IST/Clearing Product: Installation Guide

IST/Clearing 2.4.0

Version 1.4 - CL24010012017-R0

June 2017

Table of Contents

Table of Figures

Introduction

Purpose

The IST Product Installation Guide is used to installation and configuration IST/Clearing application. The following are the product versions supported by this Installation Guide:

- IST/Clearing- 2.4

Audience

This manual is intended for system administrators and users responsible for installing the IST/Clearing application.

Prepare for Install

These are illustrated in the diagram below. Before you begin, review the *IST /Clearing Implementation Guide*. Prepare the environment as described in this section. Installation involves a number of tasks. These are illustrated in the diagram below:

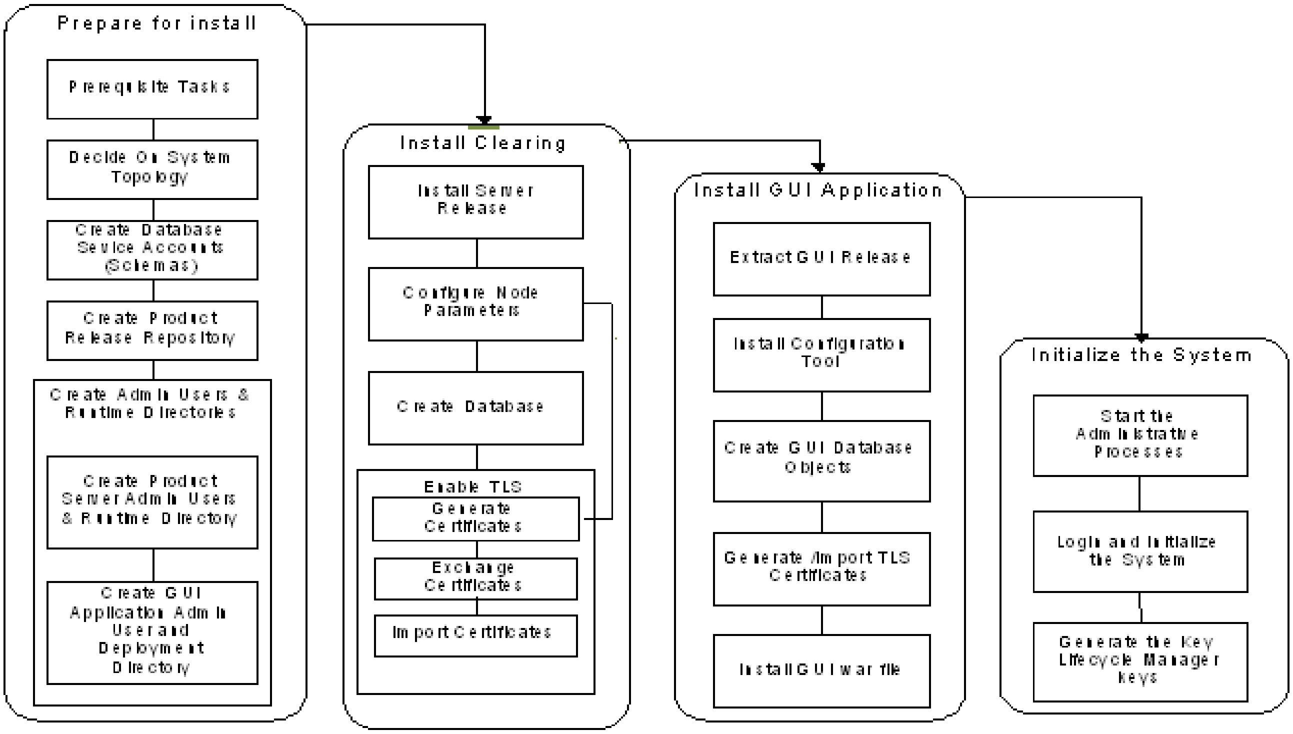

Prepare for install
Prerequisite Tasks
Decide On System Topology
Create Database Service Accounts (Schemas)
Create Product Release Repository
Create Admin Users & Runtime Directories
Create Product Server Admin Users & Runtime Directory
Create GUI Application Admin User and Deployment Directory
Install Clearing
Install Server Release
Configure Node Parameters
Create Database
Enable TLS
Generate Certificates
Exchange Certificates
Import Certificates
Install GUI Application
Extract GUI Release
Install Configuration Tool
Create GUI Database Objects
Generate /Import TLS Certificates
Install GUI war file
Initialize the System
Start the Administrative Processes
Login and Initialize the System
Generate the Key Lifecycle Manager keys

Figure 1: Installation Tasks

Product Topology

An IST/Clearing system consists of a set of nodes and a GUI application installed on web server. A node is a collection of one or more processes that run in an IST/Foundation mailbox region. The GUI application communicates with a Clearing node through an administrative process, istnodeagt.

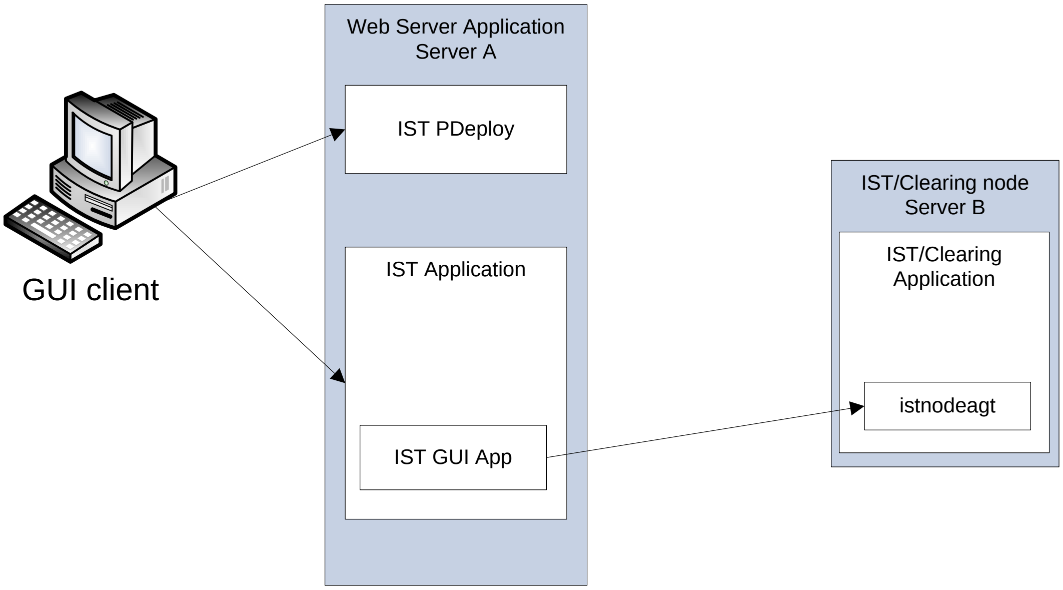


Figure 2: Simple IST/Clearing System

Each node runs in a UNIX system within an IST/Foundation mailbox region. The diagram above shows a logical view of an IST/Clearing system.

As part of system design, an IST consultant will assist you to determine the preferred topology to support your operational requirements.

System Requirements

Minimum Requirements

- UNIX OS: IBM® AIX 7.1, or HP® HPUX 11.31, or Oracle® Solaris 11 (on M-series or T-series), Red Hat® Linux RHEL 6.6, 6.7 (x64)
- 200 GB for storage hard-disk space for files and logs.
- Perl Interpreter 5.6 or later.
- Java 8

Database System

Refer to the respective vendor guide for information specific to the database.

- Database (one of the following):
    - Oracle® 11g
    - Oracle® 12c
    - DB2 9.7
    - DB2 10.1
    - DB2 11.1
- RAM as per database vendor's specification.
- 100 GB of available hard-disk space.

Web Server System

Refer to the respective vendor guide for information specific to the web application servers.

- Web application server:- IBM® WebSphere® 8.5.5, Apache® Tomcat® 8, Oracle® Weblogic 12c
- 50 GB for storage of for files and logs.

Client PC Minimum Requirements:

Processor: Intel® i7 or equivalent ;

- Microsoft® Windows®:- Windows 7® or later
- 4 – 8 GB of RAM.
- Web browser with support for Java 8 JRE (latest version required):- Microsoft® Internet Explorer® 11 or later
- 100 MB of available hard-disk space (used Java for caching).
- Monitor - 1024x768 resolution or higher. A Widescreen is recommended for Monitoring and Control.
- Java 1.8

System Topology

Prior to installation, collect all system information required for product and GUI application installation:

1. Decide on the system where each product server(s) will run, where the authentication and entitlement processes will run, and where the web server will run.
2. Create the database service accounts described and record the passwords for later use.
3. Gather all system network names, database service account names and passwords.
4. Create a diagram of the topology and include all relevant information.
5. Complete the tables below for use during installation.

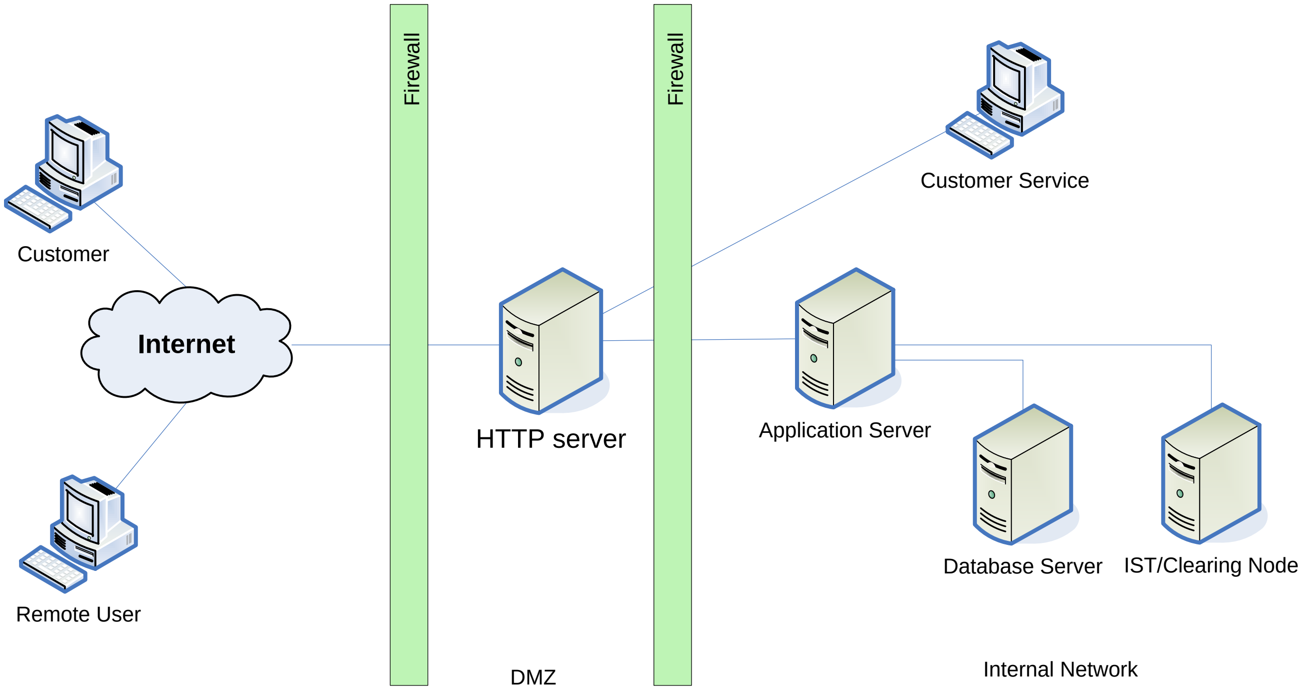


Figure 3: System Topology Sample Diagram

Clearing Installation and Runtime Environment

The following information is required during installation:

Nodes

Record the hostname and IP address of the IST/Clearing node.

Node ID	Hostname	IP
Node01		

Record the port that will be used on the node.

Ports

Specify the ports to be used on each node. Use the default or change if required. Ensure ports are not used by any other process.

Installation Parameter	Process	Parameter	Default	Change to	Internal
Guiserver_port	guiserver	gui.host localhost port	9991		yes
Auth_port	oassrv	oassrv.port	8701		Yes
Auth_control_port	oassrv	oassrv.control_port	8702		yes
Ent_port	oentsrv	oent.service	8703		yes
Xml_service_port		xmlapi.port	5031		
Xml_service_tls_port			5032		
Tok_port	tokenizer	Port.name	7531		

istnodeagt.cfg Ports

istnodeagt ports are the ports that each node will listen on for request from the GUI application.

Use the default or change if required. Ensure ports are not used by any other process.

Installation Parameter	Process	Parameter	Default	Change to	Internal
Nodeagt_msg_port	istnodeagt	nodeagt.msg_port	9992		yes
nodeagt_ctrl_port	istnodeagt	control port	9993		yes

Database Parameters

Oracle Parameters

For Oracle sqlnet.ora setup with the following entries is required:

```
DIAG_ADR_ENABLED=FALSE
DIAG_DDE_ENABLED=FALSE
DIAG_SIGHANDLER_ENABLED=FALSE
```

sqlnet.ora can be configured in the following locations:

- $ORACLE_HOME/network/admin/sqlnet.ora, or
- $HOME/tns_admin/sqlnet.ora

If $HOME/tns_admin/sqlnet.ora is used then you should put tnsnames.ora in that directory as well, and an environment variable in the clearing admin's UNIX profile that points to that directory:

```
export TNS_ADMIN=$HOME/tns_admin
```

Refer to the section on .profile for an example.

Record the following for use during installation:

- Database_name (Oracle SID or Service Name).:
- Database_tnsname:

DB2 Parameters

Create the DB2 database in restrictive mode and create a 32K tablespace and bufferpool.

For example:

```
create database clearing on /istsw7/db2data dbpath on /u00/db2data/clearing restrictive;
connect to clearing;
create bufferpool bp32k size 100 automatic pagesize 32k;
create tablespace ts32k pagesize 32k bufferpool bp32k;
```

In DB2 you must first create the roles before running the grants, otherwise the users will not get the correct privileges.

Refer to the best practices guide to further details:

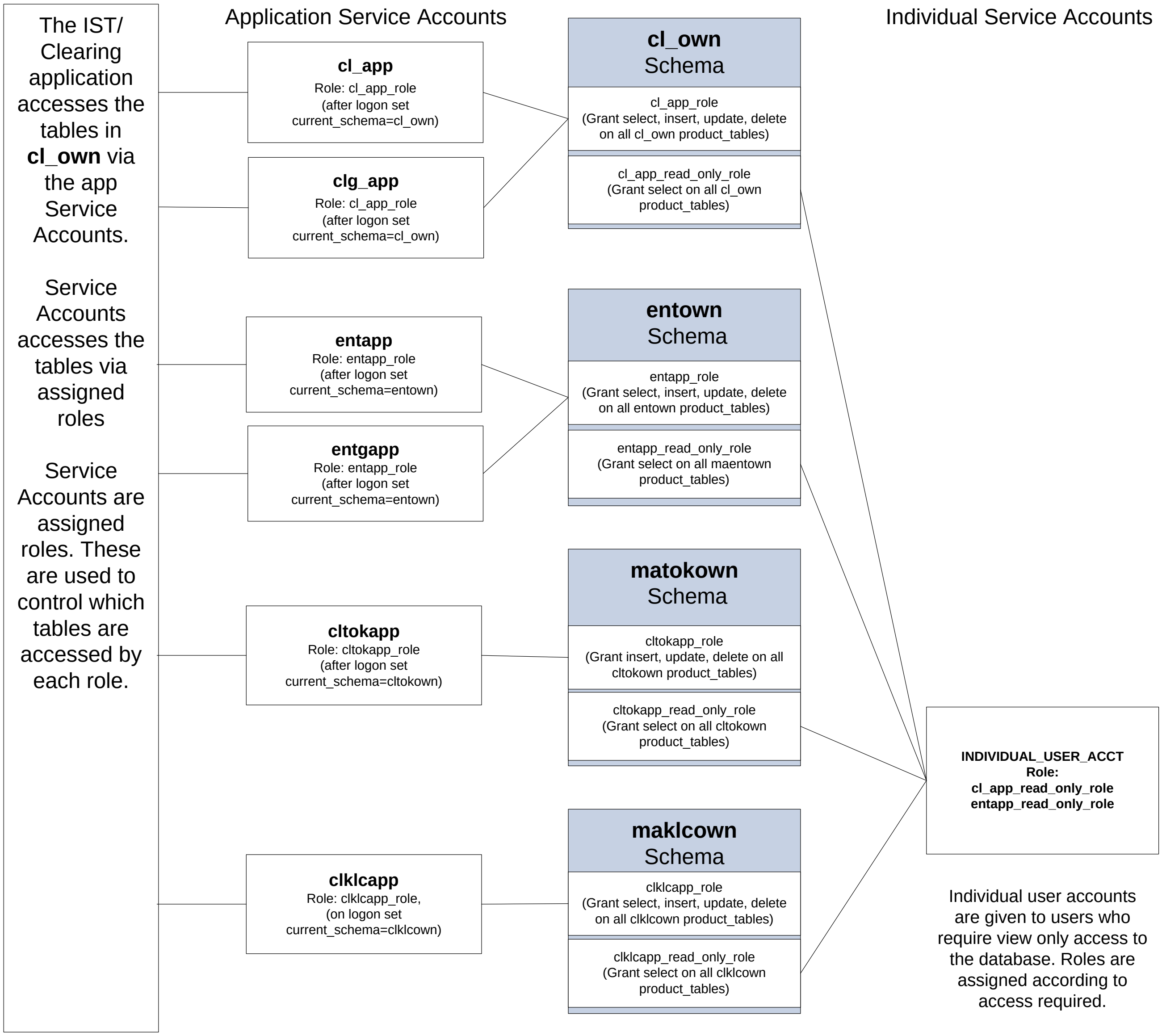
http://public.dhe.ibm.com/software/dw/data/bestpractices/DB2BP_Restrictive_Databases_0612.pdf

Database Model

The database can be setup with different configurations. The configuration described below is recommended. You can choose to use the installation tools to perform the database tasks or have it done by a Database administrator (DBA). A set of scripts are created by the install tool and made available for a DBA to apply.

The first step is to have the DBA:

1. Create all database service accounts to be used.
2. Create the roles, described in "Database Roles".
3. Assign roles as indicated in in Role Assignments table .
4. Create/execute the triggers.


Application Service Accounts
Individual Service Accounts
cl_app
Role: cl_app_role
(after logon set current_schema=cl_own)
clg_app
Role: cl_app_role
(after logon set current_schema=cl_own)
entapp
Role: entapp_role
(after logon set current_schema=entown)
entgapp
Role: entapp_role
(after logon set current_schema=entown)
cltokapp
Role: cltokapp_role
(after logon set current_schema=cltokown)
clklcapp
Role: clklcapp_role,
(on logon set current_schema=clklcown)
cl_own
Schema
cl_app_role
(Grant select, insert, update, delete on all cl_own product_tables)
cl_app_read_only_role
(Grant select on all cl_own product_tables)
entown
Schema
entapp_role
(Grant select, insert, update, delete on all entown product_tables)
entapp_read_only_role
(Grant select on all maentown product_tables)
matokown
Schema
cltokapp_role
(Grant insert, update, delete on all cltokown product_tables)
cltokapp_read_only_role
(Grant select on all cltokown product_tables)
maklcown
Schema
clklcapp_role
(Grant select, insert, update, delete on all clklcown product_tables)
clklcapp_read_only_role
(Grant select on all clklcown product_tables)
INDIVIDUAL_USER_ACCT
Role:
cl_app_read_only_role
entapp_read_only_role

The IST/ Clearing application accesses the tables in **cl_own** via the app Service Accounts.

Service Accounts accesses the tables via assigned roles

Service Accounts are assigned roles. These are used to control which tables are accessed by each role.

Individual user accounts are given to users who require view only access to the database. Roles are assigned according to access required.

Figure 4: Database Service Accounts (Schemas)

All objects such as tables are created under an account (schema) that owns all the database objects. The processes that require access to the tables will do so using one of the service accounts. These service accounts have read, insert, update and delete access, but no rights to alter tables or to grant access to tables. Access is granted using roles that have rights only to those tables required by the application.

Owner Service Accounts

cl_own — This service account owns all Clearing objects (such as tables). This account is used for initial setup and is managed by the DBA once all objects are created.

cltokown — This service account owns Tokeinzer objects (such as tables). This account is used for initial setup and is managed by the DBA once all objects are created.

clklcown

This service account owns all Key Life Cycle objects (such as tables). This account is used for initial setup and is managed by the DBA once all objects are created.

entown

This service account owns all authentication and entitlement objects (such as tables). This account is used for initial setup and is managed by the DBA once all objects are created.

Application Service Accounts

cl_app

This service account will be used by the Clearing application to access the Clearing tables. Roles are assigned to provide select, insert, updated and delete privileges.

clg_app

This service account will be used by the Clearing GUI application to access the Clearing tables. The cl_app_role is assigned to provide select, insert, updated and delete privileges to the objects in cl_own

entapp

This service account will be used by the authentication and entitlement processes to connect to the authentication and entitlement tables. The entapp_role is assigned to provide select, insert, update and delete privileges to the objects in entown.

entgapp

This service account will be used by the Clearing GUI application to access the authentication and entitlement tables. The entapp_role is assigned to provide select, insert, update and delete privileges to the objects in entown.

cltokapp

This service account will be used by the tokenizer process to access the To tables. The cltokapp_role is used to provide select, insert, update and delete privileges to the objects in cltokown

clklcapp:

This service account will be used by the key life cycle management process to access the KLC tables. The clklcapp_role is assigned to provide select, insert, updated and delete privileges to the objects in clklcown

Individual Service Accounts

<user-ID>:

This type of service account is provided to some individual users, generally with read only access. This account is used view but not change data. Read only roles are assigned depending on what data the person is allowed to view.

