One Identity Single Sign-on for Java 3.3.2

Release Notes

[May 2019]

These release notes provide information about the One Identity Single Sign-on for Java 3.3.2 release.

Topics:

Welcome to One Identity Single Sign-on for Java

One Identity Single Sign-on for Java is a suite of components providing Kerberos single sign-on for Java SE and for Java web applications, running on any operating system, in enterprise environments that use Microsoft Active Directory.

Single Sign-on for Java includes:

- A pure Java implementation of Kerberos, GSSAPI and SPNEGO with tight integration to Active Directory, including support for cross-domain and cross-forest authentication, and Active Directory Site auto-discovery for scalability.
- Active Directory group membership information that can be used as a basis for Java EE roles.
- Optional integration with One Identity Authentication Services for simplified configuration on Unix and Linux.
- Development libraries, examples and documentation for creating your own Java Kerberos / GSSAPI and single sign-on applications.
- For Java fat clients on Windows that expect to automatically use the Active Directory credentials of the logged-in user (without requiring any registry modifications), the WinSSPIProvider class and its accompanying winSSPI.dll
- Java command line utilities for managing Kerberos credentials.

Single Sign-on for Java was previously named VSJ (Vintela Single Sign-on for Java) and this name is still reflected in Java class names and package names, in JAR files, and in other filenames.

Supported platforms

One Identity Single Sign-on for Java supports Java Servlet Specification 2.4 or higher on any operating system.

New features

New features in Single Sign-on for Java 3.3.2:

- Support for Windows Server 2012 resource-based constrained delegation. Previous releases supported the original "account-based" constrained delegation that was introduced in Windows Server 2003; this release automatically supports both. Whereas account-based constrained delegation is restricted to a single domain, resource-based constrained delegation supports cross-realm and cross-forest delegation. In order for Single Sign-on for Java to use resource-based constrained delegation, all domain controllers in the relevant domain(s) must run Windows Server 2012 or above.

- Support for Windows Server 2012 User Claims in the service ticket. This can be an alternative to LDAP lookups for User attributes. The domain(s) must have Claims enabled and configured. This is implemented by an optional plugin in the plugin/ad-claims directory.
- JASPIC (JSR 196) ServerAuthModule. This is an optional alternative to using the servlet filter. The Java application server must implement JASPIC and support the deployment / configuration of a ServerAuthModule. Please see the Javadoc (in doc/VSJ/apidocs) for the com.wedgetail.idm.sso.jaspic package.
- JGSS provider support for the JDK 1.7 com.sun.security.jgss.ExtendedGSSContext and JDK 1.8 com.sun.security.jgss.ExtendedGSSCredential API. For details please see the class Javadoc (in doc/VSJ-Kerberos/apidocs) for the com.dstc.security.kerberos.provider.WedgetailGSSProvider and the com.dstc.security.kerberos.winSSPI.WinSSPIProvider.
- `vsj-kerberos.properties` resource. Settings such as jcsi.kerberos.* that previously could only be specified as Java system properties may now also be specified in an optional /vsj-kerberos.properties resource on the classpath. A setting from vsj-kerberos.properties has lower precendence than a corresponding system-property setting.

See also:

- Enhancements
- Resolved issues

Enhancements

The following is a list of enhancements implemented in Single Sign-on for Java 3.3.2.

Table 1: General enhancements

Enhancement	Issue ID
Commons Logging is now optional. Previously the Apache Commons Logging library was required on the classpath; now, if it is not present, this release defaults to using `java.util.logging` directly. You can use `-Djcsi.kerberos.skipCommonsLogging=true` to explicitly ignore Commons Logging.	
Active Directory Site auto-discovery for the VSJ Kerberos layer. Previously this was automatically enabled for VSJ (the servlet filter) but not for applications that used only VSJ Kerberos; it is now automatically enabled even for VSJ Kerberos.	

Enhancement	Issue ID
JGSS provider: improved support in com.dstc.security.kerberos.provider.WedgetailGSSProvider for some non-fat-client use cases, including the Microsoft JDBC Driver for SQL Server.	

Deprecated features

The following is a list of features that are no longer supported starting with Single Sign-on for Java 3.3.2.

