PN 00926

Sterling Commerce
Product Documentation

Sterling External Authentication Server Version 2.2.00

Release Notes

Sterling Commerce
An IBM Company

Sterling External Authentication Server Version 2.2.00 Release Notes

Second Edition

(c) Copyright 2001-2009. Sterling Commerce, Inc. All rights reserved. Additional copyright information is located at the end of this document.

STERLING COMMERCE SOFTWARE

*****TRADE SECRET NOTICE*****

THE STERLING EXTERNAL AUTHENTICATION SERVER SOFTWARE ("STERLING COMMERCE SOFTWARE") IS THE CONFIDENTIAL AND TRADE SECRET PROPERTY OF STERLING COMMERCE, INC., ITS AFFILIATED COMPANIES OR ITS OR THEIR LICENSORS, AND IS PROVIDED UNDER THE TERMS OF A LICENSE AGREEMENT. NO DUPLICATION OR DISCLOSURE WITHOUT PRIOR WRITTEN PERMISSION. RESTRICTED RIGHTS.

This documentation, the Sterling Commerce Software it describes, and the information and know-how they contain constitute the proprietary, confidential and valuable trade secret information of Sterling Commerce, Inc., its affiliated companies or its or their licensors, and may not be used for any unauthorized purpose, or disclosed to others without the prior written permission of the applicable Sterling Commerce entity. This documentation and the Sterling Commerce Software that it describes have been provided pursuant to a license agreement that contains prohibitions against and/or restrictions on their copying, modification and use. Duplication, in whole or in part, if and when permitted, shall bear this notice and the Sterling Commerce, Inc. copyright notice. As and when provided to any governmental entity, government contractor or subcontractor subject to the FARs, this documentation is provided with RESTRICTED RIGHTS under Title 48 52.227-19. Further, as and when provided to any governmental entity, government contractor or subcontractor subject to DFARs, this documentation and the Sterling Commerce Software it describes are provided pursuant to the customary Sterling Commerce license, as described in Title 48 CFR 227-7202 with respect to commercial software and commercial software documentation.

These terms of use shall be governed by the laws of the State of Ohio, USA, without regard to its conflict of laws provisions. If you are accessing the Sterling Commerce Software under an executed agreement, then nothing in these terms and conditions supersedes or modifies the executed agreement.

Where any of the Sterling Commerce Software or Third Party Software is used, duplicated or disclosed by or to the United States government or a government contractor or subcontractor, it is provided with RESTRICTED RIGHTS as defined in Title 48 CFR 52.227-19 and is subject to the following: Title 48 CFR 2.101, 52.227-19, 227.7201 through 227.7202-4, FAR 52.227-14, and FAR 52.227-19(c)(1-2) and (6/87), and where applicable, the customary Sterling Commerce license, as described in Title 48 CFR 227-7202 with respect to commercial software and commercial software documentation including DFAR 252.227-7013, DFAR 252,227-7014, DFAR 252.227-7015 and DFAR 252.227-7018, all as applicable.

The Sterling Commerce Software and the related documentation are licensed either "AS IS" or with a limited warranty, as described in the Sterling Commerce license agreement. Other than any limited warranties provided, NO OTHER WARRANTY IS EXPRESSED AND NONE SHALL BE IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR USE OR FOR A PARTICULAR PURPOSE. The applicable Sterling Commerce entity reserves the right to revise this publication from time to time and to make changes in the content hereof without the obligation to notify any person or entity of such revisions or changes.

Connect:Direct is a registered trademark of Sterling Commerce. Connect:Enterprise is a registered trademark of Sterling Commerce, U.S. Patent Number 5,734,820. All Third Party Software names are trademarks or registered trademarks of their respective companies. All other brand or product names are trademarks or registered trademarks of their respective companies.

Sterling Commerce, Inc.

4600 Lakehurst Court Dublin, OH 43016-2000 * 614/793-7000

Contents

Sterling External Authentication Server Version 2.2.00 Release Notes

The *Sterling External Authentication Server Version 2.2.00 Release Notes* document supplements Sterling External Authentication Server version 2.2 documentation. Release notes are updated with each release of the product and contain last-minute changes and product requirements, as well as other information pertinent to installing and implementing Sterling External Authentication Server. Read the document in its entirety before installation.