The owner users must have privileges: .

- create, select, insert, update, delete, and alter tables, triggers and stored procedures.
- grant privileges to the roles for their respective schemas.
- create views.

Database Roles

The following roles are required

clbasic_role	Privilege to connect to the database, and which can be used to assign that privilege to other users.
cl_app_role	Privileges to select, insert, update, delete on all Clearing tables in CLown.
cltokapp_role	Privileges to select, insert, update, delete on all tokenizer tables in cltokown.
clklcapp_role	Privileges to select, insert, update, delete on all key lifecycle tables in clklcown.
cl_app_read_only_role	Privileges to select the Clearing product tables created in cL_own.
cltokapp_read_only_role	Privileges to select tokenizer tables created in cltokown.
clklcapp_read_only_role	Privileges to select keylifecycle tables created in clklcown.
entapp_role	Privileges to insert, update, delete on all authentication and entitlement tables in entown.
entapp_read_only_role	Privileges to select entitlement tables created in entown.

Service Accounts and Role Assignment

Roles are to be assigned to service accounts as shown in table below.

Module	Service Account	Role	Password
Clearing	cl_app	clbasic_role, clapp_role	
GUI	clg_app	clbasic_role, clapp_role	
Authentication and Entitlement	entapp	clbasic_role, clentapp_role	
GUI	entgapp	clbasic_role, clentapp_role	
Tokenizer	cltokapp	clbasic_role, cltokapp_role	
Key Lifecycle Management	clklcapp	clbasic_role, clklcapp_role	

Individual		clbasic_role, cl_app_read_only_role, entapp_read_only_role	

The passwords are not displayed when entered into the installation tool, and are stored in the respective configuration files.

Oracle Users - After Logon Trigger

Create Oracle users and setup after logon trigger for each APP service account as in the table below. The after logon trigger will set the current schema to the respective owner account. Access is controlled by the roles.

Service Account	After logon trigger

cl_app:	`create or replace TRIGGER CL_APP.after_logon_trg`
	`AFTER LOGON ON CL_APP.SCHEMA`
	`BEGIN`
	`  DBMS_APPLICATION_INFO.set_module(USER, 'Initialized');`
	`  EXECUTE IMMEDIATE 'ALTER SESSION SET current_schema=CL_OWN';`
	`END;`

clg_app	`create or replace TRIGGER CLG_APP.after_logon_trg`
	`AFTER LOGON ON CL_APP.SCHEMA`
	`BEGIN`
	`  DBMS_APPLICATION_INFO.set_module(USER, 'Initialized');`
	`  EXECUTE IMMEDIATE 'ALTER SESSION SET current_schema=CL_OWN';`
	`END;`

entapp	`create or replace TRIGGER ENTAPP.after_logon_trg`
	`AFTER LOGON ON CLENTAPP.SCHEMA`
	`BEGIN`
	`  DBMS_APPLICATION_INFO.set_module(USER, 'Initialized');`
	`  EXECUTE IMMEDIATE 'ALTER SESSION SET current_schema=ENTOWN';`
	`END;`

entgapp	`create or replace TRIGGER ENTGAPP.after_logon_trg`
	`AFTER LOGON ON ENTGAPP.SCHEMA`
	`BEGIN`
	`  DBMS_APPLICATION_INFO.set_module(USER, 'Initialized');`
	`  EXECUTE IMMEDIATE 'ALTER SESSION SET current_schema=ENTOWN';`
	`END;`

cltokapp:	`create or replace TRIGGER CLTOKAPP.after_logon_trg`
	`AFTER LOGON ON CLTOKAPP.SCHEMA`
	`BEGIN`
	`  DBMS_APPLICATION_INFO.set_module(USER, 'Initialized');`
	`  EXECUTE IMMEDIATE 'ALTER SESSION SET current_schema=CLTOKOWN';`
	`END;`

clklcapp:	`create or replace TRIGGER CLKLCAPP.after_logon_trg`
	`AFTER LOGON ON CLKLCAPP.SCHEMA`
	`BEGIN`
	`  DBMS_APPLICATION_INFO.set_module(USER, 'Initialized');`
	`  EXECUTE IMMEDIATE 'ALTER SESSION SET current_schema=CLKLCOWN';`
	`END;`

DB2 Users

In DB2 users are not the same as schemas so you must create as many users as there are schemas on the database host. The user names must be lowercase.

Create group clearing

Create group staff

User	Group
cl_own	clearing
entown	clearing
cltokown	clearing
clklcown	clearing
cl_app	clearing
clg_app	clearing
entapp	clearing
entgapp	clearing
cltokapp	clearing
clklcapp	clearing
<individual-user>	staff

Assign Database Roles - Oracle

The database roles must be created before the IST tables. The following can be used to create roles and assigning grants to the service accounts:

```
create role clbasic_role;
create role cl_app_role;
create role cl_app_read_only_role;
create role cltok_app_role;
create role cltok_app_read_only_role;
create role clklc_app_role;
create role clklc_app_read_only_role;
create role entapp_role;
create role entapp_read_only_role;

grant connect on database to role clbasic_role;
grant role clbasic_role to cl_own, entown, clklcown, cltokown;

grant role clbasic_role to role cl_app_read_only_role;
grant role clbasic_role to role entapp_read_only_role;
grant role clbasic_role to role cltokapp_read_only_role;
grant role clbasic_role to role clklcapp_read_only_role;

grant cl_app_role, cl_app_read_only_role to cl_app;
alter user cl_app default role cl_app_role, cl_app_read_only_role;

grant cl_app_role, cl_app_read_only_role to clg_app;
alter user clg_app default role cl_app_role, cl_app_read_only_role;

grant entapp_role, entapp_read_only_role to entapp;
alter user entapp default role entapp_role, entapp_read_only_role;

grant entapp_role, entapp_read_only_role to entgapp;
alter user entgapp default role entapp_role, entapp_read_only_role;

grant cltok_app_role, cltok_app_read_only_role to cltok_app;
alter user  cltokapp default role cltokapp_role, cltokapp_read_only_role;

grant clklc_app_role, clklc_app_read_only_role to clklc_app;
alter user clklcapp  default role clklcapp_role, clklcapp_read_only_role;

grant cl_app_read_only_role,  clent_app_read_only_role, to <individual-user>;
alter user <individual-user> default role cl_app_read_only_role,  ent_app_read_only_role;
```

Assign Database Roles – DB2

In DB2 you must first create the roles before running the grants, otherwise the users will not get the correct privileges. The set of statements below is an sample set to setup a DB2 database for Clearing.

```
create database clearing on /istcl/db2data dbpath on /u00/db2data/clearing restrictive;
connect to clearing;
create bufferpool bp32k size 100 automatic pagesize 32k;
create tablespace ts32k pagesize 32k bufferpool bp32k;
create schema authorization entown;
create schema authorization cltokown;
create schema authorization clklcown;
create schema authorization cl_own;
create role cl_app_role;
create role cl_app_read_only_role;
create role entapp_role;
create role entapp_read_only_role;
create role cltokapp_role;
create role cltokapp_read_only_role;
create role clklcapp_role;
create role clklcapp_read_only_role;
create role clbasic_role;

grant connect on database to role clbasic_role;
grant select on SYSIBM.SYSDUMMY1 to role clbasic_role;
grant usage on workload SYSDEFAULTUSERWORKLOAD to role clbasic_role;
grant use of tablespace userspace1 to role clbasic_role;
--

grant EXECUTE on package NULLID.SQLC2J23 to role clbasic_role;
grant EXECUTE on package NULLID.SQLC2J25 to role clbasic_role;
grant EXECUTE on package NULLID.SQLC3J22 to role clbasic_role;
grant EXECUTE on package NULLID.SQLC4J22 to role clbasic_role;
grant EXECUTE on package NULLID.SQLC5J22 to role clbasic_role;
grant EXECUTE on package NULLID.SQLC6J22 to role clbasic_role;
-- for CLI
grant EXECUTE on package NULLID.SYSSH100 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH101 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH102 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH200 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH201 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH202 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH300 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH301 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH302 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH400 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH401 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH402 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSN300 to role clbasic_role;

grant execute on package nullid.SYSSN100 to role clbasic_role;
grant execute on package nullid.SYSSN101 to role clbasic_role;
grant execute on package nullid.SYSSN102 to role clbasic_role;
grant execute on package nullid.SYSSN200 to role clbasic_role;
grant execute on package nullid.SYSSN201 to role clbasic_role;
grant execute on package nullid.SYSSN202 to role clbasic_role;
grant execute on package nullid.SYSSN300 to role clbasic_role;
grant execute on package nullid.SYSSN301 to role clbasic_role;
grant execute on package nullid.SYSSN302 to role clbasic_role;
grant execute on package nullid.SYSSN400 to role clbasic_role;
grant execute on package nullid.SYSSN401 to role clbasic_role;
grant execute on package nullid.SYSSN402 to role clbasic_role;

grant use of tablespace ts32k to role clbasic_role;

grant createtab on database to clentown, cltokown, clklcown, cl_own;

grant select on syscat.tables to cl_own, clentown, clklcown, cltokown, cl_app;
grant select on syscat.indexes to cl_own, clentown, clklcown, cltokown;
grant select on syscat.schemata to cl_own, clentown, clklcown, cltokown;
grant select on syscat.columns to cl_own, clentown, clklcown, cltokown;
grant select on syscat.indexcoluse to cl_own, clentown, clklcown, cltokown;
grant select on syscat.tabconst to cl_own, clentown, clklcown, cltokown;
grant select on syscat.references to cl_own, clentown, clklcown, cltokown;

grant role clbasic_role to cl_own, clentown, clklcown, cltokown;
grant role clbasic_role to role cl_app_read_only_role;
grant role clbasic_role to role entapp_read_only_role;
grant role clbasic_role to role cltokapp_read_only_role;
grant role clbasic_role to role clklcapp_read_only_role;

grant cl_app_role, cl_app_read_only_role to cl_app;
grant cl_app_role, cl_app_read_only_role to clg_app;
grant clentapp_role, clentapp_read_only_role to entapp;
grant clentapp_role, clentapp_read_only_role to entgapp;
grant cltokapp_role, cltokapp_read_only_role to cltokapp;
grant clklcapp_role, clklcapp_read_only_role to clklcapp;
```

Validate Release Files

A release is delivered, encrypted, in a gzipped-tar file with extension .rcc. ***For example:***

- CLC_2.4.0.10.01_LIN-2632-I686-64_201701120000001.tar.gz.rcc

The rcc file may contain one or more gzipped tar files, and are installed using and the build_env installation tool, also included in the rcc file.

The contents of each rcc file must be extracted using the FISValidate.exe before installation. This process checks the integrity of the file and decrypts it.

FISValidate:

- Validates the release using the supplied hash key provided in the .rpt.txt file. It checks the integrity of the release to remove the possibility of tampering during shipment.
- Decrypts the .rcc file.

FIS Secure Code Delivery and Validation

The FISValidate tool is an executable file, provided with the release to validate and extract the release files. It is available as a UNIX executable file

1. Download the files, including FISValidate, *.rcc and .rpt.txt files, to a local directory. If Unix FisValidate is used, then the files can be stored in Unix server itself.
2. Decrypt the release:
    a. On Windows
        i. Open a cmd window and change directory to the location where the release is stored.
        ii. Execute FISValidate.exe on each file to be validated using the following command: FISValidate.exe < file/folder with .rcc extension > <hash string> where:

FISValidate	Is the validation tool provided with the release.
< file/folder with .rcc extension >	Is the path to the .rcc file.
<hash sting>	Is the string contained in the corresponding .rpt.txt file provided for the release.

b. On UNIX

c. Excecute FISValidate < file/folder with .rcc extension > <hash string> where:

FISValidate	Is the validation tool provided with the release.
< file/folder with .rcc extension >	Is the path to the .rcc file.
<hash sting>	Is the string contained in the corresponding .rpt.txt file provided for the release.

Example:

```
FISValidate CL_2.4.0.10.01_LIN-2632-I686-64_201701120000001.tar.gz.rcc
baf1b8efc28e63dd06669ba3fab9338e09ae304b
```

Output of a successful validation is displayed as in the example below:

```
Validating hash
Hash value is correct
Decrypting file CL_2.4.0.10.01_LIN-2632-I686-64_201701120000001.tar.gz.rcc
Decryption to CL_2.4.0.10.01_LIN-2632-I686-64_201701120000001.tar.gz complete Validate processing
completed successfully
```

3. Transfer the file to the UNIX system where it is to be installed.

A rcc file contains one or more files. For example a full IST/Clearing server release would have a set of files similar to the following:

- ./tgz/build_env
- ./tgz/overriding_option_installer
- ./tgz/FO_7.7.0.10.01_LIN-2632-I686-64_BASE.tgz
- ./tgz/FO_7.7.0.10.01_LIN-2632-I686-64_ORA-121.tgz
- ./tgz/CL_2.4.0.10.01_LIN-2632-I686-64_BASE.tgz

The server and GUI applications are installed from their respective directories, and in separate environments.

Installation and Runtime Directories, and Release Repository

The product release repository is a directory, named tgz, where release files are stored. The tgz directory must be in a directory, set as the HOME environment variable, and owned by the admin user. Only the current set of gzipped-tar files and build_env are to be stored in the repository. Extracting the contents of a release will create and store the files in the tgz directory.

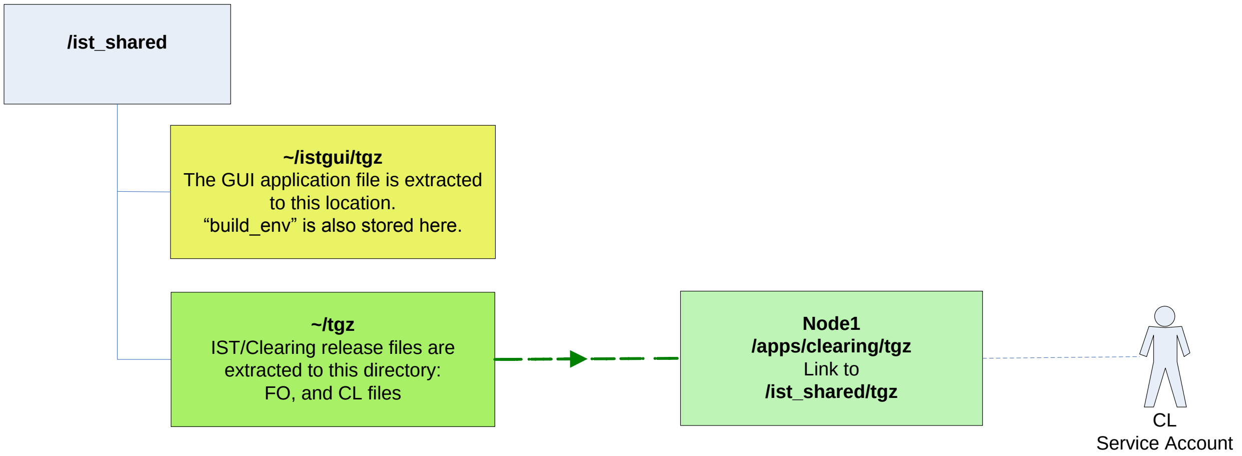

/ist_shared
~/istgui/tgz
The GUI application file is extracted to this location.
“build_env” is also stored here.
~/tgz
IST/Clearing release files are extracted to this directory:
FO, and CL files
Node1
/apps/clearing/tgz
Link to
/ist_shared/tgz
CL
Service Account

Figure 5: Installation and Runtime Directories

Administration, Release Repository and Runtime Directories

An admin user is required on each server, and the GUI application. Admin users are operating system user IDs, which are used to administer the runtime directories for each product server and the GUI application installation environment.

To install, the following are required in each runtime directory:

- A "tgz" release repository directory on a shared files system, /ist_shared/tgz
- The "build_env" and “`overriding_option_installer`” installation tool.

Extracting the contents of the validated rcc file will create the tgz directory and store the *.gz release files in it.

Create Admin Accounts and the Application Runtime Directory

IST/Clearing runs as a single node. Each server must have an account used to run the application:

- The generic account must be created with its own group. For example “clearing”. The “clearing” group must not be shared with other users.
- The admin user’s password should not be shared.
- The system should accessed using individual user (service) accounts via a sudo type access to the generic account.

On the server:

1. Create the “clearing” admin user account for the application. For example:

User:	clearing (uid 222)
Group:	clearing (gid 555)

2. Create a directory where the IST/Clearing application is to be installed. *For example:*

   /apps/clearing

   The admin user must have read and write permissions to the /apps/Clearing directory, and the HOME environment variable in the admin user's ".profile" must be set to this directory.

   For example:

   export HOME=/apps/clearing

3. Edit the user's ".profile" and add the entries as described in “.profile Entries”
4. Login as the admin user via an individual user ID.
5. Change directory to $HOME, "/apps/clearing" in the example.
6. Copy the decrypted file(s) obtained from the FISValidate procedure to the home directory, $HOME:
   a) For a clearing node copy the CL file.
7. Extract the contents:

```
gzip -dc <decrypted_file> | tar -xvf -
```

The release gzipped tar files and build_env are extracted to $HOME/tgz.

8. Create a directory, known as the protected directory, to be used to store key and truststore files, configuration files containing passwords, debug files and data files. This can be any directory accessible by the clearing user. For example:

   /apps/clearing/pd

   This directory is used to preserve runtime files that do not change from release to release.

Create GUI Application Administrator and GUI Deployment Directory

The GUI application release should be installed and staged for deployment on the web server host. Here the contents of the GUI application release will be extracted making the WAR files available to the web server administrator for deployment.

On the web server host:

1. Create a generic user account that will own the staging directory. For example***:***

User: guiadmin

Group: clearing

The guiadmin user’s password should not be shared, and should be accessed using individual user (service) accounts via a sudo type access.

2. Create a directory where the GUI application files are to be staged. For example:

   /apps/guiadmin/iststage

   This directory should be owned by the generic guiadmin u***ser.***

   The guiadmin user, must have read and write permissions to this directory, and the HOME environment variable in the admin user's ".profile" must be set to this directory. For example:

   ```
   export HOME=/apps/guiadmin/iststage
   ```

3. Edit the user's ".profile" and add entries as described in“.profile" Entries”
4. Login to the system and sudo to the generic guiadmin user.
5. Change directory to $HOME, "/apps/guiadmin/iststage" in the example.
6. Copy the decrypted file(s) obtained from the FISValidate procedure to the home directory, $HOME.
7. Extract the contents:

   ```
   gzip -dc <decrypted_file> | tar -xvf -
   ```

   The release gzipped tar files and build_env are extracted to $HOME/tgz.

IST System Installation Procedure

Three tools are provided in the release: build_env , override_option_installer and pdeploy.

The installation tool, build_env is used to create the server runtime environment for each product as well as the GUI deployment environment. Override_option_installer tool is used to override default installation settings.

The pdeploy, tool is used for the following:

- Generating the scripts used to create the tables and other objects in the owner service account (schema).
- Populating the tables with system records
- Setting up initial user and configuration parameters

Pdeploy displays the applicable parameters for installation configuration according to the product (type of node) being installed.

Product Parameter Name	Product	Usage
clearing	IST/Clearing	Creating a Clearing node and the CL database
ent	Entitlement	Specify ent when creating the Authentication and Entitlement
tok	Tokenization	Specify tok when setting up tokenization.
klc	Key lifecycle Management	Specify klc when setting up key lifecycle management.

To install an IST/Clearing system:

1. Follow the steps in, “Installing the IST/Clearing System” that describe the steps to install the server runtime environment for each node type, and create the database tables.
2. Follow the steps in “Installing the GUI Application” that describe the steps to install the GUI application files and deploy the GUI application.
3. Follow the steps in “
4. Enabling TLS for the IST Process ” and the Setup GUI Application Back-end TLS in the respective IST GUI Application Installation Guide that describe the steps to generate the keystores and certificates required to enable TLS between the IST processes.
5. Follow the steps in “**Error! Reference source not found.**” that describe the steps to start the administrative processes, login into the GUI application, initialize the Key Lifecycle Manager keys and startup the system.

After procedures 1-4 are complete the system will be ready for transaction processing configuration.

Installing the IST/Clearing System

Installing a system involves the following procedures:

1. Building the server environment and setting up initial configuration parameters for the runtime environment for each node.
2. Creating the database, i.e. creating tables and roles.

