Gentran Integration Suite

UNIX/Linux Cluster Upgrade

Version 4.3

Sterling Commerce
An IBM Company

Contents

Chapter 1

Introduction

Use the Gentran Integration Suite *4.3 UNIX/Linux Cluster Upgrade Guide* to upgrade the Gentran Integration Suite software in a clustered (multiple node) UNIX/Linux environment. This guide includes the pre-upgrade and post-upgrade processes. It also includes information for using DB2, Microsoft SQL Server and Oracle databases with Gentran Integration Suite.

For new installations, use the Gentran Integration Suite *4.3 UNIX/Linux Cluster Installation Guide*.

Chapter 2

Pre-Upgrade Information

Before You Begin Upgrading

Before you begin upgrading to Gentran Integration Suite 4.3, be aware of the following prerequisite tasks and considerations:

- *Standard Tasks and Considerations* on page 7
- *Special Tasks and Considerations* on page 8
- *Creating a Process Output Log* on page 9
- *Copying a Microsoft SQL Server 2000 Database* on page 9
- *Copying a Microsoft SQL Server 2000 Database to an SQL Server 2005 Database* on page 10

Also, at several points in the upgrade process, you will be asked to download a file from https://support.sterlingcommerce.com. After logging in at this web page, click on the following links to reach the file: **Product Support** > Gentran Integration Suite > Gentran Integration Suite **Product Updates/Downloads**.

Note: If you are upgrading from Gentran Integration Suite 4.1 to 4.3, you must apply Gentran Integration Suite 4.1 Build 1990.

Standard Tasks and Considerations

Before you begin upgrading, be aware of all of the following standard tasks and considerations:

1. You must have a new license file to use the new licensed features of your upgraded installation.
2. Read through this entire document so that you have a clear understanding of what the upgrade requires.
3. Download the following information from the Gentran Integration Suite 4.3 library page http://www.sterlingcommerce.com/Documentation/GIS43/homepage.htm.
   - *Release Notes*
   - *System Requirements*

     With each release, Sterling Commerce introduces leading edge technology to improve and enhance its software. Review the *System Requirements* to confirm that your system and databases meet the requirements, and also to manage any necessary upgrades or changes before upgrading.

4. Archive and purge any unneeded data before upgrading.

   Archived data can only be restored from the same version and patch of Gentran Integration Suite from which it was archived. If you need to restore archived data that was archived prior to performing the upgrade, then you must have a running instance of Gentran Integration Suite that matches the version and patch from which the archive was taken.

5. Back up your database. Export your business processes, trading partners, maps, etc.
6. Review and note the adapters, business processes, and other configurations in your current version. This will help identify any need for updating transport messages, third-party adapters, or configurations to adapters, such as the File System and Command Line Adapters.
7. If you have edited a pre-defined business process, be aware that the upgrade process overwrites pre-defined business processes. Your customized business process is preserved in the system, but it is no longer the default process.
8. If you have edited any property files (.properties or .properties.in), be aware that the upgrade process overwrites these property files, unless these changes were made using the customer_overrides.properties file. Your previous property file edits might not be applicable in Gentran Integration Suite 4.3.
9. *Always* install and test your upgrade in a non-production environment before upgrading your production environment.

Special Tasks and Considerations

Before you begin upgrading, be aware of the following special tasks and considerations, depending on your type of upgrade:

- If you are using Oracle 8i with Gentran Integration Suite 4.0, upgrade to Oracle 9i before upgrading to Gentran Integration Suite 4.3.
- If you import Oracle 9 or Oracle 10 database while upgrading to Gentran Integration Suite 4.3, import the database without the indexes. For example, if you are using the Oracle import (imp) tool, you should use the INDEXES=N option. If you attempt upgrading to Gentran Integration Suite 4.3 with indexes, the upgrade will fail.

Note: If you had created any custom indexes in Oracle database, add them after performing the upgrade as they are not imported.

- If you have LDAP (Lightweight Directory Access Protocol) configuration information in the security.properties file, this information will automatically be moved to the authentication_policy.properties file.
- If your version of Gentran Integration Suite is integrated with the JBoss™, WebLogic®, or WebSphere® application server.

  Gentran Integration Suite version 4.3 is installed without integration to an application server and does not require an application server for installation or at runtime. However, Gentran Integration Suite still supports integration with JBoss, WebLogic, and WebSphere. After you upgrade to 4.3, you can restore integration with your application server if desired. To do so, use the Gentran Integration Suite EJB Adapter. For more information, refer to the documentation for the EJB Adapter.

Creating a Process Output Log

A log of process activity during the upgrade will help if troubleshooting is required. Output is automatically logged to upgrade.log. Use this procedure to generate a separate output log for each process you want to log.

To create a process output log , do the following:

1. Run the `script` command to record the process, ensuring that you have created and specified the file name in which to save the process output.

   For example, to start recording output to a file named processoutput.log, at the command line, type `script processoutput.log`.

2. After the upgrade is complete, type `exit` at the command line to stop recording.
3. You can now retrieve the file containing the process output.

   The following example shows a session in UNIX after starting the script command, specifying the output to be saved to the file named listing.log, and typing exit to stop the script command from running:

```
[2]%script listing.log
   Script started, file is listing.log
   [3]%ls
   Custard.Recipe         FavoriteRecipes  Curry.Recipe
   VindalooCurry.Recipe   Jelly.Recipe
   [4]%exit
   Script done, file is listing.log
```

Copying a Microsoft SQL Server 2000 Database

Before upgrading, it is recommended that you first make a backup of your Microsoft SQL Server 2000 database. One way to accomplish this is to make a separate copy of your existing database so that you can preserve your current system. Your existing Gentran Integration Suite instance will no longer function if you upgrade your existing database without making a copy.

Note: If you are moving from a SQL Server 2000 database to a SQL Server 2005 database, refer to *Copying a Microsoft SQL Server 2000 Database to an SQL Server 2005 Database* on page 10.

Caution: This is an optional procedure, and it is the customer’s responsibility to perform it. Sterling Commerce Customer Support cannot help with this procedure.

You can use SQL Server Data Transformation services (DTS) to make a copy of your current database.

1. Drop all of the objects from the Gentran Integration Suite 4.3 database. This includes tables, indexes, views, and procedures.

   Caution: Before you import rows into populated tables, you must drop these tables from the Gentran Integration Suite 4.3 database to eliminate the old data. If you do not, the new data is appended to the existing tables.

2. Start the DTS wizard and choose your current database as the source database and the new 4.3 database as the destination database.
3. Select **Copy all of the objects and data between SQL databases**.

4. Select **Run immediately** to complete the wizard.

   The current database is copied to the new 4.3 database.

5. Change ownership of objects copied to the new Gentran Integration Suite 4.3 user.
6. Log in to SQL Query Analyzer and run the following script in the Gentran Integration Suite 4.3 database:

   ```
   use name_of_GIS_database
   go
   declare @curown varchar(256), @newown varchar(256)
   select @curown = 'current_owner', @newown = 'new_owner'
   select 'exec sp_changeobjectowner '+ ''''
   + @curown + '.'
   + obj.name + ''','''
   + @newown + ''''
   from sysobjects obj
   where uid =
   (Select uid from sysusers where name = @curown) and type in ('U', 'V', 'P')
   and @newown in (select name from sysusers)
   order by obj.name
   ```

   - Change *name_of_GIS_database* to the name of the new Gentran Integration Suite 4.3 database.
   - Change *current_owner* to the name of the user who currently owns objects in the copied database.
   - Change *new_owner* to the name of the current DBO of the new 4.3 database.

   No other values should be changed in the script.

   An output script is generated which, when executed, will change the ownership of all of the tables.

7. Copy the output script and run it on the Gentran Integration Suite 4.3 database.

Copying a Microsoft SQL Server 2000 Database to an SQL Server 2005 Database

Before upgrading, it is recommended that you first make a backup of your Microsoft SQL Server 2000 database. One way to accomplish this is to make a separate copy of your existing database so that you can preserve your current system. If you are moving from a Microsoft SQL Server 2000 database to an SQL Server 2005 database, use the following procedure. Your existing Gentran Integration Suite instance will no longer function if you upgrade your existing database without making a copy.

Note: If you are copying a SQL Server 2000 database to another SQL Server 2000 database, refer to *Copying a Microsoft SQL Server 2000 Database* on page 9.

Caution: This is an optional procedure, and it is the customer’s responsibility to perform it. Sterling Commerce Customer Support cannot help with this procedure.

1. Perform a full database backup to the file system on the source SQL 2000 server of the source database.
2. Copy the resultant backup (.bak) file from the file system on the source server file system to the file system on the SQL 2005 server.

3. Connect to the SQL 2005 database server as a Windows authenticated user with administrative privileges on the database server using SQL Server Management Studio 2005.
4. Make sure that the destination database is not in use (disconnect any connected applications).
5. Restore the backup of the SQL 2000 database over the existing SQL 2005 database, using the Tasks|Restore|Database wizard. The restore will be from a "device," the file created above. Specify on the Options tab the correct locations for the data and log files (since the locations in the backup may not be the same as the correct locations for files on the on SQL 2005 database server); also check the box to specify that the existing database is to be overwritten. Confirm that the restore is reported successful.
6. Check to make sure that existing users in the database match existing users on the server using the command `sp_change_users_login 'report'`. If no rows are returned, go to step 8.
7. If rows are returned, execute the command `sp_change_users_login 'update_one', 'username', 'username'` substituting the unlinked login name in each execution to correct links between existing users in the restored database and existing logins on the server.
8. Examine the users of the database using the SQL Studio or sp_helpuser. If the login (existing on the server) who will be working with this database is not currently a user of the restored database, add that login as a user of the database by executing the following commands (login_name and user_name should generally be the same):

   ```
   USE database_name
   Go
   EXEC sp_grantdbaccess ' login_name ', ' user_name '
   Go
   EXEC sp_addrolemember 'db_owner', ' username '
   Go
   CHECKPOINT
   Go
   USE master
   Go
   EXEC sp_defaultdb ' username ', ' database_name '
   Go
   ```

   Note: The spaces in the quoted strings in the SQL commands should not be included in the final procedure, as spaces are significant to the proc and the commands will fail if they are there (i.e., `EXEC sp_grantdbaccess ' login_name ', ' user_name '` should be `EXEC sp_grantdbaccess 'login_name', 'user_name'`).
9. Examine the user tables in the SQL 2005 database to determine which schema they currently are in. Using the SQL Studio, the schema will be the prefix before each table listed in the Table tree. [This assumes that we will not change the schema of the user objects from whatever it is now – even if it's a schema name with the same name as a user other than the user who will be accessing the data.]
10. Execute the following command in the SQL 2005 database to ensure that the default schema for the user who will interact with the database matches the schema containing the restored user objects. If the objects are in the dbo schema, use dbo as the schema_name.

    ```
    USE database_name
    Go
    ALTER USER user_name WITH DEFAULT_SCHEMA = schema_name
    Go
    ```

Managing Database Passwords

A password is used by the application to connect to its database. 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 install Gentran Integration Suite. Encrypting these passwords is optional.

Database Password Encryption Methods

Database passwords are encrypted using one of two methods, OBSCURED or ENCRYPTED. The encryption method is decided by the value of the encryptionPrefix in propertyEncryption.properties or propertyEncryption.properties_platform_security_ext file.

Encrypting Database Passwords (UNIX)

To encrypt the database password:

1. Stop the Gentran Integration Suite.
2. Navigate to /*install_dir*/install/bin/.
3. Enter `./enccfgs.sh`.
4. Enter `./setup.sh`.
5. Enter `./deployer.sh`.
6. Enter `./run.sh` to start the application.
7. Enter your passphrase.

Decrypting Database Passwords (UNIX)

Before you can decrypt a password, you must know the encrypted password.

1. Stop the Gentran Integration Suite.
2. Navigate to /*install_dir*/install/properties.
3. Open the sandbox.cfg file.
4. Copy encrypted password from the database_PASS property. Use the text that appears after the ***database*_PASS=** text. For example, if ***database*_PASS= OBSCURED:123ABCxyz321**, you would copy the text **OBSCURED:123ABCxyz321**. (OBSCURED is the encryption method for the password.)
5. Navigate to /*install_dir*/install/bin.
6. Enter **./decrypt_string.sh encrypted _password**. For encrypted_password, use the text that you copied in Step 4.

   You are prompted for the Sterling Integrator passphrase.

   Your decrypted password appears.

7. Navigate to /*install_dir*/install/properties.
8. Edit the sandbox.cfg file to replace the encrypted password with the password that was returned in Step 6.
9. You need to decrypt the entry for **YANTRA_DB_PASS**. Repeat Steps 4 to 8 to decrypt YANTRA_DB_PASS.

Note: You should also decrypt any custom database pool passwords present in the customer_overrides.properties file or any other properties file.

10. Navigate to /*install_dir*/install/bin.
11. Enter `./setupfiles.sh`.
12. Enter `./deployer.sh`.
13. Enter `./run.sh` to start the Gentran Integration Suite.
14. Enter your passphrase.

