Setup Checklist - UNIX or Linux Preinstallation (Non-Cluster)

This document contains information to assist you when planning to install Sterling Integrator in a UNIX or Linux non-clustered environment.

When creating a name, such as an account name, permissions name, profile name, or database name, follow these conventions:

✦ Use any valid alphanumeric characters and _ (underscore).

✦ Do not use spaces or apostrophes.

You may want to make a copy of the following checklist and use it to record the information you collect:

Step	Description	Your Notes
1	Verify that your system meets the hardware and software requirements specified for this release. For more information, refer to *Checking System Requirements* on page 7.	
2	Verify that your system has the patches required by Java™ for the operating system. For HP, you must run the HP JConfig utility to obtain the required patches and kernel modifications.	
3	If you are using the GUI installation method, set up your X Windows-compatible software. The installation procedure for this software will depend on the tool that you use.	
4	For systems with multiple IP addresses, verify that the IP address on which the Sterling Integrator resides is accessible by any client computer that is running a browser interface. For all Linux operating systems only, ensure that /etc/hosts has short-names first for all entries. For example, 127.0.0.1localhostlocalhost.localdomain **Note:** You must create your own domain name. Do not use the example. **Caution**: If you do not verify the IP addresses, your system may not operate properly after installing Sterling Integrator.	
5	Verify that all client computers are using Microsoft Internet Explorer 6.x or later.	
6	If you are using a non-English environment, confirm that you are using the appropriate character set.	

Step	Description	Your Notes
7	Determine and record information about the JDK. ◆ Version of the JDK ◆ Absolute path to the JDK files and patches For more information, refer to *Installing the Java Software Development Kit* on page 7.	
8	Decide which of the following security certificates you will use: ◆ The default self-signed SSL (Secure Sockets Layer) certificate that is automatically installed. ◆ A Certificate Authority-related certificate that you install before installing Sterling Integrator. For more information, refer to *Security Certificates* on page 7.	
9	Obtain the unlimited strength JCE distribution file. For more information, refer to *Downloading the JCE Distribution File* on page 8.	
10	Determine and record the initial port number to be used by the Sterling Integrator. For more information, refer to *Determining Port Numbers* on page 8.	
11	Verity that a UNIX user account exists on the host server for each installation of the Sterling Integrator. For more information, refer to *Creating a UNIX Account* on page 9.	
12	Set Umask to 002.	
13	Determine and record information to set up default system alerts from the Sterling Integrator: ◆ The Administrative e-mail address to which system alert messages are sent. ◆ The SMTP Server IP address used for sending alert messages.	

Step	Description	Your Notes
14	Determine and record the directory in which you plan to install the Sterling Integrator. For all installation methods (GUI, text-based, manually edited silent install file), you must install into a new directory to be created by the installation process. The installation process will fail if a pre-existing directory is specified. Keep the following in mind when selecting a directory: ◆ The file system must have adequate free disk space. ◆ The name of the directory is case sensitive. The installation process creates the directory and beneath it, a directory called "install". Subdirectories like the bin and properties directories are directly beneath the install directory.	
15	Determine and record the passphrase you want to use for the Sterling Integrator system. During installation, you are prompted twice to type the passphrase, which is not displayed when you type it.	
16	Obtain the license file and record the absolute path and file name to the license file. Be sure that the path name and the file name consist of alphanumeric, ".", "_" and "-" characters. For more information, refer to *Obtaining a License File* on page 10.	
17	If you are manually editing your silent installation, create your file. For more information, refer to *Silent Installations* on page 11.	

Note: The next step is only for Sterling Integrator systems that use the HP-UX operating system.

