Gentran Integration Suite

Windows Cluster Upgrade

Version 4.3

Sterling Commerce
An IBM Company

© Copyright Sterling Commerce, an IBM Company 2000-2011. All Rights Reserved.

Additional copyright information is located on the Gentran Integration Suite documentation library:
http://www.sterlingcommerce.com/Documentation/gis43/CopyrightPage.htm

Contents

Chapter 1 Introduction 6

Chapter 2 Pre-Upgrade Information 7

Before You Begin Upgrading . . . 7
- Standard Tasks and Considerations . . . 7
- Special Tasks and Considerations . . . 8
- Creating a Process Output Log . . . 9
- Copying a Microsoft SQL Server 2000 Database . . . 9
- Copying a Microsoft SQL Server 2000 Database to an SQL Server 2005 Database . . . 10

Managing Database Passwords . . . 12
- Database Password Encryption Methods . . . 12
- Encrypting Database Passwords (Windows) . . . 12
- Decrypting Database Passwords (Windows) . . . 12

Verifying System and Database Compatibility . . . 13
Preparing Your System for the Upgrade . . . 13
Preserving Customer Changes During Updates . . . 14

Chapter 3 Upgrading in a Clustered Windows Environment 15

Preinstallation Setup Checklist for a Clustered Windows Environment . . . 15
- Checklist for Windows Preinstallation . . . 15
- Checking System Requirements . . . 18
- Installing the Java 2 Software Development Kit . . . 18
- Downloading the JCE Distribution File . . . 19
- Determining Port Numbers . . . 19
- Obtaining a License File . . . 19

Upgrading in a Clustered Windows Environment . . . 20
- Upgrading in Windows . . . 21
- Installing the JDBC Driver in SQL Server . . . 21
  - Installing the JDBC Driver in SQL Server 2000 . . . 22
  - Installing the JDBC Driver in SQL Server 2005 . . . 22
  - Configuring Snapshot for Microsoft SQL Server 2005 . . . 24
- Running the Upgrade Program in Windows . . . 24

Cluster Setup (Windows) . . . 28

Multiple Nodes . . . 28
Custom Configurations . . . 28
Node to Node Communications . . . 29
Configuring Shared File System as Document Storage . . . 30
Cluster Environment Verification . . . 30
Starting or Stopping the Cluster Environment . . . 31
Patches and Hot-Fixes (Cluster) . . . 31
Installing the Current Maintenance Patch (Cluster) . . . 32
Applying a Patch in a Clustered Environment Stopping the Whole Cluster . . . 32
Applying a Patch in a Clustered Environment Stopping One Node at a Time . . . 34
Updating the Database (dbupdate) with the startCluster Command . . . 35
Running a DB2 Schema Change Script . . . 36
Installing a Hot-Fix (Cluster) . . . 37
Before Installing a Hot-Fix . . . 37
Hot-Fix Installation . . . 37
Hot-Fix Package Delivery Method . . . 38
Performing Checksum using DB Checksum Tool . . . 39
Installing a Perimeter Server in a Clustered Windows Environment . . . 39
Setting Up Perimeter Servers with Gentran Integration Suite . . . 40
Installing a Perimeter Server in a More Secure Network (Windows Clustered) . . . 40
Installing a Perimeter Server in a Less Secure Network (Windows Clustered) . . . 42
Installing Patches in a Perimeter Server Windows Environment . . . 43
Starting and Stopping Perimeter Servers in Windows . . . 44
Reducing Perimeter Server Security Vulnerabilities . . . 44
Granting Permissions for Specific Activities By a Perimeter Server . . . 44
Performing DNS Lookup on Remote Perimeter Server . . . 46
Postinstallation in a Clustered Windows Environment . . . 47
Starting Gentran Integration Suite in Windows . . . 47
Accessing Gentran Integration Suite . . . 47
Technical Note: Changes to Network Interface Bindings . . . 47
Validating the Installation . . . 49
Downloading Gentran Integration Suite Tools . . . 49
Performing Initial Administrative Setups in Gentran Integration Suite . . . 49
Stopping Gentran Integration Suite . . . 50
Managing Nodes in a Cluster . . . 50
Adding a Node . . . 50
Removing a Node . . . 51
Uninstalling Gentran Integration Suite from a Clustered Windows Environment . . . 51
Troubleshooting: Clustered Windows Environment . . . 54

Chapter 4 Post-Upgrade Processes 57

Adding Third-Party Libraries . . . 57
Configuring Customer Overrides File When You Have a Firewall Between Nodes (Build 4324 or higher) 57
Configuring Services and Adapters . . . 58
JDBC Adapter and Lightweight JDBC Adapter . . . 58
Upgrading from Gentran Integration Suite 3.0 . . . 59
Upgrading from Gentran Integration Suite 3.1 . . . 59
File System Adapter and Command Line2 Adapters . . . 61
Command Line2 Adapter . . . 61

Command Line Adapter 61
Restoring Performance Tuning Configuration 62
Starting an Upgraded Cluster 62
Final Upgrade Notes 62
Changes to Network Interface Bindings 63
Advanced File Transfer Tab 64
Reconfiguring Archive Settings 65
Correcting Missing Manager IDs 65
Accessing User Documentation for Gentran Integration Suite 65
Using the Online Documentation 65
Documentation Available in PDF Format 66
Requesting a Documentation CD 66

Index 67

Chapter 1

Introduction

Use the Gentran Integration Suite *4.3 Windows Cluster Upgrade Guide* to upgrade the Gentran Integration Suite software in a clustered (multiple node) Windows 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 Windows 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.