Verifying System and Database Compatibility

To verify system compatibility and prepare for the upgrade, perform the following tasks:

1. Review Gentran Integration Suite *Release 4.3 System Requirements* document. Your system must meet the minimum requirements that are documented, while your database and JDBC driver versions must match the documented requirements. Complete any necessary upgrades or changes in preparation for the upgrade.
2. Collect information on any third-party libraries used for adapter configuration that were added to your current release. You must add each of these libraries to release 4.3 later in the upgrade process.
3. Locate any configuration file changes for the JDBC adapter or the Lightweight JDBC adapter in your current release. Later in the upgrade process, you will copy these changes to release 4.3.
4. Record your performance tuning configuration. You will restore these settings later in the upgrade process.

Preparing Your System for the Upgrade

Verify your system compatibility as previously described before continuing with this procedure.

1. Back up Gentran Integration Suite and your current database.

   Caution: If there are problems with your upgraded system, the only way to ensure that you can roll-back to your previous version is to back up Gentran Integration Suite and your database.

2. To avoid upgrade failures in Windows, shut down all software that performs non-system processes, including processes that:

   - Scan files and directories for viruses

- Back up file systems
- Monitor software (for example, HP OpenView)
- Disable pop-up windows

After you successfully back up Gentran Integration Suite and your database, you are ready to upgrade the software. Before you begin, see Gentran Integration Suite *4.3 Release Notes*.

Preserving Customer Changes During Updates

You can preserve your custom changes to system resources (like workflow definitions and maps) when you update your system. During updates, the system can identify when you make a custom change versus when the system makes a change through an upgrade or patch.

When a patch, installation or upgrade is performed, a baseline record of system resources is created. This baseline is not affected by any subsequent customer changes. When another patch is installed, the resources in this baseline are compared to the resources in the existing system. If a baseline and existing resource are not the same, that means that the existing resource was customized, and is not overwritten by the patch.

During an update, the baseline is updated with new system resource information, but not with custom changes to resources.

A report shows what has changed in the system that customer-specific changes did not permit to get set as defaults. This report is used in conjunction with the user interface to verify that customer overrides are not getting overwritten by the patch.

The report includes the following resource types:

- Workflow definitions
- Maps
- Schema
- Template

Chapter 3

Upgrading in a Clustered UNIX or Linux Environment

Preinstallation Setup Checklist for a Clustered UNIX or Linux Environment

The following topics will assist you with preinstallation tasks when planning an upgrade installation of Gentran Integration Suite in a clustered UNIX or Linux environment:

- *Checklist for UNIX or Linux Preinstallation* on page 15
- *Checking System Requirements* on page 20
- *Installing the Java 2 Software Development Kit* on page 21
- *Downloading the JCE Distribution File* on page 21
- *Determining Port Numbers* on page 22
- *Creating a UNIX Account* on page 22
- *Applying Database Definition Language (DDL) Statements* on page 22
- *Obtaining a License File* on page 23
- *Installing the JDBC Driver in SQL Server* on page 24

Checklist for UNIX or Linux Preinstallation

The preinstallation checklist contains the items you need to gather and tasks you need to complete prior to installing Gentran Integration Suite.

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. See *Checking System Requirements* on page 20.	
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	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

4	For the AIX 5.2 and 5.3 operating systems, establish these settings:
	◆ 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.
	◆ Change the following default entries in the /etc/security/limits file:
	fsize = -1
	core = 2097151
	cpu = -1
	data = 262144
	rss = 65536
	stack = 65536
	nofiles = 4096	

5	For the Solaris 8, 9, and 10 operating systems, 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.	

Step	Description	Your Notes

6	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 following variables:
	• Change LANG from **en_US.utf8** to **en_US**.
	• Change SUPPORTED 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:
	`gisuser hard    nofile  16384` (maximum value)
	`gisuser soft    nofile  4096` (minimum value)
	`gisuser hard    memlock 3000000`
	`gisuser soft    memlock 3000000`
	`gisuser hard    nproc   16000`
	`gisuser soft    nproc   16000`
	`gisuser hard    stack   512000`
	`gisuser soft    stack   512000`
	This updates the system ulimits.
	Save and close the /etc/security/limits.conf file.
	3 Reboot the system.	

7	For systems with multiple IP addresses, verify that the IP address on which Gentran Integration Suite 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, 127.0.0.1 localhost localhost.localdomain **Caution**: If you do not verify the IP addresses, your system may not operate properly after installing Gentran Integration Suite.	
8	Verify that all client computers are using Microsoft Internet Explorer 5.x or later.	
9	If you are using a non-English environment, confirm that you are using the appropriate character set.	

Step	Description	Your Notes
10	Determine and record information about the JDK. See *Installing the Java 2 Software Development Kit* on page 21. ◆ Version of the JDK ◆ Absolute path to the JDK files and patches	
11	Obtain the JCE distribution file and record the absolute path to the zipped file. See *Downloading the JCE Distribution File* on page 21.	
12	Determine and record the initial port number to be used by Gentran Integration Suite. See *Determining Port Numbers* on page 22.	
13	Verity that a UNIX user account exists on the host server for each installation of Gentran Integration Suite. See *Creating a UNIX Account* on page 22.	
14	Set Umask to 002.	
15	If you are using an Oracle, Microsoft SQL Server, or DB2 database, determine and record information about your database server. Be aware that this information is case sensitive. ◆ Database vendor ◆ Database user name and associated password ◆ Database (catalog) name ◆ Database host name ◆ Database host port number ◆ Absolute path and file name for the JDBC driver ◆ Version of the JDBC driver	
16	Decide if you are going to manually or automatically apply database definition language (DDL) statements (schema) to the database. See *Applying Database Definition Language (DDL) Statements* on page 22.	
17	Determine and record information to set up default system alerts from Gentran Integration Suite: ◆ The Administrative e-mail address to which system alert messages are sent. **Note:** It is recommended that you not change the Administrative e-mail address during an upgrade. If you change this address, you will have to update adapters, business processes and other items that include this information. ◆ The SMTP Server IP address used for sending alert messages.	

Step	Description	Your Notes
18	Determine and record the directory in which you plan to install Gentran Integration Suite. ◆ The installation directory must not exist because the installation process creates it. ◆ The file system must have adequate free disk space. ◆ The name of the directory is case sensitive.	
19	Determine and record the passphrase you want to use for Gentran Integration Suite system. During installation, you are prompted twice to type the passphrase, which is not displayed when you type it.	
20	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. See *Obtaining a License File* on page 23. **Note:** For a cluster, you need to get a valid license for the IP addresses of all the nodes of the cluster. The license file includes spaces for more than one IP address.	
21	Determine whether Gentran Integration Suite is using an application server (JBoss™, WebLogic® or WebSphere®). Gentran Integration Suite does not require an application server for installation or at runtime. Gentran Integration Suite supports integration with JBoss and WebLogic during the installation. You can also integrate with WebSphere, JBoss, or WebLogic after installing version 4.3 by using the Gentran Integration Suite EJB Adapter. This does not represent a WebLogic server for deploying the Application Console.	

Checking System Requirements

Before you begin, verify that your system meets the hardware and software requirements specified for this release of Gentran Integration Suite. 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 Gentran Integration Suite. For current information, see the *System Requirements* posted on the Gentran Integration Suite Documentation Library:

http://www.sterlingcommerce.com/Documentation/GIS43/homepage.htm

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.

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.

Installing the Java 2 Software Development Kit

You must install the Java 2 Software Development Kit (JDK) and the patches specific to your system. You must supply the absolute path when installing the Java 2 Software Development Kit (JDK). To determine which JDK version and patches you need, see the *System Requirements*. After you install the JDK, record the absolute path to its location on your system.

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.

Note: If you are installing Gentran Integration Suite 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) 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 *Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0* 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** 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 Gentran Integration Suite.

To specify an initial port number, follow these guidelines:

- Gentran Integration Suite requires a range of 100 consecutive open ports between 1025 and 65535.
- The initial port number represents the beginning port number in the range.
- The port range starts with the initial port number and ends with the number that equals the initial port number plus 100. For example, if you specify 10100, then you need to make sure that 10100 through 10199 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*/properties/sandbox.cfg file for all of the port assignments.

Creating a UNIX Account

In a UNIX or Linux environment, you must create a UNIX administrative account on the host server for each installation of Gentran Integration Suite. For example, if you want to create a test environment and a production environment, you need to create two UNIX accounts on the host server, one for the test and one for the production environment. For more information about creating UNIX accounts, see your operating system documentation.

Applying Database Definition Language (DDL) Statements

When you install Gentran Integration Suite, 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 statements, the installation will automatically apply the DDL statements.

This feature increases database security by reducing the database permissions of the Gentran Integration Suite database user. The rights to create or change tables, indexes, etc. can be reserved for a secure user like a customer database administrator (DBA). Also, these database rights would not be affected by Gentran Integration Suite.

When you manually apply a DDL statement, you work with the DDL scripts that are stored in the *install_dir*/repository/scripts directory. The DDL scripts that are generated depend on the database that you are using. The following list shows the DDL scripts that are generated for each database:

- The DDLs generated for Oracle are:

  - EFrame_IndexAdds.sql
  - EFrame_Sequence.sql
  - EFrame_TableChanges.sql
- The DDLs generated for DB2 are:
  - EFrame_Sequence.sql
  - EFrame_TableChanges.sql
  - EFrame_IndexAdds.sql
- The DDLs generated for Microsoft SQL Server 2005 are:
  - EFrame_TableChanges.sql
  - EFrame_IndexDrops.sql
  - EFrame_IndexAdds.sql

Obtaining a License File

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

The license file contains a license that is associated with your specific operating system and the IP address of your system. The license provides access, for 20 years from the date of issue, to the packages your company selected and is independent of your maintenance fee. Because the license is independent of your maintenance fee, the schedule for renewing your license and license file may be different than the maintenance fee schedule.

To run a Gentran Integration Suite cluster, you need to get a valid Gentran Integration Suite license for multiple IP addresses for all the nodes where Gentran Integration Suite will be installed and configured as a cluster. The license file includes space for more than one IP address.

You must download the license file before you can install Gentran Integration Suite. Follow these steps:

1. Point your Web browser to http://www.productupdates.stercomm.com.
2. Review the *Welcome to Sterling Commerce Product Update* page and click **Next**.
3. Review the Authenticate page and click **Next**.
4. Type the License File Key, which is case-sensitive, and click **Next**. If the system displays the Retrieve Registration dialog box and you are upgrading, you may retrieve your registration information by entering your previous License File Key. If you are not upgrading, then click **Next**.
5. Verify the registration information and click **Next**.
6. On the *Server Details* page, update the fields and click **Next**.

   If the operating system, application server, or database server version is not listed in the respective lists, type the version in the respective **Description of Other**.

   All IP addresses assigned to the server in which you are installing Gentran Integration Suite should be listed in the license file.

7. Verify the list of packages and the type of license selected for each package and click **Next**. If the list of packages selected or the type of license selected is *not* correct, then contact Customer Support to correct the information.
8. Scroll to the bottom of the *Review and Download Package License File* page and click **Finish and Download**.
9. Click **Save** in the **File Download** dialog box.
10. Accept the default location for the license file or navigate to the location where you will store the license file. Note the absolute path of the file location on the Preinstallation Checklist.
11. Click **Save**.
12. Close your Web browser.

Installing the JDBC Driver in SQL Server

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

Refer to one of the following sections for your Microsoft SQL Server version:

- *Installing the JDBC Driver in SQL Server 2000* on page 24
- *Installing the JDBC Driver in SQL Server 2005* on page 25

Installing the JDBC Driver in SQL Server 2000

Go to the Microsoft web site to download this driver which, as of Gentran Integration Suite 4.3, is contained in a tarball named mssqlserver.tar. This tarball includes the jar files msbase.jar, mssqlserver.jar, and msutil.jar. Also download any appropriate patches.

Uncompressing mssqlserver.tar yields several files, including install.ksh, which is a korn shell script that installs the JDBC drivers in a specified directory.

After running the install.ksh script, you need to combine the three jar files that make up the Microsoft SQL Server JDBC drivers (msbase.jar, mssqlserver.jar, and msutil.jar). These files will be placed in the *JDBC_driver_install_dir*/lib directory. To combine these jar files, use the following procedure:

1. Make a new directory in which you will work, and copy the separate jar files to this directory.
2. For each of the separate jar files, issue the following command:

   ```
   jar -xvf jar_file_name
   ```

3. After all of the jars have been expanded, remove the META-INF directory that will be located in the working directory.
4. Create a new jar file by issuing the following command:

   ```
   jar -cvf. combinedJarName.jar *
   ```

When the Gentran Integration Suite installation asks for the location of the JDBC drivers, specify the jar file you created with the above procedure. The JDBC driver version is the same as the version of the drivers downloaded from Microsoft.

If you are using a silent installation, access msbase.jar, mssqlserver.jar, and msutil.jar using one of the following methods:

- Point to the bundled jar file.

  Example: `DB_DRIVERS=`*`absolutePath/combinedJarName`*`.jar`

- List all three files. Use their full directory path, and separate them with colons.

  Example: `DB_DRIVERS=`*`absolutePath/`*`msbase.jar:` *`absolutePath/`*`mssqlserver.jar:` *`absolutePath/`*`msutil.jar`

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 at *absolutePath*/sqljdbc_*version*/*language*/help/default.htm file. This will display the help system in your Web browser.