Step	Description	Your Notes

18	For the HP-UX operating system, establish these settings:
	
	◆ Verify kernel parameters and establish the following minimum settings by running `kctune` command:
	
	`kctune max_thread_proc 1024`
	`kctune maxdsiz 2147483648`
	`kctune maxdsiz_64bit 8589934592`
	`kctune maxssiz 369098752`
	`kctune maxssiz_64bit 536870912`
	
	◆ Run `ulimit` utility, verify, and establish the following minimum settings:
	ulimit -d = 2097152 (in kilobytes) or higher
	ulimit -s = 360448 (in kilobytes) or higher	

Step	Description	Your Notes

Note: The next two steps are only for Sterling Integrator systems that use the AIX operating system.

| 19 | During the installation process, you specify the name of the directory to be created for the Sterling Integrator. The installation process creates the directory and beneath it, a directory called "install". | |

To ensure that /*install_dir*/install has the necessary permissions, AIX users must run the following command on the parent directory of /*install_dir*/install before installation:

```
chmod -R a-s <absolute
path>/install_dir_parent
```

where *install_dir_parent* is the directory in which /*install_dir*/install will be created.

For example, to specify

```
AIX_1/applications/test1/my_install
```
as your installation directory, you could run the command from the AIX_1/applications directory (directly above the test1 directory):

```
chmod -R a-s test1
```

or from another location on the file system:

```
chmod -R a-s
/AIX_1/applications/test1
```

This ensures that when the *my_install* directory is created during installation, it inherits the correct permissions from test1.

| 20 | The `ncargs` value specifies the maximum allowable size of the ARG/ENV list (in 4K byte blocks) when running exec() subroutines. Set `ncargs` value to 16 or higher. | |

Run the following commands to display and change the `ncargs` value.

- To display the current value of ncargs:

```
lsattr -El sys0 -a ncargs
```

- To change the current value of ncargs:

```
chdev -l sys0 -a ncargs=NewValue
```

Note: The `lsattr` and `chdev` command options are `-El` (lowercase L) and `-l` (lowercase L) respectively.

Note: The next two steps are only for Sterling Integrator systems that use the Linux operating system.

| 21 | Set SELinux to disabled as shown next: | |

```
/etc/sysconfig/selinux:
SELINUX=disabled
```

Step	Description	Your Notes
22	Make the following system change:	

1 If the base locale for the system is English, edit the /etc/sysconfig/i18n file by changing the **LANG** variable from `en_US.utf8` to `en_US`.

   Save and close the /etc/sysconfig/i18n file.

2 Reboot the system.

Note: The next step is only for Sterling Integrator systems that use the RedHat Enterprise Linux operating system.

| 23 | For the RedHat Enterprise Linux operating system only, make the following system changes: | |

1 If the base locale for the system is English, edit the /etc/sysconfig/i18n file by changing the **SUPPORTED** variable from `en_US.utf8` to `en_US`. You can also allow multiple support using the following format:

   `en_US.utf8:en_US`

   Save and close the /etc/sysconfig/i18n file.

2 Edit the /etc/security/limits.conf file by adding the following lines:

```
* hard    nofile   16384  (maximum value)
* soft    nofile   4096   (minimum value)
* hard    memlock 3000000
* soft    memlock 3000000
* hard    nproc    16000
* soft    nproc    16000
* hard    stack    512000
* soft    stack    512000
```

   This updates the system ulimits.

   Save and close the /etc/security/limits.conf file.

3 Reboot the system.

Note: The next step is only for Sterling Integrator systems that use the Solaris operating system.

Step	Description	Your Notes

24	For the Solaris operating system only, set the following entries in the /etc/security/limits file:
	
	`nofiles = 4096`
	
	`set rlim_fd_max=4096` (limit is 65535) - hard limit
	
	`set rlim_fd_cur=4096` - soft limit
	
	◆ To make the setting effective as the hard limit, reboot the server or run the following command:
	
	`kill -1 inetd`
	
	◆ To make the setting effective as the soft limit, use the parent shell configuration (for example, .profile). Then, reboot the server.	

Note: The next two steps are only for Sterling Integrator systems that use the Oracle, Microsoft SQL Server 2005, or DB2 database.