In Windows, you must redirect the standard output and standard error of each command to create a log file. Do the following:

1. To redirect the standard output and standard error to create a log file, type a command similar to the following:

   ```
   process.cmd > processoutput.log 2>&1
   ```

   where *process* is the name of the command and *processoutput* is the name of the output log.

   The log-writing process time varies, depending on the size of your database and your system hardware.

   Caution: In Windows, if you attempt to view the log while it is being written, the `upgrade.cmd` script stops running and does not create a log of the upgrade process.

2. After you complete the command, you can review the output log using any text editor (for example, Microsoft Notepad).

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 (Windows)

To encrypt the database password:

1. Stop the Gentran Integration Suite.
2. Navigate to *install_dir*\install\bin.
3. Enter `enccfgs.cmd`.
4. Enter `setup.cmd`.
5. Enter `deployer.cmd`.
6. Enter `startWindowsService.cmd` to start the Gentran Integration Suite.

Decrypting Database Passwords (Windows)

To decrypt a password in Windows:

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.cmd 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.cmd`.
12. Enter `deployer.cmd`.
13. Enter `startWindowsService.cmd` to start the Gentran Integration Suite.

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 Windows Environment

Preinstallation Setup Checklist for a Clustered Windows Environment

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

- *Checklist for Windows Preinstallation* on page 15
- *Checking System Requirements* on page 18
- *Installing the Java 2 Software Development Kit* on page 18
- *Downloading the JCE Distribution File* on page 19
- *Determining Port Numbers* on page 19
- *Obtaining a License File* on page 19

Checklist for Windows Preinstallation

The preinstallation checklist for the Windows environment identifies the prerequisite tasks you must complete before installing Gentran Integration Suite.

Note: 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 **-**, **:**, **$**, **&**, or **_**.
- 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 for installing Gentran Integration Suite:

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 18.	
2	Verify that your system has the patches required by Java™ for the Windows environment. See the vendor's Java Web site for more information.	
3	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. **Caution**: If you do not verify the IP addresses, your system may not operate properly after installing Gentran Integration Suite**.**	
4	Verify that all client computers are using Microsoft Internet Explorer 5.x or later.	
5	If you are using a non-English environment, confirm that you are using the appropriate character set.	
6	Determine and record information about the Java 2 Software Development Kit (JDK). See *Installing the Java 2 Software Development Kit* on page 18. ◆ Version of the JDK. ◆ Absolute path to the JDK files and patches. The path name cannot include spaces.	
7	Obtain the JCE distribution file and record the absolute path to the zipped file. See *Downloading the JCE Distribution File* on page 19.	
8	Determine and record the initial port number to be used by Gentran Integration Suite. See *Determining Port Numbers* on page 19.	

Step	Description	Your Notes
9	If you are using a SQL Server 2000/2005 database or an Oracle 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	
10	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.	
11	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 installation directory must have adequate free disk space. ◆ The name of the directory cannot include spaces and must be less than 30 characters long. Using a directory name of more than 30 characters could create an installation that is impossible to delete.	
12	Determine and record the passphrase you want to use for Gentran Integration Suite system. During installation, you must enter the passphrase twice.	

Step	Description	Your Notes
13	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 do not contain any spaces. See *Obtaining a License File* on page 19. **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.	
14	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 run-time. 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. The hardware requirements listed are the minimum required to run Gentran Integration Suite. 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 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.

Installing the Java 2 Software Development Kit

You must install the Java 2 Software Development Kit (JDK) and the patches specific to your system. To determine which JDK version and patches you need, see the *System Requirements*. After you install the JDK, record the path to the JDK for future reference.

Caution: Two registry keys written by the installation of the Sun JDK version 1.5.0-11 are faulty and include an invalid value for the JavaHome key (the Java JDK location). If the Gentran Integration Suite installation cannot find the Java JDK location using the registry settings, you are prompted for the location of the Java JDK directory. Once the installation is complete, the registry will be updated with the correct JDK location.

Downloading the JCE Distribution File

The Java Cryptography Extension (JCE) is a set of Java packages from Sun Microsystems, Inc. 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:

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.

Determining Port Numbers

During installation, you are prompted to specify the initial port number for Gentran Integration Suite. For other ports, you can accept the default port number suggested by the installation program, or you can specify a different port number. To specify a 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. All ports in this range must be available for Gentran Integration Suite. 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.

After your installation, refer to *install_dir*`\properties\sandbox.cfg` for all of the port assignments.

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 Gentran Integration Suite 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 an 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. You will need the absolute path to install Gentran Integration Suite.
11. Click **Save**.
12. Close your Web browser.

Upgrading in a Clustered Windows Environment

Installing Gentran Integration Suite in a cluster Windows environment includes the following tasks:

- *Upgrading in Windows* on page 21
- *Installing the JDBC Driver in SQL Server* on page 21

✦ *Running the Upgrade Program in Windows* on page 24

Upgrading Gentran Integration Suite cluster 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.
- ✦ You must install and start the nodes sequentially, one at a time, starting with the first node.

Upgrading in Windows

To upgrade to Gentran Integration Suite version 4.3, follow the installation instructions in this section. These steps include special instructions for upgrading. 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 your system before continuing the upgrade, it is recommended that you fully test the patch prior to performing the upgrade. If you are running 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).

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 22
- *Installing the JDBC Driver in SQL Server 2005* on page 22

Installing the JDBC Driver in SQL Server 2000

Go to the Microsoft web site to download this driver, any appropriate patches, and the following .jar files. Be sure to place all the .jar files in the same directory.