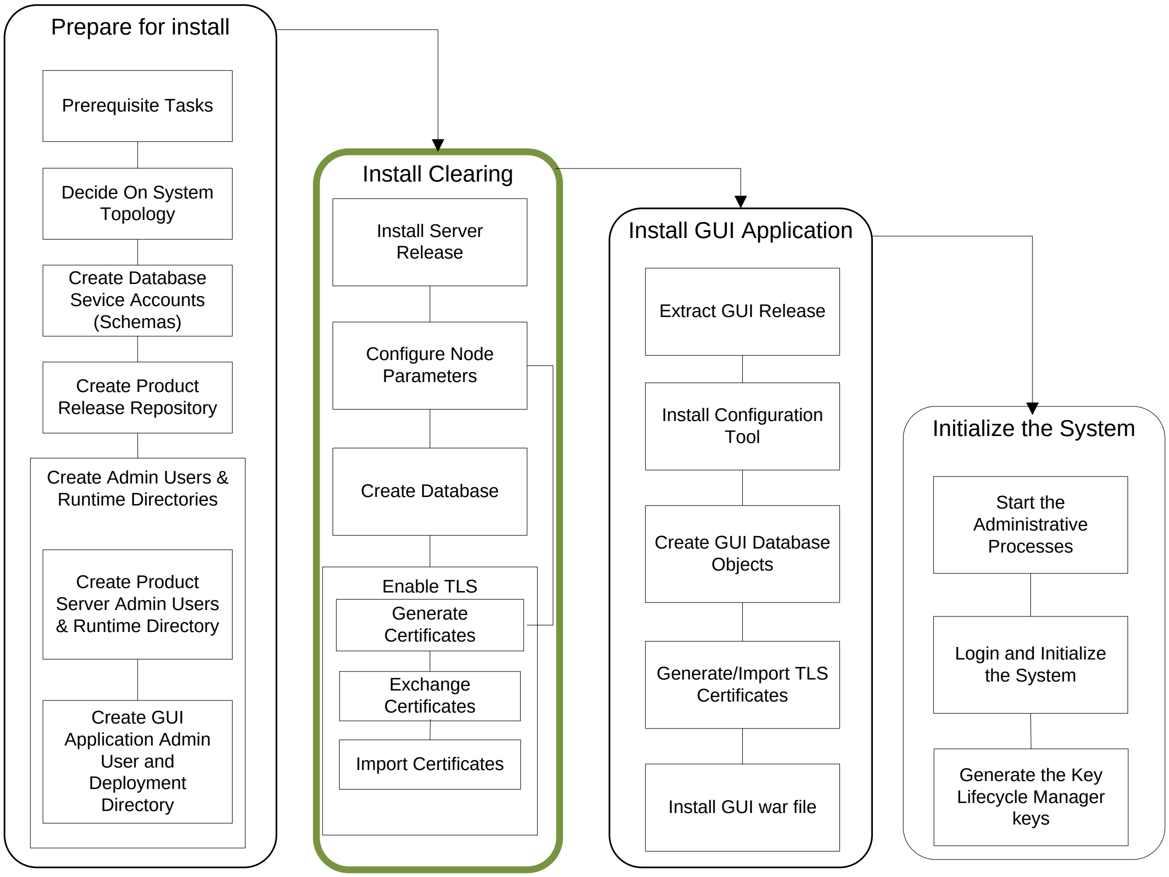

Prepare for install
Prerequisite Tasks
Decide On System Topology
Create Database Sevice Accounts (Schemas)
Create Product Release Repository
Create Admin Users & Runtime Directories
Create Product Server Admin Users & Runtime Directory
Create GUI Application Admin User and Deployment Directory
Install Clearing
Install Server Release
Configure Node Parameters
Create Database
Enable TLS
Generate Certificates
Exchange Certificates
Import Certificates
Install GUI Application
Extract GUI Release
Install Configuration Tool
Create GUI Database Objects
Generate/Import TLS Certificates
Install GUI war file
Initialize the System
Start the Administrative Processes
Login and Initialize the System
Generate the Key Lifecycle Manager keys

Figure 6: Install Nodes

Build a Node’s Runtime Environment

On each server perform the following steps to install a node

1. Login to the admin account via an individual account with “sudo ” access. This will take you to the directory where the product is to be installed. If this is not the case, check your .profile to ensure that the HOME environment variable is correctly set. Also ensure a tgz directory is in $HOME.
2. Go to $HOMe and run "build_env”

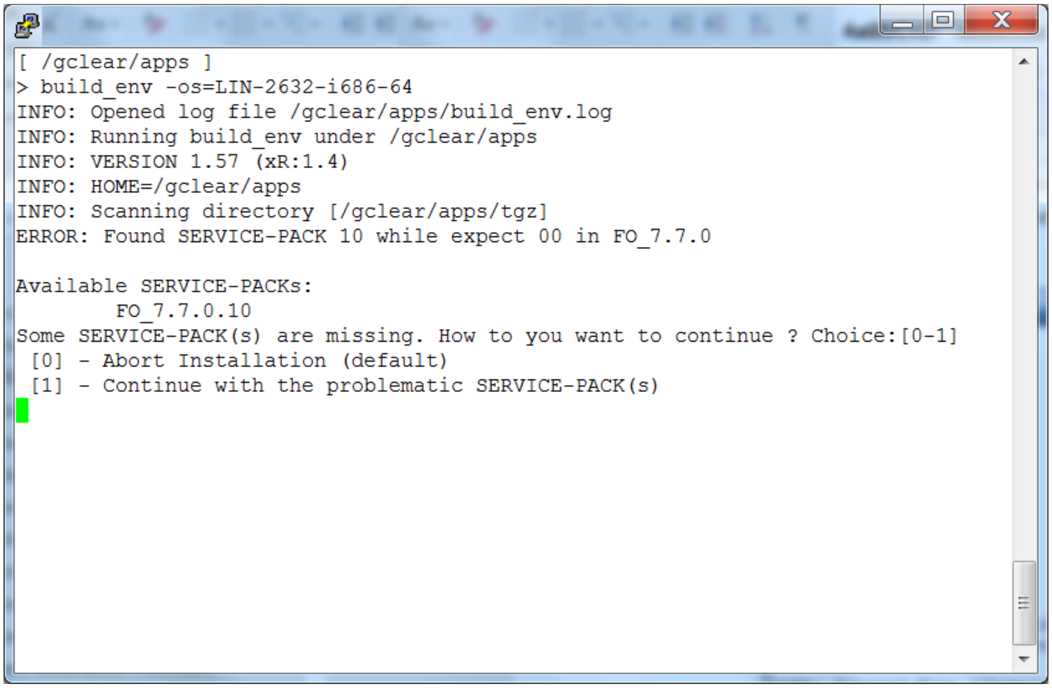
NOTE:	In some cases incremental upgrades may have been done on the OS. In such cases the OS may have to be specified on the installation command line. *For example:* A release may have been built on for IBM AIX 7.1.0 whereas the OS on the target system is AIX 7.1.2. Since the upgrade is backward compatible the AIX 7.1.0 release may be installed with the command: build_env -os=AIX-712. In such cases contact support to clarify any doubts as to the compatibility of the release.

3. At each prompt select the option as indicated below. You can abort the installation at any time.

   For example: You may want to use the tool to check the list of files that will be included in the installation without actually installing the binaries.

   Build_env checks the OS and skips all gzipped-tar files with a different OS in the file name.

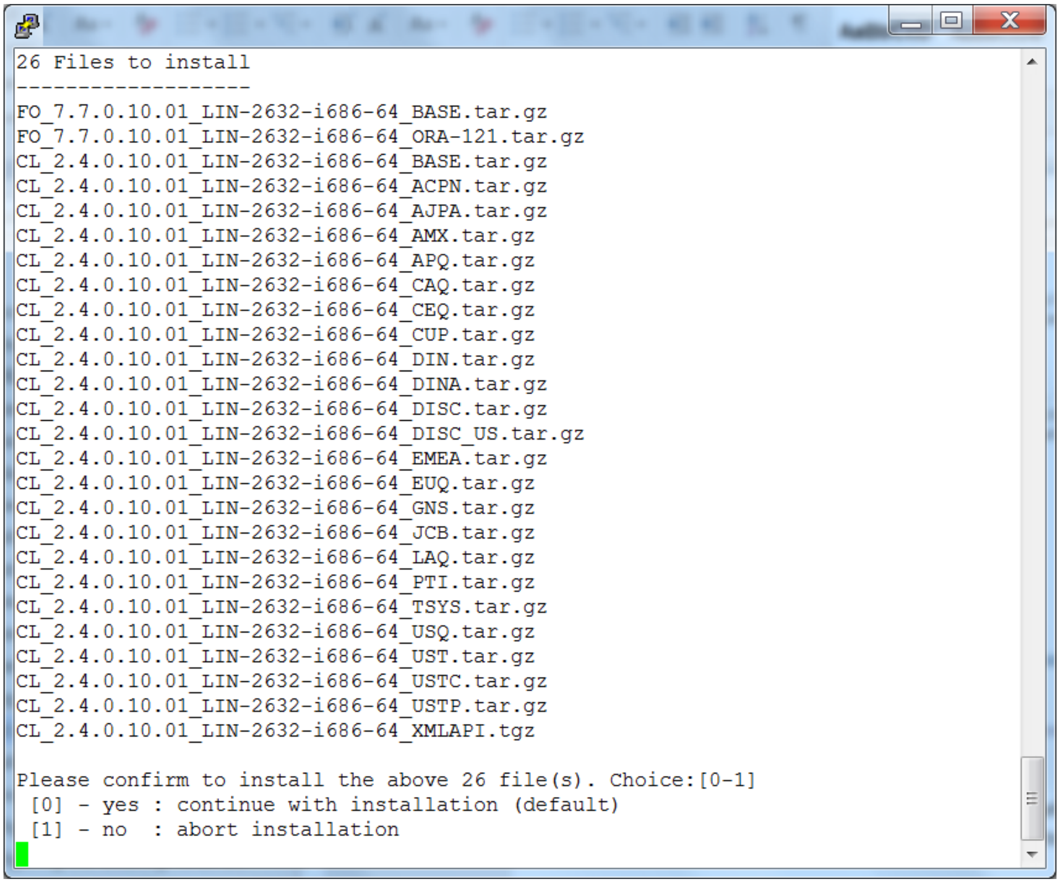
NOTE:	Screens are samples only and vary depending on the gzipped files present in "tgz".



```
[ /gclear/apps ]
> build_env -os=LIN-2632-i686-64
INFO: Opened log file /gclear/apps/build_env.log
INFO: Running build_env under /gclear/apps
INFO: VERSION 1.57 (xR:1.4)
INFO: HOME=/gclear/apps
INFO: Scanning directory [/gclear/apps/tgz]
ERROR: Found SERVICE-PACK 10 while expect 00 in FO_7.7.0

Available SERVICE-PACKs:
        FO_7.7.0.10
Some SERVICE-PACK(s) are missing. How to you want to continue ? Choice:[0-1]
 [0] - Abort Installation (default)
 [1] - Continue with the problematic SERVICE-PACK(s)
```

Figure 7 Build_env missing service pack warning

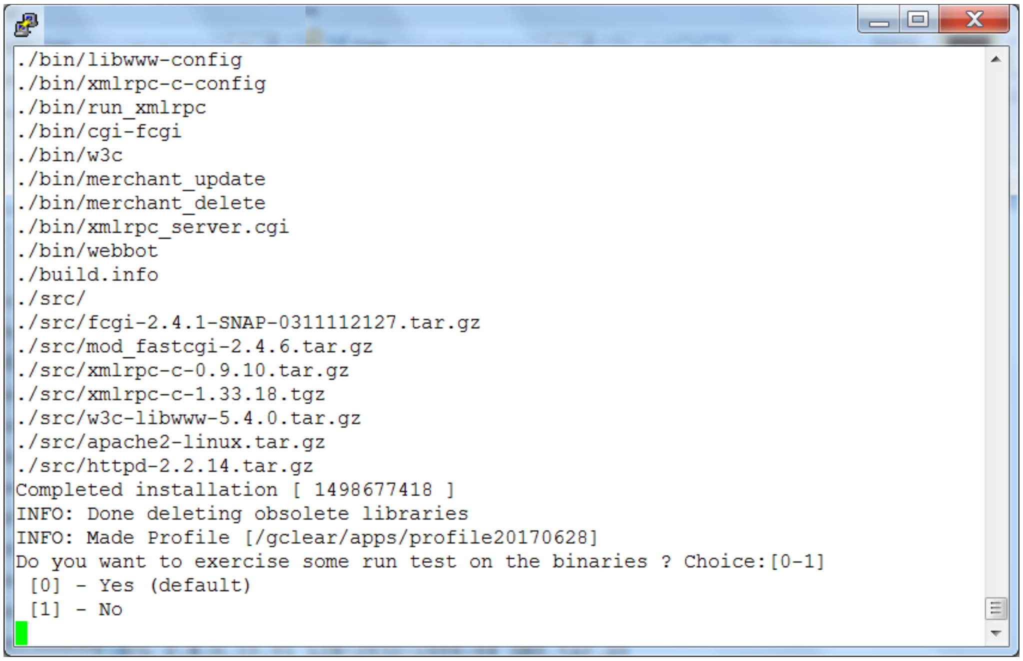
a) Build_env will warn if there are missing service packs. Select 1 to continue.



```
26 Files to install
-------------------
FO_7.7.0.10.01_LIN-2632-i686-64_BASE.tar.gz
FO_7.7.0.10.01_LIN-2632-i686-64_ORA-121.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_BASE.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_ACPN.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_AJPA.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_AMX.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_APQ.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_CAQ.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_CEQ.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_CUP.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_DIN.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_DINA.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_DISC.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_DISC_US.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_EMEA.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_EUQ.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_GNS.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_JCB.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_LAQ.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_PTI.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_TSYS.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_USQ.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_UST.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_USTC.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_USTP.tar.gz
CL_2.4.0.10.01_LIN-2632-i686-64_XMLAPI.tgz

Please confirm to install the above 26 file(s). Choice:[0-1]
 [0] - yes : continue with installation (default)
 [1] - no  : abort installation
```

Figure 8: build_env – selected list of files to install.

b) Build_env displays a list of all selected packages selected for installation. Select option 0 to continue installing or option 1 to abort the installation.



```
./bin/libwww-config
./bin/xmlrpc-c-config
./bin/run_xmlrpc
./bin/cgi-fcgi
./bin/w3c
./bin/merchant_update
./bin/merchant_delete
./bin/xmlrpc_server.cgi
./bin/webbot
./build.info
./src/
./src/fcgi-2.4.1-SNAP-0311112127.tar.gz
./src/mod_fastcgi-2.4.6.tar.gz
./src/xmlrpc-c-0.9.10.tar.gz
./src/xmlrpc-c-1.33.18.tgz
./src/w3c-libwww-5.4.0.tar.gz
./src/apache2-linux.tar.gz
./src/httpd-2.2.14.tar.gz
Completed installation [ 1498677418 ]
INFO: Done deleting obsolete libraries
INFO: Made Profile [/gclear/apps/profile20170628]
Do you want to exercise some run test on the binaries ? Choice:[0-1]
 [0] - Yes (default)
 [1] - No
```

Figure 9: Build_env Installation In Progress

c) After all available gzipped tar files are extracted and obsolete files removed, an option to perform a sanity check on the binary elements is made available as shown in Figure 8. This is an optional step and is not required.

4. Select Option 1

Select 0, or 1 for each of the 4 prompts below depending on the options you choose to use.

```
INFO: Version 1.15
INFO: OsString=[LIN-2632-i686]
INFO: Found installed product FO77010
INFO: Found installed product CL24

   = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
   = = =                                               = = =
   = = =                 W A R N I N G                 = = =
   = = =   Beware that this option will violate PADSS  = = =
   = = =                                               = = =
   = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Do you want to install "Override with file in clear (cfi-LIN-64.tgz)"
 Choice:[0-1]
 [0] - no (default)
 [1] - yes
0

   = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
   = = =                                               = = =
   = = =                 W A R N I N G                 = = =
   = = =   Beware that this option will violate PADSS  = = =
   = = =                                               = = =
   = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Do you want to install "Override with hex-dump in clear (chx-LIN-64.tgz)"
 Choice:[0-1]
 [0] - no (default)
 [1] - yes
0

   = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
   = = =                                               = = =
   = = =                W A R N I N G                  = = =
   = = =   Beware that this option will violate PADSS  = = =
   = = =                                               = = =
   = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Do you want to install "Override tokenization with ECHO only (ect-LIN-64.tgz)"
 Choice:[0-1]
 [0] - no (default)
 [1] - yes
0

   = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
   = = =                                               = = =
   = = =                W A R N I N G                  = = =
   = = =   Beware that this option will violate PADSS  = = =
   = = =                                               = = =
   = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Do you want to install "Override with shared memory unlocked (lsh-LIN-64.tgz)"
 Choice:[0-1]
 [0] - no (default)
 [1] - yes
0
:::Status(before installation):::
Current overriding options:
clear-hex-dump                  : no
clear-file                      : no
SHA1-token                      : no
ECHO-token                      : no
unlocked-shmem                  : no
INFO: Installed 0 overriding option(s)
INFO: Installation in /gclear/apps/pdir20170628
INFO: Profile in /gclear/apps/profile20170628
INFO: Log file in /gclear/apps/build_env.log

Program Completed

 - = - = - = -
```

For example Select the default , 0 (no) which implies that the tokenizer is to be used for encrypting PAN values. Otherwise if you chose not use the tokenizer option then select 1(yes) .

NOTE:	**Choosing 1 (yes) to override any of the above 4 options will make the installed application non-PADSS compliant.**

The above results in the creation of a product directory and associated profile:

i. A file with name, profile<install_date>

where,

profile	is a constant.
install_date	is the date the file was created in the format yyyymmdd. Example: profile20170628

profile<install_date> contains the environment variables required for the application to run, and is used in conjunction with the entries in the admin user's.profile.

ii. A directory with name, pdir<install_date>

where,

profile	Is a reserved constant identifier.
install_date	Is the date the file was created in the format yyyymmdd. ***Example:*** pdir20170628

This directory contains the installed product.

iii. An installation log file, build_env.log, is created and updated on subsequent installations.

iv. Create a soft link to the profile<install_date>, which executed in the user’s profile.

```
ln -s profile<install_date> profile
```

Installing Multiple Times within a Day

On occasion, it may be necessary to install multiple times within the same day. The directory pdir<install_date> will be renamed to pdir<install_date>-n, depending on the number of times the installation is done. The new environment will be created with the current date.

For example, if the current installation is pdir20170628 and you reinstall, pdir20170628 is renamed to pdir20170628_1

The new installation will be created in pdir20170628.

NOTE:	The most current installation will always be in the pdir<install_date> directory.

Service Packs, Release Candidates and Patches

Service Packs, Release Candidates and Patches are installed using the same procedure as in “Build a Node’s Runtime Environment.The installation tool will select the correct set of gzipped-tar files to install.

To install subsequent releases:

1. Ensure the run time environment variables are set.
2. Install using the following options:

```
build_env.pl -dmklink=<Protected_directory>
```

Where:

-dmklink

Imply links to the following directories:

- certdata
- cfg
- data
- files
- log

Protected_directory

Is the Protected Directory path used in pdeploy in the previous installation.

This will preserve the configuration files from the previous installation environment making them available to pdeploy in the current installation.

Pdeploy creates links for the following:

- $PRODUCT_ROOT/log
- $ISTDIR/files
- $OSITE_ROOT/cfg
- $OSITE_ROOT/data
- $OSITE_ROOT/certdata

NOTE: Ensure you logout and login again after setting the soft link to the profile<install_date>

Configuring Nodes and Creating the Database Tables

This section describes the process setup initial configuration required to initialize a node, and to create the database tables.

The configuration tool, "pdeploy" is used to generate the scripts to create the database tables and populate them with initial data. The scripts can be applied using pdeploy or by a DBA. The scripts will create required tables and insert records in the schema of the owner service account (see recommendations in section 2).

If you are upgrading the database schema from a previous version, you may be required to apply one or more upgrade scripts. Upgrade scripts can be applied using Option **Apply DB Tables Upgrade Script** and/or Option **Apply DB Records Upgrade Script** in each installation module. Alternatively a database administrator may apply the scripts.

The cl_own service account must be used to do this, since the APP service account will not have privileges to create objects in the owner account.

NOTE:	You must not run any scripts unless specifically instructed to do so in the release notes that accompany each release.

Pdeploy uses the following environment variables defined in the admin users' UNIX profile:

- $OPRODUCT_ROOT
- $OSITE_ROOT
- $ISTDIR

Pdeploy searches for SQL scripts in $OPRODUCT_ROOT/sql. It uses $OSITE_ROOT/ dbutil as a working directory to store generated database scripts. The pdeploy audit log file is stored in $OSITE_ROOT/certdata/pdeploy.

To configure the node go to the section Configuring Nodes and Creating the Database Tables

Configuring the Clearing Node and Creating the Database Tables

The steps below describe the database table creation and configuration procedures:

1. Login to the admin account via an individual account with "sudo" access. The environment will be setup using the profile<date> generated in the section Build a Node's Runtime Environment
2. Run the installation tool with the following command utility to display the server installation main menu:

   > pdeploy

   You can run pdeploy from any directory.

```
IST Installation Utility v1.214
Product Directory: /users/product-india/clrqa02/clrser/pdir20160704
                  +------------------------------------+
                  | 0. Install Server                  |
                  +------------------------------------+
IST Installation Utility v1.214
Product Directory: /users/product-india/clrqa02/clrser/pdir20160704 (2
Install Server
               +------------------------------------+
               | 0. Install Product                 |
               | 1. Install Entitlement             |
               | 2. Install Tokenizer               |
               | 3. Install Key Life Cycle          |
               | 4. Enable TLS                      |
               +------------------------------------+
```

Clearing node setup

For option 0 select steps 0 to 6 and for the options (1-3) select steps 0 to 5 to create the database tables for each of the four schemas to be created, and to configure the initial system parameters.

