

# **Gentran Integration Suite**

---

## **UNIX/Linux Non-Cluster Installation**

**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

<b>Chapter 1 Introduction</b>	<b>7</b>
<b>Chapter 2 Setting Up the Database (UNIX or Linux)</b>	<b>8</b>
Create and Configure the Database Server (UNIX/Linux) . . . . .	8
Database Sizing . . . . .	8
Capacity Planning . . . . .	8
Tracking and Estimating Future Disk Requirements . . . . .	9
JDBC Drivers Installation . . . . .	9
Oracle Installation . . . . .	9
Choose a Character Set . . . . .	9
Oracle Database User Privileges . . . . .	10
Configure an Oracle Database for Production . . . . .	11
Oracle Database Server . . . . .	12
Setting Database Parameters in Oracle . . . . .	12
Roll Back or Undoing Changes in Oracle . . . . .	13
Grant Permissions in Oracle . . . . .	13
Installing the JDBC Driver in Oracle (UNIX/Linux) . . . . .	14
Enable Failover in a Multiple Node Oracle RAC Database Cluster (UNIX/Linux) . . . . .	14
Install Microsoft SQL Server 2000/2005 . . . . .	15
Set Database Parameters in SQL Server . . . . .	15
SQL Server Database User Privileges . . . . .	15
Configure a SQL Server Database for a Production Environment . . . . .	15
Install the JDBC Driver in SQL Server . . . . .	16
Install the JDBC Driver in SQL Server 2000 . . . . .	16
Install the JDBC Driver in SQL Server 2005 . . . . .	16
Configuring Snapshot for Microsoft SQL Server 2005 . . . . .	17
Install DB2 . . . . .	17
DB2 Database User Privileges . . . . .	17
Configure a DB2 Database for Production . . . . .	17
Use a DB2 Database Server . . . . .	18
Install Client Components, Compilers, and Fixpack . . . . .	18
Set Parameters for DB2 . . . . .	18
Grant Permissions for DB2 . . . . .	19
Install JDBC Drivers for DB2 . . . . .	19
Use a MySQL Database Server (Non-Clustered Only) . . . . .	19

Starting and Stopping MySQL Database . . . . .	19
Managing Database Passwords . . . . .	20
Database Password Encryption Methods . . . . .	20
Encrypting Database Passwords (UNIX) . . . . .	20
Decrypting Database Passwords (UNIX) . . . . .	20

---

## **Chapter 3 Installing in a Non-Clustered UNIX or Linux Environment** **22**

---

Preinstallation Setup Checklist for a Non-Clustered UNIX or Linux Environment . . . . .	22
Checklist for UNIX or Linux Preinstallation . . . . .	22
Checking System Requirements . . . . .	27
Java 2 Software Development Kit Installation . . . . .	28
Download the JCE Distribution File . . . . .	28
Port Numbers . . . . .	29
UNIX Accounts . . . . .	29
Database Definition Language (DDL) Statements . . . . .	29
Obtain a License File . . . . .	30
Silent Installations . . . . .	31
Install the JDBC Driver in SQL Server . . . . .	32
Install the JDBC Driver in SQL Server 2000 . . . . .	32
Install the JDBC Driver in SQL Server 2005 . . . . .	32
Install in a Non-Clustered UNIX or Linux Environment . . . . .	33
Patches and Hot-Fixes (Non-Cluster) . . . . .	36
Install the Current Maintenance Patch in UNIX or Linux (Non-Cluster) . . . . .	36
Run the DB2 Schema Change Script . . . . .	38
Install a Hot-Fix (Non-Cluster) . . . . .	38
Hot-Fix Package Delivery Method . . . . .	39
Perform a Checksum using DB Checksum Tool . . . . .	40
Install a Perimeter Server in a Non-Clustered UNIX or Linux Environment . . . . .	41
Set Up Perimeter Servers with Gentran Integration Suite . . . . .	41
Install a Perimeter Server in a More Secure Network (UNIX/Linux Non-Clustered) . . . . .	42
Install a Perimeter Server in a Less Secure Network (UNIX/Linux Non-Clustered) . . . . .	43
Install Patches in a Perimeter Server UNIX or Linux Environment . . . . .	44
To Update a Remote Perimeter Server in a Non-Clustered UNIX or Linux environment: . . . . .	44
Start Perimeter Servers in UNIX or Linux . . . . .	45
Stop Perimeter Servers in UNIX or Linux . . . . .	45
Reduce Perimeter Server Security Vulnerabilities . . . . .	45
Grant Permissions for Specific Activities By a Perimeter Server . . . . .	45
Performing DNS Lookup on Remote Perimeter Server . . . . .	47
Post Installation in a Non-Clustered UNIX or Linux Environment . . . . .	47
Start Gentran Integration Suite in UNIX or Linux . . . . .	48
Access Gentran Integration Suite . . . . .	48
Technical Note: Changes to Network Interface Bindings . . . . .	48
Validate the Installation . . . . .	50
Download Gentran Integration Suite Tools . . . . .	50
Perform Initial Administrative Setups in Gentran Integration Suite . . . . .	50
Stop Gentran Integration Suite . . . . .	51
Uninstall Gentran Integration Suite from a Non-Clustered UNIX or Linux Environment . . . . .	51
Troubleshooting: UNIX or Linux Environment (Non-Clustered) . . . . .	53

---

**Chapter 4 Installing and Configuring MESA Developer Studio 55**


---

Overview for Installing and Configuring MESA Developer Studio . . . . .	55
Assumptions and Prerequisites . . . . .	55
Steps to Set Up MESA Developer Studio . . . . .	56
Eclipse Terms . . . . .	56
Configuring J2SE on Your PC . . . . .	57
Verifying that MESA Developer Studio Uses the Correct JRE . . . . .	57
Starting the WebDAV Server . . . . .	58
Gentran Integration Suite (UNIX) . . . . .	58
Installing MESA Developer Studio Components . . . . .	58
Changing Proxy Preferences . . . . .	59
Installing New Features . . . . .	59
Setting Up a Gentran Integration Suite Instance . . . . .	60
Editing Connection Information . . . . .	60
Viewing Configuration Details . . . . .	61
Refreshing the Instance . . . . .	61
Installing Additional MESA Developer Studio Components and Updates . . . . .	61
Installing Reporting Services Plug-Ins . . . . .	62

---

**Chapter 5 Configuring Properties 63**


---

Properties to Prevent Cross-Site Script Vulnerabilities . . . . .	63
Setting the Database Connection Properties . . . . .	63
Properties for LDAP User Authentication . . . . .	64

---

**Chapter 6 Configuring Utilities 66**


---

Installation Utilities . . . . .	66
Loading Gentran Integration Suite Database Factory Defaults . . . . .	66
Verifying the Database . . . . .	67

---

**Appendix A Configuring for a Non-English Environment 69**


---

Installing the Language Pack on UNIX/Linux . . . . .	69
Installing on a Remote Computer . . . . .	70
Loading Gentran Integration Suite Language Pack Factory Defaults . . . . .	70
Loading Gentran Integration Suite Language Pack Translations . . . . .	70
Switching Gentran Integration Suite Base Language . . . . .	70
Configuring Encodings for Gentran Integration Suite . . . . .	71
Configuring Locales . . . . .	72

---

**Appendix B Using Gentran Integration Suite with Gentran:Server for UNIX 74**


---

About Gentran:Server for UNIX and Gentran Integration Suite . . . . .	74
Installing and Configuring Attunity® Data Connect . . . . .	75
Configuring Gentran Integration Suite to Run with Gentran:Server for UNIX . . . . .	76

<b>Appendix C Migrating from Gentran:Server for UNIX to Gentran Integration Suite</b>	<b>78</b>
---	-----------

---

<b>Index</b>	<b>79</b>
--------------	-----------

---

---

## Introduction

Use the Gentran Integration Suite *4.3 UNIX/Linux Non-Cluster Installation Guide* to install Gentran Integration Suite 4.3 in a non-clustered (single node) UNIX/Linux environment.

This guide focuses on these installation tasks, including:

- ◆ Setting up the database
- ◆ Installing the Gentran Integration Suite software
- ◆ (If licensed) Installing and configuring MESA Developer Studio
- ◆ Configuring properties files
- ◆ Configuring installation utilities
- ◆ Configuring the application for a non-English environment
- ◆ Using Gentran Integration Suite with Gentran:Server for UNIX

For upgrades, use the Gentran Integration Suite *4.3 UNIX/Linux Non-Cluster Upgrade Guide*.

---

# Setting Up the Database (UNIX or Linux)

---

---

## Create and Configure the Database Server (UNIX/Linux)

You must install, create, and configure a database so that each Gentran Integration Suite instance has a dedicated schema and login for the database. See *System Requirements* for supported version information.

**Caution:** If you are reinstalling Gentran Integration Suite, be aware that data in your existing database will be deleted. To prevent this, either back up the existing database or save it under a different name.

**Caution:** After creating and configuring your database, recycle the database. Then stop and restart to apply the changes.

In a UNIX or Linux environment, Gentran Integration Suite supports the following databases:

- ◆ Oracle 9i or 10g, for more information, refer to *Oracle Installation* on page 9.
- ◆ Microsoft SQL Server 2000, for more information, refer to *Install Microsoft SQL Server 2000/2005* on page 15.
- ◆ Microsoft SQL Server 2005, for more information, refer to *Install Microsoft SQL Server 2000/2005* on page 15.
- ◆ DB2, for more information, refer to *Install DB2* on page 17.
- ◆ MySQL (non-clustered only), for more information, refer to *Use a MySQL Database Server (Non-Clustered Only)* on page 19.

## Database Sizing

Database sizing is designed to give you estimates of the database growth and to assist in planning the disk requirements.

## Capacity Planning

There are many factors to consider when estimating the amount of disk space that will be required for Gentran Integration Suite. As a result, trying to consider all growth factors is impractical because the user may not know the answers to many questions that are required to do a detailed forecast. Over the years the cost of disks has dramatically decreased, and the capacity and speed of disks has increased. The method of



how information system managers order disk capacity has also changed from purchasing disk arrays that are dedicated to a particular database server and project to the concept of SANS.

Gentran Integration Suite provides a methodology to estimate your initial disk requirements. Consider the confidence that you have in your data estimates when making the final purchase decision and adjust accordingly. After the initial purchase and production deployment, disk growth should be tracked for future purchase forecasts.

## Tracking and Estimating Future Disk Requirements

You should regularly track your actual database storage usage and number of database records. Correlating these two metrics will enable you to plan your future disk requirements. Moreover, determining the average amount of space used for each order line or shipment line enables you to accurately predict your future growth requirements.

## JDBC Drivers Installation

Gentran Integration Suite requires the appropriate JDBC driver. See *System Requirements* for supported version information. The supported versions of the JDBC driver build the correct Gentran Integration Suite directory structure.

After you obtain the correct JDBC driver file, record the absolute path to its location on your system. You must supply this absolute path when you install Gentran Integration Suite.

For more information about accessing and installing these files, refer to the sections for each database (MySQL, Oracle, DB2, and Microsoft SQL Server).

## Oracle Installation

You can use an Oracle database for maintaining information on Gentran Integration Suite. The following sections provide the necessary steps to install and configure an Oracle database for production:

- ◆ *Choose a Character Set* on page 9
- ◆ *Oracle Database User Privileges* on page 10
- ◆ *Configure an Oracle Database for Production* on page 11

### Choose a Character Set

To install Oracle with single or multiple byte characters, perform these steps:

1. If you do not have Oracle installed, perform the installation procedures in your Oracle Installation manuals.
2. Run the create instance procedure. Use a character set appropriate for your desired language, using the following command:

```
CHARACTER SET "AL32UTF8"
```

3. Configure the INIT<INSTANCE\_NAME>.ORA file for Oracle as follows:

```
open_cursors= <set to appropriate value>
```

For example, the minimum value for WebLogic equals number of threads (across all application servers) + (connection pool size X prepared statement pool size).

```
cursor_sharing=exact
compatible=<10.2.0.1>
timed_statistics=true
db_block_size=8192
optimizer_mode=CHOOSE
```

If you are using multi-byte character set, set the following and restart Oracle:

```
nls_length_semantics=CHAR
```

Alternatively you can run:

```
alter session set nls_length_semantics = CHAR
```

prior to running any create table scripts.

Setting this attribute ensures that the field sizes are not impacted by the number of bytes a data type can store. For example, Varchar(40) would now be able to store 40 Japanese characters instead of 40/3 bytes in the AL32UTF-8 character set.

**Note:** When you change the multi-byte character set to **CHAR** by setting `nls_length_semantics = CHAR`, Oracle reserves space equivalent to 'n' chars, which is more than 'n' bytes. Therefore, when you run the `dbverify.cmd` command, the reduced entries in table columns are printed in the `Yantra_TableDrops.sql` file.

4. Download the Oracle JDBC driver `ojdbc14.jar` from the Oracle web site and copy to a well-known location for reference during installation.

## Oracle Database User Privileges

**Caution:** The access given by these Oracle permissions might violate your internal security policies, since they give the Gentran Integration Suite user access to all schemas in the Oracle database. You might need to refine your permissions to give the user access to just the necessary non-Gentran Integration Suite database objects.