- msbase.jar
- mssqlserver.jar
- msutil.jar files

After you obtain the JDBC driver file and .jar files, record the absolute path to their location on your system. You must supply this absolute path when you install Gentran Integration Suite. When you select these files during the installation, you can use one of the following methods:

Note: It is recommended that you use the first method (select all three files), because the second method (select a combined jar file) generates warning messages that might be confusing.

- In the browse window, select all three files by holding down the **Ctrl** key and clicking each file name.
- In the browse window, select a combined jar file, which you create using the following method:
  a. Make a new directory in which you will work, and copy the separate jar files to this directory.
  b. For each of the separate jar files, issue the following command:

     ```
     jar -xvf jar_file_name
     ```

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

     ```
     jar -cvf combinedJarName.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*.exe to a temporary directory.
2. Run sqljdbc_*version_language*.exe.
3. When prompted, enter an installation directory to which you will unpack zip file that contains the driver. It is recommended that you unpack the zip file in your **Program Files** directory with the default directory **Microsoft SQL Server 2005 JDBC Driver**. You will access this directory path during the installation of Gentran Integration Suite.

   Note: Make sure that you specify the full path to the installation directory. For example, C:\Program Files\Microsoft SQL Server 2005 JDBC Driver.

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

4. When the 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;
```

Running the Upgrade Program in Windows

Note: The following instructions assume that you received an installation CD for Gentran Integration Suite. 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. Do *not* change the directory structure of the newly unzipped files. 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.

To install Gentran Integration Suite in a clustered Windows environment, refer to your preinstallation checklist and follow the steps below.

Note: To install more than one instance of Gentran Integration Suite on the same Windows server, 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.

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. Close all open Windows programs and any command prompt windows.
2. Insert Gentran Integration Suite installation CD in the appropriate drive.
3. On the installation CD, navigate to the **windows\install** folder.
4. Double-click **setupfiles.exe**. Then click **Next** to start the installation program.
5. Review the license agreement, and click **Yes** to accept the terms.
6. The installation program searches for the JDK, using the registry settings. If the program cannot find the JDK location using the registry settings, you are prompted for the location of the JDK directory. Use the **Browse** button to search for the directory. For more information, refer to the caution information in *Installing the Java 2 Software Development Kit* on page 18.

   Click **Next**.
7. You are prompted to choose an installation directory for Gentran Integration Suite. Click **Browse** and navigate to the folder you want to use as the installation directory. This directory is referred to as *install_dir* in subsequent prompts.

8. You are prompted to browse to the location of the license file. Select the license file, and click **Next**.

   If you have not installed a license file, you can minimize this window, obtain the license file, and then return to the installation process.

9. You are prompted to browse to the location of the JCE distribution file. Select the JCE distribution file, and click **Next**. The program verifies the path name.

10. A screen appears with the following four checkboxes:

    - **I want to install a cluster node 2 or higher**

      Select this checkbox **only** when upgrading node 2 or higher of a cluster.

    - **I want to upgrade from a prior version**

      Select this checkbox when you are running the upgrade installation program on node 1.

      Note: You will not select this checkbox for cluster node 2 or higher. For those upgrade installations, you will use the **I want to install a cluster node 2 or higher** option.

    - **I want to enable FIPS mode**

      Select this checkbox if you are enabling the Federal Information Processing Standards (FIPS) mode.

    - **I want GIS to automatically create the database schema**

      This checkbox is selected by default. Make sure that it is selected, as the option of manually creating the database schema is not supported on the Windows environment.

    After choosing your checkbox option, click **Next**

11. The system displays a command window. Leave the command window open. You can minimize the command window, but do not close it or the installation program cannot prompt you for information or display status messages.

12. The system displays a message window listing information you will need in subsequent steps. Click **OK** to continue.

13. You are prompted about overriding the host IP address for this installation.

    - To accept the default host IP address, click **Next**.
    - To specify another host IP address, enter the IP address you want to use. Click **Next**.

    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.

14. Type the administrative e-mail address to which you want system alert messages to be sent. Click **Next**.

    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.

15. Type the SMTP mail server host name that you want to use for alert messages. Click **Next**.

16. Type your system passphrase in both the Passphrase box and the Confirm box. Use the same passphrase you used for your previous Gentran Integration Suite installation. Click **Next**.
17. Type the initial port number for Gentran Integration Suite server. Use the same initial port number you used for your previous Gentran Integration Suite installation. Click **Next**.

    The installation creates subsequent ports based on the initial port number. These port assignments are written to *install_dir*`\properties\sandbox.cfg`.
18. Select the database you want to use and click **Next**.

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

    - If you select Microsoft SQL Server 2000 or 2005, enter the following information and click **Next**:

      • Database host name

      • Database host port number

      • Database name

      • User ID

      • Password

      • Password confirmation