4. When the Gentran Integration Suite 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.

Configuring Snapshot for Microsoft SQL Server 2005

The snapshot feature in Microsoft SQL Server 2005 allows you to view a read-only copy of the database even when it is locked. It is recommended to configure snapshot feature as it reduces deadlocks. Run the following command to enable snapshot feature:

```
ALTER DATABASE db_name SET READ_COMMITTED_SNAPSHOT ON;
```

Upgrading in a Clustered UNIX or Linux Environment

Upgrading Gentran Integration Suite in a clustered UNIX or Linux environment includes the following tasks:

- *Upgrading in UNIX or Linux* on page 26
- *Running the Upgrade Program in UNIX or Linux* on page 26
- *Node to Node Communications* on page 32

Upgrading in UNIX or Linux

To upgrade to Gentran Integration Suite version 4.3 for a clustered installation, follow the steps in *Running the Upgrade Program in UNIX or Linux* on page 26. Also refer to *Installing the Current Maintenance Patch in UNIX or Linux* on page 35.

Before running the upgrade program, refer to the *Pre-Upgrade Information* section. After running the upgrade program, refer to the *Post-Upgrade Processes* section.

Caution: It is important to remember that upgrading to 4.3 involves a full installation of Gentran Integration Suite. You need to prepare for an upgrade the same way that you would prepare for an installation.

Caution: Before the upgrade, you should always make a backup of your production database. If you make a separate copy of your database in order to preserve your existing database, then perform the upgrade on the copy of the production database.

This upgrade does not overwrite your current Gentran Integration Suite directory structure on disk. Instead, it creates a new installation of Gentran Integration Suite 4.3 that will point to and upgrade the database of your current installation of Gentran Integration Suite. This means your original instance will no longer be operational after performing the upgrade. After the upgrade, you will be starting your Gentran Integration Suite instance only from the newly created directory structure.

Note: When you copy your database, if you encounter *Data Overflow* or *Invalid Time Format* errors while copying the WORKFLOW_CONTEXT table, run this query:

```
UPDATE WORKFLOW_CONTEXT SET ENTERQ = NULL, EXITQ = NULL where ENTERQ IS
NOT NULL OR EXITQ IS NOT NULL
```

It is also recommended that you thoroughly test this process in a test or development environment prior to implementing in a production environment.

Note: If you need to patch Gentran Integration Suite before continuing the upgrade, it is recommended that you fully test the patch prior to performing the upgrade. If you are running Gentran Integration Suite 4.0 at a patch less than 4.0.3-5, you **MUST** patch to version 4.0.3-5 or higher before continuing the upgrade.

Caution: This upgrade changes the administrative password to the default password. After the upgrade, change the password back to the administrative password to minimize security risks. This is the Admin password for logging into the UI (/dashboard or /ws).

Running the Upgrade Program in UNIX or Linux

The following instructions assume that you received an installation CD. If you downloaded Gentran Integration Suite or a Service Pack (SP) from the Electronic Software Distribution (ESD) Portal, unzip the downloaded file to an empty directory. The directory containing the unzipped files is an electronic image of an installation CD. Use this directory wherever there is a reference to the installation CD in the following instructions. Ignore any instructions to place the installation CD in a drive.

Upgrading Gentran Integration Suite nodes is similar to a standard Gentran Integration Suite upgrade, with the following restrictions on all nodes:

- All nodes must use the same database.

- All nodes must use the same passphrase.
- All nodes must use the same operating system.
- When installing nodes on different machines, the port numbers must be the same.

  Note: Installing nodes on different machines helps you take more advantage of the reliability, availability and scalability features of clustering, including failover.
- When installing nodes on the same machine, you must install the second instance in a different directory and use a different initial port number. This second port number must be at least 100 higher or lower than the first port number.
- You must install and start the nodes sequentially, one at a time, starting with the first node.

To run cluster, you need to get a valid Gentran Integration Suite license for multiple IP addresses of all the nodes where Gentran Integration Suite will be installed and configured as a cluster. One license can include more than one IP address.

Note: Clustering is not supported for Gentran Integration Suite systems that use the MySQL database.

To upgrade in a clustered UNIX or Linux environment, refer to your preinstallation checklist and follow the steps below. The upgrade installation for the first node of the cluster will be the same as for a single node installation.

Note: During the installation, various messages are displayed, including some warning messages. These warning messages require no action on your part and are included so that helpful data is recorded in the log file.

Note: Before your upgrade installation, shut down your base installation. This will free up the port number that you used in your base installation.

1. Place the Gentran Integration Suite installation CD in the appropriate drive.
2. From the installation CD, copy GIS.jar to your home directory or base directory and change to that directory.

   If you are using FTP to copy the files, verify that your session is set to binary mode.
3. To begin the installation, type the absolute path to the JDK followed by the following command:

   Note: On Linux, do not use any soft/symbolic links in the path to the `jar` file. Make sure that you specify the full path to the `jar` file.

   ```
   absolutePath/bin/java -jar absolutePath/GIS.jar -upgrade
   ```

   If Gentran Integration Suite is running, stop the previous installation before proceeding.
4. The program checks for the presence of the JCE unlimited strength policy files. If they are not installed, you are prompted for the path to the JCE distribution file. If prompted, type the absolute path name to the JCE distribution file and press **Enter**. Verify the file name by typing **y** and pressing **Enter**.
5. Type the absolute path to the license file and press **Enter**. The license file must reside on the local UNIX/Linux host. If you saved the license file to a Windows client, transfer the license file to the UNIX/Linux host. Verify the file name by typing **y** and pressing **Enter**.
6. Type the absolute path of the installation directory and verify that the directory is correct. Verify the directory name by typing **y** and pressing **Enter**.

   The program checks the amount of available disk space for the installation.

7. When prompted, change to the installation directory and run the command `installSi.sh`.
8. Review the license agreement. Type **y** and press **Enter** to accept the agreement.
9. You are prompted whether to override the host IP address.
   - To override the host IP address, enter another IP address and press **Enter**.
   - To accept the default host IP address, press **Enter**.

   Note: If you are installing Gentran Integration Suite on VMware, you should provide the IP address of the virtual machine and not of the VMware host. For example, if 10.251.124.160 is the IP address of the VMware server and 10.251.124.156 is the IP address of the Windows 2003 server it is hosting, you should use 10.251.124.160 as the IP address to install Gentran Integration Suite.
10. Type the same system passphrase that you you used for your previous Gentran Integration Suite installation. Then type the passphrase again to confirm it.
11. You are prompted whether to enable the FIPS (Federal Information Processing Standards) mode. If you want to enable FIPS, type **Yes** and press **Enter**. Otherwise, press **Enter** to use the default value of **No**.
12. You are prompted whether to integrate with WebLogic or JBoss during the installation. If you want to integrate, type **Yes**, enter the required information, and press **Enter**. Otherwise, press **Enter** to use the default value of **No**.

    Note: You can integrate with the JBoss, WebLogic or WebSphere application server after you have installed Gentran Integration Suite.
13. Type the same initial port number you used for your previous Gentran Integration Suite installation.

    A list of the port assignments appears. The installation uses the initial port number to set up port assignments. These port assignments are written to *install_dir*/properties/sandbox.cfg.
14. You are prompted whether to change the default port values.
    - To accept the default values, press **Enter** to use the default value of **No**.
    - To change the default values, type **Yes** and press **Enter**. For each port, you are prompted to either choose the default value or type in a new value. Press **Enter** to accept the default value, or type the new value and press **Enter**.
15. Type the administrative e-mail address to which you want system alert messages to be sent. Press **Enter**.

    Note: It is recommended that you not change the Administrative e-mail address during an upgrade. If you change this address, you will have to update adapters, business processes and other items that include this information.
16. Type the SMTP mail server host name that you want to use for system alert messages and other administrative notices. Press **Enter**.
17. You are prompted for the database you want to use.

    Note: Clustering is not supported for Gentran Integration Suite systems that use the MySQL database.

    Type the appropriate number for the database that you are using (Oracle, DB2, Microsoft SQL Server 2000 or Microsoft SQL Server 2005). Enter the following information when prompted, using the database information from your current installation of Gentran Integration Suite (that is, the installation that you are upgrading):

- Database user name
- Database password
- Database password again for confirmation
- Database (catalog) name
- Database host name
- Database host port number
- Absolute path and file name for the JDBC driver (For DB2, use the Type 4 JDBC driver). For more information about accessing the driver for Microsoft SQL Server, refer to *Installing the JDBC Driver in SQL Server* on page 24.
- Version of the JDBC drivers

The upgrade program verifies the database connection. If a connection cannot be established, you receive an error and can re-enter the database information.

18. At the *What datatype is used by the previous version?* prompt, choose one of the following data types:

    In an upgrade, both the old and new versions of Gentran Integration Suite must use the same data type. To determine the data type, refer to the *install_dir*`/properties/sandbox.cfg` properties file. If sandbox.cfg does not have an ORACLE_USE_BLOB property, use the Long Raw data type. Use the BLOB data type when **ORACLE_USE_BLOB=true** and **ORACLE=true**.

    - Long Raw
    - BLOB

19. At the *Automatically create database schema* prompt, take one of the following actions:

    - To automatically apply database definition language (DDL) statements, press **Enter** to use **Yes**.

      If you type **Yes**, and do not choose to manually apply the DDL statements, the installation applies both the DDL statements and the resources.

    - To manually apply database definition language (DDL) statements, type **No** and press **Enter**. For more information about this option (including the unique names of the DDLs for each database vendor), refer to *Applying Database Definition Language (DDL) Statements* on page 22.

      If you manually create the database schema, you will have to run the command `installSi.sh` again after manually creating the schema. When you re-run the `installSi.sh` command, answer **No** to the *Automatically create database schema* prompt.

      The installation process will continue and complete without any errors. The installation process will validate the database with a Gentran Integration Suite tool called DBVerify and warn you if there are issues, and will exit the installation.

      The application of DDLs should be done in the same order as when you enter **Yes** at the *Automatically create database schema* prompt. You can find this order by referring to the installSI.log file of an installation where **Yes** was entered at the *Automatically create database schema* prompt.

20. At the *Continue with the installation?* prompt, verify the installation setup information that you entered. Then, type **Yes** or press **Enter** to continue.

    The upgrade process continues automatically and installs the following components:

    - Core files (services, adapters, and predefined business processes)
    - Package files
    - System certificates
    - License file

21. When the installation of node 1 is finished, the system displays the following message:

    Installation has completed successfully.

    The cluster configuration for the server has completed successfully. If you are also installing the Standards Library, you can now install it.

    After these installation tasks, you can do one of the following:

    - Continue to the next steps to install the other nodes of the cluster.
    - Change to the *install_dir*/bin directory and execute the `run.sh` command to start the server. Later, you can continue to the next steps to install the other nodes of the cluster.

    If you encounter problems or errors during installation, see the section *Troubleshooting: Clustered UNIX or Linux Environment* on page 56.

    If you are installing a perimeter server, refer to *Installing a Perimeter Server in a Clustered UNIX or Linux Environment* on page 42.

22. Install each subsequent node, from node 2 onwards, using the `-cluster` option, which prevents any database initialization and update. The installation passphrase must be the same across all nodes.

    Examples:

    - For node 2 onwards, type the following command:

      ```
      absolutePath/bin/java -jar absolutePath/GIS.jar -cluster -upgrade
      ```

    - For a silent installation, type the following command:

      ```
      absolutePath/bin/java -jar absolutePath/GIS.jar -f silent.install
      -cluster -upgrade
      ```

23. From node 2 onwards, when you are prompted, run the `installSi.sh` command from the installation directory.

    If you get a *permission denied* message, run the following commands from the installation directory:

    ```
    a. chmod 777 installSi.sh
    b. installSi.sh
    ```

    The installation proceeds. Enter information using the following guidelines:

    - If you are installing nodes on separate machines, use the same information that you used during the first installation.

- If you are installing multiple nodes on the same machine, use an initial port number that is 100 port numbers higher or lower than the initial port number on other nodes. Each node will be configured on a different port range.
- If you are installing multiple nodes on the same machine, use a different installation directory for each node.

After all the nodes are installed, proceed to the next step.

24. (If installing multiple nodes on the same machine) Go to the *install_dir*/properties directory of nodes 2 and higher and change the mcast_port property in the jgroups_cluster.properties.in file to point to the value of the mcast_port property in the *install_dir*/properties/jgroups_cluster.properties file on node 1.

    Note the two different property file names:

    - jgroups_cluster.properties file (node 1)
    - jgroups_cluster.properties.in (nodes 2 and higher)

    a. (IPv6 only) For all nodes, change mcast_property from 239.255.166.17 to **FFFF:239.255.166.17**.

    b. (IPv6 only) In the sandbox.cfg file, add **HOST_ADDR=<*IPv6_hostname*>**.

25. (If installing multiple nodes on the same machine) Go to the *install_dir*/properties directory of nodes 2 and higher and change the multicastBasePort property in the noapp.properties.in file to point to the value of the multicastBasePort property in the *install_dir*/properties/noapp.properties file on node 1.

