Sterling External Authentication Server

Release Notes

Version 24.1

Last Updated: 04/28/2014

Sterling External Authentication Server

Release Notes

Version 24.1

Last Updated: 04/28/2014

Note
Before using this information and the product it supports, read the information in "Notices" on page 9.

This edition applies to version 2.4 of IBM Sterling External Authentication Server(product number xxxx-xxx) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Sterling External Authentication Server Release Notes

System Requirements

IBM® Sterling External Authentication Server has the following hardware and software requirements.

Component or Functionality	Hardware	Software	RAM	Disk
Sterling External Authentication Server	Microsoft Windows compatible systems	Microsoft Windows Server 2003 Service Pack 1 (32-bit) Microsoft Windows Server 2008 R2 (64-bit) Sterling External Authentication Server supports 64-bit JRE with Windows Server 2008 R2	512 MB	200 MB
	HP 9000 (PA-RISC)	HP-UX, version 11.23 Sterling External Authentication Server supports 64-bit JRE with this operating system.	512 MB	200 MB
	IBM System p5 and IBM Power Systems	AIX, versions 6.1 and 7.1 Sterling External Authentication Server supports 64-bit JRE with this operating system.	512 MB	200 MB
	SUN SPARC system	Solaris, version 10 Sterling External Authentication Server supports 64-bit JRE with this operating system.	512 MB	200 MB
	x64/x86 64-bit	Red Hat Enterprise Linux Advanced Server, version 5 and 6 SuSE SLES, version 10 and 11 Sterling External Authentication Server supports 64-bit JRE with these operating systems.	512 MB	200 MB
	zLinux 64-bit	Red Hat Enterprise Linux Advanced Server, version 5 and 6 SuSE SLES, version 10 and 11 Sterling External Authentication Server supports 64-bit JRE with these operating systems.	512 MB	200 MB
		• Open LDAP versions 2.2 and 2.3 • Sun Microsystems SunONE 5.2 • IBM Tivoli 6.x • Microsoft Windows 2003 Domain Functional Level Active Directory • Active Directory 2008	512 MB	200 MB

Component or Functionality	Hardware	Software	RAM	Disk
Sterling External Authentication Server GUI		Use one of the following: • Internet browser using Java WebStart • JRE version 1.6, installed with Sterling External Authentication Server	256 MB	
Authentication using Tivoli Access Manager		• Red Hat Advanced Server 4.0 • Tivoli Access Manager 5.1 • IBM Access Manager Runtime for Java • JRE version 1.4.2 **Note:** See Prerequisites to Authenticate with Tivoli Access Manager (TAM) for more information.	30 MB per TAM authentication definition	
VMware ESX and VMware vSphere		Any native operating system supported by Sterling External Authentication Server. Consider VMware-specific configuration, administration, and tuning issues. Your VMware administrator must address any issues. IBM does not provide advice regarding VMware-specific issues.		

Prerequisites to Authenticate with Tivoli Access Manager (TAM)

After Sterling External Authentication Server and Tivoli Access Manager (TAM) are installed on the same computer, you can set up authentication with TAM. Before you install the TAM API, install version 1.4.2 of the Java Runtime Environment (JRE) and configure it for use with TAM.

To configure JRE for TAM, set the JAVA_HOME environment variable to point to the appropriate JRE and install the TAM API using install_amjrte. The TAM API installation creates an IBM configuration file. TAM authentication definitions you create in Sterling External Authentication Server must reference the IBM configuration file and the JRE to support authentication with TAM.

Using Sterling External Authentication Server for Authentication with TAM

To use Sterling External Authentication Server for authentication with TAM:

1. Install 1.4.2 JRE on the target system, either as a system JRE or a private JRE for a user.
2. Set the JAVA_HOME environment variable to point to the JRE, then run the IBM wizard, install_amjrte to install the TAM API into the JRE.

   Refer to *IBM Tivoli Access Manager, Base Installation Guide, Version 5.1* for information.
3. Run the java utility, com.tivoli.pd.jcfg.SvrSslCfg. IBM provides the com.tivoli.pd.jcfg.SvrSslCfg class used as the configuration utility. Running the utility creates a configuration file and an SSL key and other configuration data needed to communicate securely with the TAM servers. See Configure the TAM API for more information.
4. In Sterling External Authentication Server, create TAM authentication definitions (profiles) in the **Target JRE location** field and the configuration file created by the Java utility in step 3 (**TAM Config File URL** field).