Step	Description	Your Notes
25	If you are using an Oracle, Microsoft SQL Server 2005, or DB2 database, determine and record information about your database server. Be aware that this information is case sensitive. ◆ Database user name and associated password ◆ Database (catalog) name ◆ Database host name ◆ Database host port number ◆ (Oracle and Microsoft SQL Server 2005 only) Absolute path and file name for one JDBC driver ◆ (DB2 only) Absolute paths and file names for two JDBC drivers For more information about encrypting and decrypting passwords, refer to: ◆ *Encrypting Database Passwords* on page 9 ◆ *Decrypting Database Passwords* on page 9 **Note:** If you are using an Oracle 10.2.x database, you must set it up for native compilation by allocating space and by setting the plsql_native_library_dir parameter.	
26	If you are using an Oracle, SQL Server 2005, or DB2 database, decide if you are going to manually or automatically apply database definition language (DDL) statements (schema) to the database. For more information, refer to *Applying Database Definition Language (DDL) Statements* on page 10.	

Checking System Requirements

Before you begin, verify that your system meets the hardware and software requirements specified for this release of Sterling Integrator. The hardware requirements listed are the minimum required. Your system requirements will exceed these if you are running other applications on the same machine as the Sterling Integrator. For current information, see the most recent *System Requirements* for Sterling Integrator.

The installation strictly enforces the following system requirements:

✦ Operating system version (must match requirement exactly)

   The minimum patch level for the operating system is enforced, but you can apply higher patch levels.

✦ JDK version (must match requirement exactly)

✦ Disk space

   The disk space is a minimum for the installation. The system should be separately sized to handle whatever load is going to be put on the system.

✦ Database.

✦ JDBC driver version (supports exact matches and wildcard matches).

If any of the above requirements are not met, the installation will fail and print/log a report of all items that were non-compliant. You then need to upgrade to a supported version.

Installing the Java Software Development Kit

You must install the Java Software Development Kit (JDK) and the patches specific to your system. Refer to the *System Requirements* for:

◆ JDK version and patch numbers

◆ JDK download procedure

After you install the JDK, write down the absolute path to its location on your system. You will use this path information during the installation.

Security Certificates

Before installing Sterling Integrator, you must decide which of the following security certificates you will use:

✦ The default self-signed SSL (Secure Sockets Layer) certificate that is automatically generated by the installation.

✦ A Certificate Authority-related certificate that you generate before installing Sterling Integrator.

If you install with the default SSL certificate, but you later want to switch to a CA-related certificate, you can make that change using the sslCert property in the noapp.properties.in file.

Downloading the JCE Distribution File

The Java Cryptography Extension (JCE) is a set of Java packages from Sun Microsystems, Inc. or IBM that provides a framework and implementations for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms. By default, Sterling Integrator uses the limited strength JCE file that is included in the JDK that you use during the installation. Installing unlimited strength JCE file will overwrite the limited strength JCE file.

Note: If you are installing Sterling Integrator outside of the United States, check to see if you can get the JCE unlimited strength jurisdiction policy files. The unlimited strength jurisdiction policy files can only be exported to countries to which the United States permits the export of higher-level encryption.

To obtain this file for the Sun JDK 1.5 (Solaris, Linux) and the HP-UX JDK 1.5 (HP-UX):

1. Open your browser and navigate to http://java.sun.com/javase/downloads/index_jdk5.jsp.

2. At the bottom of the page, locate the *Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0* item and click the **Download** button.

3. Download the jce_policy-1_5_0.zip file to your system.

4. Once the file resides on your system, note the exact directory and file name for this zipped file. You will need this information during the installation process.

To obtain this file for the IBM JDK 1.5 (AIX, Linux):

1. Open your browser and navigate to https://www14.software.ibm.com/webapp/iwm/web/reg/pick.do?source=jcesdk.

2. Enter your IBM ID and password. If you do not have an IBM ID, follow the IBM registration instructions provided on the Sign In page.

3. Click **Submit**.

4. Select *Unrestricted JCE Policy files for SDK 1.4.2* and click **Continue**.

   Note: The Unrestricted JCE Policy files for the 1.4.2 SDK are also used for the 1.5.0 SDK.

5. Review your personal information and the license agreement.

   Select **I agree** check box and click **I confirm** to continue.

6. Download the unrestrict142.zip file to your system.

7. Once the file resides on your system, note the exact directory and file name for this zipped file. You will need this information during the installation process.

Determining Port Numbers

During installation, you are prompted to specify the initial port number for the Sterling Integrator.