- **Deprecation of Kerberos DES encryption types**, per RFC 6649. The default list of Kerberos encryption types is now AES256, AES128 and RC4-HMAC (18, 17 and 23); the single-DES encryption types (DES-CBC-CRC, DES-CBC-MD4 and DES-CBC-MD5) have been removed from the default list. The "jcsi.kerberos.encTypes" system property can be used to override the default.

Resolved issues

The following is a list of issues addressed and enhancements implemented in One Identity Single Sign-on for Java 3.3.2.

Table 2: Resolved issues: javax.servlet layer

Resolved Issue	Issue ID
IllegalArgumentException during initialization on Tomcat 8.0.0 -- 8.0.24	3632
SID-to-name mapping table: updated Active Directory well-known group SIDs	----
ADFSv1: allow InvalidFederationTokenException to be intercepted	----

Table 3: Resolved issues: Java SE layer (GSSAPI/Kerberos)

Resolved Issue	Issue ID
When sending a delegated TGT, all encryption types newer than DES / 3DES *should* encrypt the KRB_CRED	1077
GSSContext.initSecContext(byte[],int,int) should allow `null` in first invocation	3572
JGSS providers: add support for OpenJDK 1.6 and (current early-access versions of) JDK 1.9	3628

Resolved Issue	Issue ID
Only use OK-AS-DELEGATE if at least one of requestCredDeleg(true), requestDelegPolicy(true) or jcsi.kerberos.honorOkAsDelegate=true is set	3633
GSS initiator should use correct Kerberos name-type (e.g. KRB_NT_SRV_HST) in TGS-REQ	3636
KrbError toString(): hex dump some e-data in KRB-ERROR	----

This release also resolves the following issues that were previously addressed in patches to the 3.3 release:

Table 4: Resolved issues: From Patch 3598

Resolved Issue	Issue ID
JGSS providers: add support for Sun / Oracle / OpenJDK 1.7 and above	3598

Table 5: Resolved issues: From Patch 3601

Resolved Issue	Issue ID
Detect unavailable domain controllers expeditiously, then try alternative domain controllers. Explicitly set timeouts for TCP connection establishment (for KDC requests over TCP and for automatic site discovery over TCP), rather than depending on the default timeout from the OS / JVM.	3601

Table 6: Resolved issues: From Patch 3603 / TP1 / TP2 / TP3

Resolved Issue	Issue ID
NTLM: Support increased NTLM security	3603

Table 7: Resolved issues: From Patch 3609

Resolved Issue	Issue ID
For LDAP requests, explicitly set timeouts for TCP connection establishment rather than depending on the default timeout from the OS / JVM.	3607
Fix erroneous backoff-time calculation for domain controllers that were unavailable for two or more attempts.	3608

Table 8: Resolved issues: From Update_20150605

Resolved Issue	Issue ID
Kerberos: Avoid KDC_ERR_ETYPE_NOSUPP in domains where not all DCs support the same set of encryption types	3585
S4U2Self: Recognize expired S4U2Self tickets and replace them with fresh ones	3611
Kerberos: Generate channel bindings that interoperate with major C implementations (MIT, Heimdal, Active Directory), not with the letter of the RFCs	3612
ADFSv1 enhancements: new 'fsProxyExtraParams' and 'omitDomainInPrincipalName' options	3613
When sending LDAP SASL requests, avoid unnecessary generation of small TCP packets (and triggering of Nagle's algorithm)	3615
When LDAP requests to a particular server are problematic, correctly mark that server as problematic and prefer other servers for subsequent LDAP requests.	3622
When selecting a server to handle a new LDAP request, prefer servers that do not currently have outstanding LDAP requests. Also eliminate some unnecessary serialization on shared instances in the LDAP code.	3623
Java fat clients on Windows: Kerberos session-key retrieval *is* supported now on Windows 6.0	3625
AttributeUserPrincipalFormatter: If the attribute value is not set for a particular User, do *not* automatically substitute the user's sAMAccountName	3626
Java fat clients on Unix/Linux: tolerate X-CACHECONF entries in MIT / Heimdal credential-cache files	3627

System requirements

Before installing One Identity Single Sign-on for Java 3.3.2, ensure your system meets the following minimum system requirements:

Table 9: System requirements

Requirement	Details
Active Directory domain controllers	Microsoft Windows Server 2008 or higher. Some optional functionality -- resource-based constrained delegation, and Claims from the service ticket -- requires Windows Server 2012 or higher.
JVM	Java SE 5.0 (1.5) or higher on any operating system.