    Note the two different property file names:

    - noapp.properties file (node 1)
    - noapp.properties file.in (nodes 2 and higher)

26. On each node, starting with node 1, run the command `startCluster.sh` *`nodeNumber`* from the *install_dir*/bin directory where *`nodeNumber`* is the sequential number assigned to each node starting with 1. For example, on the first two nodes, you would run the following commands:

    Node 1

    a. `startCluster.sh 1`

       When the cluster environment is configured, you will get a message *BUILD SUCCESSFUL*.

    Node 2

    a. `startCluster.sh 2`

    b. Enter the passphrase.

       When the cluster environment is configured, you will get the message *Deployment to application server successful*.

Note: You should run `startCluster.sh` command only after you install Gentran Integration Suite. You should not run `startCluster.sh` command when you restart a Gentran Integration Suite instance. However, if you have installed a patch or a hot-fix, refer *Custom Configurations* on page 34 to start the cluster without updating the database settings.

27. Go to the *install_dir*/bin directory for each node and issue the following command to start the node, starting with the first node:

    ```
    run.sh
    ```

    When prompted, type the password that you entered earlier.

    When the `run.sh` command completes, the following message appears:

    Open your browser to (URL)

To make a dynamic addition of new nodes to the cluster, install new nodes to the cluster using the `-cluster` option as described above and configure the servers for the cluster.

For information on customizations, patches and hot-fixes for your installation of Gentran Integration Suite, refer to *Installation Customization and Maintenance (Cluster)* on page 34.

Note: After performing the upgrade, refer to *Installing the Current Maintenance Patch in UNIX or Linux* on page 35 install the latest patch.

Node to Node Communications

Cluster nodes are configured to communicate with each other using JGroups, an open source toolkit that provides flexibility for protocol configuration. JGroups provides rich open management features, along with multiple protocol support. JGroups supports multicast (UDP) and TCP-based communication protocols.

When JGroups is configured to use multicast (UDP), all cluster nodes communicate with each other on a specific IP address and port. The multicast ports are configured based on the installation base port. All clusters that are on the same subnet configured on the same base port will end multicasting messages on the same multicast IP address and port.

To avoid this, each cluster on the same subnet needs to be configured on different base ports. Install your clusters on different port ranges or on different network segments with multicast forwarding restricted, so that they will not interfere with each other. The default multicast address used in Gentran Integration Suite release 4.3 is **239.255.166.17**. This address is configurable, with a port range of 10 ports, starting with the multicast base port for the instance.

All nodes participating in the same cluster must be installed on the same multicast base port (the multicastBasePort property in the noapp.properties file). This is usually computed from the system base (non-multicast) port, but can be configured separately in the noapp.properties file, to allow different nodes in a cluster to be installed at different (non-multicast) port ranges. Also, all the nodes in the cluster should be installed in the same subnet.

For node to node communications, the properties are defined in jgroups_cluster.properties. The attributes used to define communications are:

`property_string` - default value is UDP

`distribution_property_string` - default value is TCP. This attribute should never be set to UDP.

If you want to change the communication for cluster multicast from TCP to UDP, contact Gentran Integration Suite Support. In addition, if you are using TCP for both property_string and distribution_property_string, the initial_hosts list for TCPPING should contain all hosts in the cluster.

For more information about UDP, TCP and JGroups communications, refer to the Gentran Integration Suite *4.3 Clustering* documentation.

Cluster Environment Verification

This section explains the verification process for the cluster environment.

- Verify the following properties:
  - The property CLUSTER=true is included in *install_dir*`/properties/sandbox.cfg`.
  - The cluster property in centralops.properties and noapp.properties is true and the clustered_env property in ui.properties is set to **true**
- Using the System Troubleshooter, you can verify the cluster environment by viewing the following information for each node:
  a. Queue information
  b. JNDI Tree for each node
  c. Host, state, status, adapters, and memory usage information
  d. Perimeter Server
  e. Shows adapter status for each node with a dropdown box listing all nodes in cluster
- Select **Operations** > **System** > **Troubleshooter** to display all the cluster nodes, ops URL, node URL, the status of the node and which node holds the token.
- You can track errors and exceptions in the system by selecting **Operations** > **System** > **Logs**. In a clustered environment, the logs are provided for each node. A dropdown list shows all the nodes. By selecting the node, the logs corresponding to the nodes are displayed. You can see each log item in this page for each node after all nodes start.
- The Activity Monitor UI provides the status of running business process and scheduled services. Using this feature, you can monitor all service activities including the node on which each activity is executing.
- To display the current threads that are running on specific node, select **Operations** > **System** > **Troubleshooter**, and then select the Threads for a node.

Starting or Stopping the Cluster Environment

You can start the cluster environment by running the following command on each node, starting with node 1 (it is recommended to start node 1 first.):

```
$ run.sh
```

If you are restarting the entire cluster, please run the following commands:

- Node 1:

  ```
  run.sh restart
  ```

  This option is used for cleaning the cluster data/settings, etc. to do a clear start.
- Nodes 2 and higher:

  ```
  run.sh
  ```

You can stop a cluster by using one of the following options:

- The `hardstop.sh` command from each node. This runs a `kill -9` command.
- The `softstop.sh` command from each node. This does a regular cleanup and shutdown of all components.

Caution: Running `softstop.sh` command in a multiple node (clustered) environment will suspend all scheduled business processes. It is recommended to run the `hardstop.sh` command when stopping individual nodes of a cluster.

- Shut down the whole cluster by selecting **Operations** > **System** > **Troubleshooter**, and then clicking the **Stop the System** link.
- Shut down specific nodes by selecting **Operations** > **System** > **Troubleshooter**, and then clicking the **shutdown** link.

Installation Customization and Maintenance (Cluster)

The following sections explain how to customize Gentran Integration Suite, using the following methods:

- *Custom Configurations* on page 34
- *Configuring Shared File System as Document Storage* on page 35

The following sections also explain how to update Gentran Integration Suite, using the following methods:

- *Installing the Current Maintenance Patch in UNIX or Linux* on page 35

  Patches contain cumulative fixes for a specific version of Gentran Integration Suite. Because each patch contains the fixes from previous patches, you only need to install the most recent patch.
- *Installing a Hot-Fix (Cluster)* on page 39

  A hot-fix is one or more fixes applied to a specific existing patch.

Custom Configurations

As part of a default cluster configuration, certain values in the database for service or adapter configurations, default document storage type, etc., are updated to get the cluster working. The default settings include no shared or mounted file system available with “line of sight” from all cluster nodes, etc. Certain service or adapter configurations are forcibly deployed on node1 and default document storage type is set up to “Database” for all business processes.

After you install the cluster and evaluate the customer configurations and requirements, the above conditions might change and custom configurations will be incorporated. To keep these custom configuration changes from being overwritten, the following cluster configuration script has an option to update the database:

```
startCluster.sh nodeNumber true/false
```

- *`nodeNumber`* is the cluster node number
- Type **true** to perform database update and **false** to prevent any database updates.

The first time you configure a cluster, run the `startCluster.sh` command with the database update option set to **true** to have all cluster-related configurations take effect.

```
startCluster.sh nodeNumber true
```

For cluster configurations after the first configuration, you can execute the `startCluster.sh` command with the database update option turned off. This prevents any configuration changes from affecting the system, especially after installing patches/hot-fixes.

```
startCluster.sh nodeNumber false
```

Note: For information about installing a patch on a cluster installation, refer to *Installing the Current Maintenance Patch in UNIX or Linux* on page 35.

Configuring Shared File System as Document Storage

In a cluster, the default document storage is database, so that all of the nodes in the cluster have line of sight to the documents to access and process the documents. However, using the database for document storage has performance implications over using the file system for document storage.

To use the file system as document storage in cluster, the file system needs to be a shared/mounted/clustered file system with all nodes having line of sight to the file system. Have your system administrator set up the shared/mounted/clustered file system.

For each node, follow this procedure to configure a shared file system in a cluster:

1. Go to the *install_dir*/properties directory.
2. Change the document_dir property in jdbc.properties.in to point to the shared file system directory configured to store the documents.
3. Run the `setupfiles.sh` command in the *install_dir*/bin directory.
4. Restart Gentran Integration Suite (all nodes).

This configures a shared file system directory as document storage.

Installing the Current Maintenance Patch in UNIX or Linux

Patches contain cumulative fixes for a specific version of Gentran Integration Suite. Because each patch contains the fixes from previous patches, you only need to install the most recent patch.

Note: During patch installation, the dbVerify utility compares the list of standard indexes with those present in the database and drops the custom indexes. You should recreate the custom indexes after the patch installation is complete.

All nodes in a cluster must be patched to the same level. You should stop all nodes in the cluster before installing a patch and then install the patch on each node.

It is possible, in some cases, to apply patches to nodes while others are still processing. However, a patch containing any of the following requires the entire cluster to be down:

- Critical cluster functionality
- Engine-related changes
- Changes to the database

Attempting to apply patches while part of the cluster is running should only be done with the advice of Sterling Commerce Customer Support.

To help you determine which patch to use, the files are named using the following naming convention:

si_43_build_*build number*.jar (for example, si_43_build_4307.jar)

Information about a patch is located in a PDF file with a similar name. The naming convention for PDF files containing information about a particular patch is:

si_43_build_*build number*_patch_info.pdf (for example, si_43_build_4307_patch_info.pdf)

Both the jar and the PDF files are available on the Sterling Commerce Support on Demand Web site, at https://support.sterlingcommerce.com. You should periodically check the web site to verify that you have the most recent patch.

Note: The patch installation may use one or more patch property override files. These files will be named *propertyFile_patch*.properties. Do not alter these files.
Additionally, property changes made directly in .properties or .properties.in files may be overwritten during the patch installation. Properties overridden using the customer_overrides.propertie**s** file are not affected.

To install the latest patch for Gentran Integration Suite in a clustered UNIX or Linux environment, follow the steps below:

1. Go to the Sterling Commerce Support on Demand Web site, at https://support.sterlingcommerce.com.
2. Download the most recent patch file for your version of Gentran Integration Suite and record the absolute path to the downloaded file. If you use FTP, use Binary mode. Do not rename the file.
3. Verify that the database server is up and ready to accept connections.
4. Stop Gentran Integration Suite.
5. Perform a full backup of Gentran Integration Suite installation directory, including all subdirectories. Also back up your database.
6. If you edited any property files, ensure that the associated .properties.in files have the most current changes. Property files will be overwritten with the contents of the associated .properties.in files during the patch installation.
7. Is the database password encrypted? If **Yes**, decrypt the password. For more information about decrypting database password, refer *Decrypting Database Passwords (UNIX)* on page 12.
8. Change to the directory where Gentran Integration Suite is installed and install the patch using the following commands:
   a. `cd install_dir/bin` and press **Enter**.
   b. Run the following command to install the patch:

   ```
   InstallService.sh
   <path>/si_<version>_sp_0_patch_<number>_<app_server>.jar
   ```

   where:
   <*path*> = Fully qualified path to maintenance patch file
   <*version*> = Gentran Integration Suite Version

<*number*> = Patch number
<*app_server*> = Application Server

Example: `InstallService.sh /opt/patch/si_22_sp_0_patch_1_jboss.jar`

Information about the patch installation is automatically logged to *install_dir*/logs/InstallService.log.

If the patch attempts to modify the database schema and the modification fails, you will receive an error message about the failure. The message provides the error message code from the database and the SQL command that failed. The failure information is also logged to the system.log file and to the patch.log file.

9. If you decrypted the database password, re-encrypt the password. For more information about encrypting database password, refer *Encrypting Database Passwords (UNIX)* on page 12.
10. Run the `startCluster.sh 1` command to reconfigure the cluster environment after installing the patch.

    Note: Ensure that you run `startCluster.sh` *`nodenumber`* `false` command to prevent configuration changes that may affect the system. Refer to *Custom Configurations* on page 34 before configuring the cluster environment.
11. Restart Gentran Integration Suite.

If you are using a perimeter server in a DMZ, see *Installing Patches in a Perimeter Server Environment* on page 27.

Updating the Database (dbupdate) with the startCluster Command

The `startCluster.sh` *`nodeNumber`* command on node 1 will automatically update the database, unless you use the command `startCluster.sh 1 false`. The `startCluster.sh` *`nodeNumber`* command on all other nodes will not update the database.

When you configure Gentran Integration Suite cluster for the first time, you should run the `startCluster.sh` command with the database update value set to **true** (`startCluster.sh 1 true`), or just `startCluster.sh 1`, since on node 1, dbupdate defaults to **true**. This makes all cluster-related configurations take effect. The database update will synchronize the scheduled jobs between the nodes by assigning them all to node 1.

The `startCluster.sh` command with the database update value turned off (`startCluster.sh 1 false`) prevents any configuration changes from affecting the system, especially after you install patches or hot-fixes.

For current database updates, the following services are tied to node 1:

- Schedule
- FileSystem
- CmdLine
- CDServerAdapter
- CDAdapter
- CDRequesterAdapter
- CEUServerAdapter
- HttpServerAdapter

- B2B_HTTP_COMMUNICATIONS_ADAPTER
- HTTP_COMMUNICATIONS_ADAPTER
- HTTPClientAdapter
- FTPClientAdapter
- FtpServerAdapter
- SFTPClientAdapter

The following services have storage set to the database:

- HttpServerAdapter
- CEUServerExtractServiceType
- CDSERVER_ADAPTER

The default storage of all workflows is set to the database.