Unless specifically stated for a given task, the Gentran Integration Suite user does not require database administrator (DBA) privileges.

The following are some of the basic privileges that are given to the Gentran Integration Suite administrative user who is involved in creating and modifying the Oracle database:

- ◆ ALTER SESSION
- ◆ CREATE PROCEDURE
- ◆ CREATE SEQUENCE
- ◆ CREATE SESSION
- ◆ CREATE SYNONYM
- ◆ CREATE TABLE

- ◆ CREATE VIEW
- ◆ EXECUTE ANY PROCEDURE
- ◆ INSERT ANY TABLE
- ◆ UPDATE ANY TABLE
- ◆ SELECT ANY TABLE

The following are some of the basic privileges given to the application user whose involvement is restricted just to running the application:

- ◆ ALTER SESSION
- ◆ EXECUTE ANY PROCEDURE
- ◆ INSERT ANY TABLE
- ◆ UPDATE ANY TABLE
- ◆ SELECT ANY TABLE

## Configure an Oracle Database for Production

You need to configure your Oracle database for running in a production environment with Gentran Integration Suite. To configure an Oracle database for a production environment, you must:

- ◆ Size the database by estimating the required disk space. For more information, refer to *Database Sizing* on page 8.
- ◆ Create views and db\_link or synonyms for integrating with the Sterling Warehouse Management System installation. Set the database connection properties.
- ◆ Set the database connection properties.

To create the Oracle database to handle multiple byte characters, do the following:

1. Do not modify the Gentran Integration Suite DDL.
2. Choose the correct data encoding format for your language.
3. Choose the character set suitable for your language.

To configure Oracle database for your production environment manually, you must set up and run a series of scripts to create the tables, indexes, sequences, and so forth for your schema.

These script files reside in the `/install_dir/install/database/oracle/scripts` directory. The table, index, and sequence creation DDLs are created during installation. These reside in `/install_dir/install/repository/scripts` directory.

To set up scripts (if you are using locally managed tablespaces or another utility to size your database), do the following:

1. Create tablespaces where the Gentran Integration Suite tables and indexes reside.
2. If you are manually creating database tables after installation (instead of having installation create them automatically), do the following:

Modify the `/install_dir/install/repository/scripts/EFrame_TableChanges.sql` file to reference your newly created tablespaces.

The DDLs in the Gentran Integration Suite scripts create a standard set of indexes. You may need to create additional indexes or modify existing indexes according to your business practice.

To run the scripts, do the following:

1. Log into the Oracle server manager as `sysdba`.
2. Create the user that is the designated schema owner.
3. Grant the privileges listed in the Installation Checklist to the newly created user.
4. Log out of the Oracle Server Manager and log back in as the newly created user.
5. Verify the database.
6. Load Gentran Integration Suite database factory defaults.
7. Check for the degree of parallelism.

## Oracle Database Server

You can use an Oracle 9i or 10g database with Gentran Integration Suite. See *System Requirements* for supported version information.

To use an Oracle 9i or 10g database, follow this process:

- ◆ Create the database. Refer to the Oracle documentation for information about creating the database, including creating a schema repository, login, and tablespace. Be sure to install the correct version and patches.
- ◆ Configure the database by completing the following tasks:
  - ◆ *Setting Database Parameters in Oracle* on page 12
  - ◆ *Roll Back or Undoing Changes in Oracle* on page 13
  - ◆ *Grant Permissions in Oracle* on page 13
  - ◆ *Installing the JDBC Driver in Oracle (UNIX/Linux)* on page 14
  - ◆ *Enable Failover in a Multiple Node Oracle RAC Database Cluster (UNIX/Linux)* on page 14

### Setting Database Parameters in Oracle

Gentran Integration Suite requires the following parameter settings in your Oracle database:

Parameter	Value
Number of open cursors	Greater than or equal to 2000
cursor_sharing	EXACT
Database block buffers	Greater than or equal to 19200 <b>Note:</b> Sterling Commerce recommends that this be set to 0 if SGA memory equals greater than 0.

Parameter	Value
System Global Area (SGA) memory (10g only)	Greater than 0 <b>Note:</b> Sterling Commerce recommends that the database block buffers be set to <b>0</b> if SGA memory equals greater than 0.
Shared pool size	Greater than or equal to 90000000
Large pool size	Greater than or equal to 614400
Java pool size	Greater than or equal to 20971520
Number of processes	Greater than or equal to 500
Log buffer	Greater than or equal to 163840
Database block size	Greater than or equal to 8192
Sort area size	Greater than or equal to 65536
Sort area retained size	Greater than or equal to 65536
Max extends	Unlimited
Character set	AL32UTF8

## Roll Back or Undoing Changes in Oracle

You can roll back or undo changes in Oracle using one of the following methods:

- ◆ (Oracle versions earlier than 9i) Gentran Integration Suite recommends that you configure a rollback segment for every four concurrent users. Each rollback segment must be extendable to 25MB. The values of the initial segment and the next segment can vary between 256 KB and 10 MB. Note that these ranges will vary based on the size of your database and the number of business rules it contains.
- ◆ (Oracle versions 9i or later) These versions support AUTO UNDO management. It is recommended that you use this option. This will avoid any manual monitoring of UNDO segments.

If a server is upgraded from Oracle 8i, set the UNDO\_MANAGEMENT=AUTO parameter in init<SID>.ora. Your database administrator needs to determine the UNDO\_RETENTION setting. Ensure that the file system which has the UNDOTBS1 tablespace has enough space to use the AUTOGROW setting.

## Grant Permissions in Oracle

Grant the following permissions to the user:

```
GRANT "CONNECT" TO <USER>
GRANT SELECT_CATALOG_ROLE TO <USER>
ALTER USER <USER>DEFAULT ROLE "CONNECT",
        SELECT_CATALOG_ROLE
GRANT CREATE PROCEDURE TO <USER>
GRANT CREATE TRIGGER TO <USER>
GRANT CREATE TYPE TO <USER>
GRANT EXECUTE ANY PROCEDURE TO <USER>
GRANT EXECUTE ANY TYPE TO <USER>
GRANT SELECT ANY TABLE TO <USER>
```

```
GRANT SELECT ANY DICTIONARY TO <USER>
```

For Oracle 10g 10.2.x, also grant the following permission:

```
GRANT "RESOURCE" TO <USER>;
ALTER USER <USER> DEFAULT ROLE "CONNECT", "RESOURCE", SELECT_CATALOG_ROLE;
```

**Note:** If you are using Oracle AQ for Oracle 9i or Oracle 10g, then grant the AQ\_ADMINISTRATOR\_ROLE permission.

## Installing the JDBC Driver in Oracle (UNIX/Linux)

Gentran Integration Suite requires the appropriate JDBC driver for Oracle Database 10g and Oracle 9i databases. These drivers are thin client based pure Java JDBC drivers. See *System Requirements* for supported version information.

The supported versions of the JDBC driver will build the correct Gentran Integration Suite directory structure.

After obtaining the correct JDBC driver, record the absolute path to its location on your system. You must supply this absolute path when installing Gentran Integration Suite.

## Enable Failover in a Multiple Node Oracle RAC Database Cluster (UNIX/Linux)

To enable failover in a multiple node Oracle RAC database cluster in UNIX/Linux, do the following:

1. Navigate to the *install\_dir/install/properties* directory to modify *sandbox.cfg* file.
2. In the *sandbox.cfg* file, add a new property for ORACLE\_JDBC\_URL, which contains the Oracle RAC connection URL.

The following example shows the suggested URL form and the way it is organized. However, the property value must be one string of text starting with ORACLE\_JDBC\_URL=. Your database administrator (DBA) can modify this URL as needed.

```
jdbc:oracle:thin:@
(DESCRIPTION=
  (ADDRESS_LIST=
    (FAILOVER=ON)
    (LOAD_BALANCE=OFF)
    (ADDRESS=(PROTOCOL=TCP)(HOST=myhost1)(PORT=1521))
    (ADDRESS=(PROTOCOL=TCP)(HOST=myhost2)(PORT=1521))
  )
  (CONNECT_DATA = (SERVER = DEDICATED)(SERVICE_NAME = myservicename))
)
```

3. Run the *setupfiles.sh* command from the *install\_dir/install/bin* directory.
4. Set the propagation delay on the RAC server to 0.

## Install Microsoft SQL Server 2000/2005

You can use a SQL Server database for maintaining information on Gentran Integration Suite. See *System Requirements* for supported version information.

If you do not have SQL Server installed, follow the installation procedures in your SQL Server Installation manual. Refer to the SQL Server documentation for information about creating the database, including creating a schema repository, login, and tablespace. Be sure to install the correct version and patch.

**Note:** Ensure that Named Pipes & TCP/IP protocols are enabled in the network utility of the SQL Server. For SQL Server 2005, do not use case-sensitive column names in the database. Case-sensitive names will prevent the SQL Server 2005 System Management Console from loading.

### Set Database Parameters in SQL Server

To create a database, ensure that the collation property you select supports all the characters for your database.

The following parameter settings are required in your SQL Server database:

Parameter	Value
Collation Setting	SQL_Latin1_General_CP850_BIN
Sort order	Binary
Security authentication	SQL Server and Windows
Torn Page Detection	Off
Parallelism	Use one processor (do not use all available processors)

### SQL Server Database User Privileges

In SQL Server, you must grant DBO (Database Owner) permission to the user. The DB\_DDLADMIN role is required for creating objects in the SQL Server database.

### Configure a SQL Server Database for a Production Environment

You need to configure your SQL Server database for running in a production environment with Gentran Integration Suite. To configure a SQL Server database for a production environment, you must:

- ◆ Size the database by estimating the required disk space. For more information, refer to *Database Sizing* on page 8.
- ◆ Run the database scripts to create tables, indexes and so forth for the SQL Server database.
- ◆ Set the database connection properties.

To run the scripts for the SQL Server database, do the following:

1. Make sure you have a SQL Server client installed on your computer.
2. Run the CustomDBView script.
3. Examine the log files for errors.

## Install 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.

### Install the JDBC Driver in SQL Server 2000

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

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

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

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

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

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

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

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

- ◆ Point to the bundled jar file.

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

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

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

### Install the JDBC Driver in SQL Server 2005

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

1. Download `sqljdbc_version_language.tar.gz` to a temporary directory.
2. To unpack the zipped tar file, navigate to the directory where you want the driver unpacked and type the following command:

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



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

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

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

4. When the 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;
```

## Install DB2

You can use a DB2 database for maintaining information on Gentran Integration Suite. The following sections provide the necessary steps to install and configure a DB2 database for production.

Before you begin:

- ◆ The appropriate codepage needs to be selected for international language characters (for example, UTF-8).

To install DB2, do the following:

1. If you do not have DB2 installed, follow the installation procedures in your DB2 Installation manual.
2. Copy the jars to a well-known location for reference during installation. The two jar files have to be repackaged as one file for the installer. Unzip the files into a folder and rezip them as one jar file.  
**Note:** Various Gentran Integration Suite scripts, such as the one used for loading the factory defaults, specify a *DB\_Driver*. The *DB\_Driver* specified must include **both** of these JAR files.
3. You need to set the following parameter to avoid memory leaks and DB2 crashes:

```
db2set DB2_NUM_CKWP_DAEMONS=0
```

## DB2 Database User Privileges

The DBADM role is required for performing administrative operations in the DB2 database.

## Configure a DB2 Database for Production

You need to configure your DB2 database for running in a production environment with Gentran Integration Suite. To configure a DB2 database for a production environment, you must size the database by estimating the required disk space. It is not recommended to use multiple schemas in a database. If necessary, you can

create multiple databases (one per user) to prevent schema collisions. For more information, refer to *Database Sizing* on page 8.

The installation script creates tables and indexes. Certain tables require a page size of 16K. You should have a tablespace to accommodate such tables. DB2 automatically places tables and indexes in the available tablespaces using its internal logic. You can move the tables to a different tablespace after the installation is complete.

## Use a DB2 Database Server

You can use a DB2 database with Gentran Integration Suite. See *System Requirements* for supported version information. To use a DB2 server, follow this process:

- ◆ Create the database. Refer to the DB2 documentation for information about creating the database, including creating a schema repository, login, and tablespace. Be sure to install the correct version and patch. Be sure to install the client components and compilers before you install the fixpack.
- ◆ Configure the database by completing the following tasks:
  - ◆ *Install Client Components, Compilers, and Fixpack* on page 18
  - ◆ *Set Parameters for DB2* on page 18
  - ◆ *Grant Permissions for DB2* on page 19
  - ◆ *Install JDBC Drivers for DB2* on page 19

### Install Client Components, Compilers, and Fixpack

Gentran Integration Suite uses stored procedures for DB2. You must install or set up the following components:

1. Install the Administration client.
2. Install Gentran Integration Suite Development clients.
3. Install the necessary fix pack after you install the client components and compilers. Otherwise, the clients will overwrite the fix pack binaries.
4. Set the path for the compiler by using the **db2set** command.

For more information about these tasks, see the IBM documentation.

### Set Parameters for DB2

The following parameter settings are required in your DB2 database:

Parameter	Value
APPLHEAPSZ	greater than or equal to 10000
APP_CTL_HEAP_SZ	greater than or equal to 512
MAXAPPLS	greater than or equal to 150

Parameter	Value
LOCKLIST	greater than or equal to 30000
MAXLOCKS	100
Database code page	UTF-8

## Grant Permissions for DB2

Grant DBADM permissions to the user.

## Install JDBC Drivers for DB2

For DB2, install the appropriate DB2 JDBC Type 4 driver and any correlating patches. See *System Requirements* for supported version information.

You can obtain these files from the IBM Web site. After you obtain this JDBC driver, record the absolute path to its location on your system. You must supply this absolute path during installation.

If the JDBC driver provided by your database vendor is distributed among multiple files, you must place all the files that comprise the JDBC driver into one .jar file. Follow these steps to create one .jar file:

1. Identify all the vendor database jar files for the JDBC driver.
2. Create a temporary working directory (mkdir wd; cd wd).
3. Extract the contents of each file used for the JDBC driver using the jar utility into the temporary working directory (jar -xf /path/to/db2jcc.jar and jar -xf /path/to/db2jcc\_license.jar).
4. Bundle the files in the temporary working directory into one file using the jar utility (jar -cf /path/to/new\_db2\_all.jar \*).
5. Record the absolute path to the .jar file you created on the Preinstallation Checklist.

The Type 4 driver does not require a separate Java listener running on the database server. Instead, connect directly to the DB2 port.

## Use a MySQL Database Server (Non-Clustered Only)

Only UNIX/Linux non-clustered installations of Gentran Integration Suite can use the MySQL database.

You can choose to use the MySQL database server that is bundled with Gentran Integration Suite. Choosing this database during the installation procedure creates and configures it for you. MySQL is installed locally on the same server as Gentran Integration Suite and cannot be installed on a separate server.

### Starting and Stopping MySQL Database

If you change the hostname after installing Gentran Integration Suite, you should change the MySQL database password and then use `control_mysql.sh` script to start or stop MySQL database.

**Note:** You should complete the following task only if you change the hostname.

To change the MySQL database password after changing the hostname:

1. Start the MySQL database by running the `control_mysql.sh start` command.
2. Change the root user password to `<new_hostname + old_mysqlport>`. Refer to the following example command:

```
/<absolute path>/mysql/bin/mysqladmin --port=43003  
--socket=/tmp/mysql.43003.sock --user=root --password=blriedlin0143003  
password "blriedlin01Temp43003"
```
3. Stop the MySQL database by running the `control_mysql.sh stop` command.

---

## Managing Database Passwords

A password is used by the application to connect to its database. The password is stored as clear text in a property file on the system. If the security policies at your company require you to encrypt these passwords, you can do so after you install Gentran Integration Suite. Encrypting these passwords is optional.

### Database Password Encryption Methods

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

### Encrypting Database Passwords (UNIX)

To encrypt the database password:

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

### Decrypting Database Passwords (UNIX)

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

1. Stop the Gentran Integration Suite.
2. Navigate to `/install_dir/install/properties`.
3. Open the `sandbox.cfg` file.

4. Copy encrypted password from the `database_PASS` property. Use the text that appears after the `database_PASS=` text. For example, if `database_PASS= OBSCURED:123ABCxyz321`, you would copy the text `OBSCURED:123ABCxyz321`. (OBSCURED is the encryption method for the password.)
  5. Navigate to `/install_dir/install/bin`.
  6. Enter `./decrypt_string.sh encrypted_password`. For `encrypted_password`, use the text that you copied in Step 4.  
You are prompted for the Sterling Integrator passphrase.  
Your decrypted password appears.
  7. Navigate to `/install_dir/install/properties`.
  8. Edit the `sandbox.cfg` file to replace the encrypted password with the password that was returned in Step 6.
  9. You need to decrypt the entry for `YANTRA_DB_PASS`. Repeat Steps 4 to 8 to decrypt `YANTRA_DB_PASS`.
- Note:** You should also decrypt any custom database pool passwords present in the `customer_overrides.properties` file or any other properties file.
10. Navigate to `/install_dir/install/bin`.
  11. Enter `./setupfiles.sh`.
  12. Enter `./deployer.sh`.
  13. Enter `./run.sh` to start the Gentran Integration Suite.
  14. Enter your passphrase.

---

# Installing in a Non-Clustered UNIX or Linux Environment

**Caution:** Gentran Integration Suite should be installed behind a company firewall for security purposes. See the Perimeter Server and Security topics in the Gentran Integration Suite documentation library for more information on secure deployment options.

---

## Preinstallation Setup Checklist for a Non-Clustered UNIX or Linux Environment

The following topics will assist you with preinstallation tasks when planning to install Gentran Integration Suite in a non-clustered UNIX or Linux environment:

*Checklist for UNIX or Linux Preinstallation* on page 22

*Checking System Requirements* on page 27

*Java 2 Software Development Kit Installation* on page 28

*Download the JCE Distribution File* on page 28

*Port Numbers* on page 29

*UNIX Accounts* on page 29

*Database Definition Language (DDL) Statements* on page 29

*Obtain a License File* on page 30

*Silent Installations* on page 31

*Install the JDBC Driver in SQL Server* on page 32

## Checklist for UNIX or Linux Preinstallation

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

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

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

Do not use spaces or apostrophes.

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

Step	Description	Your Notes
1	Verify that your system meets the hardware and software requirements specified for this release. See <i>Checking System Requirements</i> on page 27.	
2	Verify that your system has the patches required by Java™ for the operating system. For HP, you must run the HP JConfig utility to obtain the required patches and kernel modifications.	
3	<p>For the HP-UX operating system, establish these settings:</p> <ul style="list-style-type: none"> <li>◆ Verify kernel parameters and establish the following minimum settings by running <code>kctune</code> command:           <pre>kctune max_thread_proc 1024 kctune maxdsiz 2147483648 kctune maxdsiz_64bit 8589934592 kctune maxssiz 369098752 kctune maxssiz_64bit 536870912</pre> </li> <li>◆ Run <code>ulimit</code> utility, verify, and establish the following minimum settings:           <pre>ulimit -d = 2097152 (in kilobytes) or higher ulimit -s = 360448 (in kilobytes) or higher</pre> </li> </ul>	

---

Step	Description	Your Notes
4	<p>For the AIX 5.2 and 5.3 operating systems, establish these settings:</p> <ul style="list-style-type: none"><li>◆ The <code>ncargs</code> value specifies the maximum allowable size of the ARG/ENV list (in 4K byte blocks) when running <code>exec()</code> subroutines. Set <code>ncargs</code> value to 16 or higher.</li></ul> <p>Run the following commands to display and change the <code>ncargs</code> value.</p> <p>To display the current value of <code>ncargs</code>:</p> <pre>lsattr -El sys0 -a ncargs</pre> <p>To change the current value of <code>ncargs</code>:</p> <pre>chdev -l sys0 -a ncargs=NewValue</pre> <p><b>Note:</b> The <code>lsattr</code> and <code>chdev</code> command options are <code>-El</code> (lowercase L) and <code>-l</code> (lowercase L) respectively.</p> <ul style="list-style-type: none"><li>◆ Change the following default entries in the <code>/etc/security/limits</code> file:</li></ul> <pre>fsize = -1 core = 2097151 cpu = -1 data = 262144 rss = 65536 stack = 65536 nofiles = 4096</pre>	
5	<p>For the Solaris 8, 9, and 10 operating systems, set the following entries in the <code>/etc/security/limits</code> file:</p> <pre>nofiles = 4096 set rlim_fd_max=4096 (limit is 65535) - hard limit set rlim_fd_cur=4096 - soft limit</pre> <ul style="list-style-type: none"><li>◆ To make the setting effective as the hard limit, reboot the server or run the following command:</li></ul> <pre>kill -1 inetd</pre> <ul style="list-style-type: none"><li>◆ To make the setting effective as the soft limit, use the parent shell configuration (for example, <code>.profile</code>). Then, reboot the server.</li></ul>	

---



Step	Description	Your Notes
6	<p>For the RedHat Enterprise Linux operating system only, make the following system changes:</p> <ol style="list-style-type: none"><li>1 If the base locale for the system is English, edit the <code>/etc/sysconfig/i18n</code> file by changing the following variables:<ul style="list-style-type: none"><li>• Change LANG from <b>en_US.utf8</b> to <b>en_US</b>.</li><li>• Change SUPPORTED from <b>en_US.utf8</b> to <b>en_US</b>.</li></ul>You can also allow multiple support using the following format: <b>en_US.utf8:en_US</b></li><li>2 Save and close the <code>/etc/sysconfig/i18n</code> file.</li><li>3 Edit the <code>/etc/security/limits.conf</code> file by adding the following lines:<pre>&lt;username&gt; hard nofile 16384 (maximum value)  &lt;username&gt; soft nofile 4096 (minimum value)  &lt;username&gt; hard memlock 3000000 &lt;username&gt; soft memlock 3000000 &lt;username&gt; hard nproc 16000 &lt;username&gt; soft nproc 16000 &lt;username&gt; hard stack 512000 &lt;username&gt; soft stack 512000</pre>This updates the system ulimits.</li><li>4 Save and close the <code>/etc/security/limits.conf</code> file.</li><li>5 Reboot the system.</li></ol>	
7	<p>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.</p> <p>For all Linux operating systems only, ensure that <code>/etc/hosts</code> has short-names first for all entries. For example, <code>127.0.0.1 localhost localhost.localdomain</code></p> <p><b>Caution:</b> If you do not verify the IP addresses, your system may not operate properly after installing Gentran Integration Suite.</p>	
8	Verify that all client computers are using Microsoft Internet Explorer 5.x or later.	
9	If you are using a non-English environment, confirm that you are using the appropriate character set.	

Step	Description	Your Notes
10	Determine and record information about the JDK. See <i>Java 2 Software Development Kit Installation</i> on page 28. <ul style="list-style-type: none"> <li>◆ Version of the JDK</li> <li>◆ Absolute path to the JDK files and patches</li> </ul>	
11	Obtain the JCE distribution file and record the absolute path to the zipped file. See <i>Download the JCE Distribution File</i> on page 28.	
12	Determine and record the initial port number to be used by Gentran Integration Suite. See <i>Port Numbers</i> on page 29.	
13	Verify that a UNIX user account exists on the host server for each installation of Gentran Integration Suite. See <i>UNIX Accounts</i> on page 29.	
14	Set Umask to 002.	
15	If you are using an Oracle, Microsoft SQL Server, or DB2 database, determine and record information about your database server. Be aware that this information is case sensitive. <ul style="list-style-type: none"> <li>◆ Database vendor</li> <li>◆ Database user name and associated password</li> <li>◆ Database (catalog) name</li> <li>◆ Database host name</li> <li>◆ Database host port number</li> <li>◆ Absolute path and file name for the JDBC driver</li> <li>◆ Version of the JDBC driver</li> </ul>	
16	Decide if you are going to manually or automatically apply database definition language (DDL) statements (schema) to the database. See <i>Database Definition Language (DDL) Statements</i> on page 29.	
17	Determine and record information to set up default system alerts from Gentran Integration Suite: <ul style="list-style-type: none"> <li>◆ The Administrative e-mail address to which system alert messages are sent.</li> <li>◆ The SMTP Server IP address used for sending alert messages.</li> </ul>	

Step	Description	Your Notes
18	<p>Determine and record the directory in which you plan to install Gentran Integration Suite.</p> <ul style="list-style-type: none"> <li>◆ The installation directory must not exist because the installation process creates it.</li> <li>◆ The file system must have adequate free disk space.</li> <li>◆ The name of the directory is case sensitive.</li> </ul>	
19	<p>Determine and record the passphrase you want to use for Gentran Integration Suite system.</p> <p>During installation, you are prompted twice to type the passphrase, which is not displayed when you type it.</p>	
20	<p>Obtain the license file and record the absolute path and file name to the license file. Be sure that the path name and the file name consist of alphanumeric, ".", "_", and "-" characters. See <i>Obtain a License File</i> on page 30.</p>	
21	<p>Determine whether Gentran Integration Suite is using an application server (JBoss™, WebLogic® or WebSphere®).</p> <p>Gentran Integration Suite does not require an application server for installation or at runtime.</p> <p>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.</p>	

## Checking System Requirements

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

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

The installation strictly enforces the following system requirements:

Operating system version (must match requirement exactly)

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

JDK version (must match requirement exactly)

Disk space

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

If any of the above requirements are not met, the installation will fail and print/log a report of all items that were non-compliant.

## Java 2 Software Development Kit Installation

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

### Download the JCE Distribution File

The Java Cryptography Extension (JCE) is a set of Java packages from Sun Microsystems, Inc. or IBM that provides a framework and implementations for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms.

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

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

1. Open your browser and navigate to [http://java.sun.com/javase/downloads/index\\_jdk5.jsp](http://java.sun.com/javase/downloads/index_jdk5.jsp).
2. At the bottom of the page, locate *Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0* and click the **Download** button.
3. Download the `jce_policy-1_5_0.zip` file to your system.
4. Once the file resides on your system, note the exact directory and file name for this zipped file. You will need this information during the installation process.

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

1. Open your browser and navigate to <https://www14.software.ibm.com/webapp/iwm/web/reg/pick.do?source=jcesdk>.
2. Enter your IBM ID and password. If you do not have an IBM ID, follow the IBM registration instructions provided on the Sign In page.
3. Click **Submit**.
4. Select *Unrestricted JCE Policy files for SDK 1.4.2* and click **Continue**.

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

5. Review your personal information and the license agreement.  
Select **I agree** and click **I confirm** to continue.
6. Download the `unrestrict142.zip` file to your system.
7. Once the file resides on your system, note the exact directory and file name for this zipped file. You will need this information during the installation process.

## Port Numbers

During installation, you are prompted to specify the initial port number for Gentran Integration Suite.

To specify an initial port number, follow these guidelines:

Gentran Integration Suite requires a range of 100 consecutive open ports between 1025 and 65535.

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

The port range starts with the initial port number and ends with the number that equals the initial port number plus 100. For example, if you specify 10100, then you need to make sure that 10100 through 10199 are not used by any other applications on your system.

All port assignments can be found in the *install\_dir/properties/sandbox.cfg* file.

HTTP ports are assigned in pairs to facilitate an HTTPS listener on the second port. The following ports are assigned:

B2B\_HTTP\_PORT= baseport+6 and baseport+7

WEBX\_PORT= baseport+8 and baseport+9

SOAP\_PORT= baseport+10 and baseport+11

Two ports (HTTP\_SERVER\_PORT and LIST\_PORT) are required to access Sterling Secure Proxy from browsers. If you plan to configure Sterling Secure Proxy from a higher security network, you need both of these ports open in your firewall.

## UNIX Accounts

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

## Database Definition Language (DDL) Statements

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

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

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

The DDLs generated for Oracle are:

- ◆ EFrame\_IndexAdds.sql
- ◆ EFrame\_Sequence.sql
- ◆ EFrame\_TableChanges.sql

The DDLs generated for DB2 are:

- ◆ EFrame\_Sequence.sql
- ◆ EFrame\_TableChanges.sql
- ◆ EFrame\_IndexAdds.sql

The DDLs generated for Microsoft SQL Server 2005 are:

- ◆ EFrame\_TableChanges.sql
- ◆ EFrame\_IndexDrops.sql
- ◆ EFrame\_IndexAdds.sql

## Obtain a License File

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

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

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

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

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

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

7. Verify the list of packages and the type of license selected for each package and click **Next**. If the list of packages selected or the type of license selected is *not* correct, then contact Customer Support to correct the information.

8. Scroll to the bottom of the Review and Download Package License File page and click **Finish and Download**.
9. Click **Save** in the **File Download** dialog box.
10. Accept the default location for the license file or navigate to the location where you will store the license file. Note the absolute path of the file location on the Preinstallation Checklist.
11. Click **Save**.
12. Close your Web browser.

## Silent Installations

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

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

Examples of silent installation text file entries:

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

**Note:** The following DB\_\* variables are not used for MySQL.

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

A reference in your installation script to this variable file.

Example:

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

## Install 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.

### Install the JDBC Driver in SQL Server 2000

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

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

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

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