The Sterling External Authentication Server package consists of the distribution media and product publications. The Sterling External Authentication Server application is distributed as follows:

- File downloaded from the Sterling Commerce Electronic Software Distribution Portal

  See *Installing Sterling External Authentication Server from the ESD Portal* on page 15 for instructions.
- Distribution media, as appropriate for your product, where Sterling Commerce ships the physical distribution media.

Requirements

Your use of Sterling External Authentication Server version version 2.2.00 has the following requirements.

Hardware and Software

Sterling External Authentication Server requires the following hardware and software:

Component or Functionality	Hardware	Software	RAM	Disk Space
Sterling External Authentication Server	Windows compatible systems	Windows operating system options: ◆ Microsoft Windows XP ◆ Microsoft Windows 2003 Server	512 MB	200 MB
	HP 9000 Platform	HP-UX versions 11.11 and 11.23	512 MB	200 MB
	IBM RISC System/6000 platform	AIX version 5.3	512 MB	200 MB
	SUN SPARC systems	Solaris versions 9 and 10	512 MB	200 MB
	Intel Pentium system	Red Hat Advanced Server versions 4.0 and 5.0 SuSE SLES versions 9 and 10 Solaris versions 9 and 10	512 MB	200 MB
		Open LDAP versions 2.2 and 2.3 Sun Microsystems SunONE 5.2 IBM Tivoli 5.2 with Fixpack 3 Microsoft Windows 2003 Domain Functional Level Active Directory		
Sterling External Authentication Server GUI		Use one of the following: ◆ Internet browser for accessing the GUI using Java WebStart ◆ Java Runtime Environment version 1.5, 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 ◆ Java Runtime Environment version 1.4.2, used with authentication definitions created for Tivoli Access Manager. **Note:** See *Prerequisites for Authentication with Tivoli Access Manager (TAM) Using JRE Version 1.4.2* on page 7 for more information.	30 MB per TAM authentication definition	

License Key File

No license key file is required for Sterling External Authentication Server.

Customer Center Portal User Name and Password

The new Customer Center portal offers you a single location to administer everything associated with your Sterling Commerce products and services. It provides access to online tools, on-demand applications, community forums, product information, industry news, support updates, and support case management.

To log in to the Customer Center, go to http://customer.sterlingcommerce.com. If you do not have a Support On Demand user name and password, click the Join Now link and follow the instructions for new users. If you have a a Support on Demand account, define a new password the first time you log on.

Additional Requirements

Sterling External Authentication Server version 2.2.00 has the following additional requirements.

Prerequisites for Authentication with Tivoli Access Manager (TAM) Using JRE Version 1.4.2

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

To configure JRE for TAM, you must set the JAVA_HOME environment variable to point to the appropriate JRE and install the TAM API using the IBM wizard, 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, complete the following steps:

1. Install the 1.4.2 JRE on the target system, either as a system JRE or as a private JRE for a specific 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 Chapter 8 of the *IBM Tivoli Access Manager, Base Installation Guide, Version 5.1* for more information.

3. Run the java utility, com.tivoli.pd.jcfg.SvrSslCfg. IBM provides the com.tivoli.pd.jcfg.SvrSslCfg class that serves as a configuration utility. Running the utility creates a configuration file and generates an SSL key and other configuration data needed to communicate securely with the TAM servers. See *Configuring the TAM API* on page 8 for more information.
4. In Sterling External Authentication Server, create TAM authentication definitions (profiles) that reference the JRE installed in step 1 (**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 1.5, 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 specification of the target JRE that has been 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 Chapter 11, *Create Tivoli Access Manager Authentication Definitions*, in the *Sterling External Authentication Server Implementation Guide* for more information and instructions to create a TAM authentication definition.

Configuring the TAM API

The following example demonstrates how the IBM Java utility is used to configure the Sterling External Authentication Server into the TAM API. The configuration file created by this utility must be referenced when setting up a TAM authentication definition for use 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 preceding 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 list of parameters to review how the Java utility generates the SSL key and configuration file that enable using 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.

Parameter	Description
-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 EA.
-key_file	Specifies the java key store that is 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 version 2.2.00 has the following feature and enhancement:

Version	Feature or Enhancement
Version 2.2	Support for a single sign-on solution in Sterling Secure Proxy between a trading partner using the HTTP protocol and Sterling File Gateway connecting to the MyFileGateway application. Sterling External Authentication functions as the authentication token server for SSP.
Version 2.2, patch 1	A script can be used to stop the EA server. For UNIX installations, the script is stopSeas.sh. For Windows installations, the script is stopSeas.bat. The script is located in the *install_dir*/bin directory, where *install_dir* is the directory where EA is installed.