Applying a Patch in a Clustered Environment Stopping the Whole Cluster

For a critical patch where the whole cluster needs to be down, use the following process:

1. Stop the whole cluster.
2. Install the patch on each node by running the following command from the *install_dir*/bin directory:

   ```
   InstallService.sh si_engine_####.jar
   ```

   Apply the patch to node 1 first, and then to the subsequent nodes: node 2, node 3, etc. For node 1, REINIT_DB is true in the *install_dir*/properties/sandbox.cfg file. For subsequent nodes, REINIT_DB is false, which prevents database updates from repeating on each node's patch installation. This is automatically set during the patch installation for all nodes except node 1 if the installation is done using the `-cluster` option.
3. Configure each node as a cluster node by running the `startCluster.sh` *`nodeNumber`* command.

   Note: Ensure that you run `startCluster.sh` *`nodenumber`* `false` command to prevent configuration changes that may affect the system. Refer to *Custom Configurations* on page 34 before configuring the cluster environment.
4. Restart the whole cluster.

Applying a Patch in a Clustered Environment Stopping One Node at a Time

For a patch where you can stop the cluster one node at a time, use the following process:

Note: Apply the patch to node1 first, and then to the subsequent nodes: node2, node3, etc.

1. Shut down the node using the *`install_dir`*`/bin/hardstop.sh` command.
2. Wait three minutes.
3. Install the patch by running the following command from the *install_dir*/bin directory:

   ```
   InstallService.sh si_version number_sp_sp number_patch_patch
   number_application server.jar
   ```

   For node1, REINIT_DB is true in *install_dir*/`properties/sandbox.cfg`. For subsequent nodes, REINIT_DB is false, which prevents database updates from repeating on each node's patch installation. This is automatically set during the patch installation for all nodes except node1 if the installation is done using the “-cluster” option.

4. Configure the node as a cluster node by running the `startCluster.sh` *`nodeNumber`* command.

   Note: Ensure that you run `startCluster.sh` *`nodenumber`* `false` command to prevent configuration changes that may affect the system. Refer to *Custom Configurations* on page 34 before configuring the cluster environment.

5. Open the *install_dir*`/properties/sandbox.cfg` file in a text editor. Perform the following steps:

   a. If REINIT_DB is true, back up the sandbox.cfg file and change REINIT_DB to false.

   b. Save and close the sandbox.cfg file.

   This prevents database updates from being repeated for each node.

6. Repeat steps 1 through 4 for each subsequent node.

7. Restart the whole cluster.

Running a DB2 Schema Change Script

After you install Gentran Integration Suite, Release 4.3 build 4316 or later, run the `fix_db2_schema.sql` script. If you are using DB2 as a remote host for Gentran Integration Suite, running `fix_db2_schema.sql` script applies new schema changes and fixes SQL exception error that may occur during large file transfers.

To run `fix_db2_schema.sql` script:

1. Install Gentran Integration Suite, Release 4.3 build 4316 or later.

2. Apply the new schema changes by running `fix_db2_schema.sql` script.

   ```
   cd <install_dir>/bin ./db_execFile.sh –i
   <install_dir>/bin/sql/fix_db2_schema.sql -o <output_file> -j -s -p
   ```

   The script will:

   - Rename the affected tables and indexes
   - Recreate the affected tables and indexes with the correct datatypes.
   - Migrate the data from the renamed tables to the recreated tables.

3. After verifying the changes, run drop statements to drop the old tables.

The old tables can remain in the system, but occupies additional database space. The `fix_db2_schema.sql` script contains commented statements to drop the affected tables. It is recommended to run these statements manually after verifying that data was migrated successfully.

Installing a Hot-Fix (Cluster)

After you install Gentran Integration Suite you may need to install a hot-fix. A *hot-fix* is one or more fixes applied to a specific existing patch.

Before Installing a Hot-Fix

Before you can install a hot-fix developed for your company, you must have completed the following:

- Received the case ID number from Sterling Commerce Customer Support
- Created a full backup of Gentran Integration Suite
- Created a full backup of your database

Hot-Fix Installation

To install a hot-fix on a UNIX or Linux system:

1. Log in to the computer that you are installing the hot-fix on.
2. Is the database password encrypted? If **Yes**, decrypt the password. For more information about decrypting database password, refer *Decrypting Database Passwords (UNIX)* on page 12.

   Apply the hot-fix to node 1 first, and then to the subsequent nodes: node 2, node 3, etc. For node 1, REINIT_DB is true in *install_dir*/install/properties/sandbox.cfg. For subsequent nodes, REINIT_DB is false, which prevents database updates from repeating on each node's hot-fix installation.
3. At the command line, type `ftp theworld.stercomm.com`.
4. Type your user name and password. If you do not know your user name and password, contact Sterling Commerce Customer Support.
5. Type `bin` and press **Enter** to select Binary as your transfer mode.
6. At the FTP prompt, type `get ccaseid.jar`, where *caseid* is the ID number you received from Customer Support. For example, c123.jar, where 123 is the ID number.

   Note: You can put the file to any directory for which you have write permission.
7. Shut down Gentran Integration Suite.
8. Change to the *install_dir*/bin directory.
9. Type the following command to install the hot-fix:

   ```
   InstallService.sh absolutePath/ccaseid.jar
   ```

   Caution: You may need to complete this step twice depending on the patch. Read the output from the `InstallService.sh` script carefully to see if you need to complete this step twice.
10. If you decrypted the database password in step 2, re-encrypt the password. For more information about encrypting database password, refer *Encrypting Database Passwords (UNIX)* on page 12.
11. Restart Gentran Integration Suite.
12. In the *install_dir*/bin directory, run the `dump_info.sh` command to verify that the hot-fix was successfully installed.
13. After installing the hot-fix, run the `startCluster.sh nodeNumber` command to configure the node to a cluster node. For example, if a node was node 2 before the hot-fix, run the `startCluster.sh 2` command.

    Note: Ensure that you run `startCluster.sh nodenumber false` command to prevent configuration changes that may affect the system. Refer to *Custom Configurations* on page 34 before configuring the cluster environment.
14. Run the `run.sh` command in the *install_dir*/bin directory to start the server.

Hot-Fix Package Delivery Method

The hot-fix package delivery method has changed effective Gentran Integration Suite, Release 4.3 Build 4324 onwards. The hot-fix package will be delivered as a jar file that contains only the files that were modified. However, the installation procedure for a hot-fix remains the same. Refer to *Hot-Fix Installation* on page 40 for hot-fix installation procedure.

The following list describes the features of the new hot-fix package model:

- Modified components are packaged as an installable file (jar).
- Hot-fix version is maintained in the hotfix.properties file. It does not update the SI_VERSION table.

  Run `dumpinfo.sh` command to display the hot-fix version. You can also verify the hot-fix version in Gentran Integration Suite Support user interface page.
- Size of the hot-fix package is small.
- Hot-fix must be installed on the same build version that was used to build it. For example, if a test system is on Gentran Integration Suite, Release 4.3 Build 4324 and the hot-fix is built for 4324, it can be installed on that test system. However, if the production system is on Gentran Integration Suite, Release 4.3 Build 4323, you must apply Gentran Integration Suite, Release 4.3 Build 4324 prior to applying the hot-fix.
- You can locate the hot-fix read me file in the Gentran Integration Suite root (*install_dir*) directory. For example, *install_dir*/hotfix_readme.txt.
- If you have Sterling File Gateway installed in your environment, the hot-fix for Sterling File Gateway is installed automatically.

Performing Checksum using DB Checksum Tool

A checksum is a simple redundancy check used to detect errors in data. In Gentran Integration Suite 4.3, a verification process is used to compare the checksum between the existing default resource and the resource added after applying a patch or upgrading. The DB Checksum tool, a resource difference tool generates a granular report of the changes in the system that was not permitted to be set as defaults.

The DB Checksum tool generates the difference in resource checksum between the default resource and the latest system resource from the database.

To run DB Checksum tool, do the following:

1. Navigate to the `<`*`install_dir`*`>/bin` directory.

2. Run the following command from the `<install_dir>/bin` directory:

   ```
   db_checksum_tool.sh [-d] [-i [1 | 2 | 3 | 4 | 5]] [-r [wfd | map | schema |
   sii | template]] [-o <output file>] [-g] [-h]
   ```

   where:

   `-d` is the mode to dump the difference of resource checksum between the default resource and latest system resource.

   `-i` is the resource type integer (optional).

   `1` is WFD

   `2` is MAP

   `3` is SCHEMA

   `4` is SII

   `5` is TEMPLATE

   `-r` is the resource name (optional).For example, wfd, map, schema, sii, or template.

   `-o` is the file name to output all the messages (optional).

   `-g` is the file name that lists all the ignored resources (optional).

   `-h` is the help screen.

3. The DB Checksum tool performs the relevant checksum operation based on the command options and generates the output message.

Installing a Perimeter Server in a Clustered UNIX or Linux Environment

Installing a Gentran Integration Suite perimeter server in a clustered UNIX or Linux environment includes the following tasks:

- ✦ *Setting Up Perimeter Servers with Gentran Integration Suite* on page 42
- ✦ *Installing a Perimeter Server in a More Secure Network (UNIX/Linux Clustered)* on page 43
- ✦ *Installing a Perimeter Server in a Less Secure Network (UNIX/Linux Clustered)* on page 44
- ✦ *Installing Patches in a Perimeter Server UNIX or Linux Environment* on page 45
- ✦ *Starting and Stopping Perimeter Servers in UNIX or Linux* on page 46
- ✦ *Reducing Perimeter Server Security Vulnerabilities* on page 47

Setting Up Perimeter Servers with Gentran Integration Suite

Using a perimeter server is optional.

A *perimeter server* is a software tool for communications management that can be installed in a DMZ. The perimeter server manages the communications flow between outer layers of your network and the

TCP-based transport adapters. A perimeter server can solve problems with network congestion, security, and scalability, especially in high-volume, Internet-gateway environments. A perimeter server requires a corresponding perimeter client.

The Gentran Integration Suite installation program installs a perimeter client and a local mode server. The local mode server is useful for testing purposes or in environments that do not require a secure solution. However, if you require high-volume, secure connections, you must install a perimeter server in a remote zone. This remote zone can be more or less secure than your integration server.

When you install a perimeter server, use these guidelines:

- Licensing for a perimeter server is determined by the licensing restrictions on the corresponding B2B adapters.
- Each perimeter server is limited to two TCP/IP addresses – internal interface and external interface. *Internal interface* is the TCP/IP address that the perimeter server uses to communicate with Gentran Integration Suite. *External interface* is the TCP/IP address that the perimeter server uses to communicate with trading partners.

  To use additional TCP/IP addresses, install additional perimeter servers.
- You can have multiple perimeter servers installed on the same computer interacting with one instance of Gentran Integration Suite. To install a perimeter server on a computer with an existing instance, install the new perimeter server in a different installation directory.
- The combination of internal TCP/IP address and port must be unique for all perimeter servers installed on one computer.
  - If a perimeter server is installed using the wildcard address, then all ports must be unique.
  - If a perimeter server is installed using the wildcard address, then its port is not available for use by adapters that use the server or any other perimeter server on that computer.
  - The internal and external interface may use the same TCP/IP address. However, the port used by the perimeter server is not available to the adapters that use the server.

Installing a Perimeter Server in a More Secure Network (UNIX/Linux Clustered)

To install a perimeter server in a UNIX or Linux clustered environment:

1. Insert the installation CD in the appropriate drive.
2. Copy the ps_2000.jar installation files from the installation CD to your home directory or base directory. If you are using FTP to copy the file, make sure your session is set to binary mode.
3. To begin the installation, type the absolute path to the following jar file:

   ```
   absolutePath/bin/java -jar install_dir/packages/ps_2000.jar
   ```

   The program verifies the operating system and required patch level and the location and version of the JDK.
4. Enter the full path name of the installation directory.

5. If there is an existing installation in the directory you specify, you can update it using the same settings.

   At the prompt *There is an existing install at that location, update it while keeping existing settings?*, if you type **yes** and press **Enter**, the installation will proceed without additional entries.

   Note: If you want to change any of the settings, you must use a new directory, or delete the old installation before performing the new installation. You cannot overwrite an existing installation, and you cannot use an existing directory that does not contain a valid installation. The existing installation must be Gentran Integration Suite 4.3 or later.

6. Confirm that the installation directory is correct.

   The program verifies the amount of available disk space.

7. At the prompt *Is this server in a less secure network than the integration server?*, type **No** and press **Enter**.
8. At the prompt *Will this server need to operate on specific network interfaces?*, if you type **yes** and press **Enter**, the program returns a list of the available network interfaces available on your host. Select the interfaces for the server to use.
9. Enter the TCP/IP address or DNS name that the integration server (Gentran Integration Suite) will listen on for the connection from this server.
10. Verify the TCP/IP address or DNS name.
11. Enter the port that the integration server (Gentran Integration Suite) will listen on for the connection from this server. The port number must be higher than 1024.
12. Enter the local port that the perimeter server will use for the connection to the integration server (Gentran Integration Suite). The port number must be higher than 1024, except specify a port of zero if you want the operating system to select any unused port.
13. Verify the port.