```
jar -xvf jar_file_name
```

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

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

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

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

Point to the bundled jar file.

Example: `DB_DRIVERS=absolutePath/combinedJarName.jar`

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

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

### Install the JDBC Driver in SQL Server 2005

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

1. Download `sqljdbc_version_language.tar.gz` to a temporary directory.
2. To unpack the zipped tar file, navigate to the directory where you want the driver unpacked and type the following command:

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



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

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

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

4. When the 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.

---

## Install in a Non-Clustered UNIX or Linux Environment

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

Before you begin, consider the following:

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.

If you are using FTP to copy the files, verify that your session is set to binary mode.

In Linux, do not use any soft/symbolic links in the path to the *jar* file. Make sure that you specify the full path to the *jar* file.

To install in a non-clustered UNIX or Linux environment, refer to your preinstallation checklist and follow the steps below.

1. Place the Gentran Integration Suite installation CD in the appropriate drive.
2. From the installation CD, copy *GIS.jar* to your home directory or base directory and change to that directory.
3. If Gentran Integration Suite is running, stop the previous installation before proceeding.
4. To begin the installation, type the absolute path to the JDK followed by the absolute path to the *GIS.jar* file, using the following command:

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

The program verifies support for your operating system and JDK. It also confirms that you have the required operating system patch levels.

5. The program checks for the presence of the JCE unlimited strength policy files. If they are not installed, you are prompted for the path to the JCE distribution file. If prompted, type the absolute path name to the JCE distribution file and press **Enter**. Verify the file name by typing **y** and pressing **Enter**.

6. Type the absolute path to the license file and press **Enter**. The license file must reside on the local UNIX/Linux host. If you saved the license file to a Windows client, transfer the license file to the UNIX/Linux host. Verify the file name by typing **y** and pressing **Enter**.
7. Type the absolute path of the installation directory and verify that the directory is correct. Verify the directory name by typing **y** and pressing **Enter**.

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

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

- ◆ To override the host IP address, enter another IP address and press **Enter**.
- ◆ To accept the default host IP address, press **Enter**.

**Note:** If you are installing Gentran Integration Suite on VMware, you should provide the IP address of the virtual machine and not of the VMware host. For example, if 10.251.124.160 is the IP address of the VMware server and 10.251.124.156 is the IP address of the Windows 2003 server it is hosting, you should use 10.251.124.160 as the IP address to install Gentran Integration Suite.

11. Type your system passphrase. Then type the passphrase again to confirm it.
12. You are prompted whether to enable the FIPS (Federal Information Processing Standards) mode. If you want to enable FIPS, type **Yes** and press **Enter**. Otherwise, press **Enter** to use the default value of **No**.
13. You are prompted whether to integrate with WebLogic or JBoss during the installation. If you want to integrate, type **Yes**, enter the required information, and press **Enter**. Otherwise, press **Enter** to use the default value of **No**.

**Note:** You can integrate with the JBoss, WebLogic or WebSphere application server after you have installed Gentran Integration Suite.

14. Type the initial port number for Gentran Integration Suite.

A list of the port assignments appears. The installation uses the initial port number to set up port assignments. These port assignments are written to `install_dir/properties/sandbox.cfg`.

15. You are prompted whether to change the default port values.
  - ◆ To accept the default values, press **Enter** to use the default value of **No**.
  - ◆ To change the default values, type **Yes** and press **Enter**. For each port, you are prompted to either choose the default value or type in a new value. Press **Enter** to accept the default value, or type the new value and press **Enter**.
16. Type the administrative e-mail address to which you want system alert messages to be sent. Press **Enter**.
17. Type the SMTP mail server host name that you want to use for system alert messages and other administrative notices. Press **Enter**.
18. You are prompted for the database you want to use.
  - ◆ If you are using MySQL, type **5** and press **Enter**. The MySQL that is bundled with Gentran Integration Suite will be installed locally on the same server.

- ◆ If you are using Oracle, DB2, Microsoft SQL 2000 or Microsoft SQL 2005, type the appropriate number and press **Enter**. Enter the following information when prompted:
  - Database user name
  - Database password
  - Database password again for confirmation
  - Database (catalog) name
  - Database host name
  - Database host port number
  - Absolute path and file name for the JDBC driver (For DB2, use the Type 4 JDBC driver). For more information about accessing the driver for Microsoft SQL Server, refer to *Install the JDBC Driver in SQL Server* on page 32.
  - Version of the JDBC drivers

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

19. (If using Oracle, DB2, Microsoft SQL 2000 or Microsoft SQL Server 2005) At the *Automatically create database schema* prompt, take one of the following actions:

- ◆ To automatically apply database definition language (DDL) statements, press **Enter** to use **Yes**.  
If you type **Yes**, and do not choose to manually apply the DDL statements, the installation applies both the DDL statements and the resources.
- ◆ To manually apply database definition language (DDL) statements, type **No** and press **Enter**. For more information about this option (including the unique names of the DDLs for each database vendor), refer to *Database Definition Language (DDL) Statements* on page 29.

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

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

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

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

The installation process continues automatically and installs the following components:

- ◆ MySQL (if you selected MySQL)
- ◆ Core files (services, adapters, and predefined business processes)
- ◆ Package files

- ◆ System certificates
- ◆ License file

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

*Installation has completed successfully.*

If you encounter problems or errors during installation, see the section *Troubleshooting: UNIX or Linux Environment (Non-Clustered)* on page 53.

If you are installing a perimeter server, refer to *Install a Perimeter Server in a Non-Clustered UNIX or Linux Environment* on page 41.

22. Start Gentran Integration Suite by changing to the `install_dir/bin` directory and running the `run.sh` command.

For more information about starting Gentran Integration Suite, refer to *Start Gentran Integration Suite in UNIX or Linux* on page 48.

23. Enter the passphrase.

The final startup processes run, concluding with the following message:

*Depending on system load, it may take several minutes for the UI to be ready.*

For information on patches and hot-fixes for your installation of Gentran Integration Suite, refer to *Patches and Hot-Fixes (Non-Cluster)* on page 36.

## Patches and Hot-Fixes (Non-Cluster)

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

*Install the Current Maintenance Patch in UNIX or Linux (Non-Cluster)* on page 36

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.

*Install a Hot-Fix (Non-Cluster)* on page 38

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

### Install the Current Maintenance Patch in UNIX or Linux (Non-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.

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

`si_43_build_build number.jar` (for example, `si_43_build_4307.jar`)

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

si\_43\_build\_ *build number* \_patch\_info.pdf (for example, si\_43\_build\_4307\_patch\_info.pdf)

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

**Note:** The patch installation may use one or more patch property override files. These files will be named *propertyFile\_patch.properties*. Do not alter these files.

Additionally, property changes made directly in *.properties* or *.properties.in* files may be overwritten during the patch installation. Properties overridden using the *customer\_overrides.properties* file are not affected.

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

1. Go to the Sterling Commerce Support on Demand Web site, at <https://support.sterlingcommerce.com>.
2. Download the most recent patch file for your version of Gentran Integration Suite and record the absolute path to the downloaded file. If you use FTP, use Binary mode. Do not rename the file.
3. If you are using a database other than MySQL, verify that the database server is up and ready to accept connections.
4. Stop Gentran Integration Suite.
5. Perform a full backup of Gentran Integration Suite installation directory, including all subdirectories.
6. Perform a backup of your database.
7. If you edited any **property** files, ensure that the associated **properties.in** files have the most current changes. Property files will be overwritten with the contents of the associated *properties.in* files during the patch installation.
8. Is the database password encrypted? If **Yes**, decrypt the password. For more information about decrypting database passwords, refer *Decrypting Database Passwords (UNIX)* on page 20.
9. Change to the directory where Gentran Integration Suite. Enter: `cd install_dir/bin`
10. Enter:

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

where:

<path> = Fully qualified path to maintenance patch file

<version> = Gentran Integration Suite Version

<number> = Patch number

<app\_server> = Application Server

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

Information about the patch installation is displayed and 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.

11. Press **Enter** to continue.
12. Press **Enter** to continue.
13. If you want to accept the license agreement, enter **Y**.
14. Enter the **passphrase**. Information about the patch installation is displayed. After the patch has been applied, the following message is displayed: `Deployment to application server successful`
15. If you decrypted the database password, re-encrypt the password. For more information about encrypting database passwords, refer *Encrypting Database Passwords (UNIX)* on page 20.
16. Start Gentran Integration Suite.

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

## Run the DB2 Schema Change Script

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

To run `fix_db2_schema.sql` script:

1. Install Gentran Integration Suite, Release 4.3 build 4316 or later.
2. Apply the new schema changes by running `fix_db2_schema.sql` script.

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

The script will:

- ◆ Rename the affected tables and indexes
  - ◆ Recreate the affected tables and indexes with the correct data types.
  - ◆ 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.

## Install a Hot-Fix (Non-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 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

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

1. Log in to the computer that you are installing the hot-fix on.
2. Is the database password encrypted? If **Yes**, decrypt the password. For more information about decrypting database passwords, refer *Decrypting Database Passwords (UNIX)* on page 20.
3. At the command line, type `ftp theworld.stercomm.com`.
4. Type your user name and password. If you do not know your user name and password, contact Sterling Commerce Customer Support.
5. Type `bin` and press **Enter** to select Binary as your transfer mode.
6. At the FTP prompt, type `get ccaseid.jar`, where *caseid* is the ID number you received from Customer Support. For example, `c123.jar`, where 123 is the ID number.

**Note:** You can put the file to any directory for which you have write permission.

7. Shut down Gentran Integration Suite.
8. Change to the `install_dir/bin` directory.
9. Type the following command to install the hot-fix:
 

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

**Caution:** You may need to complete this step twice depending on the patch. Read the output from the `InstallService.sh` script carefully to see if you need to complete this step twice.
10. If you decrypted the database password in step 2, re-encrypt the password. For more information about encrypting the database password, refer *Encrypting Database Passwords (UNIX)* on page 20.
11. Restart Gentran Integration Suite.
12. In the `install_dir/bin` directory, run `dump_info.sh` to verify that the hot-fix was successfully installed.

## 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 *Install a Hot-Fix (Non-Cluster)* on page 38 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 `dump_info.sh` command to display the hot-fix version. You can also verify the hot-fix version in Gentran Integration Suite Support user interface page.

Size of the hot-fix package is small.

Hot-fix must be installed on the same build version that was used to build it. For example, if a test system is on Gentran Integration Suite, Release 4.3 Build 4324 and the hot-fix is built for 4324, it can

be installed on that test system. However, if the production system is on Gentran Integration Suite, Release 4.3 Build 4323, you must apply Gentran Integration Suite, Release 4.3 Build 4324 prior to applying the hot-fix.

You can locate the hot-fix read me file in the Gentran Integration Suite root (*install\_dir*) directory. For example, *install\_dir/hotfix\_readme.txt*.

If you have Sterling File Gateway installed in your environment, the hot-fix for Sterling File Gateway is installed automatically.

## Perform a Checksum using DB Checksum Tool

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

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

To run DB Checksum tool, do the following:

1. Navigate to the *<install\_dir>/bin* directory.
2. Run the following command from the *<install\_dir>/bin* directory:

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

where:

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

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

1 is WFD

2 is MAP

3 is SCHEMA

4 is SII

5 is TEMPLATE

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

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

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

*-h* is the help screen.

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



---

## Install a Perimeter Server in a Non-Clustered UNIX or Linux Environment

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

*Set Up Perimeter Servers with Gentran Integration Suite* on page 41

*Install a Perimeter Server in a More Secure Network (UNIX/Linux Non-Clustered)* on page 42

*Install a Perimeter Server in a Less Secure Network (UNIX/Linux Non-Clustered)* on page 43

*Install Patches in a Perimeter Server UNIX or Linux Environment* on page 44

*Start Perimeter Servers in UNIX or Linux* on page 45

*Reduce Perimeter Server Security Vulnerabilities* on page 45

### Set Up Perimeter Servers with Gentran Integration Suite

Using a perimeter server is optional.

A *perimeter server* is a software tool for communications management that can be installed in a DMZ. The perimeter server manages the communications flow between outer layers of your network and the TCP-based transport adapters. A perimeter server can solve problems with network congestion, security, and scalability, especially in high-volume, Internet-gateway environments. A perimeter server requires a corresponding perimeter client.

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

When you install a perimeter server, use these guidelines:

Licensing for a perimeter server is determined by the licensing restrictions on the corresponding B2B adapters.

Each perimeter server is limited to two TCP/IP addresses – internal interface and external interface. *Internal interface* is the TCP/IP address that the perimeter server uses to communicate with Gentran Integration Suite. *External interface* is the TCP/IP address that the perimeter server uses to communicate with trading partners.

To use additional TCP/IP addresses, install additional perimeter servers.

You can have multiple perimeter servers installed on the same computer interacting with one instance of Gentran Integration Suite. To install a perimeter server on a computer with an existing instance, install the new perimeter server in a different installation directory.

The combination of internal TCP/IP address and port must be unique for all perimeter servers installed on one computer.

- ◆ If a perimeter server is installed using the wildcard address, then all ports must be unique.
- ◆ If a perimeter server is installed using the wildcard address, then its port is not available for use by adapters that use the server or any other perimeter server on that computer.

- ◆ The internal and external interface may use the same TCP/IP address. However, the port used by the perimeter server is not available to the adapters that use the server.

## Install a Perimeter Server in a More Secure Network (UNIX/Linux Non-Clustered)

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

1. Insert the installation CD in the appropriate drive.
2. Copy the ps\_2000.jar installation files from the installation CD to your home directory or base directory. If you are using FTP to copy the file, make sure your session is set to binary mode.
3. To begin the installation, type the absolute path to the following jar file:

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

The program verifies the operating system and required patch level and the location and version of the JDK.

4. Enter the full path name of the installation directory.
5. If there is an existing installation in the directory you specify, you can update it using the same settings.

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

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

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

13. Verify the port.

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

*Installation of Perimeter Service is finished*

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

## Install a Perimeter Server in a Less Secure Network (UNIX/Linux Non-Clustered)

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

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

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

The program verifies the operating system and required patch level and the location and version of the JDK.

4. Enter the full path name of the installation directory.
5. If there is an existing installation in the directory you specify, you can update it using the same settings.

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

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

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

13. Enter the port that the perimeter server will listen on for the connection from integration server (Gentran Integration Suite). The port number must be higher than 1024.
14. Verify the port.  
When the perimeter server is installed, the following message is displayed:  
*Installation of Perimeter Service is finished*
15. Change to the installation directory.
16. Enter `startupPs.sh` to start the perimeter server.

## Install Patches in a Perimeter Server UNIX or Linux Environment

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

To Update a Remote Perimeter Server in a Non-Clustered UNIX or Linux environment:

1. Update your installation of Gentran Integration Suite 4.3 with the latest maintenance patch. Obtain the maintenance patch file from the Sterling Commerce Support on Demand Web site, at <https://support.sterlingcommerce.com>. These patch files have a name that identifies a build number. For example, `si_43_build_4307.jar`. For more information, refer to *Install the Current Maintenance Patch in UNIX or Linux (Non-Cluster)* on page 36.
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.sh` command.
5. To begin the installation, type the following command:  
`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.sh` to start the perimeter server.

## Start Perimeter Servers in UNIX or Linux

To start a perimeter server in UNIX or Linux:

1. Change the directory to `install_dir`.
2. Enter `startupPs.sh`.

## Stop Perimeter Servers in UNIX or Linux

To stop a perimeter server in UNIX or Linux:

1. Change the directory to `install_dir`.
2. Enter `stopPs.sh`.

## Reduce Perimeter Server Security Vulnerabilities

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

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

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

## Grant 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 *Install a Perimeter Server in a More Secure Network (UNIX/Linux Non-Clustered)* on page 42.
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 "httphost: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.

The following example grants permission to a target FTP Server. 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/ httphost/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 "10.117.15.87:1364", "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: <ul style="list-style-type: none"> <li>◆ true - enable remote DNS resolution</li> <li>◆ false - disable remote DNS resolution</li> </ul>

## Post Installation in a Non-Clustered UNIX or Linux Environment

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

*Start Gentran Integration Suite in UNIX or Linux on page 48*

*Access Gentran Integration Suite on page 48*

*Validate the Installation on page 50*

*Download Gentran Integration Suite Tools on page 50*

*Perform Initial Administrative Setups in Gentran Integration Suite on page 50*

*Stop Gentran Integration Suite on page 51*

## Start Gentran Integration Suite in UNIX or Linux

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

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

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

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

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

The system returns you to a UNIX prompt

## Access Gentran Integration Suite

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

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

### Technical Note: Changes to Network Interface Bindings

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



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

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

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

**Default entries**