Obtaining Product Updates

Product updates and update summaries, including issues resolved for previous versions of Sterling External Authentication Server, are available on the Support On Demand Web site.

To obtain product updates:

1. Log on to your Customer Center Web site.
2. Follow the links to **Support on Demand**.
3. From the **Product Support** menu on the left navigation bar, click **Sterling** > **Product Updates & Downloads**.
4. Follow the links for your product until you locate the updates for your product and platform.

Description of Support Requests Resolved for This Release

The following table describes the Support Requests (SRs) resolved for Sterling External Authentication Server version 2.2.00 since the last cumulative fix release. For the history of issues resolved prior to this release, navigate to the Product Updates & Downloads site for your product and platform using the instructions in *Obtaining Product Updates* on page 6 and review the Fix List.

SR Number	Description
1372223	Authentication fails after maintenance update 2 for version 2.0.01 is applied.
1372446	For each transfer, a socket closure generates the message "Possible truncation attack?".
1372714	A “browse for exit button” error is generated when EA is started from the Web browser.

Special Considerations

This section contains considerations in addition to the procedures contained in this document and the other Sterling External Authentication Server documents. Refer to the following notes before installing the product.

Single Sign-On Consideration

Sterling External Authentication supports a single sign-on connection between a trading partner and a Sterling File Gateway server (SFG), using Sterling Secure Proxy (SSP). The single sign-on connection uses tokens to authenticate the connection between SSP and SFG. Sterling External Authentication manages the tokens.

For instructions on how to configure a single sign-on connection, including how to customize the Sterling External Authentication Server token configuration, refer to *Configure an HTTP Connection Between SFG and SSP To Enable Single Sign-On for a Trading Partner* in the Sterling Secure Proxy documentation set.

The EA help does not document the procedures and fields used for single sign-on.

Configuration Considerations

Refer to the following notes when configuring EA:

- The System Settings dialog box, which allows you to configure the listeners, SSL keystore, and trusted certificates, 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.

- Sterling External Authentication Server uses strong, but limited, cryptography. If you want to use stronger encryption, replace the default jurisdiction policy files with the Unlimited Strength Jurisdiction Policy Files 5.0, available from the JCE provider. See *Jurisdiction Policy File Use* on page 11 for more information and instructions.
- SuSE Linux Enterprise Server 10 has problems with the installation program. When you install Sterling External Authentication Server on this platform, you may receive the following error:

```
Configuring the installer for this system's environment...
awk: error while loading shared libraries: libdl.so.2: cannot open shared object
file: No such file or directory
:
(more error messages)
```

  If you encounter this error, type the following information to patch the installer:

```
cat SEAS.Lin.V2001.bin | sed "s/export LD_ASSUME_KERNEL/#xport LD_ASSUME_KERNEL/"
> SEAS.SLES10.V2001.bin
chmod +x SEAS.SLES10.V2001.bin
./SEAS.SLES10.V2001.bin -i console
```

- The uninstall program does not work on the SuSE Linux Enterprise Server 10 platform.

Jurisdiction Policy File Use

TLS and SSL protocols are implemented in the Sterling External Authentication Server, both server and GUI components, using the standard Java™ 5.0 API, Java™ Secure Socket Extension (JSSE) and default provider package. JSSE, in turn, utilizes the standard Java™ 5.0 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 shipped with Sterling External Authentication Server:

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

where *install_dir* is the directory where Sterling External Authentication Server is installed.

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 5.0, available from the JCE provider.

To replace the default jurisdiction policy files:

1. Access the Sun Web site and select **Java 2 Standard Edition** from the **Download** menu.
2. Scroll to **Other Downloads** and click the link for Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0.
3. Click **Download**.