    When the perimeter server is installed, the following message is displayed:

    Installation of Perimeter Service is finished

14. Change to the installation directory.
15. Run the `startupPs.sh` command to start the perimeter server.

Installing a Perimeter Server in a Less Secure Network (UNIX/Linux Clustered)

To install a perimeter server in a UNIX or Linux clustered environment:

1. Insert the installation CD in the appropriate drive.
2. Copy the ps_2000.jar installation files from the installation CD to your home directory or base directory. If you are using FTP to copy the file, make sure your session is set to binary mode.

3. To begin the installation, type the absolute path to the following .jar file:

   ```
   absolutePath/bin/java -jar install_dir/packages/ps_2000.jar
   ```

   The program verifies the operating system and required patch level and the location and version of the JDK.
4. Enter the full path name of the installation directory.
5. If there is an existing installation in the directory you specify, you can update it using the same settings.

   At the prompt *There is an existing install at that location, update it while keeping existing settings?,* if you type **yes** and press **Enter**, the installation will proceed without additional entries.

   Note: If you want to change any of the settings, you must use a new directory, or delete the old installation before performing the new installation. You cannot overwrite an existing installation, and you cannot use an existing directory that does not contain a valid installation. The existing installation must be Gentran Integration Suite 4.3 or later.
6. Confirm that the installation directory is correct.

   The program verifies the amount of available disk space.
7. At the prompt *Is this server in a less secure network than the integration server?,* type **Yes** and press **Enter**.
8. At the prompt *Will this server need to operate on specific network interfaces?*, if you type **yes** and press **Enter**, the program returns a list of the available network interfaces available on your host. Select the interfaces for the server to use.
9. Enter the TCP/IP address or DNS name for the internal interface to use to communicate with the integration server (Gentran Integration Suite.). Press Enter to use a wildcard for this address.
10. Verify the TCP/IP address or DNS name for the internal interface.
11. Enter the TCP/IP address or DNS name for the external interface to use to communicate with trading partners. Press Enter to use a wildcard for this address.
12. Verify the TCP/IP address or DNS name for the external interface.
13. Enter the port that the perimeter server will listen on for the connection from integration server (Gentran Integration Suite). The port number must be higher than 1024.
14. Verify the port.

    When the perimeter server is installed, the following message is displayed:

    Installation of Perimeter Service is finished
15. Change to the installation directory.
16. Run the `startupPs.sh` command to start the perimeter server.

Installing Patches in a Perimeter Server UNIX or Linux Environment

Remote perimeter servers are not automatically updated by a service pack or patch. You must reinstall the perimeter server using the new perimeter server installation file supplied with the service pack or patch.

Updating a Remote Perimeter Server in a Clustered UNIX or Linux Environment

To update a remote perimeter server in a clustered UNIX or Linux environment:

1. Update your installation of Gentran Integration Suite 4.3 with the latest maintenance patch. Obtain the maintenance patch file from the Sterling Commerce Support on Demand Web site, at https://support.sterlingcommerce.com. These patch files have a name that identifies a build number. For example, si_43_build_4307.jar. For more information, refer to *Installing the Current Maintenance Patch in UNIX or Linux* on page 35.
2. Locate the perimeter server patch file (ps_*version_number*.jar file) in the *install_dir*/packages directory of your installation of Gentran Integration Suite 4.3. These patch files have a name that identifies a version number. For example, ps_2006.jar.
3. Copy the perimeter server patch file to the home directory or base directory on the remote server.
4. Stop the perimeter server using the `stopPs.sh` command.
5. To begin the installation, type the following command:

   ```
   absolutePath/bin/java -jar ps_version_number.jar
   ```

   `absolutePath` is the directory name where the Java version is installed.

   The program verifies the operating system and required patch level and the location and version of the JDK.
6. Type the full path to the installation directory. If you do not want to change any settings for your perimeter server, specify the same directory where the remote perimeter server was originally installed.
7. If there is an existing installation in the directory you specify, you can update it using the same settings.

   At the prompt *There is an existing install at that location, update it while keeping existing settings?*, if you type **yes** and press **Enter**, the installation will proceed without additional entries.

   Note: If you want to change any of the settings, you must use a new directory, or delete the old installation before performing the new installation. You cannot overwrite an existing installation, and you cannot use an existing directory that does not contain a valid installation. The existing installation must be Gentran Integration Suite 4.3 or later.

   When the perimeter server is installed, the following message is displayed:

   Installation of Perimeter Service is finished
8. Change to the installation directory.
9. Run the `startupPs.sh` command to start the perimeter server.

Starting and Stopping Perimeter Servers in UNIX or Linux

To start a perimeter server in UNIX or Linux:

1. Change the directory to *install_dir*/bin.
2. Run the `startupPs.sh` command.

To stop a perimeter server in UNIX or Linux:

1. Change the directory to *install_dir*/bin.
2. Run the `stopPs.sh` command.

Reducing Perimeter Server Security Vulnerabilities

When Gentran Integration Suite is deployed with a remote perimeter server in a more secure network zone, there is a security vulnerability. An intruder may compromise the host where the proxy resides, and take over the persistent connection to the perimeter server residing in the more secure zone. If this happens, the perimeter server will relay all the intruder's network requests past the firewall into this internal zone.

To prevent an intrusion, limit the activities the remote perimeter server can perform on behalf of the proxy to specifically those activities that the proxy needs to do for its operation.

Control these limitations by using a configuration residing in the secure network zone with the remote perimeter server, inaccessible by the proxy that could become compromised.

Granting Permissions for Specific Activities By a Perimeter Server

1. Install a remote perimeter server, choosing the option for a more secure network zone. Refer to the full perimeter server installation instructions, as described in *Installing a Perimeter Server in a More Secure Network (UNIX/Linux Clustered)* on page 43.
2. At the installation prompt *Is this server in a less secure network than the integration server?*, select **No**, which is the option for a more secure network zone.
3. In the perimeter server installation directory there will be a text file named restricted.policy that must be customized. Its initial contents are:

```
// Standard extensions get all permissions by default grant codeBase
"file:${{java.ext.dirs}}/*" {permission java.security. AllPermission;};

 grant {
    // Grant all permissions needed for basic operation.

    permission java.util.PropertyPermission "*", "read";

    permission java.security.SecurityPermission "putProviderProperty.*";

    permission java.io.FilePermission "-", "read,write";
    permission java.io.FilePermission ".", "read";

    // Needed to allow lookup of network interfaces.
    permission java.net.SocketPermission "*", "resolve";
 };

 grant {
    // Adjust for your local network requirements.

    // Needed to connect out for the persistent connection.  Do not remove this.
    permission java.net.SocketPermission "localhost:12002", "connect";

   // For each target FTP Server that a FTP Client Adapter will connect to in passive
mode.
    //
    // permission java.net.SocketPermission "ftphost:21", "connect"; // Control
connection.
   // permission java.net.SocketPermission "ftphost:lowPort-highPort", "connect"; //
Passive data connections.

    // For each target FTP Server that a FTP Client Adapter will connect to in active
mode.
    //
    // permission java.net.SocketPermission "ftphost:21", "connect"; // Control
connection.
    // permission java.net.SocketPermission "localhost:lowPort-highPort", "listen";
// Active data port range.
    // permission java.net.SocketPermission "ftphost", "accept"; // Active data
connections.

    // For each target HTTP Server that an HTTP Client Adapter will connect to.
    //
    // permission java.net.SocketPermission "htttphost:443", "connect";

    // For each target C:D snode that the C:D Server Adapter will connect to.
    //
    // permission java.net.SocketPermission "snode:1364", "connect";
};
```

4. Edit this file to add permission lines for each back-end server that you intend to allow the proxy to access. There are commented out examples for each type of server.

   The first two grant sections are required for correct perimeter server operation. Do not modify these sections.

Example

The following example grants permission to a target FTP Server:

Note: In the example, servers are configured to listen on the following ports: 33001 (for FTP), 33002 (for HTTP), and 1364 (for C:D). These port numbers can be edited.

```
// To restrict or permit the required Host/Server to communicate with the  PS, update
the “ftphost/ htttphost/snode” with
      that of the Server IP and provide the appropriate PORT number where the Server
will listen. //

   // For each target FTP Server
   // permission java.net.SocketPermission "10.117.15.87:33001", "connect"; //
Control connection.
   // permission java.net.SocketPermission "10.117.15.87:lowPort-highPort",
"connect"; // Passive data connections.
   // 10.117.15.87 indicates IP of the FTP Server for which the permission is granted
by PS for communicating with client //

   // For each target HTTP Server
   //
   // permission java.net.SocketPermission "10.117.15.87:33002", "connect";
   // 10.117.15.87 indicates IP of the HTTP Server for which the permission is granted
by PS for communicating with client //


   // For each target C:D snode
   //
   // permission java.net.SocketPermission "snode:1364", "connect";
   //  10.117.15.87 indicates IP of the Connect Direct Node for which the permission
is granted by PS for communication //
```

5. Turn on restrictions. In the install directory is the perimeter server settings file:

   remote_perimeter.properties.

   Edit it to change the "restricted" setting to a value of true.

6. In the future, any attempt by the perimeter server to access disallowed network resources will be rejected and logged in the perimeter server log written to the perimeter server installation directory.

Performing DNS Lookup on Remote Perimeter Server

By default, a perimeter server performs DNS lookup in the main server JVM. If you have limited DNS in your secure area, you can configure the remote perimeter server to look up trading partner addresses in the DMZ.

To enable DNS lookup to occur at the remote perimeter server, edit the perimeter.properties file to change the following parameter:

Note: Do not edit the properties files. Make all the changes in the customer_overrides.properties file.

Property Name	Description
<*psname*>.forceRemote DNS	Enables remote DNS resolution for the perimeter server, where <*psname*> is the name of the perimeter server. Valid values: ◆ true - enable remote DNS resolution ◆ false - disable remote DNS resolution

Postinstallation in a Clustered UNIX or Linux Environment

After installing Gentran Integration Suite, you should complete the following tasks:

- *Starting Gentran Integration Suite in UNIX or Linux* on page 50
- *Accessing Gentran Integration Suite* on page 50
- *Validating the Installation* on page 52
- *Downloading Gentran Integration Suite Tools* on page 52
- *Performing Initial Administrative Setups in Gentran Integration Suite* on page 52
- *Stopping Gentran Integration Suite* on page 53

Starting Gentran Integration Suite in UNIX or Linux

To start Gentran Integration Suite in a clustered UNIX or Linux environment, follow these steps:

1. Change the directory to *install_dir*/bin.
2. Run the `run.sh` command.
3. Enter the passphrase that you supplied during installation. If you receive a message about an invalid or corrupt license file, see the section *Troubleshooting: UNIX or Linux Environment*.

   When startup is complete, a message like the following is displayed:

   Open your Web browser to http://host:port/dashboard, where *host:port* is the host and port number where Gentran Integration Suite resides on your system.

   Make a note of the URL address so you can access Gentran Integration Suite later.

   The system returns you to a UNIX prompt.

Accessing Gentran Integration Suite

To log in to Gentran Integration Suite the first time, follow these steps:

1. Be sure that Gentran Integration Suite is started and running.
2. Open a browser window and type the address displayed at the end of startup.
3. The login page displays.
4. Type the default user ID (**admin**) and password (**password**). The default login is at an administrative level. One of your first tasks as an administrator is to change the administrative password and to register other users with other levels of permission.

Technical Note: Changes to Network Interface Bindings

To increase the security of the Administrator Console user interface, Gentran Integration Suite version 4.3 binds only to specific network interfaces. By default, previous versions had been bound to all network interfaces. After installing, if the URL for returns *Page cannot be displayed*, you can adjust property settings to correct the problem.

1. On the server where Gentran Integration Suite resides, edit the noapp.properties.in file.
   a. Locate the **admin_host** parameter. The default settings are as follows:

      hostname1 is the name of primary network interface, the one given highest priority by Gentran Integration Suite.

      localhost is the name of the network interface on the server where Gentran Integration Suite resides.

      ```
      Default entries
      admin_host.1    = hostname1
      admin_host.2    = localhost
      ```

   b. Correct the parameters as necessary.

      If no interface is being displayed, edit *hostname1* so that it correctly identifies the primary network interface that accesses Gentran Integration Suite.

      If an additional network interface needs to access Gentran Integration Suite, add an additional *admin_host* entry, as shown below.

      ```
      Edited entries
      admin_host.1    = hostname1
      admin_host.2    = localhost
      admin_host.3    = hostname2
      ```

2. Stop Gentran Integration Suite.
3. Run the `setupfiles.sh` utility located in the *install_dir*/bin directory.
4. Restart Gentran Integration Suite.

For the Dashboard user interface, Gentran Integration Suite version 4.3 provides unrestricted binding to network interfaces through the perimeter server. To restrict access to the Dashboard user interface, you can adjust property settings so that only one network interface accesses Gentran Integration Suite.

1. On the server where Gentran Integration Suite resides, edit the perimeter.properties.in file.
   a. Locate the **localmode.interface** parameter. The default setting is unrestricted, as shown below.