```
admin_host.1    = hostname1
admin_host.2    = localhost
```
  - b. Correct the parameters as necessary.
 

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

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

**Edited entries**

```
admin_host.1    = hostname1
admin_host.2    = localhost
admin_host.3    = hostname2
```
2. Stop Gentran Integration Suite.
3. Run the `setupfiles.sh` utility located in the `install_dir/bin` directory.
4. Restart Gentran Integration Suite.

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

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

**Unrestricted Setting (Default)**

```
localmode.interface=*
```
  - b. To restrict access to the Dashboard, type the network interface that you want Gentran Integration Suite to support.
 

**Restricted Setting**

```
localmode.interface=hostname1
```
2. Stop Gentran Integration Suite.
3. Run the `setupfiles.sh` utility located in the `install_dir/bin` directory.
4. Restart Gentran Integration Suite.

## Validate the Installation

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

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

## Download Gentran Integration Suite Tools

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

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

Map Editor and associated standards

Graphical Process Modeler

Web Template Designer

(If licensed) MESA Developer Studio plug-ins, including:

- ◆ MESA Developer Studio Software Development Kit (SDK)
- ◆ MESA Developer Studio Skin Editor

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

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

## Perform 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.

For security purposes, change default user ID passwords immediately after installation is completed. See the *Editing My Account Information* task in the documentation library.

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*.

## Stop Gentran Integration Suite

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

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

Open your browser and access Gentran Integration Suite. From the **Administration** menu, select **Operations > System > Troubleshooter**. Click **Stop the System**.

From the UNIX command line, do the following:

- a. Change directory to *install\_dir/bin*.
- b. Enter `softstop.sh`.
- c. Then type your passphrase.

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

1. From the UNIX command line, change directory to *install\_dir/bin*.
2. Enter `hardstop.sh`.

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

---

## Uninstall Gentran Integration Suite from a Non-Clustered UNIX or Linux Environment

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

Gentran Integration Suite application is automatically removed from the server.

The MySQL database is automatically removed from the server (if you are using MySQL).

Additionally, you may perform the following tasks:

Manually remove Attunity Data Connect. For more information, refer to product information provided with Attunity Data Connect software.

Manually remove the JDK that was installed

Free any database space in Oracle, Microsoft SQL Server, or DB2 databases

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

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