Product licensing

If you have a vsj-license.jar (or legacy jcsi_license.jar) file that you have used with previous releases, this release is fully compatible with that license file.

If you have purchased Single Sign-on for Java you should have received a production vsj-license.jar file (typically packaged in a "license.zip" file to avoid problems in transit).

If you require a trial key for Single Sign-on for Java, please contact your sales representative. The trial key is a vsj-license.jar file that has a time limit.

To activate a license (either trial or purchased commercial)

1. The vsj-license.jar file should be made available on the same classpath as the vsj-standard-3.3.2.jar file; for example, in a web application, both of these files may be placed in the WEB-INF/lib directory.
2. If you are working with the examples that are included in this release, copy the vsj-license.jar file alongside the vsj-standard-3.3.2.jar file in the ./lib directory before starting to build the examples.

Upgrade and installation instructions

This release, 3.3.2, includes and replaces:

- The original VSJ Standard Edition 3.3 release and its cumulative patch releases:
  - VSJ Standard Edition 3.3 Patch 3463
  - VSJ Standard Edition 3.3 Patch 3540
  - VSJ Standard Edition 3.3 Patch 3548
  - VSJ Standard Edition 3.3 Patch 3596
  - VSJ Standard Edition 3.3 Patch 3603 TP1, TP2, TP3
  - VSJ Standard Edition 3.3 Update 20150605
- Incremental patches:
  - VSJ Patch 3598
  - VSJ Patch 3601
  - VSJ Patch 3609
- VSJ WebSphere Edition 3.2

This release does **not** include VSJ Patch 3112 (optional incremental patch: 64-bit version of winSSPI.dll), but VSJ Patch 3112 may be used with this release.

If you are upgrading from a previous release, please ensure that you no longer use the JAR file from that release (e.g. vsj-standard-3.3.jar) and instead use only the vsj-standard-3.3**.2**.jar file that is included in this release.

Installation instructions

Refer to the One Identity Single Sign-on for Java Administration Guide for installation instructions.

The Simple example, in ./examples/simple, is designed to act as a good starting point and is also helpful for detecting configuration problems.

Contents of the release package

The One Identity Single Sign-on for Java release package contains the following products:

1. One Identity Single Sign-on for Java 3.3.2: vsj-standard-3.3.2.jar
2. jcifs-1.3.18.jar (only needed if idm.allowNTLM=true is configured)
3. Apache Commons Logging and Log4J (optional, included for convenience in building the sample code)
4. Sample source code and web applications, in the ./examples tree
5. Javadoc, in subdirectories of ./doc
6. Optional DLL (winSSPI.dll), enables Java fat clients on Windows to transparently use the Active Directory Kerberos credentials of the logged-in user
7. Optional plugin for Windows Server 2012 Claims
8. Optional plugin for integration with Jespa (third-party component sold by IOPLEX Software, adds NTLMv2 support)
9. Optional ADFSv1 support
10. jcifs-1.3.18.zip -- LGPL source code (with no modifications) for jCIFS

The release package does **not** contain:

- vsj-license.jar: See Product Licensing.
- Documentation: The Administration Guide, previously called the Reference Manual, which is now hosted on the Support site under Single Sign-On for Java - Technical Documentation.

More resources

Additional information is available from the following:

- Online product documentation: https://support.oneidentity.com/single-sign-on-for-java/technical-documents

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe.

This release has the following known capabilities or limitations: Limitations are to be discussed before such I18N is introduced into the product. No known limitations.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.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 at www.YouTube.com/OneIdentity
- 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 https://www.oneidentity.com/legal/license-agreements.aspx. Source code for components marked with an asterisk (*) is available at http://opensource.quest.com.