    - If you select Oracle, you are asked whether the Oracle instance is being used for an upgrade. Answer **Yes**, and refer to the *Pre-Upgrade Information* section before you answer subsequent prompts.

      Enter the following information and click **Next**:

      • Database host name

      • Database host port number

      • Database name

      • User ID

      • Password

      • Password confirmation
19. If you selected Oracle or either version of Microsoft SQL Server as your database, verify that you have the required JDBC drivers installed.
    a. Verify that you have the required JDBC driver file copied to a local folder on your computer. Use a descriptive name for this folder that will help you later access the driver.
    b. Browse to the location of the JDBC driver file. Select the file and click **Open**. For more information about how to select the file for Microsoft SQL Server, refer to *Installing the JDBC Driver in SQL Server* on page 21.
    c. In the **Version Number** field, type **x_x** and click **Next**. Refer to *System Requirements* for the actual version number.
20. Click **Yes** to proceed with the installation.

21. The installation completes automatically. When the installation of node 1 is finished, the system places an icon on your Windows desktop and displays a message that Gentran Integration Suite was successfully installed. Click **OK**. Click **Next**. Click **Finish**.

    If you encounter problems or errors during installation, see the section *Troubleshooting: Windows Environment*.

22. Starting from node 2, start the installation as normally done for all Gentran Integration Suite installations. Use the following command:

    install_dir\setup.exe

23. When prompted, select all options that apply to your upgrade installation.

    Select the checkbox to indicate that you are installing a cluster on node 2 or higher. **Do not** select the checkbox indicating an upgrade from a prior version. Your upgrade installations on node 2 or higher will use the database that was upgraded on node 1, so you do not need to use the upgrade option for those node 2 or higher.

Note: The database schema is only built once. When installing a cluster on node 2 and higher, you must ensure *I want GIS to automatically create the database schema* is selected even though it does not create a second database schema.

24. Click **Next**.

    The following message appears:

    Please wait while Setup bootstraps Gentran Integration Suite install..

    After bootstrap completes you will get a message notifying what you will require to proceed further (application port number and database server information).

    Note: You need to use the same database that you used for the installation in Step 1.

25. Click **Next**.

26. Complete the rest of the installation process as normally done for a Windows Gentran Integration Suite installation, but do not start the Gentran Integration Suite instances.

    After all of the nodes are installed, go to the next step.

27. (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 jgroups_cluster.properties.in to point to the value of node 1's mcast_port property in jgroups_cluster.properties.

    Note the different property file names:

    - jgroups_cluster.properties (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*>**.

28. (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 noapp.properties.in to point to the value of node 1's multicastBasePort property in noapp.properties.

    Note the different property file names:

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

29. On each node, starting with node 1, perform cluster configuration by running the command `startCluster.cmd` *`nodeNumber`* from the Gentran Integration Suite *install_dir*\bin directory where *`nodeNumber`* is the sequential number assigned to each node starting with 1.

    For example, use the following commands on the first two nodes:

    a. `startCluster.cmd 1`

    b. `startCluster.cmd 2`

Note: You should run `startCluster.cmd` command only after you install Gentran Integration Suite. You should not run `startCluster.cmd` 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 28to start the cluster without updating the database settings.

30. Bring up all instances of Gentran Integration Suite by running `run.cmd` from the *install_dir*\bin directory for each instance, starting with the first node.

To dynamically add new nodes to the cluster, install the new node in the same way that you installed node2 in a new cluster installation. Run the `startCluster.cmd` command with the new node number.

Note: After performing the upgrade, refer to *Installing the Current Maintenance Patch (Cluster)* on page 32 to install the latest patch.

Cluster Setup (Windows)

The following sections explain how to set up a cluster installation after upgrading all nodes of the cluster.

Multiple Nodes

Gentran Integration Suite supports the installation of multiple nodes on the same machine. Each node will be configured on a different port range. Install the second node on the same machine on a different port range following the installation instructions discussed in the previous section. Once the installation is complete and cluster setup is complete, go to the properties directory of the node installed and change the multicastBasePort property in noapp.properties.in to point to node1's multicastBasePort. After changing this property, run the `setupfiles.cmd` command.

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.cmd` *`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 `startCluster.cmd` with the database update option set to **true** to have all cluster-related configurations take effect.

`startCluster.cmd` *`nodeNumber`* `true`

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

`startCluster.cmd` *`nodeNumber`* `false`

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 Gentran Integration Suite 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.

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 a 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.cmd` command in the *install_dir*\bin directory.
4. Restart Gentran Integration Suite (all nodes).

This configures a shared file system directory as document storage.

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

Note: To run a cluster, you need to get a valid Gentran Integration Suite license for multiple IP address of all the nodes where Gentran Integration Suite will be installed and configured as a cluster.

You can start the cluster environment by running the following command on each node, starting with node1 (it is recommended to start node 1 first.):