```
rm -rf install_dir
```

This step deletes MySQL, if you are using this bundled component.

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

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

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

- ◆ Map Editor and associated standards

Refer to the *Map Editor Guide* for information about removing the Map Editor.

- ◆ Graphical Process Modeler

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

- ◆ Web Template Designer

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

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

To remove these items, follow this procedure:

- a. Using Windows Explorer, locate the installation directory of Eclipse (For example, C:\Program Files\eclipse).
- b. Navigate to the features directory and delete the folders for anything from Sterling Commerce, gisstudio, skineditor, and servicesdk.
- c. Navigate to the plugins directory and delete the folders for anything from Sterling Commerce, gisstudio, skineditor, and servicesdk.

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

---

## Troubleshooting: UNIX or Linux Environment (Non-Clustered)

---

Situation	Message or Symptom	Explanation/Resolution
Installing	You encounter errors or problems during installation.	<p><b>Explanation</b> Installation creates a log file.</p> <p><b>Resolution</b> Examine the log file generated during installation:</p> <ul style="list-style-type: none"> <li>◆ <code>install_dir/InstallSI.log</code></li> </ul>
Installing	When you entered an absolute path during installation, a message indicated that the command was not found.	<p><b>Explanation</b> You entered an incorrect path. Check your typing or check the information.</p> <p><b>Resolution</b> Enter the correct path.</p>
Installing	During installation, you entered the absolute path to the license file. However, a message indicates that the license file cannot be found.	<p><b>Explanation</b> You either did not obtain the license file, the license file is corrupt, or you downloaded the license file to a PC but have not moved it to the server.</p> <p><b>Resolution</b> If you need to obtain the license file, see the section <i>Obtaining a License File</i>. If the license file resides on a PC, save the license file to the server.</p>
Installing	Memory and ulimit errors	<p><b>Explanation</b> The installation fails with memory and ulimit errors.</p> <p><b>Resolution</b></p> <ul style="list-style-type: none"> <li>◆ Refer Viewing or Editing Performance Configuration Settings in <i>Performance Management</i> documentation and modify your memory settings accordingly.</li> <li>◆ Refer <i>Checklist for UNIX or Linux Preinstallation</i> on page 22 and tune <code>ulimit</code> settings.</li> </ul>

---

Situation	Message or Symptom	Explanation/Resolution
Installing a desktop tool or resource	<p>Cannot download any of the following:</p> <p><b>Note:</b> 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.</p> <ul style="list-style-type: none"> <li>◆ Map Editor and associated standards</li> <li>◆ Graphical Process Modeler</li> <li>◆ Web Template Designer</li> <li>◆ (If licensed) MESA Developer Studio plug-ins (Software Development Kit (SDK), Skin Editor)</li> <li>◆ (If licensed) Reporting Services, which requires MESA Developer Studio if you want to use the plug-ins to create fact models and custom reports.</li> </ul>	<p><b>Explanation</b></p> <p>When you install Gentran Integration Suite, system files are created that contain an internal IP address. If you install Gentran Integration Suite behind a firewall, and your firewall is configured to accept an external IP address from a client computer, you may not be able to download the desktop tools and resources. The firewall will reject the internal IP address from a client residing outside of the firewall.</p> <p><b>Resolution</b></p> <p>Modify the system files that contain the invalid IP address. Follow these steps:</p> <ol style="list-style-type: none"> <li>1 Navigate to the <code>install_dir/bin</code> directory.</li> <li>2 Enter the following command followed by the external IP address: <code>patchJNLP.sh external_IP address</code></li> <li>3 Stop Gentran Integration Suite.</li> <li>4 Restart Gentran Integration Suite.</li> </ol>
Accessing	<p>Attempts to access the URL for Gentran Integration Suite display the message: <i>Page cannot be displayed</i></p>	<p>See <i>Technical Note: Changes to Network Interface Bindings</i> on page 48.</p>

## Chapter 4

---

# Installing and Configuring MESA Developer Studio

---

---

## Overview for Installing and Configuring MESA Developer Studio

Gentran Integration Suite MESA Developer Studio is an Integrated Development Environment (IDE) that uses Eclipse software plug-ins. Use the MESA Developer Studio to connect with a Gentran Integration Suite instance for resource access and control of operations of Gentran Integration Suite, change the template that Gentran Integration Suite uses, and develop custom services—all from within a development environment.

In addition to MESA Developer Studio, the following plug-ins are available:

- MESA Developer Studio SDK – for developing and deploying custom services and adapters.

- MESA Developer Studio Skin Editor – for customizing the look and feel of Gentran Integration Suite interface.

- Reporting Services – a separately-licensed set of plug-ins used to create fact models and reports for 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.

## Assumptions and Prerequisites

Read the following assumptions and prerequisites prior to installing MESA Developer Studio:

- Basic knowledge of Gentran Integration Suite and its architecture. This is especially important if you are using MESA Developer Studio SDK to create services and adapters.

- Basic knowledge of Eclipse is assumed. For more information, see the Eclipse online help or go to the Eclipse web site.

- Extensive knowledge of how to create and deploy a service.

- Thorough knowledge of and experience with the Java programming language for creating services.

You have the required MESA Developer Studio (and if purchased, Gentran Integration Suite) product licensing.

## Steps to Set Up MESA Developer Studio

Setting up MESA Developer Studio is a multi-step process which should be completed in the order described. The following is a checklist for each stage in the process. The checklist provides an overview of the entire process. Separate instructions for completing each step are available:

1. Install and configure Gentran Integration Suite.
2. Download and install the latest Gentran Integration Suite patch.
3. Download and install a full release version of Eclipse. For more information, see the download page of the Eclipse web site.

**Note:** MESA Developer Studio requires specific plug-in versions. We recommend you to install Eclipse for MESA development only. If you are using Eclipse with development projects other than MESA, disable plug-ins that report conflicts.

4. Download and install the latest version of Java 2 SDK Standard Edition 5.0 (or higher) on the same PC that you installed Eclipse. It is important that you have the full SDK and not just the JRE.

After installation, additional configuration is required.

5. Verify that MESA Developer Studio uses the correct JRE.
6. Start the WebDAV server (for Gentran Integration Suite installations on UNIX and iSeries only).
7. Install the MESA Developer Studio (and if purchased, Gentran Integration Suite) Plug-ins.
8. Set up Gentran Integration Suite Instance in MESA Developer Studio.
9. Set up Gentran Integration Suite resources to be used with MESA Developer Studio.

## Eclipse Terms

The following Eclipse terms might be used in this documentation when describing MESA Developer Studio components:

**Project** - All the resources related to a particular implementation reside in a project. It can contain folders, files, and other Eclipse objects.

**Workspace** - Directory where work is stored.

**Workbench** - UI window that contains these elements:

- ◆ **Perspective** - group of views and editors in a Workbench window that correspond to a certain project.
- ◆ **View** - visual component within the Workbench and dependent on the perspective that was selected. Used to navigate or display information such as properties or messages.
- ◆ **Editors** - visual component in the Workbench used to create, change, or browse a resource.



---

## Configuring J2SE on Your PC

In order for Eclipse to work correctly, you must have Java 2 SDK Standard Edition 5.0 (or higher) installed on the same PC you installed Eclipse. You need to have the full SDK installed. The JRE alone is not enough. You must close Eclipse to download and install the JDK. After installing J2SE, you must configure your PC to use it.

To configure your PC for the new JDK:

1. Select **Start > Settings > Control Panel > System** (Windows 2000) or **Start > Control Panel > System** (Windows 2003).
2. Click the Advanced tab.
3. Click **Environment Variables**.
4. Under System Variables, click **New**.
5. Complete the following and click **OK**:
  - ◆ Variable Name - type **JAVA\_HOME**.
  - ◆ Variable Value - type the directory path for the location where you installed the J2SE SDK. The default location is C:\j2sdk5.0\.
6. Click **OK** to exit.

---

## Verifying that MESA Developer Studio Uses the Correct JRE

In addition to adding a home directory on Windows for this JDK instance, you must also verify that MESA Developer Studio uses the correct JRE.

To verify the MESA Developer Studio JRE:

1. Open Eclipse.
2. From the Window menu, select **Preferences**.
3. Expand the Java section and select **Installed JREs**. The Installed JREs window appears.
4. If C:\j2sdk5.0 is not listed (location and version may be different, but version should be as listed or higher), click **Add** and go to next step.

If it is listed, make sure it is selected and click **OK**. You are ready to use MESA Developer Studio.

5. Complete the following and click **OK**:
  - ◆ JRE Name - type any name for this JRE.
  - ◆ JRE home directory - click Browse to select the home directory you defined in the *Configuring J2SE on Your PC* section.
  - ◆ Default VM Arguments - leave blank.
  - ◆ JRE system libraries - make sure Use default system libraries is selected.

6. Click **OK** to exit.

---

## Starting the WebDAV Server

MESA Developer Studio uses a WebDAV server to provide access to Gentran Integration Suite resources, including MESA Developer Studio plug-in updates. This WebDAV server is automatically installed with Gentran Integration Suite for use with MESA Developer Studio.

The WebDAV server starts automatically with Gentran Integration Suite in Windows.

You must start the WebDAV server manually with Gentran Integration Suite in UNIX.

### Gentran Integration Suite (UNIX)

You do not need to have Gentran Integration Suite running to start the WebDAV server.

**Note:** You must start the WebDAV server for each Gentran Integration Suite instance you want to work with in MESA Developer Studio.

To start the WebDAV server:

1. Open a UNIX command window.
2. Go to Gentran Integration Suite install directory. This is usually *installDir/bin*.
3. Start the WebDAV server by executing the `runDAVServer.sh` command.
4. You are asked to enter your installation password. You must enter this information only once for each Gentran Integration Suite installation because the password is written permanently to the properties file. This step is optional, however if you do not enter the password you will not be able to start and stop Gentran Integration Suite instances from MESA Developer Studio.
5. After the startup process is complete, the WebDAV port is listed. Make a note of this number. Format is base install port + 46. The WebDAV port is needed when requesting to download and install the MESA Developer Studio plug-ins.

**Note:** The default WebDAV port is the base install port + 46. This port is assigned when you install Gentran Integration Suite and should not be changed. The WebDAV port number is used when installing the plug-ins and when adding a Gentran Integration Suite instance to MESA Developer Studio.

---

## Installing MESA Developer Studio Components

You must install and configure MESA Developer Studio to connect with the desired Gentran Integration Suite instances for resource access and for control operations of Gentran Integration Suite from within MESA Developer Studio. Use this procedure to install Gentran Integration Suite plug-ins, as well.

## Changing Proxy Preferences

You might need to change you proxy server settings to enable an HTTP proxy connection between the PC where you have Eclipse installed and the server where Gentran Integration Suite is installed.

To change proxy settings:

1. From the Windows menu, select **Preferences > Install/Update**.
2. Under Proxy settings, type your proxy information.
3. Click **OK**.

## Installing New Features

To install MESA Developer Studio:

1. Open Eclipse.
2. Select a default workspace folder location. You can add additional workspace folder locations at any time. The Package View in the lower left area of the MESA Developer Studio workspace displays a local explorer view of your project folders. This enables you to store files that you check out.
3. From the Eclipse Help menu, select **Software Updates > Find and install**.
4. Select **Search for new features to install**.
5. Click **Next**.
6. Click **New Remote Site**.
7. Complete the following information and click **OK**.
  - ◆ Name – type a descriptive name for the application server.
  - ◆ URL – type the IP address or name of your server. Format is `http://<servername>:<WebDAVportnumber>/eclipse`.

Your new site will appear in the list of sites to include in the search.

8. Select the checkbox to the left of the new site. Click **Finish**.

The system verifies the selected site and displays the results. On the search results page, expand the update site node and select from the following plug-ins, according to your licenses:

- ◆ MESA Developer Studio
- ◆ Service SDK
- ◆ Skin Editor
- ◆ Gentran Integration Suite (automatically selects all three Gentran Integration Suite plug-ins: Fact Model Editor, Report Editor, and Report Format Editor)

### Cautions:

- ◆ Do not change the default installation path for the plug-ins.

- ◆ If you are selecting Gentran Integration Suite, you must also select the MESA Developer Studio plug-in (unless you have already installed MESA Developer Studio). Dependencies require that the MESA Developer Studio plug-in be installed either before or at the same time as Gentran Integration Suite plug-ins.
9. Click **Next**. Accept the terms of the license and click **Next**.
  10. Click **Finish**.
  11. Click **Install All** to accept the feature verification.

You must restart Eclipse for the changes to take affect.

---

## Setting Up a Gentran Integration Suite Instance

You can only view resources that are available for the specified Gentran Integration Suite instance. If a desired resource resides in a different Gentran Integration Suite installation you must configure a new instance in MESA Developer Studio to work with it.

**Note:** If you are installing Gentran Integration Suite, you must complete this task.

1. From the Window menu, select **Open Perspective > Other**.
2. Select MESA Developer Studio and click **OK**.
3. In the MESA Developer Studio view in the upper left, right-click and select **New instance**.
4. Complete the following information and click **Finish**:
  - ◆ Hostname - name of machine for Gentran Integration Suite install.
  - ◆ Port - WebDAV port assigned at install.
  - ◆ Name - name you assign to this Gentran Integration Suite connection.
  - ◆ User name - valid Gentran Integration Suite user name (for example, admin).
  - ◆ Password - valid Gentran Integration Suite password.

MESA Developer Studio attempts to establish a connection to the instance using the WebDAV server. The status of the instance is displayed:

- ◆ Red – the instance has not been started.
- ◆ Yellow – the instance was started but is not yet running.
- ◆ Green – the instance is running.

**Note:** Refresh the workspace to see a newly added environment.

## Editing Connection Information

Once you have set up Gentran Integration Suite instance for use with MESA Developer Studio, you can edit the connection information, view configuration details, test the connection, and refresh the connection.

To edit the connection information:

1. Right-click on the instance name.
2. Select **Edit**.
3. Edit the settings as needed.
4. Click **Finish**.  
MESA Developer Studio attempts to establish a connection to the instance using the new information. The status is displayed (green, yellow, or red) according to the status of the instance.

## Viewing Configuration Details

To view configuration details, double-click on the instance name.

**Note:** The ports on the Overview window are static. Only the ports present at install are displayed. Any changes or additions made after installation are not displayed.

## Refreshing the Instance

Use Refresh if you have locked or unlocked business processes and maps through in Gentran Integration Suite, and you want to see their current status in MESA Developer Studio.

To refresh Gentran Integration Suite instance connection:

1. Right-click on the instance name.
2. Select **Refresh**

The Progress Information window appears and closes automatically when the refresh process is complete. The status is displayed (green, yellow, or red) according to the status of the instance.

---

## Installing Additional MESA Developer Studio Components and Updates

You can install additional MESA Developer Studio components not installed at the time of the original installation at any time. To install additional components follow the steps listed in the section *Installing MESA Developer Studio Components*. The system verifies that the license file has newly licensed components and installs them.

The system verifies that the additional components are licensed in Gentran Integration Suite. If not, you are asked to provide new connection parameters to Gentran Integration Suite instance that has the appropriate license for the additional MESA Developer Studio components. Once the license check is complete, the new components are activated.

If you are updating an existing component, restart Eclipse in order for the new component to be updated.

## Installing Reporting Services Plug-Ins

Reporting Services works with Gentran Integration Suite MESA Developer Studio, which is an Integrated Development Environment (IDE) that uses Eclipse software plug-ins. The Reporting Services Fact Model Editor, Report Editor, and Report Format Editor are all accessed as Eclipse 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.

To set up the Reporting Services plug-ins:

1. Follow the procedures for the MESA Developer Studio configuration.

**Note:** When completing the procedure *Installing MESA Developer Studio Components*, ensure that you select both the Reporting Services plug-ins and the MESA Developer Studio plug-in for download and installation in Eclipse.

**Caution:** The MESA Developer Studio plug-in is a prerequisite for the Reporting Services plug-ins. You must install it either with or prior to installing the Reporting Services plug-ins.

After installing the MESA Developer Studio and Reporting Services plug-ins, complete the following tasks:

2. Start the WebDAV server for your Gentran Integration Suite instance.
3. Start the Event Listeners.
4. Configure your Eclipse installation to point to Gentran Integration Suite WebDAV server.
5. Customize the Window Perspective in Eclipse to include Sterling Commerce Reporting Services. This makes the Reporting Services options available directly from the Eclipse menus. In Eclipse, select **Window > Customize Perspective**. In the Shortcuts pane on the left, select **Sterling Commerce Reporting Services** and click **OK**.

## Chapter 5

---

# Configuring Properties

After installing Gentran Integration Suite, you must set up a few property and script files in order for Gentran Integration Suite to run properly. This chapter describes the properties you must set up before configuring Gentran Integration Suite to run according to your business needs.

---

## Properties to Prevent Cross-Site Script Vulnerabilities

In some cases, data to and from Gentran Integration Suite can contain HTML characters that impact the display and the original intent of the input. In addition, data can be input that contains malicious HTML, such as commands embedded within <SCRIPT>, <OBJECT>, <APPLET>, and <EMBED> tags.

In Gentran Integration Suite, potentially malicious data being output to the browser can be rendered harmless by implementing the provided encoding mechanism. This prevents these malicious scripts from being run by the browser.

Any presence of these characters triggers Gentran Integration Suite to safely encode the data.

For more detailed information about malicious scripts, see the following articles:

CERT Advisory, Malicious HTML Tags Embedded in Client Web Requests. Available from the CERT web site.

CERT Advisory, Frequently Asked Questions About Malicious Web Scripts Redirected by Web Sites. Available from the CERT web site.

---

## Setting the Database Connection Properties

Database properties are configured during installation. They are put in *install\_dir/properties/jdbc.properties* files.

**Note:** After making modifications to the required files, rebuild the resource jar.

To enable database connection pooling, create the pool, configure the data source entry for JNDI, and specify it as the datasource name. For connection pooling used by other application servers refer to the vendor's manual on connection pooling.

---

## Properties for LDAP User Authentication

This section assumes you understand how LDAP servers work. Sterling Commerce also recommends that you read the following documents on LDAP technology:

W. Yeong, T. Howes, and S. Kille, RFC 1777 - *Lightweight Directory Access Protocol*. March 1995. Available at <http://rfc.net/rfc1777.html>.

Mark Wilcox, *Implementing LDAP*. Wrox Press, 1999.

By default, all authentication is performed against the Gentran Integration Suite database. When a user enters a login ID and password, it is validated against the login ID and password that is stored in the database. This requires the administrator of Gentran Integration Suite to set up login IDs and passwords for each user.

Alternatively, the Application Console supports LDAP-based user authentication. You may choose to use an LDAP server for authentication. When using LDAP, the users, user groups, and access control must be set up in Gentran Integration Suite.

Gentran Integration Suite also supports password expiration through LDAP. Your custom code for user authentication is interfaced with the Gentran Integration Suite authentication mechanism. If your custom code contains `ExpireInDays` with a numeric value of `<X>`, then a message to reset the password appears on the Gentran Integration Suite home page. If the map contains `ChangePasswordLink`, then the message contains a link to the location specified. Clicking on the link opens a new window with the given `ChangePasswordLink`.

Since the various implementations of LDAP handle password expiration differently, a sample `YFSLDAPAuthenticator` is provided as an example of one particular implementation. This is located in the `install_dir/xapidocs/code_examples` directory.

To set properties for LDAP-based authentication, do the following:

1. Install the LDAP server (see the installation instructions from your LDAP server vendor).
2. If a JAAS-compliant provider is used, create a JAAS configuration file with the following lines:

```
LDAP
{
    // refer to the JAAS compliant service provider for the login
    module details.
    <Class Name of the Login Module as specified by the Security
    provider> required
    debug=true;
};
```

3. Specify the LDAP properties described in the following table:



Property	Description
<b>WebLogic startWLS startup file</b>	
-Djava.security.auth.login.config	If you are using JAAS and WebLogic, specify the full path to your JAAS configuration file.
<b>In the Configurator UI</b>	
Configure organizations, organization units, and users.	All users who need to access Gentran Integration Suite must be set up under the LDAP server. All Gentran Integration Suite users must belong to the same organizational unit.

## Chapter 6

---

# Configuring Utilities

Gentran Integration Suite supplies sample script files (.sh for UNIX and .cmd for Windows) that you must customize using the directions provided in this chapter.

This chapter describes all the utilities supplied by Gentran Integration Suite, organized by the order in which you are likely to use them. It describes generic customizations that apply to most or all utilities. Further details specific to each utility are provided throughout the rest of this guide.

---

## Installation Utilities

**Note:** On UNIX, all utilities within the *install\_dir/bin* directory must have permissions set to **755**.

Installation utilities enable you to install Gentran Integration Suite. These utilities are present in the *install\_dir/bin* directory. Some of the utilities used for installing the various configurations of Gentran Integration Suite are the following:

loadDefaults

This utility loads the standard installation database configuration, known as the "factory defaults".

dbverify

This utility verifies the changes between your database setup and the entity XML files.

## Loading Gentran Integration Suite Database Factory Defaults

To load Gentran Integration Suite database factory defaults:

1. Load the defaults, using the script applicable to your operating system. From the command line, run `loadDefaults.sh` on UNIX and Linux or `loadDefaults.cmd` on Windows and pass the absolute file path to the installer:

```
loadDefaults.sh
install_dir/installed_data/platform/factorysetup/installer.xml
```

**Note:** If the factory default installation stops before it is finished, a file name "installer.xml.restart" is created. This file records the location where the installation was stopped, and it is used the next time the factory defaults are installed.

## Verifying the Database

Gentran Integration Suite provides a database verification and correction tool to ensure database schema integrity. To set up the Database Verification Tool:

1. From the command line, run the `dbverify.sh` or `dbverify.cmd` script and pass the `userID` and `password` parameters as follows:

```
dbverify.sh/cmd userID password
```

**Note:** When using Oracle, modify the `yfs.tables.sql` file to reference your newly created tablespaces.

2. If you want to ignore the third-party tables when verifying the database, modify the `dbverify.sh` (or `.cmd` on Windows) script, which is located in the `install_dir/bin` folder.

Add the **-DIgnore3rdPartyTables=Y** parameter as specified in the below example. The third-party tables are not defined in Gentran Integration Suite entity XML or extension XML file. For example,

```
%JAVA_HOME%\bin\java -DIgnore3rdPartyTables=Y
com.yantra.tools.dbverify.DbVerifyCommandLine -b %INSTALL% -u %USERNAME% -p
%PASSWD% -d %DRIVER% -url %URL% -g Y -DT
%INSTALL%/template/api/YFSDataTypes.xml
```

**Note:** If you have custom or third-party tables in your database and you receive an exception while running the `dbverify.sh` (or `.cmd` on Windows) script, use this parameter to ignore the custom or third-party tables.

3. The differences between the entity XMLs and the database are generated in the form of SQL scripts, which can be run against the database to rectify the differences. The following scripts are generated:

- ◆ `EFrame_Sequence.sql` - This script creates all of the additional sequences that need to be created.

**Note:** If you are using a Microsoft SQL Server 2000/2005 database, `EFrame_Sequence.sql` is not created when you run the `dbverify` command.

**Note:** When reducing the size of a column, a comment will be logged in the `EFrame_TableDrops.sql` rather than a `sql` statement in the `EFrame_TableAlters.sql`.

- ◆ `EFrame_TableChanges.sql` - This script contains all the table column differences that need to be applied on the database schema. Modify this file to reference your tablespaces.
- ◆ `EFrame_TableDrops.sql` - This script removes any extra tables in the database.
- ◆ `EFrame_IndexAdds.sql` - This script adds all of the indexes that need to be created in the database. Modify this file to reference your tablespaces.
- ◆ `EFrame_IndexDrops.sql` - This script removes any extra indexes in the database.

- ◆ EFrame\_TextIndexUpdates.sql - This script contains all the text search indexes related differences that need to be applied on the database schema.
4. Run *install\_dir/database/scripts/dbtype/ImportExport\_View.sql* and *Interop\_Views.sql* scripts manually, where *dbtype* is either *mySQL*, *DB2*, *Oracle*, *SQL server 2000* or *SQL server 2005*, depending on what you are using for a DBMS.

For example, if there is a mismatch in the size of a datatype for a column [varchar2(20) to varchar2(40)] that has an associated index, the DBVerify tool generates SQL statements for:

- ◆ Dropping the index
- ◆ Changing the size of the datatype for the column
- ◆ Creating the new index

All three SQL statements listed above appear in different \*.sql files. The appropriate \*.sql files must be run in a proper order as follows:

- a. Run *EFrame\_IndexDrops.sql* for dropping the index.
- b. Run *EFrame\_TableChanges.sql* for altering the size of the datatype for a column.
- c. Run the *EFrame\_IndexAdds.sql* for creating a new index.

If the SQL statements are not run in the sequence as mentioned above, it results in script failure.

---

# Configuring for a Non-English Environment

You can install Gentran Integration Suite in an English or a non-English environment. By modifying a few system settings, you can then configure Gentran Integration Suite for your locale.

This section includes the following topics:

*Installing the Language Pack on UNIX/Linux on page 69*

*Installing on a Remote Computer on page 70*

*Loading Gentran Integration Suite Language Pack Factory Defaults on page 70*

*Configuring Encodings for Gentran Integration Suite on page 71*

*Configuring Locales on page 72*

This chapter also explains how to install, load the factory defaults, and check the import mode of Gentran Integration Suite language packs.

---

## Installing the Language Pack on UNIX/Linux

To install Gentran Integration Suite language pack on UNIX/LINUX, insert the language CDs that you received into your CD-ROM drive and open the directory that is appropriate for your Unix operating system as follows:

**Note:** Before installing the language pack be sure that you have successfully installed Gentran Integration Suite.

If you are using AIX - open the AIX directory and run the `setup.bin` command.

If you are using HP-UX - open the HP directory and run the `setup.bin` command.

If you are using Solaris - open the Sun directory and run the `setup.bin` command.

If you are using RedHat Linux - open the Linux directory and run the `setup.bin` command.

If you are using SUSE Linux - open the Linux directory and run the `setup.bin` command.

---

## Installing on a Remote Computer

To install Gentran Integration Suite language pack on a Remote Computer, you can install Gentran Integration Suite Language Packs onto any supported remote UNIX server.

If you received any language CDs from Sterling Commerce, FTP the `setup.bin` file from the appropriate operating system directory of the CD-ROM to the remote UNIX server.

---

## Loading Gentran Integration Suite Language Pack Factory Defaults

To load the language-specific factory defaults run the `loadDefaults.sh` script for UNIX and Linux or the `loadDefaults.cmd` script for Windows available in the `install_dir/bin` directory and pass the locale-specific installer file. For example:

```
loadDefaults.cmd install_dir/database/FactorySetup/install/  
<language>_<country>_locale_installer.xml
```

The default locale that is shipped with the CD is `ja_JP`.

## Loading Gentran Integration Suite Language Pack Translations

Prior to loading Gentran Integration Suite Language Pack factory defaults, be sure that you have successfully completed all instructions in the database tier software chapter.

To load the language pack translation with custom localization literals, run the `LocalizedStringReconciler` tool in the `IMPORT` mode from the `install_dir/bin` directory as follows:

```
ant -f localizedstringreconciler.xml import  
-Dsrc= /database/FactorySetup/XMLS
```

This tool first inserts the value specified in the `<from_language>_<from_country>_ycplocalizedstrings_<to_language>_<to_country>.properties` file present in the `install_dir/database/FactorySetup/XMLS/<language>_<country>` directory into the database.

**Note:** Verify that your locale settings such as currency, time format, date, and so forth, are correct.

## Switching Gentran Integration Suite Base Language

The base language for the Application Configurator can be switched only once.

---

## Configuring Encodings for Gentran Integration Suite

Language settings for Java applications involve both character sets and encoding:

A *character set* is a set of characters (letters, numbers, and symbols such as #, \$, and &) that are recognized by computer hardware and software.

An *encoding* is a representation of data in a particular character set. An *encoding set* is a group of encodings.

For information about basic and extended encoding sets, see the java web site.

The default encoding for Gentran Integration Suite is 8-bit Unicode Transformation Format (UTF-8).

Gentran Integration Suite provides two property files that contain supported encoding sets. These properties files reside in the *install\_dir/properties* directory.

encodings.properties – Contains the default encoding set used in Gentran Integration Suite interface.

encodings\_large.properties – Contains all supported encoding sets.

The default encoding set in Gentran Integration Suite includes the following encodings:

UTF-8  
ISO-8859-1  
ISO-8859-5  
US-ASCII  
ISO\_8859-1  
EUC-JP  
UTF-16  
ISO-2022-JP

You are not limited to the encodings in the encoding.properties file. Gentran Integration Suite enables you to configure the encodings properties files to expand the number of encodings you can use.

To configure your encoding set:

1. Stop Gentran Integration Suite and wait for shutdown to complete.
2. Change to the *install\_dir/properties* directory.
3. Open the encodings\_large.properties file. Select the encodings you want to add to the encodings.properties file.
4. Open the encodings.properties.in file.
5. At the end of the encodings.properties.in file, add the encodings you selected from the encodings\_large.properties file. When adding encodings from one file to the other, first copy the encodings as they appear in the encodings\_large.properties file. After adding the new encodings, ensure that the index numbers are consecutive. If the index numbers are not consecutive, change the

index number or numbers as needed. For example, `encoding54` cannot follow `encoding6`. In this example, change `encoding54` to `encoding7`.

The first name in the definition (before the comma) is the name that will appear in the Gentran Integration Suite user interface. You can change this name to make it more descriptive. For example:

```
encoding4 = 819,ISO8859_1
```

may be changed to

```
encoding4 = WesternEurope,ISO8859_1
```

`ISO8859_1` is the Java canonical name and should not be changed.

- Update the first line in the `encodings.properties.in` file (*numberof*). Change *numberof* to the number of encodings added to the file. For example, if the current value is *numberof* = 6 and you add 5 new encodings, the new value is *numberof* = 11.

*numberof* indicates the total number of encodings located in the file. You must update *numberof* to ensure that the encodings you added will be visible in the user interface.

- Change to the `install_dir/bin` directory.
- Run the `setupfiles.sh` script or the `setupfiles.cmd` script (Windows only).
- Start Gentran Integration Suite.

---

## Configuring Locales

Gentran Integration Suite runs in any locale that Java supports. If you want to run Gentran Integration Suite in a non-default locale, then configure your environment to the specific locale you want to use.

To configure your operating system as a non-English environment, consult your operating system's documentation. To determine and set the locale in a UNIX or Linux environment:

- Enter **locale -a**. A list of locales is displayed.
- Set your locale by entering:

- ◆ **export LANG <locale>**
- ◆ **export LC\_ALL <locale>**

Example to set the locale to Japanese (on Solaris):

- `export LANG ja_JP`
- `export LC_ALL ja_JP`

**Note:** Some UNIX shells require the `setenv` command instead of the `export` command.

To determine and set your locale in a Windows environment:

- Select **Control Panel > Regional Options > General tab**.
- From the **Your locale (location)** list, select the language and location.



**Note:** Click **Set Default** and select the locale from the **Set the appropriate locale** list.

---

# Using Gentran Integration Suite with Gentran:Server for UNIX

You can configure Gentran Integration Suite to run with Gentran:Server for UNIX.

This section includes the following topics:

*About Gentran:Server for UNIX and Gentran Integration Suite on page 74*

*Installing and Configuring Attunity® Data Connect on page 75*

*Configuring Gentran Integration Suite to Run with Gentran:Server for UNIX on page 76*

---

## About Gentran:Server for UNIX and Gentran Integration Suite

Gentran Integration Suite has the ability to access information located in Gentran:Server for UNIX version 5.3 or 6.0. The following restrictions apply:

You must be using Gentran Integration Suite in one of the following environments:

- ◆ UNIX
- ◆ Linux

You must be using one of the following Gentran:Server for UNIX product levels:

- ◆ Gentran:Server for UNIX with Process Control Manager (PCM)
- ◆ Gentran:Server for UNIX with EC Workbench (ECW)
- ◆ Gentran:Server for UNIX with Advanced Data Distribution (ADD)

By configuring Gentran Integration Suite to run with Gentran:Server for UNIX, you can:

View data from your Gentran trading partners.

Start or stop Gentran:Server data managers and view which data managers are running.

View, search, and track Gentran:Server for UNIX Life Cycle event records.

You can configure Gentran Integration Suite with Gentran:Server for UNIX either immediately following installation or at a later date. When you configure Gentran Integration Suite with Gentran:Server for UNIX, you only need to configure the features relevant to what you want to use:

In Gentran:Server for UNIX, configure trading partners and the Gentran Life Cycle.

In Gentran Integration Suite, configure tracking and operations.

---

## Installing and Configuring Attunity® Data Connect

If you want Gentran Integration Suite to use the trading partner information in your Gentran:Server for UNIX system, you must install and configure Attunity Data Connect. However, if you plan to convert your trading partner data from Gentran:Server for UNIX format to Gentran Integration Suite format, skip this section.

Attunity Data Connect is third-party software that enables you to view your Gentran trading partners' data. The Attunity Data Connect software provides JDBC access to the Gentran DISAM database fields where the trading partner information is stored.

To configure Attunity Data Connect:

1. Install Attunity Data Connect 3.3 or later using the installation procedures provided with the Attunity Data Connect software.
2. Ensure that Attunity Data Connect runs as expected.
3. Create a new DISAM data source and refresh the Attunity Data Connect server. For more information, see the Attunity Data Connect documentation.
4. Locate the following metadata description files in the *install\_dir/tp\_import/gentran/disam\_mapping* directory.
  - ◆ TP\_MAST.XML
  - ◆ TRADACOM.XML
  - ◆ ORGANIZATION.XML
  - ◆ TP\_MISC.XML
5. In each file listed in Step 4, replace the string **\$YOUR\_DATASOURCE** with the name of the data source for your Gentran:Server for UNIX system.
6. In each file listed in Step 4, replace the string **YOUR\_GENTRAN** with the path to the root directory of Gentran:Server for UNIX.
7. Run the Attunity Data Connect Dictionary (ADD) Editor.
8. Select the DISAM data source you created in step 3.
9. Import the metadata description files you updated in steps 5 and 6.
 

For information about importing XML metadata description files, see your *Attunity Data Connect* documentation.
10. Verify that the imported metadata description files are included in the list of tables.

11. Save your changes.
12. Exit the Attunity Data Connect Data Dictionary (ADD) Editor.

---

## Configuring Gentran Integration Suite to Run with Gentran:Server for UNIX

To configure Gentran Integration Suite to run with Gentran:Server for UNIX:

1. Set the Umask to **002** in Gentran Integration Suite.
2. Is Gentran Integration Suite installed on a different computer than Gentran:Server for UNIX?
  - ◆ If Yes, then NFS mount the \$EDI\_ROOT of Gentran:Server for UNIX onto the Gentran Integration Suite host.
  - ◆ If No, then continue with Step 3.
3. Verify that the remote shell (rsh or remsh) is working.
 

If you are unable to use the rsh/remsh shell and can only use the ssh shell, change the GS\_RSHELL variable, located in the sandbox.cfg file, when you configure Gentran Integration Suite to run with Gentran:Server for UNIX.
4. Change the directory in Gentran Integration Suite to *install\_dir/bin*.
5. Run `softstop.sh` to stop Gentran Integration Suite.
6. Run `configGSUnix.sh` to begin configuring Gentran Integration Suite to run with Gentran:Server for UNIX.
7. Press **Enter** to continue configuring Gentran Integration Suite to run with Gentran:Server for UNIX.
8. Do you want to configure Tracking and Ops using the Gentran Integration Suite interface?
  - ◆ If Yes, go to step 9.
  - ◆ If No, go to step 15.
9. Are you currently using Gentran Life Cycle?
  - ◆ If Yes, select the appropriate database you are using with Gentran:Server for UNIX and enter the following database information:
    - Database vendor
    - Absolute path of the JDBC drivers
    - Database user name
    - Database password
    - Database (catalog) name
    - Database host name using either the IP address or name of the computer where the database is installed
    - Database port number

- ◆ If No, go to step 10.
10. Is Gentran:Server for UNIX installed on the same computer as Gentran Integration Suite?
- ◆ If Yes, enter EDI\_ROOT for the local computer, and go to step 14.
  - ◆ If No, go to step 11.
11. Enter the host name of the computer where Gentran:Server for UNIX is installed.
12. Enter the EDI root where Gentran:Server for UNIX is locally mounted.
13. Verify the EDI root for the computer where Gentran:Server for UNIX is installed.
14. Indicate which version of Gentran:Server for UNIX is currently installed.
- ◆ For version 5.3, enter **1**.
  - ◆ For version 6.0, enter **2**.

If you press **Enter** without making a selection, version 6.0 is selected as the default.

15. Do you want to configure Gentran Integration Suite so that you can view Trading Partner Administration?
- ◆ If Yes, enter the following Gentran:Server for UNIX database information:
    - Absolute path for the JDBC drivers (*/attunity\_install\_dir/java*)
    - Database user name
    - Database password
    - Host name where Attunity Data Connect is installed
    - Database name
    - Attunity database port
  - ◆ If No, go to step 16.
16. Do you want to continue with the installation?
- ◆ If Yes, enter **yes** to start configuring Gentran:Server for UNIX with Gentran Integration Suite:
  - ◆ If No, enter **no** to cancel the installation.

After the installation completes, the following message displays, *Deployment to the application server successful*.

17. Enter `run.sh`.

---

# Migrating from Gentran:Server for UNIX to Gentran Integration Suite

When you are migrating maps and setting up processes in Gentran Integration Suite from Gentran:Server for UNIX, Gentran:Server for UNIX now displays translation errors, if any, in the envelope segments and does not process the erroneous envelope segments.

Gentran:Server for UNIX 6.0 and 6.1 allowed EDI envelope segments (ISA, GS, ST, SE, GE, IEA, UNB, UNH, UNT, and UNZ) with errors to be processed successfully. This has been corrected and Gentran:Server for UNIX now issues translation errors when using X12 or EDIFACT develope processes. The functional acknowledgements display the errors in the envelope segments.

**Note:** Ensure that the EDI data is corrected before starting the process.

The following examples illustrate scenarios wherein Gentran:Server for UNIX allowed successful processing of EDI segments with errors:

Gentran:Server for UNIX did not display an error when the segment count in the UNT or SE segments did not reflect the correct count of segments in a transaction.

Gentran:Server for UNIX did not display an error when the use of segment delimiters in the Map Input properties did not match the data. The user could not specify a delimiter in a map with multiple data files that used different delimiters. The user had to use the Syntax Record and specify the positions of the delimiters.

## A

accounts 29  
administrator login 48  
Attunity Data Connect 75

## C

capacity planning 8  
ccaseid.jar 39  
cross-site script vulnerabilities  
  malicious HTML 63  
  prevention 63

## D

data migrator  
  properties file 64  
data migrator properties 64  
database sizing 8  
  capacity planning 8  
  future disk estimation 9  
database user privileges  
  DB2 17  
  Oracle 10  
  Oracle, administrative user 10  
  Oracle, application user 11  
  SQL server 15  
database verification 67  
databases  
  configuring 8  
  MySQL 19  
  reinstalling 8  
DB2  
  client components 18  
  codepage selection 17  
  compilers 18  
  configuring 17  
  database sizing, See Also database sizing 17

  fix pack 18  
  installation 17  
  JDBC drivers 19  
  permissions 19  
  production environment 17  
  schema change script 38  
  setting parameters 18  
decryption, UNIX password 20  
disk estimation  
  future requirements 9

## E

Eclipse  
  removing 52  
EFrame\_IndexAdds.sql 67  
EFrame\_IndexDrops.sql 67  
EFrame\_Sequence.sql 67  
EFrame\_TableChanges.sql 11, 67  
EFrame\_TableDrops.sql 67  
EFrame\_TextIndexUpdates.sql 68  
encryption  
  UNIX password 20  
estimates of database 8

## F

factory defaults 66, 67  
fix\_db2\_schema.sql 38

## G

Gentran:Server for UNIX  
  configuring 76  
  integration with 74, 75  
Graphical Process Modeler  
  downloading 54  
  removing 52

## H

- hard stop 51
- hot-fix installation 38
- HTML characters
  - impacting display 63

## I

- installer restart file 67
- installing 33
  - DB2 17
  - hot-fixes 36
  - Oracle 9
  - patches 36
  - SQL Server
  - troubleshooting 53
  - validating installation 50
- installing database software
  - DB2. See DB2
  - Oracle 9
  - SQL Server. See SQL Server
- installing SQL Server 15
- InstallService.sh 39
- interface
  - network bindings 48

## J

- Java 2 Software Development Kit. See JDK
- JDK
  - installation 28
  - patch installation 44

## L

- language pack
  - installing 69
  - installing on remote computer 70
  - loading factory defaults 70
  - loading language pack translations 70
  - switching base language 70
- language settings
  - default encoding 71
- languages, supported 72



- LDAP user authentication 64
  - assumption 64
  - for application consoles 64
  - modifying configurator UI 65
  - modifying weblogic startup file 65
  - password expiration 64
  - password expiration, change password link 64
  - password expiration, expire in days 64
  - properties 64
- license files 30
- loading factory defaults,database factory defaults 66
- locales 72
- localization 72
- login
  - default 48

## M

- Map Editor
  - downloading 54
  - removing 52
- MESA Developer Studio
  - downloading 50, 54
  - installing 55
  - removing 52
- MySQL databases 19

## N

- named pipes 15
- network interfaces 48
- noapp.properties 49
- non-English environment 69
- non-English language 72

## O

- Oracle
  - configuring 11
  - copying JDBC driver 10
  - creating views 11
  - database sizing, See Also database sizing 11
  - installing 9
  - production environment 11
  - running create instance 9

## P

- Page cannot be displayed error 48
- password
  - decrypting password (UNIX) 20
  - default 48
  - encrypting database passwords 20
  - encrypting password (UNIX) 20
  - expiration 64
- patch installation 36
- perimeter server
  - installing 41
  - installing in a less secure network 43
  - installing in more secure network 42
  - setup 41
  - starting 45
  - stopping 45
- port numbers 29
- postinstallation 47
- property files 63
  - noapp.properties 49
  - sandbox.cfg 29, 34, 76

## R

- reinstalling
  - databases 8
- removing 51
- Reporting Services
  - configuring 62
  - downloading 50, 54
  - installing 62
  - removing 52
  - WebDAV server 62
- running
  - Oracle scripts 12
  - SQL Server scripts 15

## S

- sandbox.cfg 34, 76
- security
  - decrypting password (UNIX) 20
  - encrypting password (UNIX) 20
- setting database connection properties 63

- setting up
  - database verification tool 67
  - Oracle scripts 11
- silent installation 31
- soft stop 51
- SQL Server
  - configuring 15
  - enabling named pipes 15
  - enabling TCP/IP 15
  - production environment 15
  - sizing, See Also database sizing 15
- starting 48
- startupPs.sh 45
- stopping 51
- system
  - Gentran:Server for UNIX 74, 78
- system administration, initial 50
- system requirements 27, 28

## T

- TCP/IP 15
- troubleshooting 53
  - access 48
  - Page cannot be displayed 48

## U

- uninstalling 51
- user ID
  - default 48
- UTF-8 character set 71
- utilities
  - installation 66
- utilities, installation
  - dbVerify 66
  - loadDefaults 66

## V

- validating installation 50
- verifying database 67

**W**

Web Template Designer

  downloading 54

  removing 52

WebDAV server 58

  using with Reporting Services 62