To specify an initial port number, follow these guidelines:

✦ The Sterling Integrator requires a range of 100 consecutive open ports between 1025 and 65535.

✦ The initial port number represents the beginning port number in the range.

✦ Make sure that port numbers in the port range are not used by any other applications on your system.

For the other ports after the initial port, you can accept the default port number suggested by the installation program, or you can individually re-assign pre-assigned default port numbers within the specified port range. During installation, about 50 default ports are pre-assigned for different services. For example, if you do not want xxx32 (10132) to be a default port, you could assign that port to xxx97 or another number within the port range.

After your installation, refer to the */install_dir*/install/properties/sandbox.cfg file for all of the port assignments.

Creating a UNIX Account

In a UNIX or Linux environment, create one UNIX administrative account on the host server for all installations of the Sterling Integrator. For example, if you want to create a test environment and a production environment, create one UNIX account on the host server. For more information about creating UNIX accounts, see your operating system documentation.

Encrypting Database Passwords

The Sterling Integrator uses a password to connect to the database being used. Currently, the password is stored as clear text in a property file on the system. If the security policies at your company require you to encrypt these passwords, you can do so after you complete the installation. Encrypting these passwords is optional.

To encrypt the database password used in UNIX, follow these steps:

1. Stop the Sterling Integrator.
2. Go to */install_dir*/install/bin.
3. Run the command `enccfgs.sh`.
4. Run the command `setupfiles.sh`.
5. Run the command `deployer.sh`.
6. Start the Sterling Integrator.
7. Enter your passphrase.

Decrypting Database Passwords

To decrypt the database password used in UNIX, follow these steps:

1. Stop the Sterling Integrator.
2. Go to */install_dir*/install/bin.
3. Run the command `decrypt_string.sh` *encrypted_password* (The encrypted password is from sandbox.cfg). You are prompted for the passphrase.
4. In the *install_dir*/install/properties/sandbox.cfg file, edit the DB_PASS property to replace the encrypted password with the password that was returned in Step 3.
5. Go to *install_dir*/install/bin.

6. Run `setupfiles.sh`.

7. Run `deployer.sh`.

8. Start the Sterling Integrator.

9. Enter your passphrase.

Applying Database Definition Language (DDL) Statements

When you install Sterling Integrator, you can manually apply database definition language (DDL) statements to your database tables instead of requiring the installation process to do it directly. This enables you to apply DDL statements for database creation separately from the installation. If you do not choose to manually apply the DDL, the installation will apply both the DDL and the resources.

This feature increases database security by reducing the database permissions of the Sterling Integrator database user. The rights to create tables, indexes, etc. can be reserved for a secure user like a customer database administrator (DBA). A business can require that only a DBA with the proper permissions can make database changes. Also, these database rights would not be affected by Sterling Integrator.

Directory Structure

With interactive installations, many of the directories that you use during the installation are located two levels below the installation directory (*install_dir*) that you specify during the installation. The intermediate directory is named "install" and is automatically created during the installation.

For example, a lot of commands are run from the bin directory, which is located at */install_dir*/install/bin. Make sure that you are in the correct directory when you run a command. If you are not sure, display the list of files in your active directory.

Obtaining a License File

After your company signed the sales contract with Sterling Commerce, Sterling Commerce creates a license file containing information about your company, your system, and the packages (components) that your company selected to use, such as services, maps, and adapters.

Your first license file is a temporary keyfile that is e-mailed to you after you purchase Sterling Integrator. It allows you to run Sterling Integrator and all of the licensed features for a limited period. Before the keyfile expires, you must replace the temporary key with a permanent key to continue running Sterling Integrator. Failure to either extend your temporary keyfile or replace it with a permanent keyfile will result in the keyfile expiry and Sterling Integrator will fail to start.

The permanent license keyfile contains your specific operating system and the IP address of your system, and is valid for 20 years from the date of issue. To extend your temporary key, obtain the permanent key, or request changes to a permanent key you already have, go to the online Gentran Integration Suite/Sterling Integrator Key Request form (https://support.sterlingcommerce.com/forms/gis_key_request.aspx)and have your PSP number (a unique number that identifies a licensed software asset in your Sterling Integrator installation) available. The PSP Number is present in the temporary or previous version of the keyfile you received from Sterling Commerce. Upon submission of this form, your new keyfile will be generated and delivered to you as an attachment to an email.