Because Sterling External Authentication Server is written for JRE 1.6, it cannot run in the same JRE as the TAM interface. When you set up a TAM authentication definition (or profile) within Sterling External Authentication Server, the current implementation requires the target JRE configured with Access Manager Runtime for Java. When the definition is saved, Sterling External Authentication Server starts the TAM Authenticator in a separate process executing in the target JRE. Standard input, output, and error streams are set up to the child process for communications. See *Create and Manage Tivoli Access Manager (TAM) Authentication Definitions* in the documentation library for instructions to create a TAM authentication definition.

Configure the TAM API

The following example demonstrates how the IBM Java utility configures the Sterling External Authentication Server into the TAM API. Refer to the configuration file created by this utility when setting up a TAM authentication definition with Sterling External Authentication Server.

```
> export JAVA_HOME=/home/SeasAdmin/java/j2sdk1.4.2_12
> export PATH=$JAVA_HOME/bin:$PATH
> java com.tivoli.pd.jcfg.SvrSslCfg -action config -admin_id sec_master -admin_pwd masterpass
  -appsvr_id SterlingEAS_ID -appsvr_pwd ldapPassword -host SterlingEAS_host -mode remote
 -port 999 -policysvr tamPolicySvr:7135:1 -authzsvr tamAuthzSvr:7136:1 -cfg_file
   /home/SeasAdmin/tam/config_file.conf -key_file /home/SeasAdmin/tam/keystore_file.ks
 -domain Default -cfg_action create
```

In the example, a private JRE was installed at /home/SeasAdmin/java/ and SeasAdmin is a user account for administering Sterling External Authentication Server for TAM. Refer to the following parameters to understand how the Java utility generates the SSL key and configuration file that enable Sterling External Authentication Server for TAM authentication.

Parameter	Description
-host	Host name of the Sterling External Authentication Server.
-appsvr_id	ID you define for the Sterling External Authentication Server TAM Authenticator. SvrSslCfg creates a user and a server entry in the TAM user registry that is composed of this ID concatenated with the host name, in this case: SterlingEAS_ID/SterlingEAS_host.
-appsvr_pwd	Password for the new user account created in the TAM user registry.
-port	Listen port for definition updates. It must be specified although it is not used by Sterling External Authentication Server.
-cfg_file	Configuration file that is created by the IBM com.tivoli.pd.jcfg.SvrSslCfg utility. Reference this file from the definition you create in Sterling External Authentication Server.
-key_file	Specifies the java key store created by the utility. Private key and certificates are written to this key store for SSL communications to the TAM policy and authorization servers.

What's New in this Release

Sterling External Authentication Server has the following features and enhancements:

Version	Feature or Enhancement
Version 2.4.1.8	Enhances security by providing LDAP security authentication for Admin users using the IBM Sterling External Authentication Server. Refer to *Users Dialog* in the documentation library.

	Adds ability to control Admin login attempts and lockout timeframe. Two fields to the sysGlobals.xml file in the [SEAS_INSTALL]/conf/system directory:
	• `maxAllowedLoginAttempts`
	• `loginLockoutDelayTime`
	
	The parameter for `maxAllowedLoginAttempts` determine the maximum login attempts to be enforced. A value greater than 1 must be entered for this functionality to be enabled. The default is 0 which also disables this functionality. There are no upper limits to this parameter.
	
	This value controls the number of times an Admin user is allowed to make a login attempt without success before the account is locked out.
	
	`loginLockoutDelayTime` is used to indicate the amount of time in minutes that locked admin account is locked before it can be made active again. The default is 10 minutes. There are no upper limits for this parameter.
	
	To activate these settings, the SEAS configurations must be decrypted using the [SEAS_INSTALL]bin/decrypt script file. Once the configuration files are decrypted, the [SEAS_INSTALL]/conf/system/sysGlobals.xml must be modified with the relevant values.
	`<sysGlobalsDef>`
	`<threadCount>5</threadCount>`
	`<logLevel>INFO</logLevel>`
	`<maxAllowedLoginAttempts>0</maxAllowedLoginAttempts>`
	`<loginLockoutDelayTime>10</loginLockoutDelayTime>`
	`<enforceMinPasswordLength>false</enforceMinPasswordLength>`
	`<minPasswordLength>8</minPasswordLength>`
	`<name>sysGlobals</name>`
	`<verStamp>1</verStamp>`
	`</sysGlobalsDef>`

	Adds ability to control a minimum password length when an Admin user is created or updated through the SEAS user admin screen. One field has been added to the sysGlobals.xml file in the [SEAS_INSTALL]/conf/system directory: • `enforceMinPasswordLength` This parameter must be set to the value of `true` to enable minimum password length.
Version 2.4.1	Adds support for FIPS-mode sessions.
	Adds 64-bit JRE support for AIX 6.1 and AIX 7.1, zLinux, Red Hat 6, and SuSE 11.
Version 2.4	Adds 64-bit JRE support for Red Hat 5, AIX 5.3, Solaris 10, SuSE SLES 10, HP-UX 11.23 (PA-RISC), and Microsoft Windows Server 2008 R2.