      ```
      Unrestricted Setting (Default)
      localmode.interface=*
      ```

   b. To restrict access to the Dashboard, type the network interface that you want Gentran Integration Suite to support.

      ```
      Restricted Setting
      localmode.interface=hostname1
      ```

2. Stop Gentran Integration Suite.
3. Run the `setupfiles.sh` utility located in the *install_dir*/bin directory.
4. Restart Gentran Integration Suite.

Validating the Installation

After you install, start, and log in to Gentran Integration Suite the first time, you can validate the installation by testing a sample business process. Follow these steps:

1. Open a browser window and type the address for Gentran Integration Suite. This address was displayed at the end of startup.
2. Enter your user login and password.
3. From the **Administration** menu, select **Business Processes** > **Manager**.
4. In the Process Name field, type **Validation_Sample_BPML** and click **Go!**
5. Click **execution manager**.
6. Click **execute**.
7. Click **Go!** The *Status: Success* message displays in the upper left side of the page.

Downloading Gentran Integration Suite Tools

Gentran Integration Suite includes tools that run on a desktop or personal computer. After you install, start, and access Gentran Integration Suite, you can install the following tools by downloading them from within Gentran Integration Suite:

Note: MESA Developer Studio and Reporting Services are optional features that are purchased separately from Gentran Integration Suite. These features each require a separate license in addition to your license for Gentran Integration Suite.

- Map Editor and associated standards
- Graphical Process Modeler
- Web Template Designer
- (If licensed) MESA Developer Studio plug-ins, including:
  - MESA Developer Studio Software Development Kit (SDK)
  - MESA Developer Studio Skin Editor
- (If licensed) Reporting Services, which requires MESA Developer Studio if you want to use the plug-ins to create fact models and custom reports.

Conflicting IP addresses can cause problems when you download a desktop tool. See the section *Troubleshooting: UNIX or Linux Environment*.

Performing Initial Administrative Setups in Gentran Integration Suite

At this point, your installation is complete, and you can run Gentran Integration Suite. If you are installing Gentran Integration Suite for the first time, you need to perform some initial administrative setups before users can use Gentran Integration Suite. For example, the system administrator for Gentran Integration Suite must register users and grant permissions.

Also, it is recommended that you run several performance reports so that benchmarks are established for tuning the system in the future. For more information about preparing your Gentran Integration Suite system for effective performance tuning, refer to the performance tuning methodology information in the *Performance and Tuning Guide*.

Stopping Gentran Integration Suite

To stop Gentran Integration Suite in a clustered UNIX or Linux environment, you can either run a soft stop or a hard stop script.

A soft stop halts Gentran Integration Suite after all the business processes finish running. To run a soft stop, choose one of the following procedures:

- Open your browser and access Gentran Integration Suite. From the **Administration** menu, select **Operations > System > Troubleshooter**. Click **Stop the System**.
- From the UNIX command line, change the directory to *install_dir*/bin. Run the `softstop.sh` command. Then type your passphrase.

Caution: Running `softstop.sh` command in a multiple node (clustered) environment will suspend all scheduled business processes. It is recommended to run the `hardstop.sh` command when stopping individual nodes of a cluster.

A hard stop halts Gentran Integration Suite without waiting for business processes to finish. To run a hard stop, use the following procedure:

1. From the UNIX command line, change the directory to *install_dir*/bin.
2. Run the `hardstop.sh` command.

Caution: Running a hard stop could result in loss of data in unfinished processes.

Managing Nodes in a Cluster

You can add or remove nodes in a cluster environment. The following prerequisites should be considered before performing any modification in the cluster environment:

- New nodes should have the same range of ports available as the current nodes.
- Gentran Integration Suite license file should be updated to include the IP address of the new nodes.
- Directory structure on the new nodes should match with the directory structure of the existing nodes.
- Perimeter servers should be updated with the new IP addresses to ensure proper configuration.
- Any adapters, services, or business processes assigned to or scheduled to run on the node being removed should be assigned to run on other nodes.

The following sections provide the necessary steps to add a node and remove a node from the cluster:

- *Adding a Node* on page 54
- *Removing a Node* on page 54

Adding a Node

To add a node into the cluster:

Note: You do not need to stop the cluster environment while adding a new node.

1. Install a new Gentran Integration Suite node to be added into the cluster with the `–cluster` option during installation. To install a new node, refer *Running the Upgrade Program in UNIX or Linux* on page 26. Ensure that the new node being added is not a primary node.
2. Update `jgroups_cluster.properties` file and `jgroups_cluster.properties.in` file with the new node details.
3. Configure the new node by running the command `startcluster.sh` ***`nodeNumber`*** from the *install_dir*/bin directory. The node number should be greater than 1.

Note: You should run `startCluster.sh` command only after you install Gentran Integration Suite. You should not run `startCluster.sh` command when you restart a Gentran Integration Suite instance. However, if you have installed a patch or a hot-fix, refer *Custom Configurations* on page 34 to start the cluster without updating the database settings.

4. Start the new node by running the command `run.sh` from the *install_dir*/bin directory.

Removing a Node

To remove a node from the cluster:

1. Reassign or stop any adapters, services, or business processes assigned to or scheduled to run on the node being removed.

Note: It is recommended that you restart the Gentran Integration Suite cluster environment after removing the node from the cluster. Refer *Starting or Stopping the Cluster Environment* on page 33 to restart Gentran Integration Suite cluster environment.

2. Perform backup of the node being removed.
3. Edit `jgroups_cluster.properties` file and `jgroups_cluster.properties.in` file in all nodes to remove the IP address of the node being removed.
4. Uninstall Gentran Integration Suite in the node being removed. To stop a node and uninstall Gentran Integration Suite from a node, refer *Uninstalling Gentran Integration Suite from a Clustered UNIX or Linux Environment* on page 54.

Uninstalling Gentran Integration Suite from a Clustered UNIX or Linux Environment

When you uninstall Gentran Integration Suite, the following components are affected:

- Gentran Integration Suite application is automatically removed from the server.

Additionally, you may perform the following tasks:

- Manually remove Attunity Data Connect

  For more information, refer to product information provided with Attunity Data Connect software.
- Manually remove the JDK that was installed
- Manually remove any desktop tools that were downloaded
- Free any database space in Oracle, Microsoft SQL Server, or DB2 databases

To uninstall Gentran Integration Suite from a UNIX or Linux environment, follow these steps:

1. Stop Gentran Integration Suite and wait for shutdown to complete. If you begin removing files before all business processes and Gentran Integration Suite are stopped, you may be unable to remove Gentran Integration Suite successfully.
2. Back up the file system and database. This step is optional; however, by backing up the file system and database, you are ensured that Gentran Integration Suite is completely recoverable.
3. Open the parent directory of your installation directory (*install_dir*).
4. Enter the following command:

   ```
   rm -rf install_dir
   ```
5. If you use an Oracle, Microsoft SQL Server, or DB2 database, these remain intact even after you remove Gentran Integration Suite from the server. If you no longer want to reference the data, contact your database administrator about removing unwanted tables and recovering the database space where Gentran Integration Suite used to reside.
6. (Optional) Manually remove Attunity Data Connect at the server level and on PCs.
7. (Optional) Manually remove the JDK.
8. After you remove Gentran Integration Suite from the server, you can remove Eclipse, and any tools that were downloaded.

   Note: You can remove Eclipse plug-ins without removing Eclipse. Refer to the Eclipse on-line help for information about removing the plug-ins.

   Note: MESA Developer Studio and Reporting Services are optional features that are purchased separately from Gentran Integration Suite. These features each require a separate license in addition to your license for Gentran Integration Suite.

   - Map Editor and associated standards

     Refer to the *Map Editor Guide* for information about removing the Map Editor.
   - Graphical Process Modeler

     Refer to the *Graphical Process Modeler Guide* for information about removing the Graphical Process Modeler.
   - Web Template Designer

     Refer to the *Web Extensions Guide* for information about removing the Web Template Designer.

- (If licensed) MESA Developer Studio plug-ins, including the Software Development Kit (SDK) and Skin Editor.

  To remove these items, follow this procedure:

  a. Using Windows Explorer, locate the installation directory of Eclipse (For example, C:\Program Files\eclipse).

  b. Navigate to the features directory and delete the folders for anything from Sterling Commerce, gisstudio, skineditor, and servicesdk.

  c. Navigate to the plugins directory and delete the folders for anything from Sterling Commerce, gisstudio, skineditor, and servicesdk.

- (If licensed) Reporting Services, which requires MESA Developer Studio if you want to use the plug-ins to create fact models and custom reports.

Troubleshooting: Clustered UNIX or Linux Environment

Situation	Message or Symptom	Explanation/Resolution
Installing	You encounter errors or problems during installation.	**Explanation** Installation creates a log file. **Resolution** Examine the log file generated during installation: - *install_dir*/InstallSI.log
Installing	When you entered an absolute path during installation, a message indicated that the command was not found.	**Explanation** You entered an incorrect path. Check your typing or check the information. **Resolution** Enter the correct path.
Installing	During installation, you entered the absolute path to the license file. However, a message indicates that the license file cannot be found.	**Explanation** You either did not obtain the license file, the license file is corrupt, or you downloaded the license file to a PC but have not moved it to the server. **Resolution** If you need to obtain the license file, see the section *Obtaining a License File*. If the license file resides on a PC, save the license file to the server.

Situation	Message or Symptom	Explanation/Resolution
Installing	Memory and ulimit errors	**Explanation** The installation fails with memory and ulimit errors. **Resolution** ◆ Refer Viewing or Editing Performance Configuration Settings in *Performance Management* documentation and modify your memory settings accordingly. ◆ Refer *Checklist for UNIX or Linux Preinstallation* on page 15 and tune `ulimit` settings.
Installing a desktop tool or resource	Cannot download any of the following: **Note:** MESA Developer Studio and Reporting Services are optional features that are purchased separately from Gentran Integration Suite. These features each require a separate license in addition to your license for Gentran Integration Suite. ◆ Map Editor and associated standards ◆ Graphical Process Modeler ◆ Web Template Designer ◆ (If licensed) MESA Developer Studio plug-ins (Software Development Kit (SDK), Skin Editor) ◆ (If licensed) Reporting Services, which requires MESA Developer Studio if you want to use the plug-ins to create fact models and custom reports.	**Explanation** When you install Gentran Integration Suite, system files are created that contain an internal IP address. If you install Gentran Integration Suite behind a firewall, and your firewall is configured to accept an external IP address from a client computer, you may not be able to download the desktop tools and resources. The firewall will reject the internal IP address from a client residing outside of the firewall. **Resolution** Modify the system files that contain the invalid IP address. Follow these steps: 1 Navigate to the *install_dir*/bin directory. 2 Enter the following command followed by the external IP address: **patchJNLP.sh *external_IP address*** 3 Stop Gentran Integration Suite. 4 Restart Gentran Integration Suite.
Accessing	Attempts to access the URL for Gentran Integration Suite display the message*: Page cannot be displayed*	See *Technical Note: Changes to Network Interface Bindings* on page 50.

Chapter 4

Post-Upgrade Processes

Adding Third-Party Libraries

If you added third-party libraries to configure adapters for the previous release, you need to add each of the libraries again after you complete the upgrade process for release 4.3. See the documentation for each third party adapter you use.

Configuring Customer Overrides File When You Have a Firewall between Nodes (Build 4324 or higher)

If you have configured a firewall between nodes that blocks ports outside of the port range assigned to Gentran Integration Suite, perform the following task on all nodes:

1. Navigate to the *install_dir*/install/properties directory and locate (or create, if necessary) the customer_overrides.properties file.
2. Open the customer_overrides.properties file using a text editor.
3. Add the following properties:

   ```
   noapp.jnp_host= <host_name>
   noapp.jnprmiport=<port_number_1>
   noapp.jnprmiport2=<port_number_2>
   noapp.jndirmiport=<port_number_3>
   noapp.useSocketFactories=true
   ops.jnp_host= <host_name>
   ops.jnprmiport=<port_number_1>
   ops.jnprmiport2=<port_number_2>
   ops.jndirmiport=<port_number_3>
   ops.useSocketFactories=true
   ```

   This increases the number of threads used by the system.

4. Save and close the customer_overrides.properties file.
5. Stop Gentran Integration Suite and restart it to apply the changes.

Configuring Services and Adapters

You may need to reconfigure services and adapters after an upgrade. During an upgrade, packages for services and adapters are reprocessed to update the service configurations.

After an upgrade, the configurations of default adapters and services are re-set to their default configurations. This includes directory paths, which are restored to their default paths. You need to reconfigure those adapters and services, which include, but are not limited to:

- All default FTP adapters
- All default SFTP adapters
- Connect:Enterprise UNIX Server Adapter
- OdetteFTP Adapter
- SAP Suite Adapter
- SWIFTNet Client Service
- SWIFTNet Server Adapter

If you modified the standard configuration for a service or adapter, you may need to reconfigure or reactivate the service or adapter following an upgrade. You may also need to reconfigure adapters that used directories or scripts in the installation directory of your previous release.

Examples of services and adapters that commonly need to be reconfigured following an upgrade include:

- SyncEngine HTTP Server adapter
- Federation adapter
- FTP adapter
- System services, like the Alert service and the BP Fault Log adapter

These are just examples. Always check the configuration of your adapters following an upgrade.