```
startWindowsService.cmd
```

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

- Node 1:

```
startWindowsService.cmd restart
```

This option is used for cleaning the cluster data, settings, and so on to do a clear start.

- Nodes 2 and higher:

```
startWindowsService.cmd
```

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

- `hardstop.cmd` from each node. This stops all Windows Services for each node.
- `softstop.cmd` from each node. This does a regular cleanup and shutdown of all components.

Caution: Running `softstop.cmd` command in a multiple node (clustered) environment will suspend all scheduled business processes. It is recommended to run the `hardstop.cmd` 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.

Patches and Hot-Fixes (Cluster)

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

- *Installing the Current Maintenance Patch (Cluster)* on page 32

  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 37

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

Installing the Current Maintenance Patch (Cluster)

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 but in some cases, you can apply patches to nodes while others are still processing. 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.

Before installing the patch, refer to to the following sections for more information about working with the different nodes of a cluster during a maintenance patch installation:

- *Applying a Patch in a Clustered Environment Stopping the Whole Cluster* on page 32
- *Applying a Patch in a Clustered Environment Stopping One Node at a Time* on page 34

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 overridden during the patch installation. Properties overridden using the customer_overrides.propertie**s** file are not affected.

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. 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. Make

sure that you download the file to your local machine (for example, to your installation bin directory), and not to a network drive. Use the full path to your local machine when you install the patch.

3. Verify that the database server is up and ready to accept connections.
4. Stop all nodes of the cluster.
5. Perform a full backup of Gentran Integration Suite installation directory, including all subdirectories. Also back up your database.
6. If your database password is encrypted, decrypt the password. For more information about decrypting database password, refer *Decrypting Database Passwords (Windows)* on page 12.
7. If you edited any property files, update the customer_overrides.properties file with these changes. This will keep the edited property files from being overwritten with the contents of the associated initialization (*.properties.in) files during the patch installation. Please refer to the documentation on configuring overrides to properties files.
8. Close all command prompt windows.
9. On each node, install the patch using the following commands:
   a. Open a command prompt window.
   b. Change to the directory where Gentran Integration Suite is installed and run the following command:

      installDir\bin

   c. Run the following command to install the patch:

      InstallService.cmd
      <*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.cmd c:\patch\si_22_sp_0_patch_1_jboss.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 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 node 1 if the installation is done using the nodbinit option.

   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.
10. If you decrypted the database password, re-encrypt the password. For more information about encrypting database password, refer *Encrypting Database Passwords (Windows)* on page 12.

11. For each node, run the `startCluster.cmd nodeNumber` command to reconfigure the cluster environment after installing the patch.

    For more information about using the `startCluster.cmd` command, refer to *Updating the Database (dbupdate) with the startCluster Command* on page 35.

    Note: Ensure that you run `startCluster.cmd nodenumber false` command to prevent configuration changes that may affect the system. Refer to *Custom Configurations* on page 28 before configuring the cluster environment.

12. Restart Gentran Integration Suite.

If you are using a perimeter server in a DMZ, see *Installing Patches in a Perimeter Server Windows Environment* on page 43.

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 procedure:

Note: Apply the patch to node 1 first, and then to the subsequent nodes: node 2, node 3, etc.

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. Make sure that you download the file to your local machine (for example, to your installation bin directory), and not to a network drive. Use the full path to your local machine when you install the patch.
3. Verify that the database server is up and ready to accept connections.
4. Shut down node 1 using the `hardstop.cmd` command.

   Wait until the perimeter server of the node is completely down before installing the patch.
5. Perform a full backup of Gentran Integration Suite installation directory, including all subdirectories. Also back up your database.
6. If your database password is encrypted, decrypt the password. For more information about decrypting database password, refer *Decrypting Database Passwords (Windows)* on page 12.
7. If you edited any property files, update the customer_overrides.properties file with these changes. This will keep the edited property files from being overwritten with the contents of the associated initialization (*.properties.in) files during the patch installation. Please refer to the documentation on configuring overrides to properties files.
8. Close all command prompt windows.
9. Install the patch using the following command:
   a. Open a command prompt window.
   b. Change to the directory where Gentran Integration Suite is installed and run the following command:

      `installDir\bin`

c. Run the following command to install the patch:

```
InstallService.cmd
<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.cmd c:\patch\si_22_sp_0_patch_1_jboss.jar`

For node 1, `REINIT_DB=true` in sandbox.cfg. For subsequent nodes, `REINIT_DB=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 nodbinit option.

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.

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

    For more information about using the `startCluster.cmd 1` command, refer to *Updating the Database (dbupdate) with the startCluster Command* on page 35.

    Note: Ensure that you run `startCluster.cmd` *`nodenumber`* `false` command to prevent configuration changes that may affect the system. Refer to *Custom Configurations* on page 28 before configuring the cluster environment.

Note: Refer to *Custom Configurations* on page 28 before configuring the cluster environment.

12. 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.
13. Repeat this procedure for each subsequent node.
14. Restart Gentran Integration Suite.

If you are using a perimeter server in a DMZ, see *Installing Patches in a Perimeter Server Windows Environment* on page 43.

Updating the Database (dbupdate) with the startCluster Command

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

When you configure the Gentran Integration Suite cluster for the first time, you should run the `startCluster.cmd` command with the database update value set to **true** (`startCluster.cmd 1 true`), or just `startCluster.cmd 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.cmd` command with the database update value turned off (`startCluster.cmd 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 default storage of the following services is set to the database:

- HttpServerAdapter
- CEUServerExtractServiceType
- CDSERVER_ADAPTER

The default storage of all business processes is set to the database.

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.cmd –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 the Windows host system:

1. Is the password encrypted? If **Yes**, decrypt the password. For more information about decrypting database password, refer *Decrypting Database Passwords (Windows)* 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.

2. Open a command line session. Click the Windows **Start** menu and select **Programs** > **Accessories** > **Command Prompt**.
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 c`*`caseid`*`.jar`, where *caseid* is the ID you received from Customer Support.
7. Shut down Gentran Integration Suite.

8. Open a command prompt and change the directory to *install_dir*\bin.
9. To install the hot-fix, type the following command:

   `InstallService` *`path to ccaseid.jar`*`\ccaseid.jar .`
10. If you decrypted the password in step 1, re-encrypt the password. For more information about encrypting database password, refer *Encrypting Database Passwords (Windows)* on page 12.
11. In the command prompt, change the directory to *install_dir*\bin.
12. Type `uninstallWindowsService.cmd` and log off. This removes previous Gentran Integration Suite Windows services from the Windows cache.
13. At the command prompt, type your user name and password.
14. Change the directory to *install_dir*\bin.
15. Type `installWindowsService.cmd` to install Gentran Integration Suite Windows services.
16. Restart Gentran Integration Suite.
17. In the *install_dir*\bin directory, run `dump_info.cmd` to verify that the hot-fix was successfully installed. The successful running of `dump_info.cmd` will display the Gentran Integration Suite version number.
18. After installing the hot-fix, run the `startCluster.cmd` *`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.cmd 2` command.