3. For the clearing node select 0. Install Product from the installation menu.

   This option is used to setup the Clearing runtime environment, and create database tables and initial data. Select option 0. to display the submenu below:

```
IST Installation Utility v1.214
Product Directory: /users/product-india/clrqa02/clrser/pdir20160704
Install Product
               +------------------------------------+
               | 0. Setup System Parameters         |
               | 1. Apply System Parameters         |
               | 2. Prepare DB Scripts              |
               | 3. Create DB Tables                |
               | 4. Create DB Grant                 |
               | 5. Insert DB System Records        |
               | 6. Insert DB Inst Base Records     |
               | 7. Apply DB Tables Upgrade Script  |
               | 8. Apply DB Records Upgrade Script |
               +------------------------------------+
```

Select 0 Setup System Parameters

This option is used to specify the runtime parameters the Clearing node. The parameters are shown below:

```
Product_name [clearing  ]  Node_name [clrnode   ]
           Database_vendor [oracle    ]  Database_name [istoracle       ]
             Database_user [cpro_app       ]
         Database_password [********        ]
            Confirm_db_pwd [********        ]
               Schema_name [cpro_app       ]
              Owner_dbuser [cpro_own       ]
          Owner_dbpassword [********        ]
  Owner_dbpassword_confirm [********        ]
         Database_tns_name [istoracle                   ]
                Tablespace [                    ]
          Index_tablespace [                    ]
           Clob_tablespace [                    ]
            Institution_id [1          ]
                 Inst_type [MAIN_INST            ]
                 Inst_name [PADSS TEST INSTITUTION        ]
            Inst_curr_code [840  ]  System_cntry_code [840  ]
       Protected_directory [/users/product-india/clrqa02/clrser/ENC1/server ]
       Protected_directory [/apps/clearing/ENC
Export_import_pan_in_clear [y ]
```

```
        Xml_service_host [10.74.145.84                  ]
        Xml_service_port [5031 ]  Xml_service_tls_port [5032 ]
         Xml_enable_auth [n  ]  Xml_enable_ent [n  ]
          Xml_enable_tls [n  ]  Xml_use_tls [n  ]
          Guiserver_port [5000 ]  Nodeagt_msg_port [5001 ]
       Nodeagt_ctrl_port [5002 ]  Nodeagt_msg_timeout [25000   ]
     Nodeagt_otracelevel [INFO      ]
Nodeagt_root_trace_level [WARNING   ]  Nodeagt_use_tls [y ]
   Nodeagt_keystore_pass [*******         ]
 Nodeagt_confirm_ks_pass [*******         ]
Nodeagt_key_manager_pass [*******         ]
 Nodeagt_confirm_km_pass [*******         ]
 Nodeagt_truststore_pass [*******         ]
 Nodeagt_confirm_ts_pass [                ]
Nodeagt_need_client_auth [y ]
```

Parameter	Description
Product_name	The ID of the product that is to be configured. It is used to specify the server application to install. For a Clearing node set this to "CLEARING".
Node_name	The node to which the instance belongs to.
Database_vendor	The database vendor type: • For Oracle enter: oracle • For DB2 enter: db2
Database_name	The database connection name: For Oracle this is a Service name or a SID. For DB2 this is the instance name.
Database_user	The name of the database APP service account (e,g. CLapp) that will be used to run the Clearing application. For a product defined in Product_name this value is stored in the dbm.dbuserid parameter in istparam.cfg when option 0 Apply System Parameters is executed.
Database_password	The Database_user's password (i.e.the CLapp's password. The password is not displayed when entered and is encrypted before storage in the istparam.cfg dbm.dbpassword parameter.
Confirm_db_pwd	The database user's password re-entered for confirmation. It must be the same as the Database_password. You cannot proceed until a matching password is entered.
Schema_name	The name of the owner service APP account (schema) . This field is required and must be set as follows: For Oracle set this the same as Database_user. The service APP account (i.e. CLapp schema) For DB2 set this to the service APP schema. The schema name must be in uppercase. During table creation the schema will be created if it does not exist.

Owner_dbuser	The name of the database owner service account (e,g. CLown) that will be used to run the Clearing application. For a product defined in Product_name this value is stored in the dbm.dbuserid parameter in istparam.cfg when option 0 Apply System Parameters is executed.
Owner_dbpassword	The owner database user's password (i.e. the CLown's password. The password is not displayed when entered and is encrypted before storage in the istparam.cfg dbm.dbpassword parameter.
Owner_dbpassword_confirm	The owner database user's password re-entered for confirmation. It must be the same as the Owner_dbpassword. You cannot proceed until a matching password is entered.
Database_tns_name	This field is required and must be set as follows: For Oracle this is the TNS name entry configured in tnsnames.ora for the database For DB2 set this to the database name in Database_name
Tablespace	Identifies the name of the table space. If none is provided, the default value is used.
Index_tablespace	Identifies the name of the table space used for indexes. If none is provided, the default value is used. This is not used for DB2.
Clob_tablespace	The name of the table space to use for CLOB fields. This iis provided as an option to be uded for the audit table, IST_AUDIT, which has a number of CLOB fields.
Institution_id	The institution ID to be created when generating initial data. The first institution must be "1". Institution IDs 01 through 09 are reserved IDs and should not be used during installation.
Inst_type	The institution type. For example: MAIN_INST — Main institution. In general there should only be one institution of this type. There is currently no restriction when assigning the type, so multiple institutions can co-exist with the same type. MEMBER — A member institution.
Inst_name	The institution's name.
Inst_curr_code	The institution's three digit ISO currency code. ***Example:*** 978 Euro, 840 US Dollars.
System_cntry_code	The three digit ISO country code to be used as the system default country. This code is used to determine the currency and date patterns used in the GUI application
Protected_directory	The permanent directory where files containing sensitive data are located. This directory will have the following subdirectories created in it:

cfg	The permanent directory where configuration parameter files required by the node will be stored. A soft link will be established as follows: ln -s <Protected_directory>/cfg $OSITE_ROOT/cfg
certdata	The permanent directory where war files, keystores and installation configuration parameter files will be stored. A soft link will be established as follows: ln -s <Protected_directory>/certdata $OSITE_ROOT/certdata
data	The permanent directory where data imported/exported by an application can be stored. A soft link will be established as follows: ln -s <Protected_directory>/data $OSITE_ROOT/data
files	The permanent directory where communications configuration files are stored. A soft link will be established as follows: ln -s <Protected_directory>/files $ISTDIR/files
log	The permanent directory where debug files generated by the system will be stored. A soft link will be established as follows: ln -s <Protected_directory>/log $OPRODUCT_ROOT/log $

To retain the system default, leave this empty.

Export_import_pan_in_clear	Not applicable for clearing.
Xml_service_host	The hostname where the Apache server is to be installed (i.e. the current host). The Apache server is included as part of the release.
Xml_service_port	The port on which the XML API server will listen for http requests. This port must be a port on the host specified in Xml_service_host and must not used by any other process.
Xml_service_TLS_port	The port on which the XML API server will listen for https requests. This port must be a port on the host specified in Xml_service_host and must not used by any other process. It must be different than the port specified in Xml_service_TLS_port.
Xml_enable_auth	Indicates whether or not to enable Authentication for XML API requests. When enabled the user name and password provided in requests messages are authenticated via the Authentication

	server. The user must therefore be setup by the GUI application administrator and assigned a password.
	y = enable Authentication.
	n = disable Authentication.

Xml_enable_ent	Indicates whether or not to enable Entitlement for XML API requests.

Xml_enable_TLS	Indicates whether or not TLS is to be enforced for all requests. When enabled the XML API server expects all requests to be made via HTTPS. See the Apache documentation for information on setting up the server with an TLS certificate.
	y = enable TLS.
	n = disable TLS

Xml_use_TLS	
Guiserver_port	The TCP/IP port where IST/Clearing listens for GUI clients requests. This port should not be used by any other process. It is used to set the port in, gui.host local host port, and stored in *$OPRODUCT_ROOT/cfg/istparam.cfg* in the system being installed. After initial installation gui.host can be updated using the Configuration Service GUI application if necessary.
Nodeagt_msg_port	The server port where the Node Agent listens for requests. ***Example:*** nodeagt.msg_port 9992.
Nodeagt_ctrl_port	The server port where the Node Agent listens for control commands. ***Example:*** nodeagt.ctrl_port 9993.
Nodeagt_msg_timeout	The time in milliseconds the Node Agent will wait on an response from a backend process. The default is 25000 milliseconds.
Nodeagt_otracelevel	The Node Agent trace level. ERROR — Log error messages only FATAL — Log fatal messages only WARN — Log warning messages only INFO — Log Information messages only DEBUG — Log all messages The default is INFO.
Nodeagt_root_trace_level	The Node Agent root trace level ERROR — Log error messages only FATAL — Log fatal messages only WARN — Log warning messages only INFO — Log Information messages only

	DEBUG — Log all messages The default is WARN.
Nodeagt_use_TLS	Indicates whether or not to enable TLS communication when starting the “istnodeagt”.administrative process.
Nodeagt_keystore_pass	Specifies the value of the key-store password to be used in istnodeagt.
Nodeagt_confirm_ks_pass	The Nodeagt_keystore_pass re-entered for confirmation. You cannot proceed until a matching password is entered.
Nodeagt_key_manager_pass	Specifies the password for the key manager file.
Nodeagt_confirm_km_pass	The istnodeagt key manager_pass re-entered for confirmation. You cannot proceed until a matching password is entered.
Nodeagt_confirm_km_pass	The istnodeagt key manager_pass re-entered for confirmation. You cannot proceed until a matching password is entered.
Nodeagt_truststore_pass	Specifies the value of the trust-store password to be used in istnodeagt.
Nodeagt_need_client_auth	Specifies whether or not server authentication is required. y (Yes, Default) or n (No).

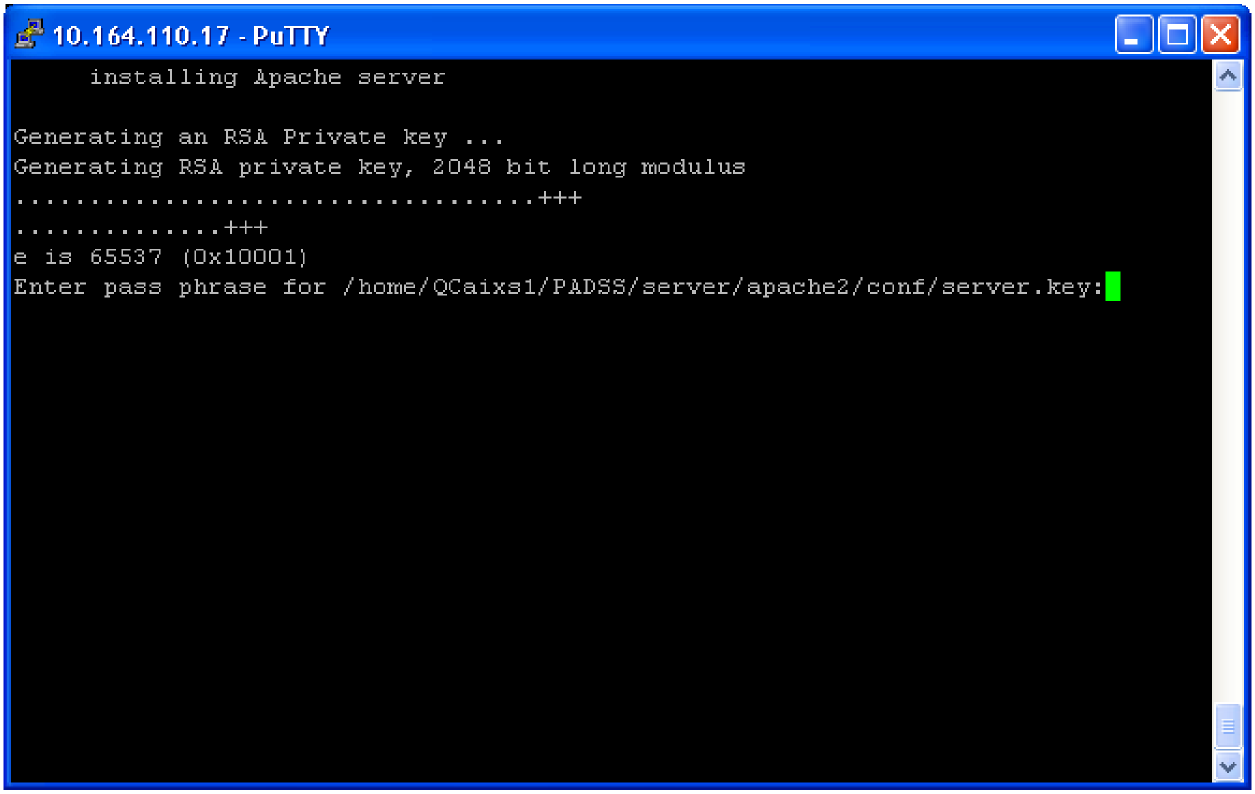
3a. Press Esc twice to go to main menu and then Select 1. Apply System Parameters

This option is used to initialize the system configuration files istparam.cfg and istnodeagt.cfg.

Istparam.cfg is created if one does not yet exist and the parameters dbm.dbuserid and dbm.dbpassword are updated with the database user and password respectively.

```
Are you sure you want to apply the system parameters? (y/n)
```

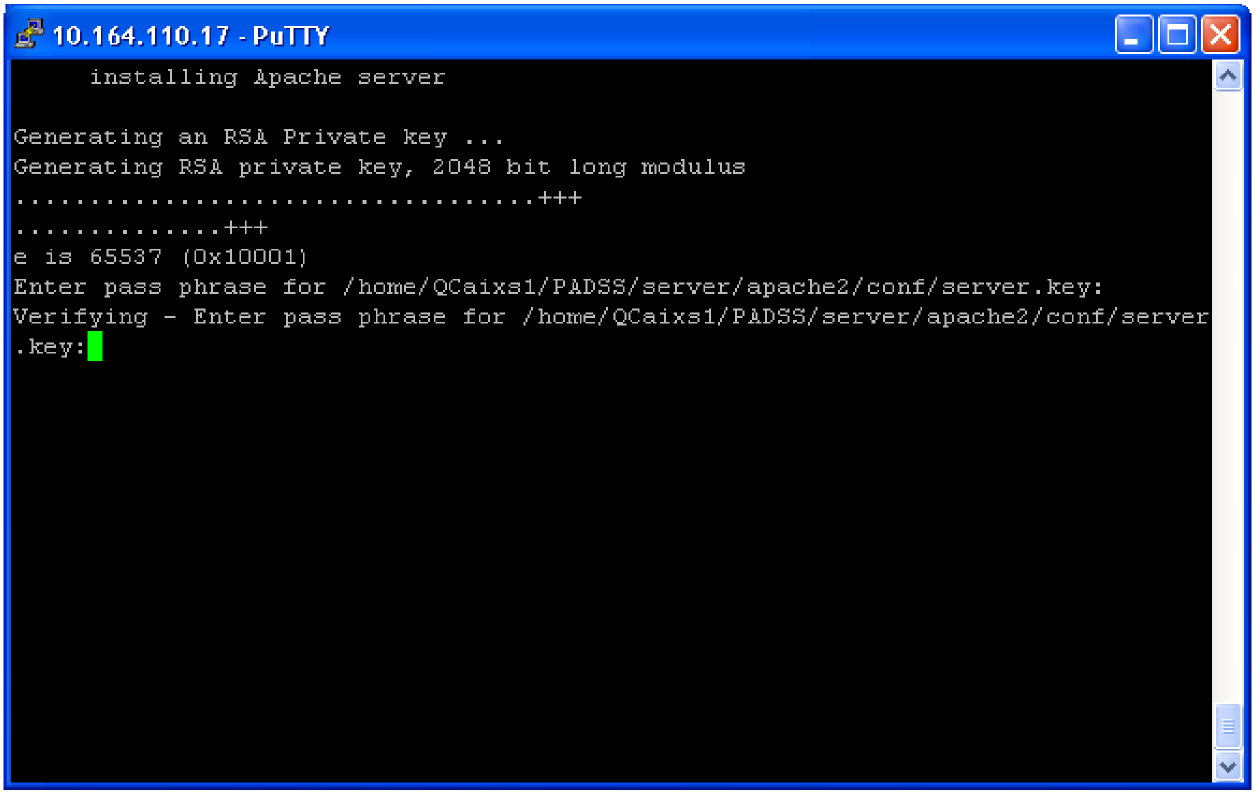
The Apache HTTP server is also configured at this point if the apache tgz is shipped along with the release.



```
     installing Apache server

Generating an RSA Private key ...
Generating RSA private key, 2048 bit long modulus
..................................+++
..............+++
e is 65537 (0x10001)
Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:
```

Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:

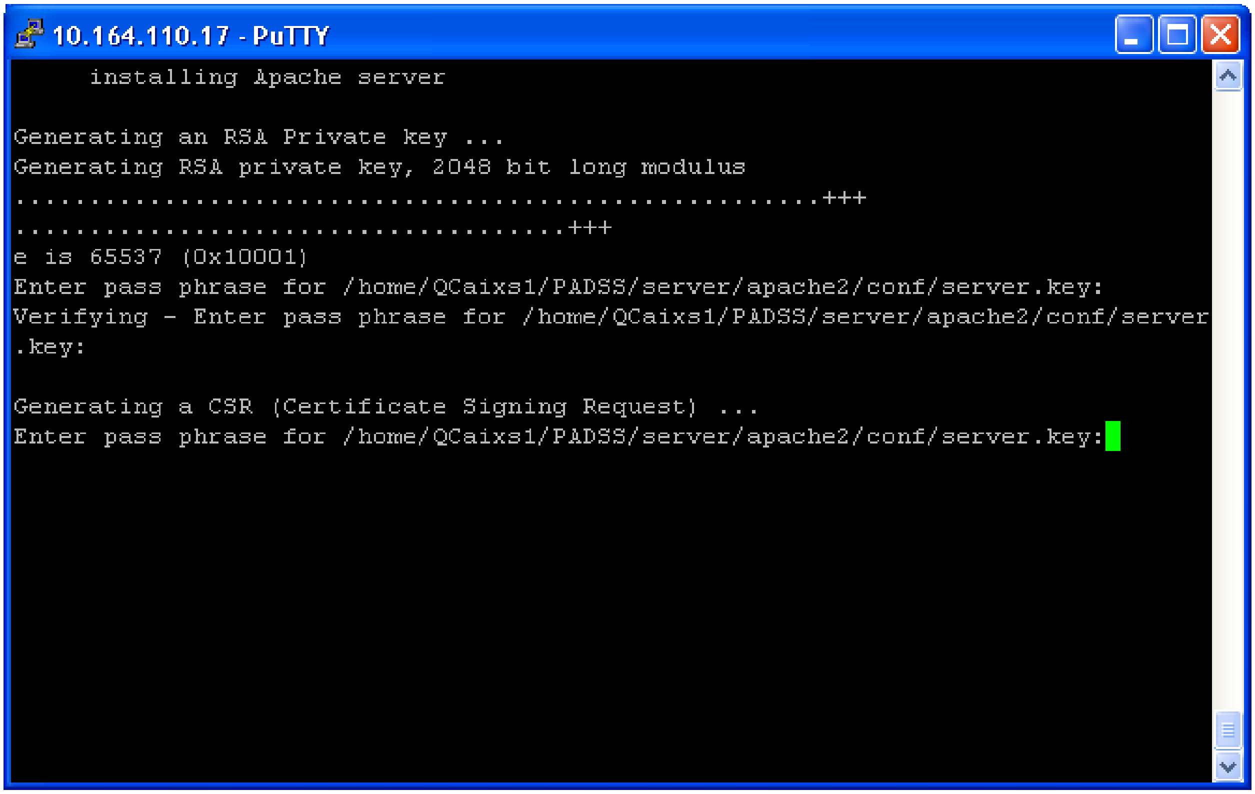
Give the passphrase key here and press enter.



```
     installing Apache server

Generating an RSA Private key ...
Generating RSA private key, 2048 bit long modulus
..................................+++
..............+++
e is 65537 (0x10001)
Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:
Verifying - Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server
.key:
```

Verifying - Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:

Confirm the Passphrase key which is entered in the previous screen. both should match.

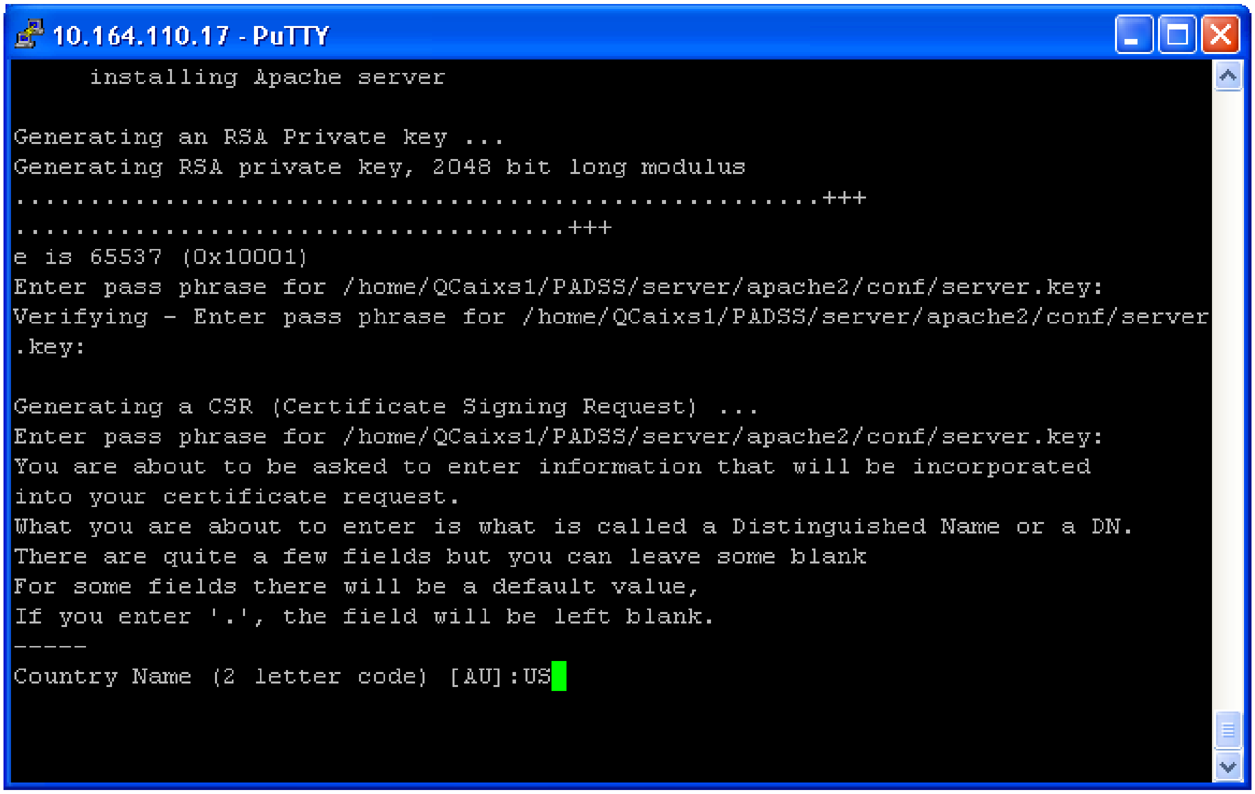


```
     installing Apache server

Generating an RSA Private key ...
Generating RSA private key, 2048 bit long modulus
.....................................................+++
....................................+++
e is 65537 (0x10001)
Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:
Verifying - Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server
.key:

Generating a CSR (Certificate Signing Request) ...
Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:
```

Generating a CSR (Certificate Signing Request) ...