The Sterling Integrator permanent license file contains a single or multiple IP addresses in your computing environment. If you change an IP address in your computing environment that is present in your Sterling Integrator license file, Sterling Integrator will cease to operate. You should take necessary precautions to avoid this potential outage, including notifying the appropriate contacts within your organization (information technology and related departments) and include the license file updates in your computing environment change plans.

Installing the Temporary Key

To install the temporary key, do the following:

1. Rename the temporary key. Use a name (for example, **assetTracking.key**) that clearly identifies the key as the original installation license key.
2. Copy the temporary key to the *absolutePath*/conf directory.
3. Rename the temporary license key file to **license.key**.

Installing the Permanent Key

To install the permanent key from the command line, do the following:

1. When you receive the permanent license key file, make a copy of it, and keep the copy in a safe place.
2. Stop Sterling Integrator.
3. Copy your license file to the machine where Sterling Integrator is installed.
4. Navigate to the *install_dir*/bin directory and run the `./AddLicenseSet.sh <path>` command, where `<path>` is the path to the license keyfile, for example, `./AddLicenseSet.sh gis_license.xml`.
5. Start Sterling Integrator.

Note: You can also install or update your license file from the Licenses screen (**Operations** > **System** > **Licenses**) when Sterling Integrator is running.

Silent Installations

You can set up an installation of Sterling Integrator so that it runs with no user interaction. For these silent installations, you need to create the following items for your installation script:

✦ A text file with information that during an interactive installation you are prompted to enter. This information is then automatically accessed by the installation script.

Examples of silent installation text file entries:

```
APSERVER_PASS = (system passphrase)
INSTALL_DIR = (full path to the installation directory)
LICENSE_FILE_PATH = (full path to the license file)
PORT1 = (initial port)
JCE_DIST_FILE = (full path to the JCE distribution file)
SI_ADMIN_MAIL_ADDR = (email address for administrative contact)
SI_ADMIN_SMTP_HOST = (SMTP mail server host name)
DB_VENDOR = (database - [MySQL|MSSQL|MSSQL2005|Oracle|DB2])
ACCEPT_LICENSE = (license agreement acceptance - [yes/no])
```

Note: The following `DB_*` variables are not used for MySQL.

```
DB_USER = (database user ID)
DB_PASS = (database password)
DB_DATA = ('net service name' or 'database name')
DB_HOST = (database hostname or IP address)
DB_PORT = (database's listener port.)
DB_DRIVERS = (fully qualified path to the database driver)
DB_DRIVERS_VERSION = (version of database drivers)
```

✦ A reference in your installation script to this variable file.

Example:

```
install_dir/JDK/bin/java -jar GISxx.jar -f silent_install_file
```

IInstalling the JDBC Driver in SQL Server

Sterling Integrator requires the correct Microsoft SQL Server driver. See *System Requirements* for supported version information. The supported version of the JDBC driver builds the correct Sterling Integrator directory structure.

Installing the JDBC Driver in SQL Server 2005

Go to the Microsoft web site to download the driver and any appropriate patches.

1. Download sqljdbc_*version_language*.tar.gz to a temporary directory.

2. To unpack the zipped tar file, navigate to the directory where you want the driver unpacked and type the following command:

```
gzip -d sqljdbc_version_language.tar.gz
```

3. To unpack the tar file, move to the directory where you want the driver installed and type the following command:

```
tar -xf sqljdbc_version_language.tar
```

After the package unpacks, you can find out more information about using this driver by opening the JDBC Help System in the */absolutePath*/sqljdbc_*version*/*language*/help/default.htm file. This will display the help system in your Web browser.

4. When the Sterling Integrator installation asks for the location of the JDBC drivers, specify the extracted jar file created after unpacking the archive (usually named sqljdbc.jar). The JDBC driver version is the same as the version of the drivers downloaded from Microsoft.