Version	Feature or Enhancement
Version 2.3	Adds single-sign on (SSO) support for the SFTP, FTP, and IBM Sterling Connect:Direct® protocols.
	Allows trading partners to manage their passwords with a self-service mechanism. This change password functionality supports the recommended IBM Sterling Secure Proxy, Sterling External Authentication Server, and SSO configuration and does not use a third party external portal to manage passwords.
	Provides support for the RSA SecurID token.
	Improved startup supports the ability to run Sterling External Authentication Server as a background process without requiring that the passphrase be saved to disk.
	The `stopSeas` script provides another secure shutdown method for the Sterling External Authentication Server.

Support Requests Resolved for This Release

No support requests are resolved for Sterling External Authentication Server since the last cumulative fix release.

Special Considerations

Refer to the following notes before installing the product.

Configuration Considerations

Consider the following when configuring Sterling External Authentication Server:

- The System Settings dialog box allows you to configure the listeners, SSL keystore, and trusted certificates and uses a separate object for each tab. When you click **OK**, the objects are updated in the following order: Listeners, SSL Keystore, and Trusted Certificates.
- The product uses strong, but limited, cryptography. To use stronger encryption, replace the default jurisdiction policy files with the Unlimited Strength Jurisdiction Policy Files 6.0, available from the JCE provider. See Jurisdiction Policy File Use for more information.

Jurisdiction Policy File Use

TLS and SSL protocols are implemented, both server and GUI components, using the standard Java 6.0 API, Java Secure Socket Extension (JSSE) and default provider package. JSSE, in turn, utilizes the standard Java 6.0 API, Java Cryptography Extension (JCE) to implement the underlying crypto algorithms.

The cipher suites available for use in SSL and TLS connections are determined by the following JCE jurisdiction policy files:

- *install_dir*/jre/lib/security/local_policy.jar
- *install_dir*/jre/lib/security/US_export_policy.jar

where *install_dir* is the location of the installation.

The jurisdiction policy files shipped with Sterling External Authentication Server enable strong, but limited, cryptography. If you need to use stronger encryption,

US customers and those in other eligible countries can replace the default jurisdiction policy files with the Unlimited Strength Jurisdiction Policy Files 6.0, available from the JCE provider.

To replace the default jurisdiction policy files:

1. Go to the main Security page for IBM's Java 6 at http://www.ibm.com/developerworks/java/jdk/security/60.
2. Scroll down the page and click the IBM SDK Policy files link.
3. Provide your IBM ID.
4. Copy the unlimited strength jurisdiction policy files to the following locations:
   - *install_dir*/jre/lib/security/local_policy.jar
   - *install_dir*/jre/lib/security/US_export_policy.jar

   where *install_dir* is the location of the product

Following are the cipher suites available for use by default and by the unlimited jurisdiction policy files:

Default SSL/TLS Cipher Suites	**Cipher Suites Available with Unlimited Strength Jurisdiction Policy Files**
	TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA	TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA	TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5	TLS_RSA_WITH_RC4_128_MD5
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA	TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA	TLS_RSA_WITH_DES_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5	TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_NULL_SHA	TLS_RSA_WITH_NULL_SHA
TLS_RSA_WITH_NULL_MD5	TLS_RSA_WITH_NULL_MD5

Known Restrictions

Sterling External Authentication Server has the following known restrictions:

- On an AIX computer, the AES128 and AES256 ciphers do not work with the SSL protocol. To enable these ciphers, use the TLS protocol.
- When you install two NIC cards for a remote perimeter server and the network interface uses different IP addresses for the cards, make sure the definition for the associated Sterling Secure Proxy engine matches what was defined when the perimeter server is installed.

  When configuring client software, use the correct IP address based on the definition for the external network interface.
- Be careful when using host name in the external network interface. Make sure it does not identify the IP address specified during the network interface configuration. If it does, use the IP address only.

- Do not run the cryptotool.sh on UNIX or the cryptotool.cmd on Microsoft Windows unless instructed to do so by IBM support.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be

incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2014. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2014.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise®, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce®, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

Printed in USA