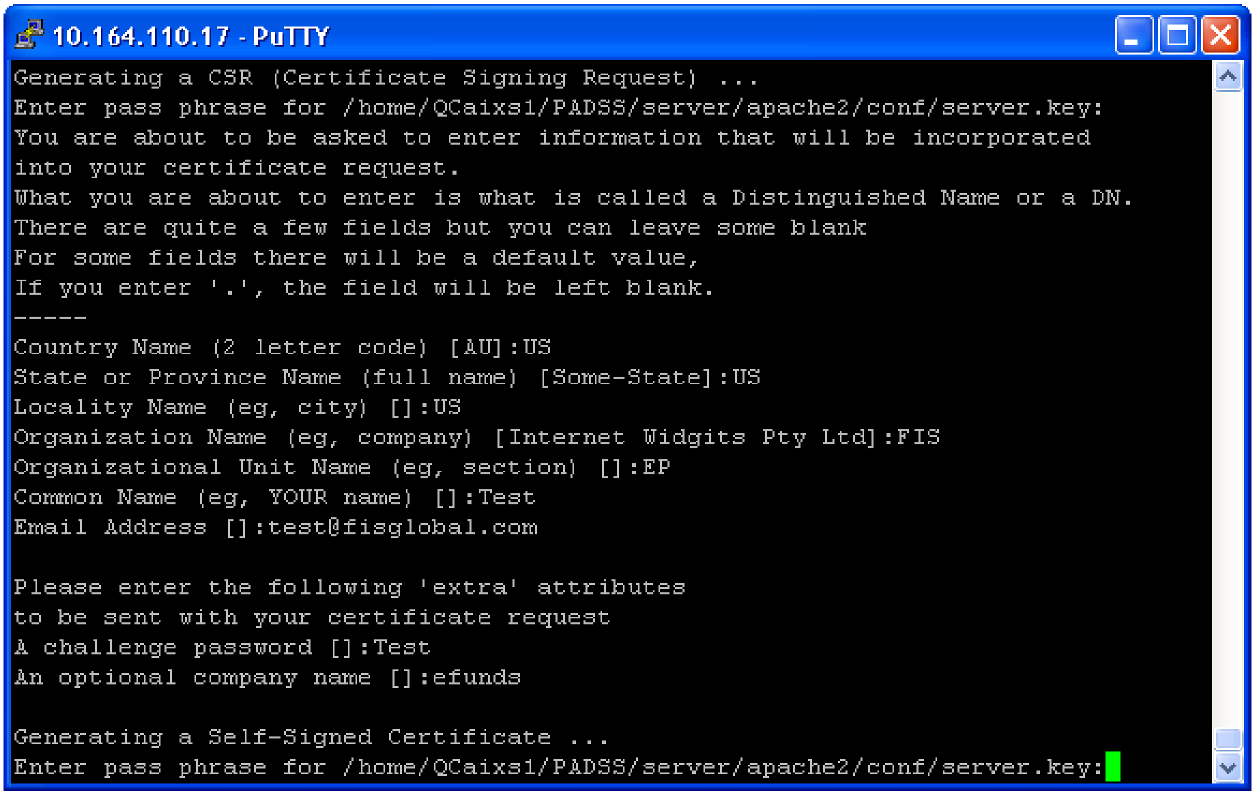
Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:

Give the same passphrase key which you already used in the previous screens.



```
     installing Apache server

Generating an RSA Private key ...
Generating RSA private key, 2048 bit long modulus
.....................................................+++
..................................+++
e is 65537 (0x10001)
Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:
Verifying - Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server
.key:

Generating a CSR (Certificate Signing Request) ...
Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
```

Country Name (2 letter code) [AU]:



```
Generating a CSR (Certificate Signing Request) ...
Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:US
Locality Name (eg, city) []:US
Organization Name (eg, company) [Internet Widgits Pty Ltd]:FIS
Organizational Unit Name (eg, section) []:EP
Common Name (eg, YOUR name) []:Test
Email Address []:test@fisglobal.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Test
An optional company name []:efunds

Generating a Self-Signed Certificate ...
Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:
```

Country Name (2 letter code) [AU]: *Enter the two letter country code here and press enter.*

State or Province Name (full name) [Some-State]: *Enter the state or province and press enter.*

Locality Name (eg, city) []: Enter city and press enter.

Organization Name (eg, company) [Internet Widgits Pty Ltd]: *Enter the company name and press enter(eg:FIS)*

Organizational Unit Name (eg, section) []: *Team name(Eg:EMEA)*

Common Name (eg, YOUR name) []: *Any common name(Eg: Test)*

Email Address []: *Any valid email (test@fisglobal.com)*

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password []:

An optional company name []:

Generating a Self-Signed Certificate ...

Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:

If the database tables are not yet created execute steps 3b through 3f. Otherwise go to step 3g.

3b. Select 2. Prepare DB Scripts

This option is used to prepare database scripts used to create the product tables and initial system records.

For initial installation select the Create Option:

```
Proceed with Prepare DB Script? (y/n)> y
```

Scripts are generated for application to the CLown service account entered in `Owner_dbuser`.

3c. Select 3. Create DB Tables

This option is used to apply the database table creation scripts generated in option 2. Alternatively the scripts can be applied by a DBA. The scripts and order to be applied are stored in $OSITE_ROOT/dbutil/dba

```
Are you sure you want to create/append Product DB
tables? (y/n) y
```

The table creation scripts are applied to the service account entered in `Owner_dbuser`

3d. Select 4. Create DB Grant

This option is used to grant privileges to the CLapp_role and CL_read_only_role.

```
        Are you sure you want to create DB Grant (y/n) y
```

3e. Select 5. Insert DB System Records

This option is used to insert initial system data into the product database. These records are non-institution specific.

```
        Are you sure you want to insert DB records? (y/n) y
```

3f. Select 6. Insert DB Inst Base Records

This option is used to insert initial institution data into the product database.

These records are institution specific and are inserted for the institution specified in the Global System Parameters.

```
        Are you sure you want to insert DB records? (y/n) y
```

3g. Press Esc twice to return to the Server Installation menu.

4. Select option 1. Install Entitlement

This option is used to create authentication and entitlement database tables configure the runtime parameters required by the administrative processes, oassrv and oentrsv. The submenu below is displayed.

```
IST Installation Utility v1.214
Product Directory: /users/product-india/clrqa02/clrser/pdir20160704
Install Entitlement
                  +-------------------------------------+
                  | 0. Setup System Parameters          |
                  | 1. Apply System Parameters          |
                  | 2. Prepare DB Scripts               |
                  | 3. Create DB Tables                 |
                  | 4. Create DB Grant                  |
                  | 5. Insert DB System Records         |
                  | 6. Apply DB Tables Upgrade Script   |
                  | 7. Apply DB Records Upgrade Script  |
                  +-------------------------------------+
```

Option	Description
Apply System Parameters	Setup the runtime configuration parameters.
Prepare DB Scripts	Prepares the SQL scripts required to create the product database tables and initial records.
Create DB Tables	Apply the table creation scripts prepared in option 2

Create DB Grant	Grants permission to roles in the CLown service account when Method A is used for the DB standard. Otherwise not applicable.
Insert DB System Records	Insert system records generated in option 2. For example the set of currency codes.
Apply DB Tables Upgrade Script	Display a list of table upgrade scripts and selectively apply each. Scripts are to be applied only if instructed to do so via the release notes.
Apply DB Records Upgrade	Display a list of data upgrade scripts and selectively apply each. Scripts are to be applied only if instructed to do so via the release notes.

4a. Select 0. Setup System Parameters

This option is used to specify the database and runtime parameters for the authentication and entitlement processes. The parameters are shown below.

```
_ENT_VARIABLES
   Product Directory: /users/product-india/clrqa02/clrser/pdir20160704

               Ent_database_vendor [oracle    ]
                 Ent_database_name [istoracle      ]
                 Ent_database_user [cent_app       ]
             Ent_database_password [********         ]
                Ent_confirm_db_pwd [********         ]
                   Ent_schema_name [cent_app       ]
                  Ent_owner_dbuser [cent_own       ]
              Ent_owner_dbpassword [********         ]
      Ent_owner_dbpassword_confirm [********         ]
             Ent_database_tns_name [istoracle                    ]
                          Ent_port [5005 ]  Ent_use_tls [y ]
             Ent_authenticate_peer [n ]
                     Security_host [10.74.145.84                  ]
                         Auth_port [5006 ]
                 Auth_control_host [10.74.145.84                  ]
                 Auth_control_port [5007 ]  Auth_encoding_transition [y ]
           Auth_min_password_length [8 ]  Auth_password_no_numeric_suffix [n ]
   Auth_password_no_numeric_prefix [n ]  Auth_password_no_repeated_chars [y ]
          Auth_password_no_user_id [y ]  Auth_password_history_depth [10 ]
                      Auth_use_tls [y ]  Auth_authenticate_peer [n ]
```

Parameter	Description
Ent_database_vendor	The database vendor type: For Oracle enter:"oracle" For DB2 enter: "db2"
Ent_database_name	The database connection name: For Oracle this is a Service name or a SID. For DB2 this is the instance name.

Ent_database_user	The name of the database APP service account (e,g. clentapp) that will be used to run the authentication and entitlement application processes. This value is used to update the oassrv and oent parameters in istparam.cfg when option 0 Apply System Parameters is executed.
Ent_database_password	The Database_service (clentapp) user's password. The password is not displayed when entered and is encrypted before it is stored in the istparam.cfg parameters: • oassrv.dbpassword • oent.dbpassword
Ent_confirm_db_pwd	The Ent database password re-entered for confirmation. You cannot proceed until a matching password is entered.
Ent_schema_name	The name of the database schema. This field is required and must be set as follows: • For Oracle set this the same as Ent_database_user. • For DB2 set this to the Ent service account schema name (clentapp). The schema name must be in uppercase. During table creation the schema will be created if it does not exist.
Ent_owner_dbuser	The name of the database APP service account (e.g. clentown) that will be used to run the authentication and entitlement application processes. This value is used to update the oassrv and oent parameters in istparam.cfg when option 0 Apply System Parameters is executed.
Ent_owner_dbpassword	The Database_service (clentown) user's password. The password is not displayed when entered and is encrypted before it is stored in the istparam.cfg parameters: • oassrv.dbpassword • oent.dbpassword
Ent_owner_dbpassword_confirm	The Ent database password re-entered for confirmation. You cannot proceed until a matching password is entered.
Ent_database_tns_name	This field is required and must be set as follows: • For Oracle this is the TNS name entry configured in tnsnames.ora for the database • For DB2 set this to the database name in Database_name This value is used to update initial database parameters in istparam.cfg parameters.
Ent_port	The TCP/IP port number on which Entitlement process listens for connections.
Ent_use_TLS	Specifies whether to not TLS is enabled for incoming requests. Set this to "y".
Ent_authenticate_peer	Indicates whether or not to authenticate the TLS certificates for requests. Applicable only if TLS is enabled. y — authenticate peer. Set this to "y"
Security_host	The hostname or IP address where the Authentication and Entitlement processes will run.

Auth_port	The TCP/IP port number on which Authentication process listens for connections. This is the port used by clients, requiring authentication service, to connect to the Authentication server.
Auth_control_host	The hostname or IP address of the host used to control the authentication server.
Auth_control_port	The TCP/IP port number on which authentication process listens for control requests. User control is not administered via this port but is required for the authentication process to initialize.
Auth_encoding_transition	Indicates whether or not to accept MD5 encrypted passwords. y = accept MD5 encrypted passwords. n = do not accept MD5 encrypted passwords. When “Auth_encoding_transition” is set to “y” users with MD5 encrypted passwords will be authenticated until their password expires. On changing their passwords the new encryption algorithm will be enforced. For an initial (fresh) installation you must set this indicator to “y” otherwise you will not be able login with the initial admin password. After changing the admin’s password this value can be set to “n’.
Auth_min_password_length	The minimum length of a user’s password. Must be 8 or greater.
Auth_password_no_numeric_suffix	Whether digits are prohibited at the beginning of the password y — digits are prohibited at the beginning of the password
Auth_password_no_numeric_prefix	Whether digits are prohibited at the end of the password y — digits are prohibited at the end of the password.
Auth_password_no_repeated_chars	Whether repeated consecutive characters are prohibited. y — repeated consecutive characters are prohibited
Auth_password_no_user_id	Whether the inclusion of the user name in the password is prohibited. y — inclusion of the user name in the password is prohibited.
Auth_password_history_depth	The number of previous passwords to check for duplicates. The default is 10.
Auth_use_TLS	Specifies whether to not TLS is to be enabled on startup for incoming requests. Set this to “y”
Auth_authenticate_peer	Indicates whether or not to authenticate the TLS certificates for requests. Applicable only if TLS is enabled. y — authenticate peer. Set this to “y”

4a. Select 1. Apply System Parameters

This option is used to configure the initial system parameters for the administrative processes, oassrv and oentsrv in istparam.cfg. oassrv and oentsrv are required to access to the system via the GUI application. The parameters can be updated using the Configuration Service screens.

```
Are you sure you want to apply the system parameters? (y/n) y
```

If the database tables are not yet created execute steps 4b through 4e. Otherwise go to step 4f.

4b. Select 2. Prepare DB Scripts

This option is used to prepare database scripts used to create the authentication and entitlement tables and initial system records.

```
Proceed with Prepare DB Script? (y/n)> y
```

Scripts are generated for application to the clentown service account entered `Ent_database_user`.

4c. Select 3. Create DB Tables

This option is used to apply the database table creation scripts generated by option 2. Alternatively the scripts can be applied by a DBA. The scripts and order to be applied are stored in $OSITE_ROOT/dbutil/dba.

```
Are you sure you want to create/append Entitlement DB
tables? (y/n) y
```

Scripts are applied to the clentown service account entered `Ent_database_user`.

4d. Select 4. Create DB Grant

This option is used to grant privileges to the clentapp_role and CL_read_only_role.

```
Are you sure you want to create DB Grant (y/n) y
```

4e. Select 5. Insert DB System Records

This option is used to execute the admin user initialization process, and to insert initial system data into the entitlement database. These records are non-institution specific.

The init admin pwd process is executed first followed by the script to insert initial data:

```
Please wait for the prompts, and then specify the username and initial password
Enter user name:rator


Enter Password


Verify password
```

4f. Press Esc twice to return to the Server Installation menu.

5. Select 2. Install Tokenizer

   This option is used to create tokenizer database tables and configure the runtime parameters required by the tokenization processes, tokenizer. The submenu below is displayed.

```
IST Installation Utility v1.214
Product Directory: /users/product-india/clrqa02/clrser/pdir20160704 (2
Install Tokenizer
                  +-------------------------------------+
                  | 0. Setup System Parameters          |
                  | 1. Apply System Parameters          |
                  | 2. Prepare DB Scripts               |
                  | 3. Create DB Tables                 |
                  | 4. Create DB Grant                  |
                  | 5. Insert DB System Records         |
                  | 6. Apply DB Tables Upgrade Script   |
                  | 7. Apply DB Records Upgrade Script  |
                  +-------------------------------------+
```

Option	Description
Apply System Parameters	Setup the runtime configuration parameters.
Prepare DB Scripts	Prepares the SQL scripts required to create the product database tables and initial records.
Create DB Tables	Apply the table creation scripts prepared in option 2
Create DB Grant	Grants permission to roles in the CLown service account when Method A is used for the DB standard. Otherwise not applicable.
Insert DB System Records	Insert system records generated in option 2. For example the set of currency codes.
Apply DB Tables Upgrade Script	Display a list of table upgrade scripts and selectively apply each. Scripts are to be applied only if instructed to do so via the release notes.
Apply DB Records Upgrade	Display a list of data upgrade scripts and selectively apply each. Scripts are to be applied only if instructed to do so via the release notes.

```
_TOK_VARIABLES
   Product Directory: /users/product-india/clrqa02/clrser/pdir20160704

                Start_tokenizer [y ]  Tok_database_vendor [oracle    ]
              Tok_database_name [istoracle      ]
              Tok_database_user [ctok_app       ]
          Tok_database_password [********        ]
             Tok_confirm_db_pwd [********        ]
                Tok_schema_name [ctok_app       ]
               Tok_owner_dbuser [ctok_own       ]
           Tok_owner_dbpassword [********        ]
   Tok_owner_dbpassword_confirm [********        ]
          Tok_database_tns_name [istoracle                                         ]
               Tok_idle_timeout [120   ]  Tok_sess_timeout [3600  ]
                    Tok_timeout [0     ]  Tok_max_client [100   ]
                 Tok_standalone [n     ]  Tok_use_tls [y ]
                Tok_server_mbox [TOKEN                                             ]
                       Tok_host [10.74.145.84                  ]
                       Tok_port [5027 ]
           Tok_server_cert_file [                                                  ]
        Tok_server_key_pwd_file [                                                  ]
            Tok_server_key_file [                                                  ]
               Tok_ca_cert_file [                                                  ]
                Tok_otracelevel [error          ]  Tok_comm_debug [0 ]
```

Table 1: Tokenizer System Parameters - Field Definition

Parameter	Description
Start_tokenizer	The database vendor type: For Oracle enter:"oracle" For DB2 enter: "db2"
Tok_database_vendor	The database connection name: For Oracle this is a Service name or a SID. For DB2 this is the instance name.
Tok_database_name	The name of the database APP service account (e,g. cltokapp) that will be used to run the authentication and entitlement application processes. This value is used to update the oassrv and oent parameters in istparam.cfg when option 0 Apply System Parameters is executed.
Tok_database_user	The name of the database APP service account (e,g. cltokapp) that will be used to run the tokenizer application process. • This value is used to update the tokenizer parameters in istparam.cfg when option 1 Apply System Parameters is executed.
Tok_database_password	The Database_user's password. The password is not displayed.
Tok_confirm_db_pwd	The Tok database password re-entered for confirmation. You cannot proceed until a matching password is entered.
Tok_schema_name	The name of the database schema. This field is required and must be set as follows: • For Oracle set this the same as Ent_database_user. • For DB2 set this to the TOK service account schema name (cltokapp). The schema name must be in uppercase. During table creation the schema will be created if it does not exist.
Tok_owner_dbuser	The name of the database APP service account (e,g. cltokown) that will be used to run the tokenizer application process. • This value is used to update the tokenizer parameters in istparam.cfg when option 1 Apply System Parameters is executed.
Tok_owner_dbpassword	The Database_user's password. The password is not displayed.

Tok_owner_dbpassword_confirm	The Tok database password re-entered for confirmation. You cannot proceed until a matching password is entered.
Tok_database_tns_name	This field is required and must be set as follows: • For Oracle this is the TNS name entry configured in tnsnames.ora for the database • For DB2 set this to the database name in Database_name This value is used to update initial database parameters in istparam.cfg parameters.
Tok_idle_timeout	Tokenizer terminate client if connection has been idle for this length of time
Tok_session_timeout	Tokenizer terminate client if connection has been created for this length of time
Tok_timeout	Number of seconds to wait for the tokenizer response
Tok_maxlclient	Max no of concurrent clients
Tok_standalone	if it is standalone or non-standalone
Tok_use_TLS	To use tls or not
Tok_server_mbox	The tokenization server mailbox name. default — TOKEN
Tok_host	The hostname or IP address of the host where the Tokenizer process will run
Tok_port	The port the tokenizer listens on for requests. Default 7531.
Tok_server_cert_file	This field is required are only used when TLS is turned on, and only for the standalone tokenizer.
Tok_server_key_pwd_file	This field is required are only used when TLS is turned on, and only for the standalone tokenizer.
Tok_server_key_file	This field is required are only used when TLS is turned on, and only for the standalone tokenizer.
Tok_ca_cert_file	This field is required are only used when TLS is turned on, and only for the standalone tokenizer.
Tok_otracelevel	The trace level to be set: • FATAL • LOG • ERROR • WARNING • INFO • DUMP • DEBUG
Tok_comm_debug	To turn on debug.

5a. Select 1. Apply System Parameters

This option is used to configure the system parameters for the tokenization process, tokenizer, in istparam.cfg.

```
Are you sure you want to apply the system parameters? (y/n) y
```

If the database tables are not yet created execute steps 5b through 5e. Otherwise go to step 5f.

5b. Select 2. Prepare DB Scripts

Select this option to prepare database scripts used to create the product tables and initial system records.

For initial installation select the Append Option:

```
Proceed with Prepare DB Script? (y/n)> y
```

Scripts are generated for application to the cltokown service account entered `Tokown_dbuser.`

5c. Select 3. Create DB Tables

This option is used to apply the database table creation scripts generated by option 2. Alternatively the scripts can be applied by a DBA. The scripts and order to be applied are stored in $OSITE_ROOT/dbutil/dba.

```
Are you sure you want to create/append Tokenizer DB
tables? (y/n) y
```

Scripts are applied to the cltokown service account entered in `Tokown_dbuser.`

5d. Select 4. Create DB Grant

This option is used to grant privileges to the cltokapp_role and cltok_read_only_role.

```
Are you sure you want to create DB Grant (y/n) y
```

5e. select 5. Insert DB System Records

This option is used to initialize the token and insert initial system data into the tokenization table. These records are non-institution specific.