    Note: Ensure that you run `startCluster.cmd` *`nodenumber`* `false` command to prevent configuration changes that may affect the system. Refer to *Custom Configurations* on page 28 before configuring the cluster environment.

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 37 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.cmd` 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.cmd [-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 Windows Environment

Installing a Gentran Integration Suite perimeter server in a clustered Windows environment includes the following tasks:

- *Setting Up Perimeter Servers with Gentran Integration Suite* on page 40
- *Installing a Perimeter Server in a More Secure Network (Windows Clustered)* on page 40
- *Installing a Perimeter Server in a Less Secure Network (Windows Clustered)* on page 42
- *Installing Patches in a Perimeter Server Windows Environment* on page 43
- *Starting and Stopping Perimeter Servers in Windows* on page 44
- *Reducing Perimeter Server Security Vulnerabilities* on page 44

Setting Up Perimeter Servers with Gentran Integration Suite

Using a perimeter server with Gentran Integration Suite is optional.

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

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, either a more secure or less secure network 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 in Gentran Integration Suite.
- 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 may 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 (Windows

Clustered)

To install a perimeter server in a Windows clustered environment:

1. Close all open Windows programs.
2. Insert Gentran Integration Suite installation CD into the appropriate drive.
3. Open a DOS command window.
4. 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, be sure your session is set to binary mode.
5. To begin the installation, run the following command, using the full path to the ps_2000.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.
6. Enter the name for the installation directory.
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.

   The program verifies the amount of available disk space.
8. At the prompt *Is this server in a less secure network than the integration server?*, type **No** and press **Enter**.

   For more information about making the perimeter more secure, refer to *Reducing Perimeter Server Security Vulnerabilities* on page 44.
9. 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.
10. Enter the TCP/IP address or DNS name that the integration server (Gentran Integration Suite) will listen on for the connection from this server.
11. Verify the TCP/IP address or DNS name.
12. Enter the port that the intergration server (Gentran Integration Suite) will listen on for the connection from this server. The port number must be higher than 1024.
13. 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.

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. Enter `installPS.cmd` to install this perimeter server as a Windows Service.
17. Enter `startPSService.cmd` to start the perimeter server.

Installing a Perimeter Server in a Less Secure Network (Windows Clustered)

To install a perimeter server in a Windows clustered environment:

1. Close all open Windows programs.
2. Insert Gentran Integration Suite installation CD into the appropriate drive.
3. Open a DOS command window.
4. 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, be sure your session is set to binary mode.
5. To begin the installation, run the following command, using the absolute path to the ps_2000.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.
6. Enter the name for the installation directory.
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.

   The program verifies the amount of available disk space.
8. At the prompt *Is this server in a less secure network than the integration server?*, type **Yes** and press **Enter**.
9. 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.
10. 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.
11. Verify the TCP/IP address or DNS name for the internal interface.

12. 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.
13. Verify the TCP/IP address or DNS name for the external interface.
14. 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.
15. Verify the port.

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

    Installation of Perimeter Service is finished
16. Change to the installation directory.
17. Enter `installPS.cmd` to install this perimeter server as a Windows Service.
18. Enter `startPSService.cmd` to start the perimeter server.

Installing Patches in a Perimeter Server Windows 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.

To update a remote perimeter server in a clustered Windows 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 (Cluster)* on page 32.
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 file to the home directory or base directory on the remote server.
4. Stop the perimeter server using the `stopPs.cmd` command.
5. To begin the installation, type *`absolutePath`*`\bin\java -jar` *`filename`*`.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. 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. Type `startupPs.cmd` to start the perimeter server.

Starting and Stopping Perimeter Servers in Windows

To start a perimeter server in Windows, use the `startPSService.cmd` command, or use the Services Control Panel.

To stop a perimeter server in Windows, use the `stopPSService.cmd` command, or use the Services Control Panel. To remove this perimeter server's definition as a Windows Service, use the `uninstallPSService.cmd` 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 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 (Windows Clustered)* on page 40.
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 Windows Environment

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

- *Starting Gentran Integration Suite in Windows on page 47*
- *Accessing Gentran Integration Suite on page 47*
- *Validating the Installation on page 49*
- *Downloading Gentran Integration Suite Tools on page 49*
- *Performing Initial Administrative Setups in Gentran Integration Suite on page 49*
- *Stopping Gentran Integration Suite on page 50*

Starting Gentran Integration Suite in Windows

To start Gentran Integration Suite in a clustered Windows environment, double-click Gentran Integration Suite icon on your Windows desktop. Gentran Integration Suite starts running.

Note: It may take several minutes for Gentran Integration Suite components to initialize and start up.

If Gentran Integration Suite does not start or if you receive a message about an invalid or corrupt license file, go to the *Troubleshooting: Windows Environment* section.

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

Open your Web browser to http://host:port/(interface), where *host:port* is the host and port number where Gentran Integration Suite resides on your system, and *(interface)* is the interface used by Gentran Integration Suite (for example, admin or dashboard).

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

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 enter the address displayed at the end of startup.
3. The login page for Gentran Integration Suite 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 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.
   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.

      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.cmd` 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, enter 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.cmd` 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 enter 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!** You see the *Status: Success* message 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 *Troubleshooting: Windows Environment* section.