Table 10: List of Third-party components

Component	License or Acknowledgement
Apache Commons Logging 1.1.3	Apache License Version 2.0 This product includes software developed at The Apache Software Foundation (http://www.apache.org/).
JCIFS 1.3.18	GNU Lesser General Public License 2.1 Copyright (C) 1996 by Jef Poskanzer <jef@acme.com>. All rights reserved. Copyright (c) 1996 Widget Workshop, Inc. All Rights Reserved. Copyright (C) 1996 by Wolfgang Platzer email: wplatzer@iaik.tu-graz.ac.at All rights reserved. Copyright (c) 1997 Systemics Ltd on behalf of the Cryptix Development Team. All rights reserved. Copyright (C) 2000 "Christopher R. Hertel" <jcifs at samba dot org> Copyright (C) 2000 Gary Rambo <grambo aventail.com> Copyright (C) 2000 "Paul Walker" <jcifs at samba dot org> Copyright (C) 2002 "Jason Pugsley" <jcifs at samba dot org> Copyright (C) 2002 "skeetz" <jcifs at samba dot org> Copyright (C) 2006 "Eric Glass" <jcifs at samba dot org> Copyright (C) 2009 "Michael B Allen" <jcifs at samba dot org>
JLDAP Mar_ndk_2003	The OpenLDAP Public License 2.4.10 Version 2.8, 17 August 2003
Log4J 1.2.17	Apache License Version 2.0

Component	License or Acknowledgement
	This product includes software developed at The Apache Software Foundation (http://www.apache.org/).
OpenSAML 1.1	Apache License Version 2.0 Copyright 2002-2005 Internet2 We wish to acknowledge the following copyrighted works that make up portions of this software: This product includes software developed by the Apache Software Foundation (http://www.apache.org/). We also thank Tom Scavo for donating the original SAML artifact implementation.
Xalan Java 2.7.1	Apache License Version 2.0 Apache Xalan (Xalan XSLT processor) Copyright 1999-2006 The Apache Software Foundation Apache Xalan (Xalan serializer) Copyright 1999-2006 The Apache Software Foundation This product includes software developed at The Apache Software Foundation (http://www.apache.org/). === Portions of this software was originally based on the following: - software copyright (c) 1999-2002, Lotus Development Corporation., http://www.lotus.com. - software copyright (c) 2001-2002, Sun Microsystems., http://www.sun.com. - software copyright (c) 2003, IBM Corporation., http://www.ibm.com. === The binary distribution package (ie. jars, samples and documentation) of this product includes software developed by the following: - The Apache Software Foundation - Xerces Java - see LICENSE.txt - JAXP 1.3 APIs - see LICENSE.txt - Bytecode Engineering Library - see LICENSE.txt - Regular Expression - see LICENSE.txt

Component	License or Acknowledgement
	- Scott Hudson, Frank Flannery, C. Scott Ananian - CUP Parser Generator runtime (javacup\runtime) - see LICENSE.txt == The source distribution package (ie. all source and tools required to build Xalan Java) of this product includes software developed by the following: - The Apache Software Foundation - Xerces Java - see LICENSE.txt - JAXP 1.3 APIs - see LICENSE.txt - Bytecode Engineering Library - see LICENSE.txt - Regular Expression - see LICENSE.txt - Ant - see LICENSE.txt - Stylebook doc tool - see LICENSE.txt - Elliot Joel Berk and C. Scott Ananian - Lexical Analyzer Generator (JLex) - see LICENSE.txt === Apache Xerces Java Copyright 1999-2006 The Apache Software Foundation This product includes software developed at The Apache Software Foundation (http://www.apache.org/). Portions of Apache Xerces Java in xercesImpl.jar and xml-apis.jar were originally based on the following: - software copyright (c) 1999, IBM Corporation., http://www.ibm.com. - software copyright (c) 1999, Sun Microsystems., http://www.sun.com. - voluntary contributions made by Paul Eng on behalf of the Apache Software Foundation that were originally developed at iClick, Inc., software copyright (c) 1999. === Apache xml-commons xml-apis (redistribution of xml-apis.jar) Apache XML Commons Copyright 2001-2003,2006 The Apache Software Foundation.

Component	License or Acknowledgement
	This product includes software developed at The Apache Software Foundation (http://www.apache.org/). Portions of this software were originally based on the following: - software copyright (c) 1999, IBM Corporation., http://www.ibm.com. - software copyright (c) 1999, Sun Microsystems., http://www.sun.com. - software copyright (c) 2000 World Wide Web Consortium, http://www.w3.org
Xerces 2.7.1	Apache License Version 2.0 (See Notice for Xalan Java 2.7.1 above.)
XML Security 1.3.0	Apache License Version 2.0 This product contains software developed by The Apache Software Foundation (http://www.apache.org/). It was originally based on software copyright (c) 2001, Institute for Data Communications Systems, <http://www.nue.et-inf.uni-siegen.de/>. The development of this software was partly funded by the European Commission in the <WebSig> project in the ISIS Programme.

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY 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 DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

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.