The init_token process is executed. If you run it again, and the first record is there (like for example with an existing system), it would leave it alone, and just insert the second one. I the second one was in place, it would leave it alone. Also, the second one is the salt for sha2

5f. Press Esc twice to return to the Server Installation menu.

6. Key Lifecycle Manager

This option is used to create the key lifecycle manager database tables and configure the runtime parameters. The submenu below is displayed:

```
 IST Installation Utility v1.214
Product Directory: /users/product-india/clrqa02/clrser/pdir20160704 (2
Install Key Life Cycle
            +-------------------------------------+
            | 0. Setup System Parameters          |
            | 1. Apply System Parameters          |
            | 2. Prepare DB Scripts               |
            | 3. Create DB Tables                 |
            | 4. Create DB Grant                  |
            | 5. Insert DB System Records         |
            | 6. Apply DB Tables Upgrade Script   |
            | 7. Apply DB Records Upgrade Script  |
            +-------------------------------------+
```

Option	Description
Apply System Parameters	Setup the runtime configuration parameters.
Prepare DB Scripts	Prepares the SQL scripts required to create the product database tables and initial records.
Create DB Tables	Apply the table creation scripts prepared in option 2
Create DB Grant	Grants permission to roles in the CLown service account when Method A is used for the DB standard. Otherwise not applicable.
Insert DB System Records	Insert system records generated in option 3. For example the set of currency codes.
Apply DB Tables Upgrade Script	Display a list of table upgrade scripts and selectively apply each. Scripts are to be applied only if instructed to do so via the release notes.
Apply DB Records Upgrade	Display a list of data upgrade scripts and selectively apply each. Scripts are to be applied only if instructed to do so via the release notes.

6a. Select 0. Setup System Parameters

This option is used to specify the runtime parameters for the authentication and entitlement processes. The parameters are shown below:

```
_KLC_VARIABLES
   Product Directory: /users/product-india/clrqa02/clrser/pdir20160704 (2

            Klc_database_vendor [oracle    ]
              Klc_database_name [istoracle      ]
              Klc_database_user [cklc_app       ]
          Klc_database_password [********        ]
             Klc_confirm_db_pwd [********        ]
                Klc_schema_name [cklc_app       ]
               Klc_owner_dbuser [cklc_own       ]
           Klc_owner_dbpassword [********        ]
   Klc_owner_dbpassword_confirm [********        ]
          Klc_database_tns_name [istoracle                   ]
                Klc_otracelevel [error          ]
```

Table 2: Key Lifecycle System Setup Parameters - Field Definition

Parameter	Description
Klc_database_vendor	The database connection name: For Oracle this is a Service name or a SID. For DB2 this is the instance name.
Klc_database_name	The name of the database APP service account (e,g. clklcapp) that will be used to run the authentication and entitlement application processes.
Klc_database_user	The name of the database APP service account (e,g. clklcapp) that will be used to run the tokenizer application process. This value is used to update the tokenizer parameters in istparam.cfg when option 1 Apply System Parameters is executed.
Klc_database_password	The Database_user's password. The password is not displayed.
Klc_confirm_db_pwd	The KLC database password re-entered for confirmation. You cannot proceed until a matching password is entered.
Klc_schema_name	The name of the database schema. This field is required and must be set as follows: For Oracle set this the same as Ent_database_user. For DB2 set this to the KLC service account schema name (clklcapp). The schema name must be in uppercase. During table creation the schema will be created if it does not exist.
Klc_owner_dbuser	The name of the database OWNER service account (e,g. clklcown) where the Clearing database objects reside.
Klc_owner_dbpassword	The KLC owner's password.
Klc_owner_dbpassword _confirm	The KLC owner database password re-entered for confirmation. You cannot proceed until a matching password is entered.
Klc_database_tns_name	This field is required and must be set as follows: • For Oracle this is the TNS name entry configured in tnsnames.ora for the database • For DB2 set this to the database name in Database_name This value is used to update initial database parameters in istparam.cfg parameters.

Klc_otracelevel	The trace level to be set: • FATAL • LOG • ERROR • WARNING • INFO • DUMP • DEBUG

6b. Select 1. Apply System Parameters

This option is used to configure the system parameters for the key lifecycle manager process, in istparam.cfg.

```
Are you sure you want to apply the system parameters? (y/n) y
```

If the database tables are not yet created execute steps 6c through 6f. Otherwise go to step 6g.

6c. Select 2. Prepare DB Scripts

Select this option to prepare database scripts used to create the product tables and initial system records.

```
Proceed with Prepare DB Script? (y/n)> y
```

Scripts are generated for application to the clklcown service account entered in `Klcown_dbuser.`

6d. Select 3. Create DB Tables

This option is used to apply the database table creation scripts generated by option 2. Alternatively the scripts can be applied by a DBA. The scripts and order to be applied are stored in $OSITE_ROOT/dbutil/dba.

```
Are you sure you want to create/append Key Life Cycle DB
tables? (y/n) y
```

Scripts are applied to the clklcown service account entered in `Klcown_dbuser.`

6e. Select 4. Create DB Grant

This option is used to grant privileges to the clklcapp_role and clklcapp_read_only_role.

```
Are you sure you want to create DB Grant (y/n) y
```

6f. Select 7. Insert DB System Records

This option is used to insert initial system data into the key lifecycle manager database.

```
Are you sure you want to insert DB records? (y/n) y
```

6g. Press Esc twice to return to the Server Installation menu.

Enabling TLS for the IST Process

The default installation enables TLS by generating self-signed certificates for each process that requires. Two options are provided on the pdeploy menu as shown below.

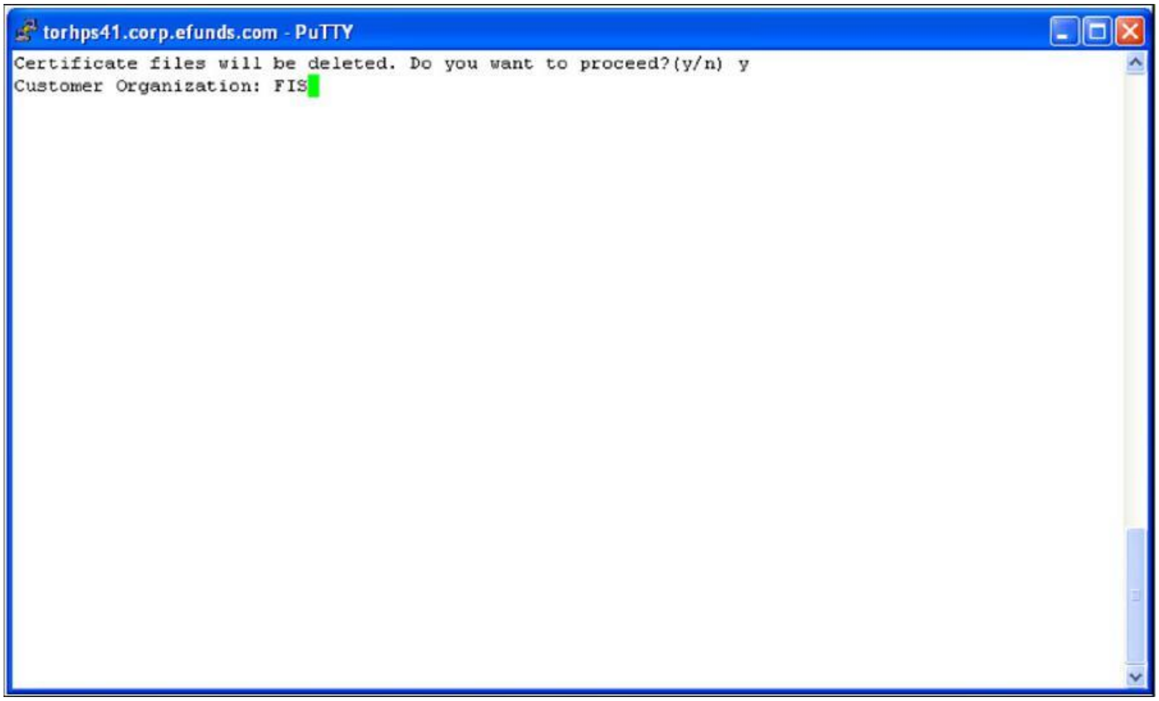
```
IST Installation Utility v1.145
Product Directory: /apps/clearing/pdir20170628 (240)

Enable TLS
                +----------------------------------------+
                | 0. Generate and Export APP Certificates|
                | 1. Import Certificates for APP         |
                +----------------------------------------+
```

The following describes the steps to create a set of self-signed certificates to enable TLS. Repeat this procedure for all nodes.

Refer to section Enabling TLS on page 75, for an overview of TLS within IST.

Generate Node Certificates

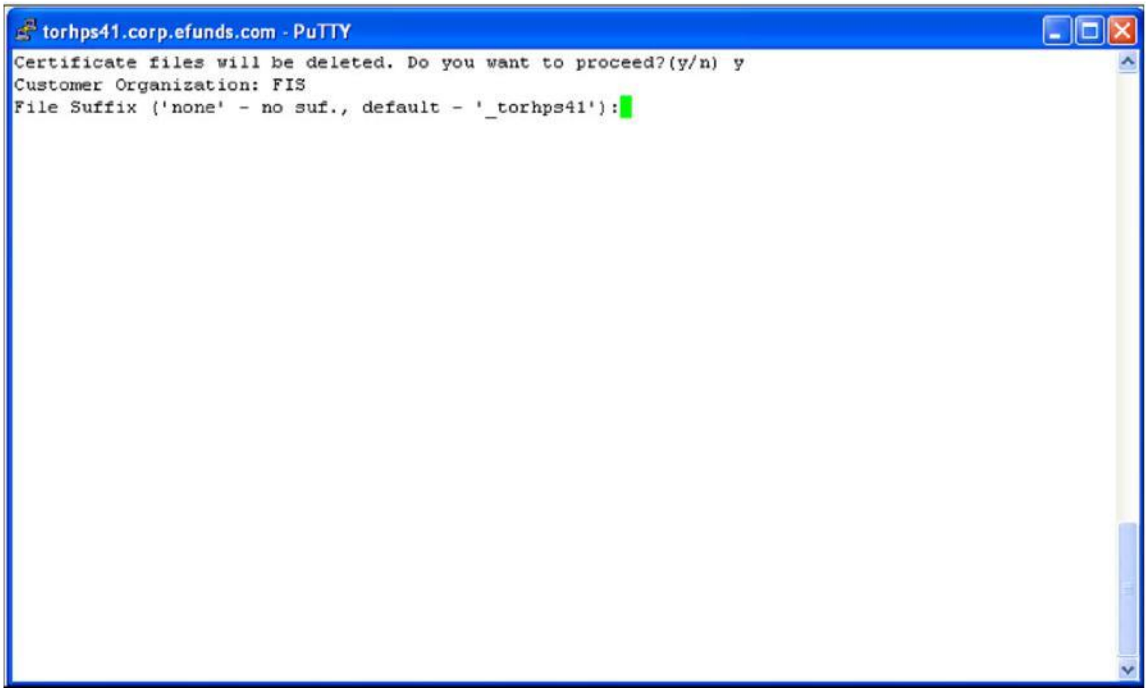
1. Login as the Clearing server admin user and run pdeploy.
2. Select **Enable TLS**.
3. Select **Generate and Export App Certificates** to generate the Clearing application certificates.



```
Certificate files will be deleted. Do you want to proceed?(y/n) y
Customer Organization: FIS
```

Figure 10: Generate

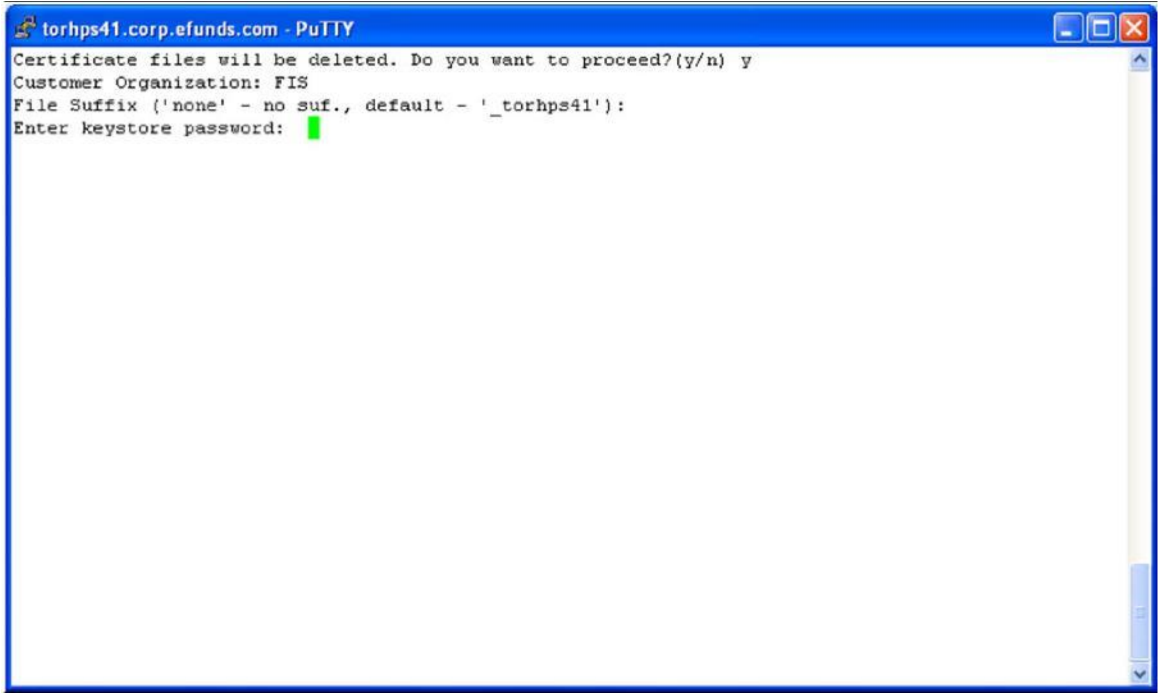
4. Enter the **organization name** (i.e your_company_name) to include in the certificates.



```
Certificate files will be deleted. Do you want to proceed?(y/n) y
Customer Organization: FIS
File Suffix ('none' - no suf., default - '_torhps41'):
```

Figure 11: Organization Name

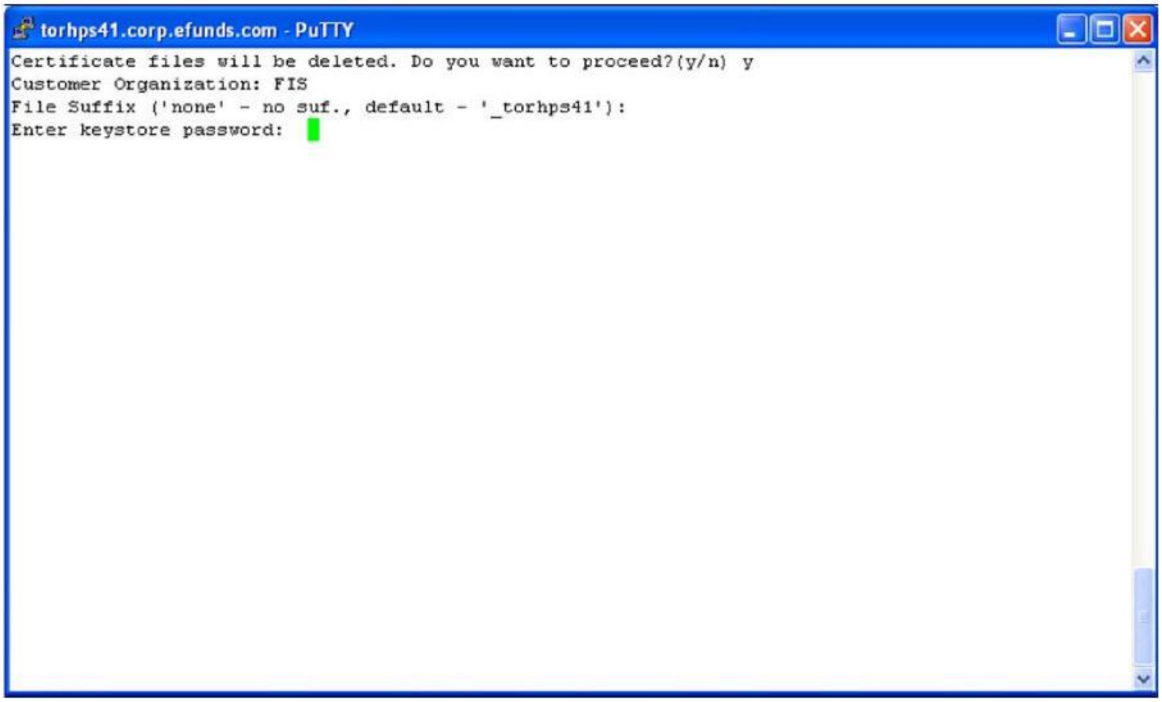
5. Specify the suffix use in the files created. This is used to identify files for the host. Enter none and press enter, or press enter accept the default, or enter an identifier to be used instead of the default.



```
Certificate files will be deleted. Do you want to proceed?(y/n) y
Customer Organization: FIS
File Suffix ('none' - no suf., default - '_torhps41'):
Enter keystore password:
```

Figure 12: File Suffix

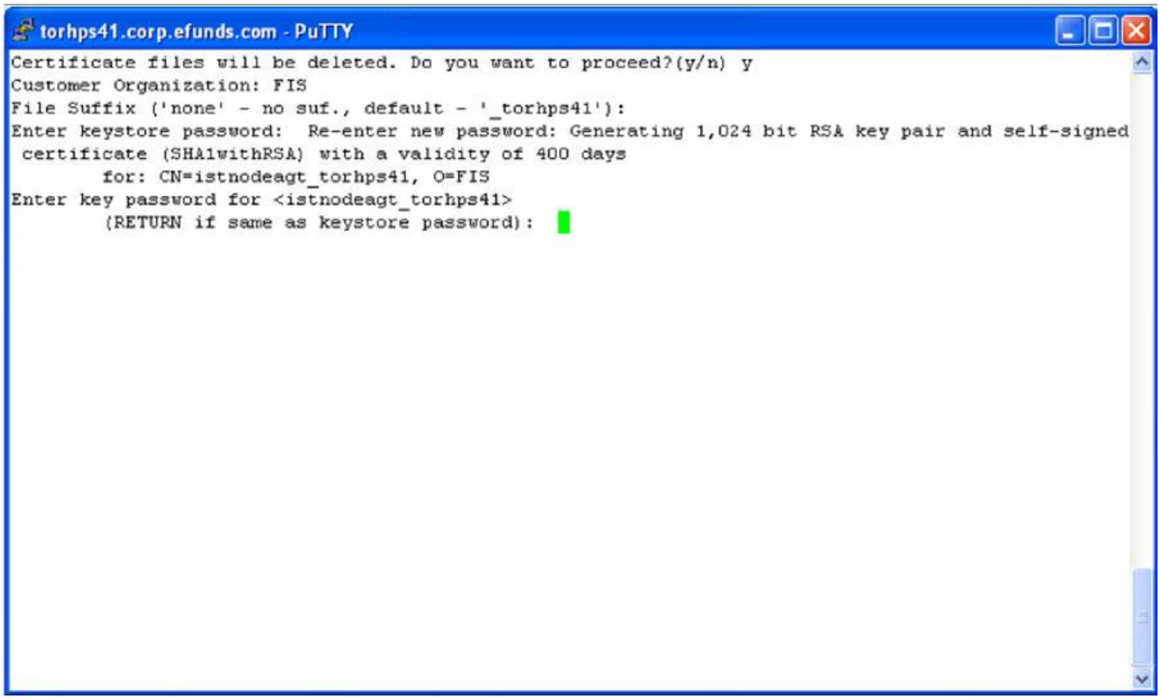
6. Enter the **keystore password**. This is the password you used for the TLS_key_manager password.



```
Certificate files will be deleted. Do you want to proceed?(y/n) y
Customer Organization: FIS
File Suffix ('none' - no suf., default - '_torhps41'):
Enter keystore password:
```

Figure 13: Keystore Password (a)