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 Windows environment, follow these steps:

1. Open Gentran Integration Suite.
2. From the **Administration** menu, select **Operations > System > Troubleshooter**.
3. Click **Stop the System** and wait for shutdown to complete.

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 50
- *Removing a Node* on page 51

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 Windows* on page 24. 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.cmd` *`nodeNumber`* from the *install_dir*\bin directory. The node number should be greater than 1.

Note: You should run `startCluster.cmd` command only after you install Gentran Integration Suite. You should not run `startCluster.cmd` 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 28to start the cluster without updating the database settings.

4. Start the new Gentran Integration Suite node. To start a node, refer *Starting Gentran Integration Suite in Windows* on page 47.

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. To restart Gentran Integration Suite cluster environment, refer *Starting or Stopping the Cluster Environment* on page 31.

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 Windows Environment* on page 51.

Uninstalling Gentran Integration Suite from a Clustered Windows 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 the JDK that was installed
- Manually remove any desktop tools that were downloaded
- Free any database space in Oracle or SQL Server databases

Note: This uninstallation procedure applies to Gentran Integration Suite 4.3, and not the version of Gentran Integration Suite from which you are upgrading.

To uninstall Gentran Integration Suite from a Windows environment, follow these steps:

1. Stop Gentran Integration Suite and wait for shutdown to complete.
2. Navigate to the *install_dir*\bin directory.
3. Run the `uninstallWindowsService.cmd` command to remove the following Windows services:
   - Gentran Integration Suite
   - Opsserver

- Noapp server
- WebDav server

You should receive a message stating that the services were successfully removed. To verify their removal, open the Services window:

a. Select **Start** > **Settings** > **Control Panel** > **Administrative Tools** (Windows 2000) or **Start** > **Administrative Tools** (Windows 2003).

b. Click **Services**.

If the services were not removed, you must delete them from the Windows registry:

a. Go to the Windows registry.

b. Locate **HK_LOCAL_MACHINE\System\Current Control Set\Services**.

c. Delete the keys for Gentran Integration Suite and Opsserver. These registry keys start with Gentran Integration Suite.

d. Reboot to apply the registry changes.

4. If the JDK is not being used by another application, remove it.

   a. Select **Start** > **Settings** > **Control Panel** (Windows 2000) or **Start** > **Control Panel** (Windows 2003).

   b. Select **Add/Remove Programs** (Windows 2000) or **Add or Remove Programs** (Windows 2003).

   c. Select **Java 2 SDK Runtime Environment Standard Edition v**<*version number*> and click **Remove**.

   d. Select **Java 2 SDK Standard Edition v**<*version number*> and click **Remove**.

   e. Close all windows and return to your desktop.

5. Remove the product installation folder from the Windows path:

   a. In your Windows desktop, right-click **My Computer**.

   b. Select **Properties**.

   c. Click the **Advanced** tab.

   d. Click **Environment Variables**.

   e. In the System variables window, select **Path**.

   f. Click **Edit**.

      The system displays the Edit System Variable dialog box.

   g. Delete the following entries located in Variable Value.

      install_dir\SI\lib\jnipass\1_0\windows;

   h. Click **OK**.

   i. Close all windows to return to your desktop.

6. Delete the folder where Gentran Integration Suite was installed, including all subfolders. For example, delete *C:\SterlingCommerce* and its subfolders.

7. If you use an Oracle or SQL Server 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 the unwanted tables and recovering the database space where Gentran Integration Suite resided.
8. After you remove Gentran Integration Suite from the server, you can remove Eclipse, and any tools that were downloaded to the desktop:

   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 Windows Environment

Situation	Message or Symptom	Explanation/Resolution
Installing	You encounter errors or problems during installation.	**Explanation** Installation creates two log files, one for the first (bootstrap) phase and a second for the actual installation phase. **Resolution** Examine the log files generated during installation: ◆ *install_dir*\bootstrap.log ◆ *install_dir*\SI\installSI.log
Installing	During installation, you select the destination directory and the installation program stops running.	**Explanation** The command window was closed after you selected the destination directory. **Resolution** Delete the destination directory and re-start the installation process. Do not close the command window.
Installing	You started the installation program but realize that the license file has not been downloaded.	**Resolution** Minimize the installation window, obtain the license file, and then continue with the installation procedure.
Installing	During installation, you identify the initial port number and then see the message: *Port number is already in use*.	**Resolution** Choose one: ◆ Use a different port number. ◆ Stop the service that is using the port number that you want to use.
Installing	During installation, you enter database information and see the message: *Information is incorrect.*	**Explanation** One or more of the criteria for the database is incorrect. **Resolution** Click **Back** to redisplay the dialog box that asks for the database information. Correct the error and click **Next**.

Situation	Message or Symptom	Explanation/Resolution
Installing	Installation appears to complete successfully, but Gentran Integration Suite services are not installed.	**Explanation** You may have reinstalled Gentran Integration Suite on a Windows server and chosen the same initial port. **Resolution** If this is the case, either reinstall Gentran Integration Suite in a different directory using a different port, or follow the steps below to uninstall the existing Gentran Integration Suite services prior to reinstalling Gentran Integration Suite. 1 Change to the *install_dir*\bin directory. 2 Run the **stopWindowsService.cmd** command and wait for all Gentran Integration Suite Windows services to stop. 3 Run the **uninstallWindowsService.cmd** command and log off. This cleanly removes the old Windows services from Windows cache and verifies that there are no scheduled jobs running in the background. 4 Delete the *install_dir* directory. 5 You can now install the new version of Gentran Integration Suite at the same port.
Installing	After installing Gentran Integration Suite, a gisInstall.* subdirectory is left in the current working directory. This can cause the file system to become full.	**Explanation** The Java installer is not allowed to delete the gisInstall.*/platform_core_2000.jar because it is “in use” by the JVM. **Resolution** Manually delete the leftover gisInstall.* subdirectory on Windows after each installation attempt.
Starting	If Gentran Integration Suite does not start, examine the log file in *install_dir*\SI\logs for an invalid or corrupt license file.	**Resolution** Obtain the license file. Then restart Gentran Integration Suite.