The following adapters need special consideration following an upgrade:

- *JDBC Adapter and Lightweight JDBC Adapter* on page 59
- *File System Adapter and Command Line2 Adapters* on page 62

JDBC Adapter and Lightweight JDBC Adapter

Storage locations of the database pool properties that allow the JDBC adapter and the Lightweight JDBC adapter to communicate with your external database have been streamlined. The poolManager.properties file has been eliminated and some of its pool properties are now included in the jdbc.properties file, along with some new properties. You will need to manually update your existing jdbc_customer.properties.in file to add some new database pool properties. If you do not have a jdbc_customer.properties.in file, create one since customer.properties are not affected by product updates. The specific actions necessary depend on your current installation.

Upgrading from Gentran Integration Suite 3.0

If you are upgrading from version 3.0 and you used the JDBC adapter or the Lightweight JDBC adapter in that version, perform the following steps:

1. Save a copy of the jdbc.properties file and the poolManager.properties file from the earlier system. You will need any properties settings you customized for your external database.
2. Set up your Lightweight JDBC adapter or JDBC adapter according to the instructions in the *Lightweight JDBC Adapter* topic or the *JDBC Adapter* topic in Gentran Integration Suite Documentation site.

Upgrading from Gentran Integration Suite 3.1

If you are upgrading from version 3.1 and you used a jdbc_customer.properties.in file in that version, perform the following steps:

1. Copy the jdbc_customer.properties.in file from Gentran Integration Suite 3.1 installation to the *install_dir*/**properties** directory in Gentran Integration Suite 4.3 installation. You will edit this copied file in the following steps.
2. Open the *install_dir*/**properties**/**jdbc_customer.properties.in** file in a text editor.

3. Add the following properties:

   Note: In the following property names, replace *databasePool* with the name of the pool.

Property	Description
databasePool.factory	Always enter: `com.sterlingcommerce.woodstock.util.frame.jdbc.ConnectionFactory`.
databasePool.behaviour	Sets the behavior that a connection pool exhibits when it runs out of connections. This property replaces the databasePool.onEmpty property in the former poolManager.properties file. Valid values: ◆ 0–The pool returns, indicating to the software to abort its current action and try again later. This value corresponds to the value **return** in the *databasePool***.onEmpty** property. ◆ 1–The pool waits the number of milliseconds specified in *databasePool***.waittime** for a connection to be returned before indicating to the software to abort and try again. This value corresponds to the value **wait** in the *databasePool***.onEmpty** property. ◆ 2–The pool creates a buffered connection (a connection above the size specified in *databasePool*.**maxsize**). When using a setting of 2, the maximum number of connections for the pool is the value specified for *databasePool***.maxsize** plus the value specified for *databasePool***.buffersize** connections. This allows connections to be created under heavy demand. This value corresponds to the value **new** in the *databasePool***.onEmpty** property.
databasePool.buffersize	Number of extra connections that the connection pool can create above the value specified for *databasePool***.maxsize** to improve handling of unanticipated loads on the system. This property is only used if *databasePool***.behaviour** is set to **2**.
databasePool.maxsize	Maximum size of the database pool. This property was previously contained in the poolManager.properties file. This value must not exceed the value specified for the *databasePool***.maxconn** parameter in the jdbc.properties file.
databasePool.initsize	Initial size of the database pool. This property was previously contained in the poolManager.properties file.
databasePool.waittime	Amount of time (in milliseconds) to wait for a connection to become available before indicating to the software to abort the current action and try again later. This property is only used if *databasePool***.behaviour** is set to **1**.

   For more information, see the *Lightweight JDBC Adapter* topic or the *JDBC Adapter* topic in Gentran Integration Suite Documentation site.

4. Run the `setupfiles.sh` utility located in the /*install_dir*/bin directory of Gentran Integration Suite installation directory.
5. Stop and restart Gentran Integration Suite to use the updated settings.

If you are upgrading from version 3.1 and you used the JDBC adapter or the Lightweight JDBC adapter but you did not use a jdbc_customer.properties.in file in that version, perform the following steps:

1. Save a copy of the jdbc.properties file and the poolManager.properties file from Gentran Integration Suite 3.1 installation. You will need any properties settings you customized for your external database.

2. Set up your Lightweight JDBC adapter or JDBC adapter according to the instructions in the *Lightweight JDBC Adapter* topic or the *JDBC Adapter* topic in Gentran Integration Suite Documentation site.

File System Adapter and Command Line2 Adapters

You must configure your File System and Command Line2 adapters before you remove the previous release directory. Reconfigure any File System and Command Line2 adapters that were configured to use directories or scripts in the installation directory for the previous Gentran Integration Suite release. Ensure that you create new directories and save scripts outside of the release 4.3 installation directory and edit each configuration to use the appropriate directories and scripts.

Note: Creating directories and saving scripts outside of the release 4.3 installation directory makes future upgrade processes easier.

Note: As of Gentran Integration Suite 4.3, the Command Line2 adapter has replaced the Command Line adapter. To replace the Command Line adapter, follow the instructions in *Command Line Adapter* on page 62.

Command Line2 Adapter

If you are using the Command Line2 adapter and have located the CLA2Client.jar file anywhere other than the default location, you must replace it with the new version. For information about the default location and how to start the Command Line2 adapter, see the Command Line2 adapter information in the online Documentation site.

If you are upgrading to Gentran Integration Suite 4.3 from a version lower than 4.0.1 and are using the Command Line2 adapter, you must update the version of the CLA2Client.jar file with the CLA2Client.jar located in the *install_dir*/client/cmdline2 directory. If you installed the CLA2Client.jar file anywhere other than the default location, you must replace each copy of the file with the new version. If you only installed it in the default location, the update occurs automatically during the upgrade process.

Command Line Adapter

If you are upgrading to Gentran Integration Suite 4.3 from a version prior to 4.0 and are using the Command Line adapter, you must update the version of the CLAClient.jar file with the CLA2Client.jar located in the *install_dir*/client/cmdline2 directory. If you installed the CLAClient.jar file anywhere other than the default location, you must replace each copy of the file with the new version. If you only installed it in the default location, the update occurs automatically during the upgrade process.

Note: CLA instances are now pointing to the CLA2 Service definition. After importing old service instances of CLA onto Gentran Integration Suite 4.3, you need to reconfigure the imported CLA services to re-set the Remote Name and Remote Port service configuration parameters. For more information, refer to the documentation for the Command Line Adapter and Command Line2 Adapter.

Restoring Performance Tuning Configuration

To restore your original performance tuning configuration to the new release, Gentran Integration Suite provides the Performance Tuning Wizard. You use the wizard to re-enter the settings you saved earlier.

Note: Before completing this procedure, see *Final Upgrade Notes* on page 63.

To restore the performance tuning configuration:

1. From Gentran Integration Suite **Administration** menu, select **Operations** > **System** > **Performance** > **Tuning**.
2. Under Edit, click **Go!**
3. Complete the Performance Tuning Wizard, using the settings you obtained from the previous release.

Starting an Upgraded Cluster

After you upgrade all nodes of a cluster, configure the cluster using the following procedure:

1. Node 1

   Go to *install_dir*/bin of each node and run the command `startCluster.sh 1 false`

Note: You should run `startCluster.sh` command only after you install Gentran Integration Suite. You should not run `startCluster.sh` command when you restart a Gentran Integration Suite instance. However, if you have installed a patch or a hot-fix, refer *Custom Configurations* on page 34 to start the cluster without updating the database settings.

2. Nodes after node 1

   Go to *install_dir*/bin of each node and run the command `startCluster.sh (`*`node number`*`)`
3. Go to *install_dir*/bin of each node and run the command `run.sh`

Final Upgrade Notes

The upgrade is complete. At this point, you should download and apply the latest maintenance update from Support on Demand before using Gentran Integration Suite.

Note: The upgrade process enables services that might have been disabled before the upgrade. If you want to disable these services again, you must disable them in Gentran Integration Suite 4.3 after the upgrade process.

After you upgrade, do not use the previous release of Gentran Integration Suite. However, you should maintain your backup for future reference.

For additional information, see the following sections:

✦ *Changes to Network Interface Bindings* on page 64

Changes to Network Interface Bindings

To increase the security of the Administrator Console user interface, Gentran Integration Suite version 4.3 binds only to specific network interfaces. After upgrading, if the previous URL for Gentran Integration Suite returns *Page cannot be displayed*, you can adjust property settings to correct the problem.

1. On the server where Gentran Integration Suite resides, edit the noapp.properties.in file.
2. Locate the **admin_host** parameter. The default settings are as follows:

   hostname1 is the name of primary network interface, the one given highest priority by Gentran Integration Suite.

   localhost is the name of the network interface on the server where Gentran Integration Suite resides.

   Default entries

   ```
   admin_host.1    = hostname1
   admin_host.2    = localhost
   ```

3. Correct the parameters.
   - If no interface is being displayed, edit *hostname1* so that it correctly identifies the primary network interface that accesses Gentran Integration Suite.
   - If an additional network interface needs to access Gentran Integration Suite, add an additional *admin_host* entry, as shown below.

     Edited entries

     ```
     admin_host.1    = hostname1
     admin_host.2    = localhost
     admin_host.3    = hostname2
     ```

4. Stop Gentran Integration Suite.
5. Run the `setupfiles.sh` utility located in the *install_dir*/bin directory.
6. Restart Gentran Integration Suite to use the updated settings.

For the Dashboard user interface, Gentran Integration Suite version 4.3 provides unrestricted binding to network interfaces through the perimeter server. To restrict access to the Dashboard user interface, you can adjust property settings so that only one network interface accesses Gentran Integration Suite.

1. On the server where Gentran Integration Suite resides, edit the perimeter.properties.in file.
2. Locate the **localmode.interface** parameter. The default setting is unrestricted, as shown below.

   Unrestricted Setting (Default)

   ```
   localmode.interface=*
   ```

3. To restrict access to the Dashboard, enter the network interface that you want Gentran Integration Suite to support.

   ```
   Restricted Setting
   localmode.interface=hostname1
   ```

4. Stop Gentran Integration Suite.
5. Run the `setupfiles.sh` utility located in the *install_dir*/bin directory.
6. Restart Gentran Integration Suite to use the updated settings.

Advanced File Transfer Tab

The Advanced File Transfer tab in the Dashboard interface will not be enabled by default after an upgrade installation of Gentran Integration Suite 4.3. You will need to configure the Dashboard to enable the tab.

If you have a license for Advanced File Transfer, perform the following steps to add the Advanced File Transfer tab:

1. Log in as **Admin**.
2. Click **Manage Layout**.
3. Click **Add Pane**.
4. Enter the following name:
   `Advanced File Transfer`
5. Click **Apply**.
6. Click the link for the new **Advanced File Transfer** tab.
7. Click **Add Portlet**.
8. Select the Add box for **Advanced File Transfer Management**.
9. Click **Apply**.
10. Select **Clear Borders and Title** from the Decoration menu.
11. Click **Apply**.
12. Click **Save and Apply**.

Reconfiguring Archive Settings

The upgrade does not automatically reconfigure the archive configuration. You must reconfigure the Backup Directory setting in Archive Manager after an upgrade.

To reconfigure your Archive settings, use the following procedure:

1. From the Administration menu, choose **Operations** > **Archive Manager**.
2. Under Configure Archive Settings, click **Go!**
3. If a message displays about the UI Lock, click **OK** to continue.
4. Click **Next**.

5. Update the Backup Directory field with the correct path information:
6. Click **Save**.
7. Confirm the settings and click **Finish**.

Correcting Missing Manager IDs

If you created a Manager ID with no corresponding User ID in your previous version of Gentran Integration Suite, the Manager ID may be missing after upgrading to Gentran Integration Suite 4.3. If this occurs, create a user in the system with a User ID that matches the missing Manager ID.

Accessing User Documentation for Gentran Integration Suite

The user documentation is available via an online documentation site on the Web. Providing the documentation in an online environment allows for frequent updates of content based on user feedback and usability.

We also understand the need for a printed copy of documentation. You can print topics of information using your Internet browser, or you can download documents in PDF format. You also have the option to request a documentation CD.

Using the Online Documentation

The documentation for Gentran Integration Suite is located on the Sterling Commerce Documentation web site. You can type a word or phrase and search the entire library for information. Or you can move through a hierarchy of contents pages to identify the topic you want. After you find the topic you want, you can read it online or print it using your browser's Print function.

To access the Documentation site, from within Gentran Integration Suite or one of its tools, select the Help ? icon. (Note that the application must reside on a computer that supports Internet access and an Internet browser.)

You can also access the Documentation site by opening your Internet browser and typing the following URL:

http://www.sterlingcommerce.com/Documentation/GIS43/homepage.htm

Documentation Available in PDF Format

The online documentation includes documents in PDF format that you can download. To download PDF documents, click the *Documentation in PDF Format* link from the main online documentation page.

Requesting a Documentation CD

You can request a CD that contains all the documentation found on the Documentation site. To submit a request, go to the following URL:

http://support.sterlingcommerce.com/forms/Gentran_GIS_UpgradeRequest.aspx

Index