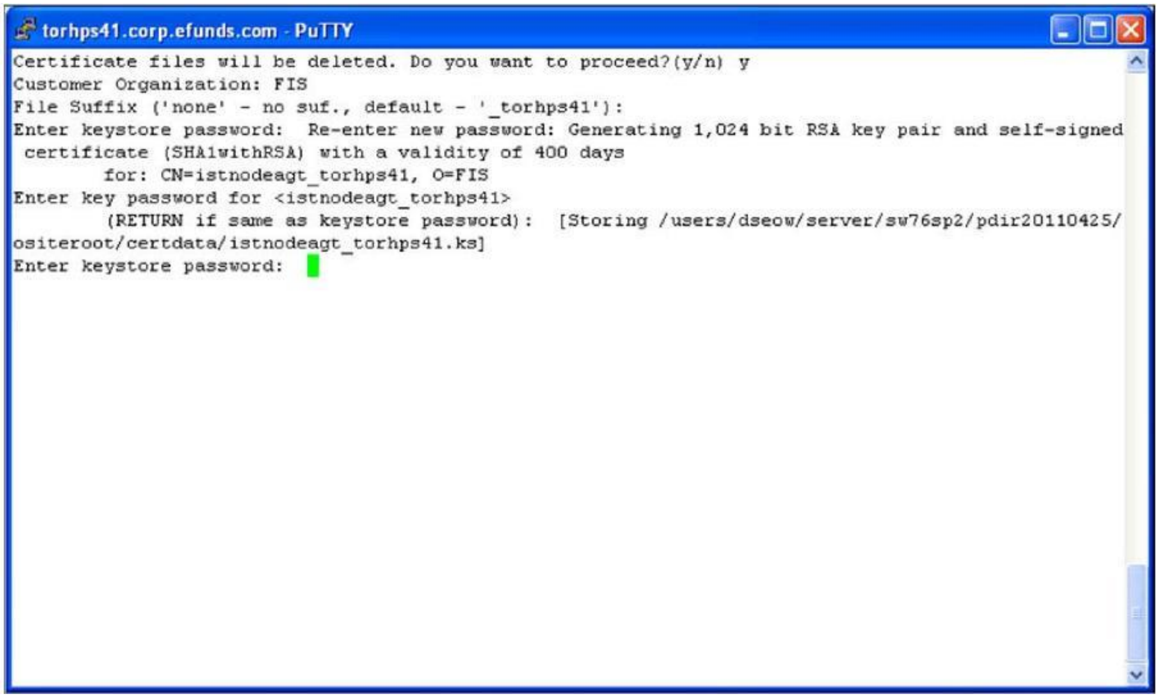
7. Reenter the **keystore password** to confirm.



```
Certificate files will be deleted. Do you want to proceed?(y/n) y
Customer Organization: FIS
File Suffix ('none' - no suf., default - '_torhps41'):
Enter keystore password:  Re-enter new password: Generating 1,024 bit RSA key pair and self-signed
 certificate (SHA1withRSA) with a validity of 400 days
        for: CN=istnodeagt_torhps41, O=FIS
Enter key password for <istnodeagt_torhps41>
        (RETURN if same as keystore password):
```

Figure 14: Keystore Password Confirmation

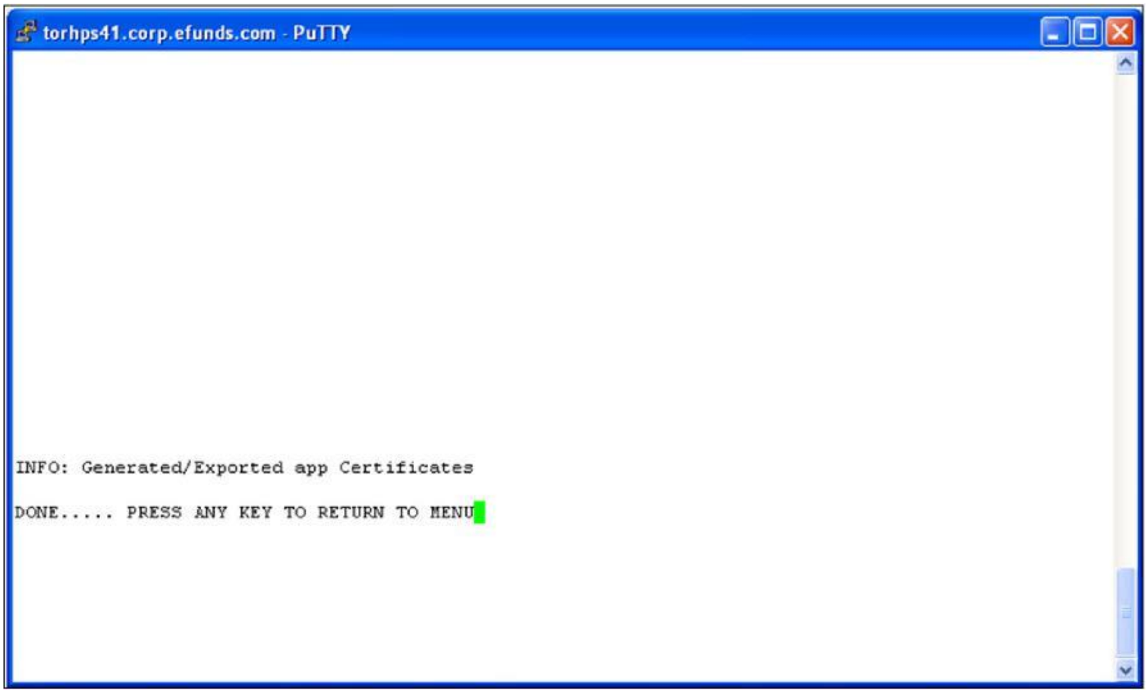
8. Press return without entering a password to use the same password as the keystore password entered before.



```
Certificate files will be deleted. Do you want to proceed?(y/n) y
Customer Organization: FIS
File Suffix ('none' - no suf., default - '_torhps41'):
Enter keystore password:  Re-enter new password: Generating 1,024 bit RSA key pair and self-signed
 certificate (SHA1withRSA) with a validity of 400 days
        for: CN=istnodeagt_torhps41, O=FIS
Enter key password for <istnodeagt_torhps41>
        (RETURN if same as keystore password):  [Storing /users/dseow/server/sw76sp2/pdir20110425/
ositeroot/certdata/istnodeagt_torhps41.ks]
Enter keystore password:
```

Figure 15: Keystore Password (b)

9. Enter the **keystore password** from step 6.



```
INFO: Generated/Exported app Certificates

DONE..... PRESS ANY KEY TO RETURN TO MENU
```

Figure 16: Keystore Password (c)

10. Assuming the suffix used in step file is "_torhps41", the following files are created for each of the administrative processes.

File	Contents
ftpclient.pem	TLS certificate of the FTPS client
ftpclient_ca.pem	FTPS client's truststore
ftpclient_key.pem	Private key corresponding to ftpclient.pem
ftpcmd.pem, ftpcmd_torhps41.pem	TLS certificate of the FTPCMD. If suffix is used both files are created.
ftpcmd_ca.pem	FTPCMD trustore.
ftpcmd_key.pem	Private key corresponding to FTPCMD
ftpsrv.pem, ftpsrv_torhps41.pem	TLS certificate of the file server. If suffix is used both files are created.
ftpsrv_ca.pem	File server's truststore
ftpsrv_key.pem	Private key corresponding to ftpsrv.pem
istnodeagt.ks	The IST node agent process's trust-store.

istnodeagt.pem, istnodeagt_torhps41.pem	The certificate to be shared with the IST node agent process's clients. This certificate file is to be imported into the GUI application's trust-store (istfrm_trust.ks). If suffix is used both files are created.
	The truststore used by the istnodeagt administrative process.
istxmlrpc.pem, istxmlrpc_torhps41.pem	The certificate to be shared with the authentication and entitlement processes. It will be imported into the authentication's and entitlement's respective trust-stores (oassrv_ca.pem and oentsrv_ca.pem).
istxmlrpc_ca.pem	The xmlapi's trust-store.
istxmlrpc_key.pem	The xmlapi's key-store.
oascmd_ca.pem	The authentication command processor's trust-store.
oascmd_key.pem	The authentication command processor's key-store.
oascmd.pem	The certificate to be shared with the authentication command processor's service provider. It will be imported into the authentication process's trust-store
oassrv_ca.pem	The authentication process's trust-store.
oassrv_key.pem	The authentication process's key-store.
oassrv.pem, oassrv_torhps41.pem	The certificate to be shared with the authentication process's clients. This certificate file is to be imported into the GUI application's trust-store (istfrm_trust.ks). If suffix is used both files are created
oentsrv_ca.pem,	The entitlement process's trust-store
oentsrv_key.pem	The entitlement process's key-store.
oentsrv.pem, oentsrv_torhps41.pem	The certificate to be shared with the entitlement process's clients. This certificate file is to be imported into the GUI application's trust-store (istfrm_trust.ks). If suffix is used both files are created.

11. Copy istnodeagt_torhps41.pem, oassrv_torhps41.pem, and oentsrv_torhps41.pem to the GUI application's certdata directory.

Import Certificates

Before executing this step generate the GUI application certificates as described in the respective GUI installation guide and copy istfrm.pem to $OSITE_ROOT/certdata.

GUI Application Back-end TLS

1. Copy the GUI application certificate. Istfrm. exported in section Export Certificate from Keystore to $OSITE_ROOT/certdata.
2. Select Import Certificates to import the GUI applications certificate into the nodes truststore:
    a) Ensure the files above were transferred and copied to $OSITE_ROOT/ certdata.
    b) Run pdeploy and select Enable TLS.

    Select Import Certificates and enter “y” to proceed.

```
Importing from remote-node:[] to local-node:[default]
Enter keystore password:
Re-enter new password:
Owner: CN=IST-GUI
Issuer: CN=IST-GUI
Serial number: 5af8b56d
Valid from: Fri Jul 01 14:05:41 IST 2016 until: Sat Aug 05 14:05:41 IST 2017
Certificate fingerprints:
         MD5:  C4:4C:44:EB:14:5A:0B:57:08:28:47:23:5D:A1:57:5E
         SHA1: 37:E1:B0:AA:91:03:E5:89:5B:BB:F5:49:7E:4C:63:AB:5C:9E:D3:00
         SHA256:
93:B4:A0:F0:26:12:47:C2:C2:22:65:F6:76:4F:12:9E:4A:46:57:17:39:A6:A2:BD:54:04:3B:7
D:E9:E0:5E:25
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 01 A4 44 4A 2E 22 C6 B3   64 C7 E8 73 AE A3 83 4A  ..DJ."..d..s...J
0010: B3 9F E6 5F                                        ..._
]
]

Trust this certificate? [no]:  Certificate was added to keystore
```

Figure 17: Import Certificate

Setup the Runtime Environments

Each time you install a new release or patch a new profile<install date> corresponding to the new product environment is created. To use the new environment you must execute the profile<install date>.

To apply the profile<install date>, edit the "**.profile**" and replace the **profile<yyyymmdd>** entry with the new profile<install date> created. Re-login to execute the "**.profile**" and apply the newly installed server environment described by profile<install date>.

The profile you run depends on which installed product release is to be executed. You should keep a record of each installation for tracking purposes. This provides a simple method to rollback to a previous release.

For example:

If the current release is incorrect, simply login as the admin user, update the ".profile" with the profile<install date> corresponding to the previously working release, execute it, and bring the system up. Refer to "Back-out a Server Upgrade" on page 62 for further information on backing out a release.

NOTE:	After setting up the runtime environment you must start the administrative processes istnodeagt, and oassrv and oentsrv in the foundation instance where Authentication and Entitlement requests are to be made. Istnodeagt must be started in a Clearing node after TLS. This is required since the Configuration Service XML files will be retrieved from that node and stored in the Protected_directory.
	For information on using the Configuration Service refer to the user documentation.

For more information on starting these processes, refer to "Start the Administration Processes"

Applying Upgrade Scripts

New releases and patch releases may require updates to the database. Upgrades to the database are supplied as a set of scripts. Scripts are to be applied only if instructed to do so in the release notes provided with the release.

Table Upgrade Scripts

From the respective submenu select option **Apply DB Tables Upgrade Script** to apply scripts to upgrade the database tables.

```
Are you sure you want to apply DB upgrade script
udm_cl_22150001_22160001.ora to cpro_app@istoracle? (y/n)
```

Files are located in $OPRODUCT_ROOT/sql/ named as follows:

udm_<prod>_<ver>_<patch>_<seq>. <db>

where:

<prod> - the product module

- "cl" the clearing identifier
- "en" the entitlement identifier
- "tk" the tokenizer identifier
- "kl" the key lifecycle manager identifier

<ver> - subsystem release version

<patch> - patch within the release version

<seq> -script sequence with the release

<db> - database type: ora = oracle, db2 = DB2

Examples:

Clearing upgrade script:- udm_cl_2400007_1.ora

Ent upgrade script:- udm_en_7700901_1.ora

Scripts are applied according to the database parameters setup in System Parameters for each install option.

Database Record Scripts

From the respective submenu select option **Apply DB Records Upgrade Script** to apply scripts to upgrade the database records. Scripts are to be applied only if instructed to do so in the release notes. If instructed to do so, highlight the script to be applied and press **Enter**.

```
Are you sure you want to apply DB upgrade script
data_cl_2401002_2401003.orato cl_own@istoracle? (y/n)
```

Files are located in $OPRODUCT_ROOT/sql/ named with format:

data_<prod>_<ver>_<patch>_<seq>.<db>

where:

<prod> - the product module

- "cl" the Clearing identifier
- "en" the entitlement identifier
- "tk" the tokenizer identifier
- "kl" the key lifecycle manager identifier

<ver> - subsystem release version

<patch> - patch within the release version

<seq> -script sequence with the release

<db> - database type: ora = oracle, db2 = DB2

Example:

```
data_cl_2401002_2401003.ora
```

Scripts are applied according to the database parameters setup in System Parameters.

Back-out an Upgrade

This section describes how to back-out an update and revert to a previous release.

The profile you run depends on which installed product release is to be executed. You should keep a record of each installation for tracking purposes. This provides a simple method to rollback to a previous release. For example: if the current release is incorrect, simply:

- Login as the admin user
- Update the ".profile" with the profile<install_date> corresponding to the previously working release
- Bring the system down
- Re-login to execute the update ".profile" to setup the environment
- Bring the system up.

For each release a new pdir<install_date> directory will be created and a history should be maintained as in the example in table Sample Installation Record.

Sample Installation Record

Install #	Directory	Profile	Comments
1	pdir20170309	profile20170309	First production
2	pdir20170529	profile 20170529	Service pack 2
3	pdir20170529_1	profile 20170529_1	First install of 2 above. Can be discarded later.

Each installation above will have an entry in build_env.log. This information will help your support team to determine the set of files installed and hence the equivalent version.

For example: If pdir20170430 is the running environment and the previous version is pdir20170309,

to revert to the previous release:

1. Login as the admin user.
2. Remove the link to profile20170430:

   ```
   rm profile
   ```

3. Add a link to the previous profile<date>

   ```
   ln –s profile20170329 profile
   ```

4. Bring down the node.

5. Re-login to execute the updated profile to make "profile20170329" take effect.
6. Bring up the node to initialize the previous release.

Install the GUI Application

This section describes the installation of the GUI release file and the steps to deploy the application in the web server. The standard way to deploy the GUI application is through the use of an application WAR file. The guiadmin user will extract the WAR file from the release and provide it to the web server administrator for deployment.

The web server administrator will then deploy the WAR file as per the web server procedure.

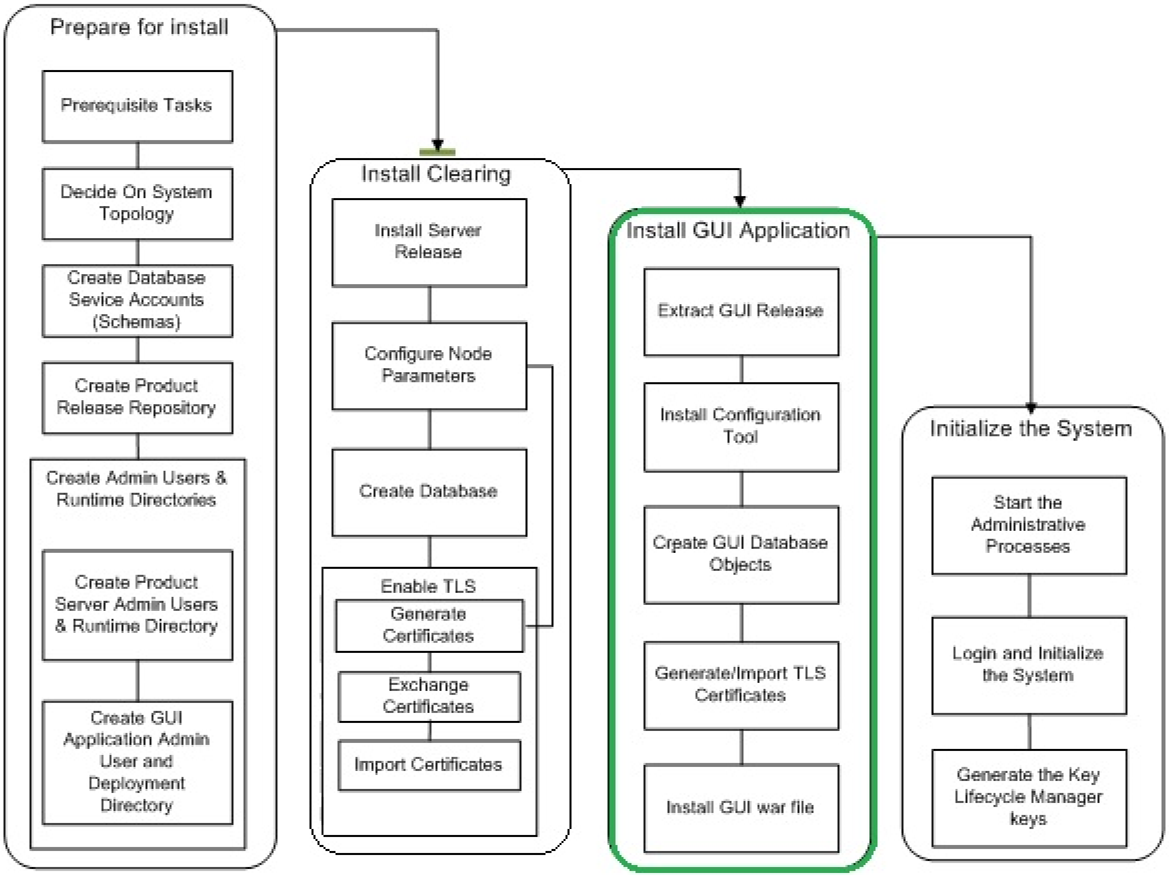

Prepare for install
Prerequisite Tasks
Decide On System Topology
Create Database Sevice Accounts (Schemas)
Create Product Release Repository
Create Admin Users & Runtime Directories
Create Product Server Admin Users & Runtime Directory
Create GUI Application Admin User and Deployment Directory
Install Clearing
Install Server Release
Configure Node Parameters
Create Database
Enable TLS
Generate Certificates
Exchange Certificates
Import Certificates
Install GUI Application
Extract GUI Release
Install Configuration Tool
Create GUI Database Objects
Generate/Import TLS Certificates
Install GUI war file
Initialize the System
Start the Administrative Processes
Login and Initialize the System
Generate the Key Lifecycle Manager keys

Figure 18: Install GUI Application

Extract the Contents of the Release File

The release contains several files:

- A war and ear file containing the GUI application to be installed by the web server administrator.
- Property files used by the application.
- SQL scripts used to create records used by application.
- Library files.

The contents of the validated rcc need to be extracted before the GUI application can be installed and deployed.

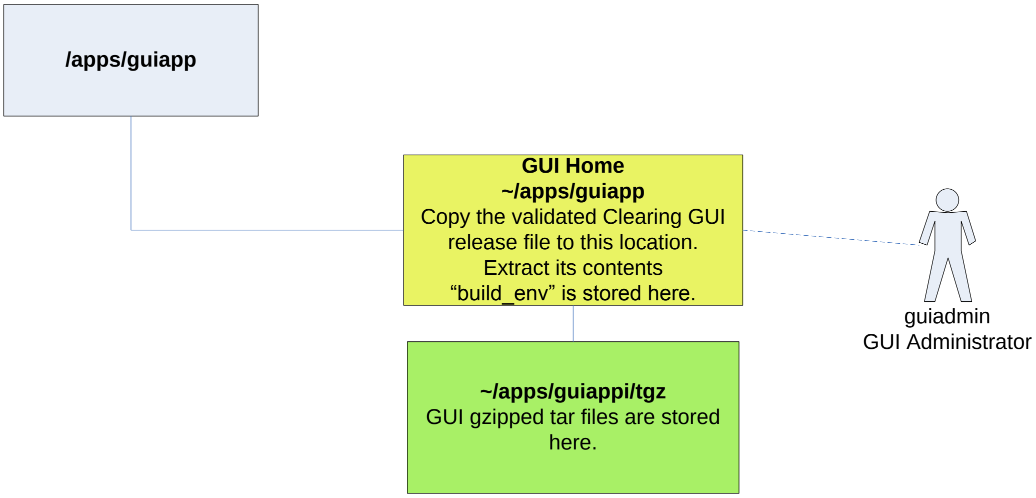

/apps/guiapp
GUI Home
~/apps/guiapp
Copy the validated Clearing GUI release file to this location.
Extract its contents
“build_env” is stored here.
~/apps/guiappi/tgz
GUI gzipped tar files are stored here.
guiadmin
GUI Administrator

Figure 19: Directory Structure for Staging GUI Releases

The staging area is in the shared filesystem and is mounted in the web server host as well so that the web server admin user has access to the ear (or war) and libraries required for installation:

0. Create the directory where the GUI application files are to be extracted. For example:

   /apps/guiapp

1. Create a guiadmin user and give read and write permissions to the directory created in step 1.
2. Edit the guiadmin user's ".profile" and add entries as described in “.profile" Entries” .

   Set /apps/guiapp as the HOME environment variable and ensure there is a path to $HOME/tgz.

   a) export HOME=/apps/guiapp

   b) export PATH=$HOME/tgz: $PATH

3. Login as the GUI administrator user.
4. Change directory to $HOME. "/apps/guiapp" in the example.
5. Copy the decrypted file(s) obtained from the FISValidate procedure to the home directory, $HOME.
6. Extract the contents:

   ```
   gzip -dc <decrypted_rcc_file> | tar -xvf -
   ```

   Example:

   ```
   gzip -dc CLC_2.4.0.10.03_ LIN-2632-I686-64_201706280000001.tar.gz |tar -xvf -
   ```

   The files in the release gzipped tar files are extracted to $HOME/tgz.

