extended Manager Mode	39A240LU00
Enterprise SSO—Advanced Login User Guide	39A236LU00
Enterprise SSO Console Administrator Guide	39A237LU00
Enterprise SSO—SSOWatch Administrator Guide	39A238LU00
Enterprise SSO API and Web Services Reference Guide	39A244LU00
Laptop Protection User's Guide	39A224LU02
File Encryption User's Guide	39A267LU00