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 Sterling External Authentication Server installation directory

The cipher suites enabled by default and by the unlimited jurisdiction policy files are displayed in the following table:

Default SSL/TLS Cipher Suites	Cipher Suites Enabled by Unlimited Strength Jurisdiction Policy Files
SSL_RSA_WITH_RC4_128_MD5 SSL_RSA_WITH_RC4_128_SHA	SSL_RSA_WITH_RC4_128_MD5 SSL_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA SSL_ RSA_WITH_DES_CBC_SHA	TLS_DHE_DSS_WITH_AES_128_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA SSL_ DHE_DES_WITH_DES_CBC_SHA	TLS_DHE_DSS_WITH_AES_256_CBC_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA SSL_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	SSL_DHE_RSA_WITH_DES_CBC_SHA SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA SSL_RSA_WITH_NULL_MD5	SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_NULL_SHA SSL_DH_anon_WITH_RC4_128_MD5	SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA	SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_ SHA SSL_RSA_WITH_NULL_MD5
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA SSL_DH_anon_WITH_DES_CBC_SHA	SSL_RSA_WITH_NULL_SHA SSL_DH_anon_WITH_RC4_128_MD5
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	TLS_DH_anon_WITH_AES_128_CBC_SHA TLS_DH_anon_WITH_AES_256_CBC_SHA
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA TLS_KRB5_WITH_RC4_128_SHA	SSL_DH_anon_WITH_3DES_EDE_CBC_SHA SSL_DH_anon_WITH_DES_CBC_SHA
TLS_KRB5_WITH_RC4_128_MD5 TLS_KRB5_WITH_3DES_EDE_CBC_SHA	SSL_DH_anon_EXPORT_WITH_RC4_40_MD5

Default SSL/TLS Cipher Suites	Cipher Suites Enabled by Unlimited Strength Jurisdiction Policy Files
TLS_KRB5_WITH_3DES_EDE_CBC_MD5 TLS_KRB5_WITH_DES_CBC_SHA	SSL_DH_anon_EXPORT_WITH_DES40_CBC_ SHA TLS_KRB5_WITH_RC4_128_SHA
TLS_KRB5_WITH_DES_CBC_MD5 TLS_KRB5_EXPORT_WITH_RC4_40_SHA	TLS_KRB5_WITH_RC4_128_MD5 TLS_KRB5_WITH_3DES_EDE_CBC_SHA
TLS_KRB5_EXPORT_WITH_RC4_40_MD5	TLS_KRB5_WITH_3DES_EDE_CBC_MD5 TLS_KRB5_WITH_DES_CBC_SHA
TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA	TLS_KRB5_WITH_DES_CBC_MD5 TLS_KRB5_EXPORT_WITH_RC4_40_SHA
TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5	TLS_KRB5_EXPORT_WITH_RC4_40_MD5
	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA
	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5

Known Restrictions

Sterling External Authentication Server version 2.2.00 has the following known restriction:

- On an AIX computer, the AES128 and AES256 ciphers do not work with the SSL protocol. To enable these ciphers, use the TLS protocol.

Installation Notes

Before you install Sterling External Authentication Server, read all the information in this section and follow the guidelines.

- Review *Sterling External Authentication Server Version 2.2.00 Release Notes* for last-minute product information and pre-installation tasks.
- Print and review *Sterling External Authentication Server Implementation Guide* from the DVD or ESD download file.
- Complete any worksheets prior to installing Sterling External Authentication Server.
- Review your security configuration to ensure compatibility with Sterling External Authentication Server before proceeding with the installation. Refer to the Sterling External Authentication Server Implementation Guide for security options.
- Verify that you have the current updates for Sterling External Authentication Server. Access current update information, including instructions for applying updates containing product fixes and enhancements, from the Customer Center Web site at http://customer.sterlingcommerce.com. See *Obtaining Product Updates* on page 9 for instructions.

Upgrading to Sterling External Authentication Server Version 2.2.00 Patch 1

You can upgrade to this version by installing over the existing files. After you upgrade, the configurations from the previous version are maintained in the *install_dir*/conf directory.

If you are upgrading from an existing version of the Sterling External Authentication Server application, use the following procedure:

1. Shut down any instance of Sterling External Authentication Server that is running and confirm that no application is accessing any EA files. You cannot upgrade the software if EA application files are in use.
2. Make a complete backup of your existing Sterling External Authentication Server installation.
3. Install Sterling External Authentication Server using instructions in *Sterling External Authentication Server Implementation Guide*.
4. If you are installing on a UNIX system:
    a. When prompted, specify the directory where the previous version is installed and press **Enter**. A prompt displays the directory and a message indicating that the Sterling External Authentication Server installation already exists.
    b. Type **C** to continue.
    c. Review the pre-installation summary, and press **Enter**.
    d. Press **Enter**. The command prompt is displayed.
5. If you are installing on a Windows system:
    a. When prompted, specify the directory where the previous version is installed and press **Next**. A prompt displays the directory and a message indicating that the Sterling External Authentication Server installation already exists.
    b. Press **Next** to continue.
    c. Review the pre-installation summary. Click **Install**.
    d. At the Installation complete screen, click **Done**.