Situation	Message or Symptom	Explanation/Resolution
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 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.cmd *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 47.

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
- 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 58
- *File System Adapter and Command Line2 Adapters* on page 61

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.cmd` utility located in the *install_dir*\bin directory of the 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 61.

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 62.

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
   a. At a DOS prompt, go to the *install_dir*\bin directory.
   b. Run the command `startCluster.cmd 1`.
   c. After `startCluster.cmd 1` completes successfully, click the start icon that was created during the installation.

Note: You should run `startCluster.cmd` command only after you install Gentran Integration Suite. You should not run `startCluster.cmd` 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 28 to start the cluster without updating the database settings.

2. Node 2
   a. At a DOS prompt, go to the *install_dir*\bin directory.
   b. Run the command `startCluster.cmd 2`.
   c. After `startCluster.cmd 2` completes successfully, click the start icon that was created during the installation.
   d. Follow this same procedure for other nodes. For example, Node 3 would use the command `startCluster.cmd 3`.

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 63
- *Advanced File Transfer Tab* on page 64
- *Reconfiguring Archive Settings* on page 65
- *Correcting Missing Manager IDs* on page 65

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.cmd` 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.cmd` 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

A

adapters 58

administration, initial 49

administrator login 47

Advanced File Transfer tab 64

C

ccaseid.jar 38

cluster
- available databases 26
- communications 29
- configuration 28
- document storage 30
- environment verification 30
- hot-fixes 37
- licenses 18, 20
- multiple nodes 28
- MySQL 26
- patches 32
- perimeter server 39
- setup 28
- upgrade installation 20

Command Line Adapter 61

Command Line2 adapter 61

configuring services and adapters 58

customer changes, preserving 14

D

DB2
- schema change script 36

decryption, Windows password 12

default
- login 47
- password 47
- user ID 47

desktop tools 56

documentation 65

downloading files 7

downloading, tools 56

dump_info.cmd 38

E

encryption
- Windows password 12

F

Federation adapter 58

File System adapter 61

files, downloading 7

fix_db2_schema.sql 36

FTP adapter 58

G

Graphical Process Modeler, downloading tips 56

H

hardstop.cmd 31, 34

hot-fix, installing 37

I

installing
- hot-fix 37
- perimeter server 39
- perimeter server (less secure network) 42
- perimeter server (more secure network) 41
- troubleshooting 54
- validating 49

installPS.cmd 42, 43

installWindowsService.cmd 38

IP addresses, correcting conflicts 56

J

Java 2 Software Development Kit. See JDK

JDBC adapter 58

JDK installation 18

L

license files 19

Lightweight JDBC adapter 58

login, default 47

M

Manager ID 65

Map Editor, downloading tips 56

MESA Developer Studio
  downloading 49, 56
  removing 53

N

network interface bindings 47, 63

network interfaces 47

noapp.properties.in 63

P

Page cannot be displayed error 47

password
  decrypting password (Windows) 12
  encrypting database passwords 12
  encrypting password (Windows) 12

password, default 47

performance tuning 62

perimeter server
  installing 39
  installing (less secure network) 42
  installing (more secure network) 41
  setup 40
  starting 44
  stopping 44

port numbers 19

postinstallation 47

post-upgrade processes 57

preserving customer changes 14

process activity log 9

process.cmd 9

property files
  database pool properties 58
  jdbc.properties 58, 60
  jdbc_customer.properties.in 59
  noapp.properties.in 63
  perimeter.properties.in 64
  poolManager.properties 58, 60
  upgrade overwrite 8

R

reconfiguring archive settings 65

Reporting Services
  downloading 49, 56
  removing 53

run.cmd 28

S

script
  dump_info.cmd 38
  hardstop.cmd 31, 34
  installPS.cmd 42, 43
  installWindowsService.cmd 38
  process.cmd 9
  run.cmd 28
  setupfiles.cmd 28, 30, 60, 63
  softstop.cmd 31
  startCluster.cmd 28, 29, 34, 35, 36, 38, 62
  startPSService.cmd 42, 43
  stopWindowsService.cmd 55
  uninstallWindowsService.cmd 38, 55
  upgrade.cmd 9

security
  decrypting password (Windows) 12
  encrypting password (Windows) 12

services 58

setupfiles.cmd 28, 30, 60, 63

setups, administrative 49

softstop.cmd 31

startCluster.cmd 28, 29, 34, 35, 36, 38, 62

startPSService.cmd 42, 43

startupPs.cmd 44

stopWindowsService.cmd 55

SyncEngine HTTP Server adapter 58

system
  removing 51
  starting 47
  stopping 50
  uninstalling 51

system administration, initial 49

system requirements 18

T

third-party libraries 57

troubleshooting 54
  access 47
  installation 49
  Page cannot be displayed 47

U

uninstallWindowsService.cmd 38, 55

upgrade
  installation 24
  prerequisites 7

upgrade.cmd 9

user documentation 65

user ID, default 47

V

validating installation 49

W

Web Template Designer, downloading tips 56