Installing Sterling External Authentication Server from the ESD Portal

These instructions contain procedures for downloading and installing the Sterling External Authentication Server version 2.2.00 release, including documentation. The exact name of the file you download from the Sterling Commerce Electronic Software Distribution (ESD) Portal depends on your operating system and platform. In the download instructions, the term ESD file refers to one of the following files:

Operating System	Platform	ESD Product Download File Name
UNIX	AIX	SEAS.V22.AIX.tar
	HP-UX	SEAS.V22.HP.tar
	Solaris SPARC	SEAS.V22.Solaris.tar
	Solaris Intel	SEAS.V22.SolarisIntel.tar
	Linux Intel	SEAS.V22.Linux.tar
Windows	Windows	SEAS.V22.Windows.zip

Downloading Product Files

These instructions assume that you download the ESD file to a computer running Windows and transfer it to the another computer, unless Windows is the target system.

To download the ESD file:

1. Log in to the ESD Portal using the instructions in *Access the ESD Portal* in your Order Confirmation e-mail from Sterling Commerce. The Download Area is displayed.
2. Find Sterling External Authentication Server version 2.2.00 for your platform and click **Download**.
3. In the **File Download** dialog box, click **Save**.
4. When the **Save As** dialog box opens, specify the location to save the file, or save the file to your desktop.

> **Note:** If Internet Explorer adds a number in brackets to the name of the downloaded file (for example, SEAS.V22.AIX[1].tar), rename the file on the Windows system before you transfer it in binary mode to the system where it will be installed.

5. Make a backup of the file and store it in a safe place to use in case of disaster recovery, hardware failure, or to reinstall the software.

6. If Windows is not the target system, transfer the file to the system where you will install it.

Caution:	Upload the ESD file to the target system in **binary** mode.

Installing the Application

To install Sterling External Authentication Server:

1. Review *Sterling External Authentication Server Version 2.2.00 Release Notes* for last-minute product information and installation requirements.
2. Follow the instructions for your platform in Chapter 2 of *Sterling External Authentication Server Implementation Guide* to install Sterling External Authentication Server.

Documentation Updates

The *Sterling External Authentication Server version 2.2 Implementation Guide* has the following last-minute updates:

Chapter 2, Install and Start EA on UNIX

On page 23, replace the procedure called *Start the EA Server on UNIX* with the following:

Start the EA Server on UNIX

When you install the EA server, you define a passphrase. It is required to start the server. You can use the default installation and start the EA server with the encrypted passphrase stored on the server or you can modify the startup to require that the user type a passphrase at startup.

Storing the passphrase eliminates the need to supply it at startup. Determine which method to use and complete the procedure for the method you select.

Start the EA Server on UNIX Using a Stored and Encrypted Passphrase

To start the EA server using the stored passphrase:

1. Navigate to *install_dir*/bin, where *install_dir* is the directory where EA is installed and type the following command:

```
./runSeas.sh
```

2. Confirm that the following messages are displayed when the server starts:

```
Starting External Authentication Server as a background process...
Program output will be redirected to runServer.out.
```

3. To determine if the server startup was successful, view the runServer.out file in the *install_dir*/bin directory. After a successful startup, a message is written to the file indicating the server is ready for service.

Start the EA Server on UNIX and Require a Passphrase

To start EA and require that the passphrase be provided:

1. Delete the sb.enc file from the *install_dir*/conf/system directory, where *install_dir* is the directory where EA is installed.
2. Navigate to the install_dir/bin directory and type the following command:

```
./runSeas.sh
```

3. You are prompted to enter a passphrase. Type the passphrase defined for EA and press **Enter**.
4. Confirm that the following messages are displayed when the server starts:

```
Starting External Authentication Server as a background process...
Program output will be redirected to runServer.out.
```

5. To determine if the server startup was successful, view the runServer.out file in the *install_dir*/bin directory. After a successful startup, a message is written to the file indicating the server is ready for service.

Chapter 2, Install and Start EA on UNIX

On page 26, replace the procedure called *Shut Down EA on UNIX* with the following:

Shut Down EA on UNIX

If you close the EA GUI, the EA server continues to run. This allows the EA Server to accept client connections. You can shut down the server using the GUI or a script.

If you want to shut down the server using the GUI, complete the following procedure:

1. From the **File** menu, select **Shutdown Server**.
2. Type the passphrase created at installation and click **OK** to close the GUI.

If you want to shut down the server using the using the stopSeas.sh script, close all open EA GUI windows and complete the following procedure:

1. Navigate to the *install_dir*/bin directory, where *install_dir* is the directory where EA is installed.
2. Type the following command:

```
./stopSeas.sh
```

3. At the prompt, type the passphrase defined at installation and press **Enter**.
4. At the administrator user ID prompt, type the administrator user ID and press **Enter**. The default administrator user ID is admin.
5. At the administrator password prompt, type the administrator password and press **Enter**. The default administrator password is admin.

Chapter 3, Install and Start EA on Windows

On page 29, replace the procedure called *Start the EA Server on Windows* with the following:

Start the EA Server on Windows

When you install the EA server, you define a passphrase. The passphrase is required to start the server. You can use the default configuration and start the EA server with the encrypted passphrase that is stored on the server or you can require that a passphrase be typed at startup.

Storing the passphrase eliminates the need to supply it at startup. Determine which method to use and complete the procedure for the method you select.

Start the EA Server on Windows Using a Stored Passphrase

To start EA with the stored passphrase, you must start EA as a Windows service.

1. Start **Administrative Tools** from **Control Panel**.
2. Double-click **Services**.
3. Double-click the **Sterling External Authentication Server v2.2** entry.
4. To configure the service to start automatically, set **Startup type** to **Automatic**.
5. Under **Service status**, click **Start**.

Start the EA Server on Windows And Require a Passphrase

To start EA and require that the passphrase be provided:

1. Delete the sb.enc file from the *install_dir*\conf\system directory, where *install_dir* is the directory used to install EA.
2. From a Windows command prompt, navigate to the *install_dir*\bin directory and type the following command:

```
runSeas.bat
```

3. You are prompted to enter a passphrase. Type the passphrase defined for EA and press **Enter**.
4. Confirm that the following messages are displayed when the server starts:

```
Sterling External Authentication Server Starting...
Waiting for bootstrap data...
Sterling External Authentication Server is ready for Service.
```

Chapter 3, Install and Start EA on Windows

On page 32, replace the procedure called *Shut Down EA on Windows* with the following:

Shut Down EA on Windows

If you close the EA GUI, the EA server continues to run. Keep the EA server open when client applications need to connect. You can shut down the server using the GUI or a script.

If you want to shut down the server using the GUI, complete the following procedure:

1. From the **File** menu, select **Shutdown Server**.
2. Type the passphrase created at installation and click **OK** to close the GUI.

If you want to shut down the server using the using the stopSeas.bat script, close all open EA GUI windows and complete the following procedure:

1. Navigate to the *install_dir*\bin directory, where *install_dir* is the directory where EA is installed.
2. Type the following command:

```
stopSeas.bat
```

3. At the prompt, type the passphrase defined at installation and press **Enter**.
4. At the administrator user ID prompt, type the administrator user ID and press **Enter**. The default administrator user ID is admin.
5. At the administrator password prompt, type the administrator password and press **Enter**. The default administrator password is admin.

Chapter 4, Configure System Resources

On page 38, modify the procedure called *Set Listener Connection Settings (Backlog and Timeout)* and add the following field to step 3:

- Session Idle Timeout

Add the following field definition to the table to define the Session Idle Timeout field:

Name	Description
Session Idle Timeout	Limits the amount of time that a client can stay connected to an EA server without any activity. When the time expires with no activity from the client to the EA server, the server closes the connection. Default is 10. To disable the timeout, set the value to 0.

Sterling External Authentication Server Documentation

The Sterling External Authentication Server documentation is available on the product media. You can view or download documentation from the Customer Center Web site at http://customer.sterlingcommerce.com. You need a Support Customer Center user name and password. See *Customer Center Portal User Name and Password* on page 7 for instructions on obtaining your user name and password.

Access to PDF files requires the latest version of Adobe Acrobat Reader, which you can download at www.adobe.com. You can search for a specific word or phrase in the text of an open Adobe PDF document or a set of PDF documents in a specified location. See the Adobe Reader Help for instructions on using the Search feature. The search lists all instances of the specified string.

The Sterling External Authentication Server documentation consists of:

- Sterling External Authentication Server Help
- *Sterling External Authentication Server Implementation Guide*
- *Sterling External Authentication Server Version 2.2.00 Release Notes*