Build GUI Application Installation Environment

The following steps are used to install the GUI application files extracted above and deploy it to the web server:

1. Login as the guiadmin user. This should take you to the home directory where the GUI files will be installed, /apps/guiapp.. Otherwise check that the HOME environment variable is correctly set.
2. Run "build_env" to install the files stored on $HOME/tgz:

```
build_env
```

The files are stored as illustrated in Figure 2.

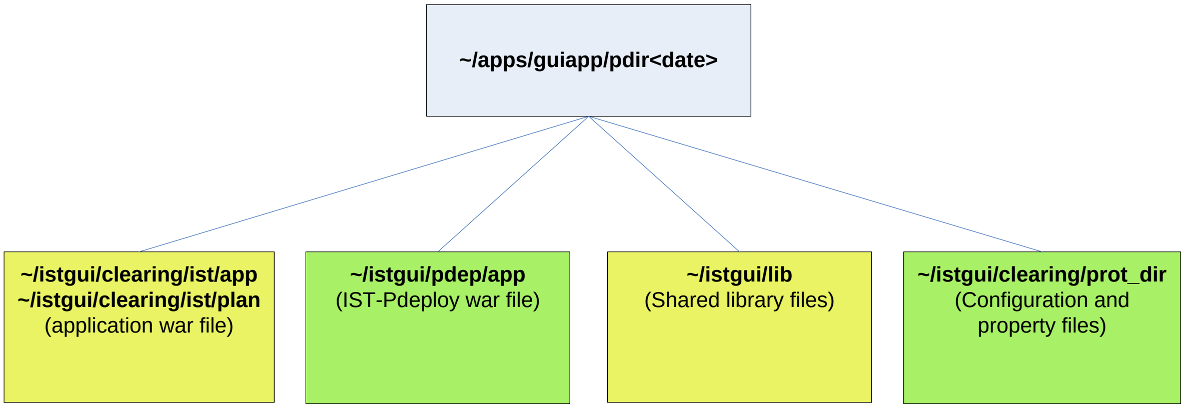


Figure 20: IST-GUI Application Directory

In some cases incremental upgrades may have been done to the OS. In such cases the OS need to be specified on the installation command line.

For example: A release may have been built on for IBM AIX 6.1.2 whereas the OS on the target system is AIX 6.1.3. Since the upgrade is backward compatible the AIX 6.1.2 release may be installed with the command:

```
build_env -os=AIX-612
```

Contact support to clarify any doubts as to the compatibility of the release.

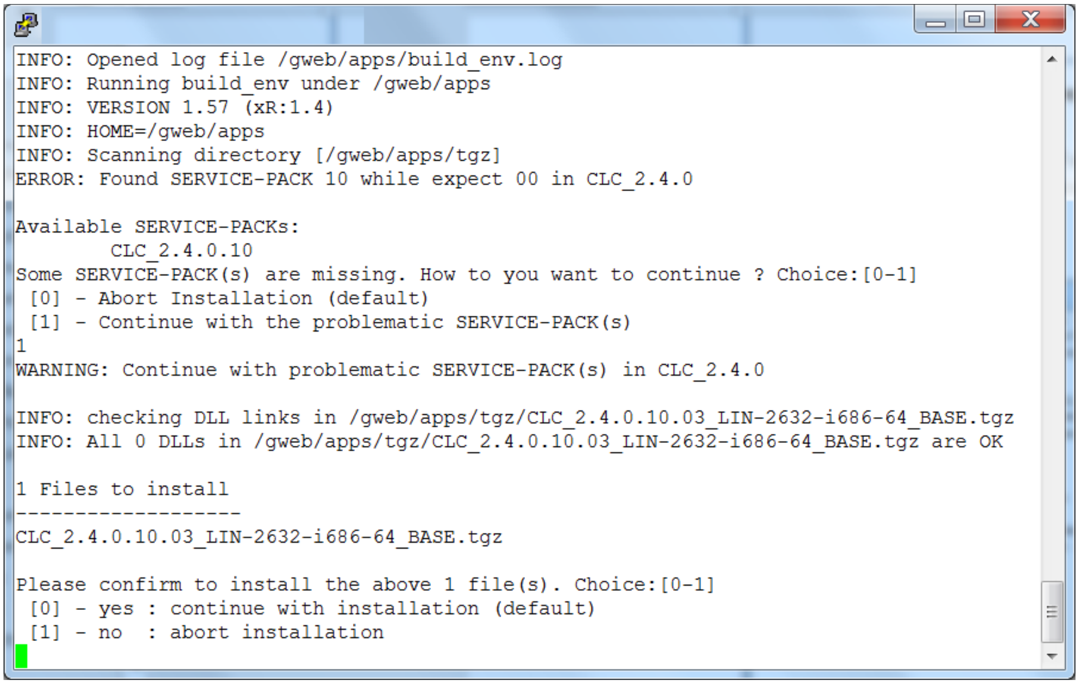
3. At each prompt select the option as indicated below. You can abort the installation at any time. For example you may want to use the tool to check the list of files that will be included in the installation without actually installing the binaries.

   Build_env checks the OS and skips all gzipped-tar files with a different OS in the file name. The screens below are samples only and vary depending on the gzipped-tar files present in "tgz".

   a) Build_env will warn if there are missing service packs, Figure 21. Select 1 to continue.

   b) Executing build_env displays a list of all the files that have been selected for installation. In the sample above: the IST GUI applications.

      Select option 0 to continue.

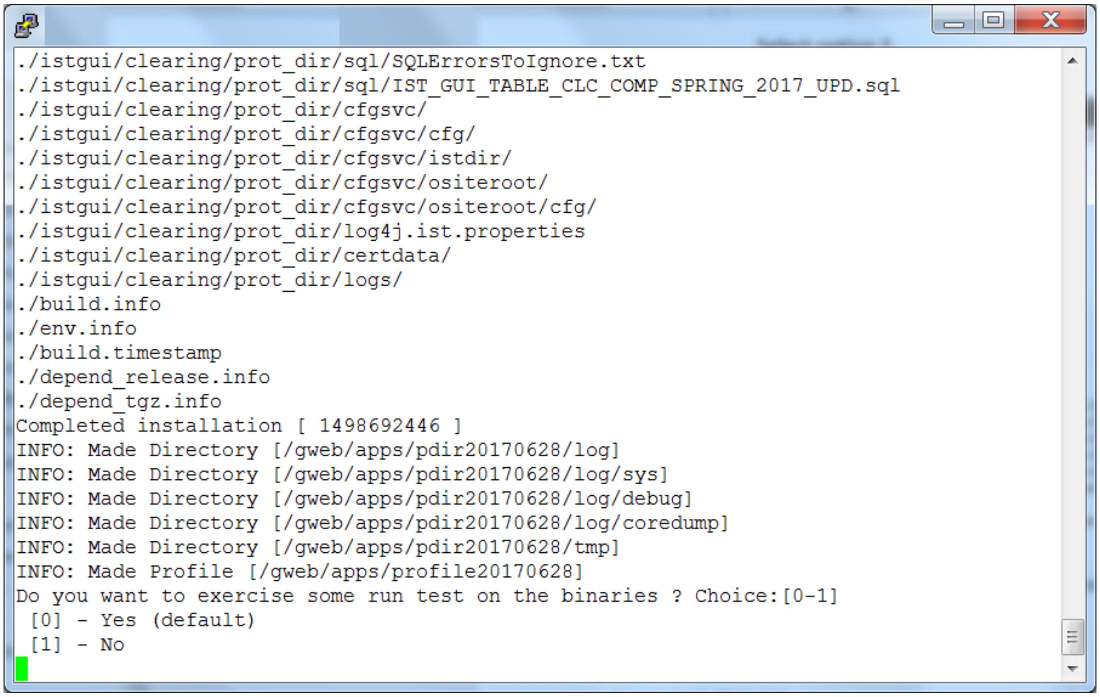


```
INFO: Opened log file /gweb/apps/build_env.log
INFO: Running build_env under /gweb/apps
INFO: VERSION 1.57 (xR:1.4)
INFO: HOME=/gweb/apps
INFO: Scanning directory [/gweb/apps/tgz]
ERROR: Found SERVICE-PACK 10 while expect 00 in CLC_2.4.0

Available SERVICE-PACKs:
        CLC_2.4.0.10
Some SERVICE-PACK(s) are missing. How to you want to continue ? Choice:[0-1]
 [0] - Abort Installation (default)
 [1] - Continue with the problematic SERVICE-PACK(s)
1
WARNING: Continue with problematic SERVICE-PACK(s) in CLC_2.4.0

INFO: checking DLL links in /gweb/apps/tgz/CLC_2.4.0.10.03_LIN-2632-i686-64_BASE.tgz
INFO: All 0 DLLs in /gweb/apps/tgz/CLC_2.4.0.10.03_LIN-2632-i686-64_BASE.tgz are OK

1 Files to install
-------------------
CLC_2.4.0.10.03_LIN-2632-i686-64_BASE.tgz

Please confirm to install the above 1 file(s). Choice:[0-1]
 [0] - yes : continue with installation (default)
 [1] - no  : abort installation
```

Figure 21: GUI Application – Service pack warning and file selected for Installation

c) After all selected gzipped-tar files are extracted an option to perform a sanity check on certain binary elements is made available. This is not applicable for the GUI installation.

Select option 1.



```
./istgui/clearing/prot_dir/sql/SQLErrorsToIgnore.txt
./istgui/clearing/prot_dir/sql/IST_GUI_TABLE_CLC_COMP_SPRING_2017_UPD.sql
./istgui/clearing/prot_dir/cfgsvc/
./istgui/clearing/prot_dir/cfgsvc/cfg/
./istgui/clearing/prot_dir/cfgsvc/istdir/
./istgui/clearing/prot_dir/cfgsvc/ositeroot/
./istgui/clearing/prot_dir/cfgsvc/ositeroot/cfg/
./istgui/clearing/prot_dir/log4j.ist.properties
./istgui/clearing/prot_dir/certdata/
./istgui/clearing/prot_dir/logs/
./build.info
./env.info
./build.timestamp
./depend_release.info
./depend_tgz.info
Completed installation [ 1498692446 ]
INFO: Made Directory [/gweb/apps/pdir20170628/log]
INFO: Made Directory [/gweb/apps/pdir20170628/log/sys]
INFO: Made Directory [/gweb/apps/pdir20170628/log/debug]
INFO: Made Directory [/gweb/apps/pdir20170628/log/coredump]
INFO: Made Directory [/gweb/apps/pdir20170628/tmp]
INFO: Made Profile [/gweb/apps/profile20170628]
Do you want to exercise some run test on the binaries ? Choice:[0-1]
 [0] - Yes (default)
 [1] - No
```

Figure 22: Extracting Files to Directory

d) The override installer options are displayed. This gives you the option to turn of the use of the tokenizer.

```
INFO: Version 1.15
INFO: OsString=[LIN-2632-i686]
INFO: bit reference binary /gweb/apps/pdir20170628/bin/overriding_check
not found
INFO: Only Java files are installable

   = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
   = = =                                               = = =
   = = =               W A R N I N G                   = = =
   = = =   Beware that this option will violate PADSS  = = =
   = = =                                               = = =
   = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Do you want to install "Override tokenization with ECHO only (ect-
javaclass.tgz)"
 Choice:[0-1]
 [0] - no (default)
 [1] - yes
0
INFO: Installed 0 overriding option(s)
INFO: Installation in /gweb/apps/pdir20170628
INFO: Profile in /gweb/apps/profile20170628
INFO: Log file in /gweb/apps/build_env.log

Program Completed
```

The option you choose depends on what was selected during the server installation. Select the default , 0 (no) which implies that the tokenizer is to be used for encrypting PANavlues. Otherwise if you chose not use the tokenizer option then select 1(yes) .

NOTE:	**Choosing not to use tokenization will make the installed application non-PADSS compliant.**

4. On completion the product directory and associated profile are created:

I. A file is created with name, profile<install_date>.where,

profile	is constant
install_date	is the date in the format yyyymmdd.

Example: profile20170628

profile<install_date> contains the environment variables required for the application to run. For GUI deployment, these are also required. and provide the facility to navigate more easily to various directories.

II. A directory is created with name, pdir<install_date> where,

pdir constant.

install_date is the date in the format yyyymmdd.

When multiple installations are done within the same day, the current pdir<install_date> is moved to pdir<install_date>_<n> where n is a number depending on the number of installations within the install date.

Example: pdir20170628

pdir20170628	current installed pdir<install _date> on January 12, 2017.
pdir20170628_1	previously installed pdir<install _date> directory on January 12, 2017, moved to pdir<date>_n.

The pdir<install_date> directory contains the GUI files to be used in the deployment.

III. The file build_env.log is updated with the installation information.

5. Create a soft link to the new profile<date> file. Delete the “profile” link first if necessary

   rm profile

   ln –s profile<date> profile

   Refer to “.profile" Entries” for entries to include in the ".profile".

6. Re-login to apply the changes above.

GUI Application Database Tasks

Database related tasks are executed using IST-PDeploy. Refer to Installing the GUI Application below.

Installing the GUI Application

IBM Websphere 7 and 8.5.5

Refer to the IST GUI Application Installation: IBM Websphere guide for details

Oracle WebLogic 12c

Refer to the IST GUI Application Installation: Oracle Weblogic guide for details.

Tomcat 7 and 8

Refer to the IST GUI Application Installation: Apache Tomcat guide for details.

Enabling TLS

This section describes the procedure to enable TLS between the IST processes.

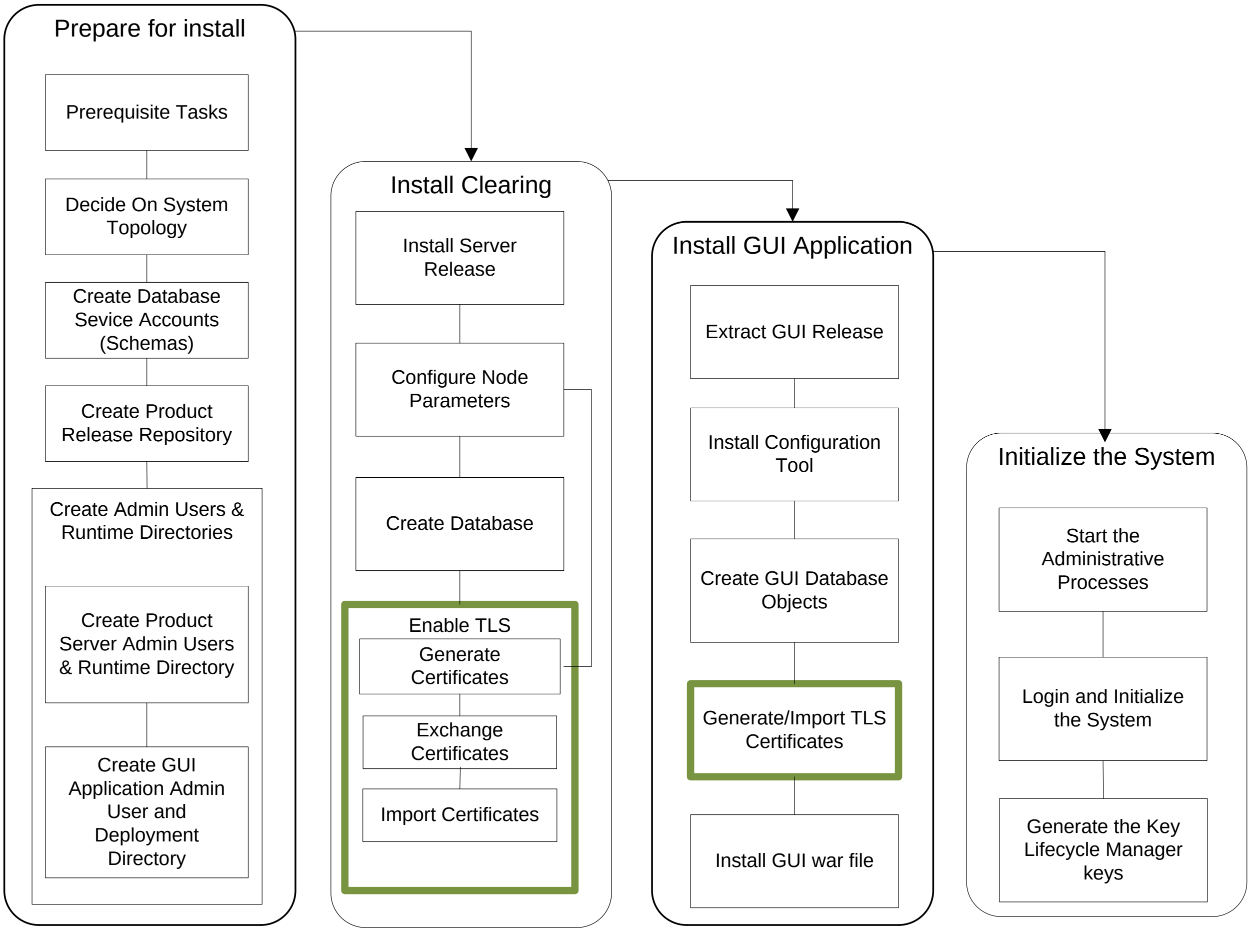

Prepare for install
Prerequisite Tasks
Decide On System Topology
Create Database Sevice Accounts (Schemas)
Create Product Release Repository
Create Admin Users & Runtime Directories
Create Product Server Admin Users & Runtime Directory
Create GUI Application Admin User and Deployment Directory
Install Clearing
Install Server Release
Configure Node Parameters
Create Database
Enable TLS
Generate Certificates
Exchange Certificates
Import Certificates
Install GUI Application
Extract GUI Release
Install Configuration Tool
Create GUI Database Objects
Generate/Import TLS Certificates
Install GUI war file
Initialize the System
Start the Administrative Processes
Login and Initialize the System
Generate the Key Lifecycle Manager keys

Figure 23: Enabling TLS Option

TLS is enabled at installation time using the options provided in the installation configuration tool, pdeploy. Enabling TLS involves generating certificates for both server processes and their clients, and the exchange of these certificates. This process is illustrated in Figure 1. The set of processes along with their respective files are also shown in Figure 15.

In section xxx application certificates were generated on each node in the system. These certificates were stored in $OSITE_ROOT/certdata.

Certificates were also generated for the GUI application and stored in the protected directory under certdata.

Certificates must now be exchanged between the GUI application and each node in the

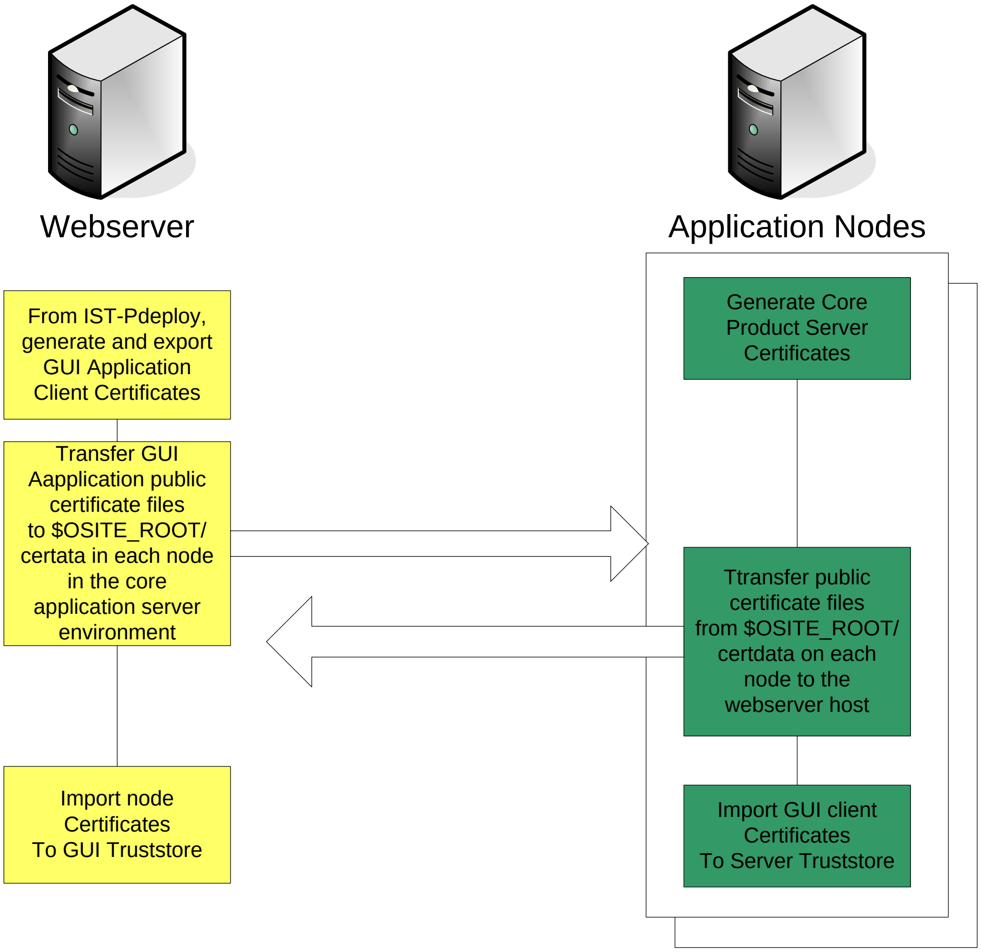

Webserver
Application Nodes
From IST-Pdeploy, generate and export GUI Application Client Certificates
Transfer GUI Aapplication public certificate files to $OSITE_ROOT/ certata in each node in the core application server environment
Import node Certificates To GUI Truststore
Generate Core Product Server Certificates
Ttransfer public certificate files from $OSITE_ROOT/ certdata on each node to the webserver host
Import GUI client Certificates To Server Truststore

Figure 24: Enabling TLS

Java Application Server

TLS must be enabled on the http listener in the Java application server.

For information on enabling TLS on the Java application server, refer to the vendor's documentation and follow the instructions.

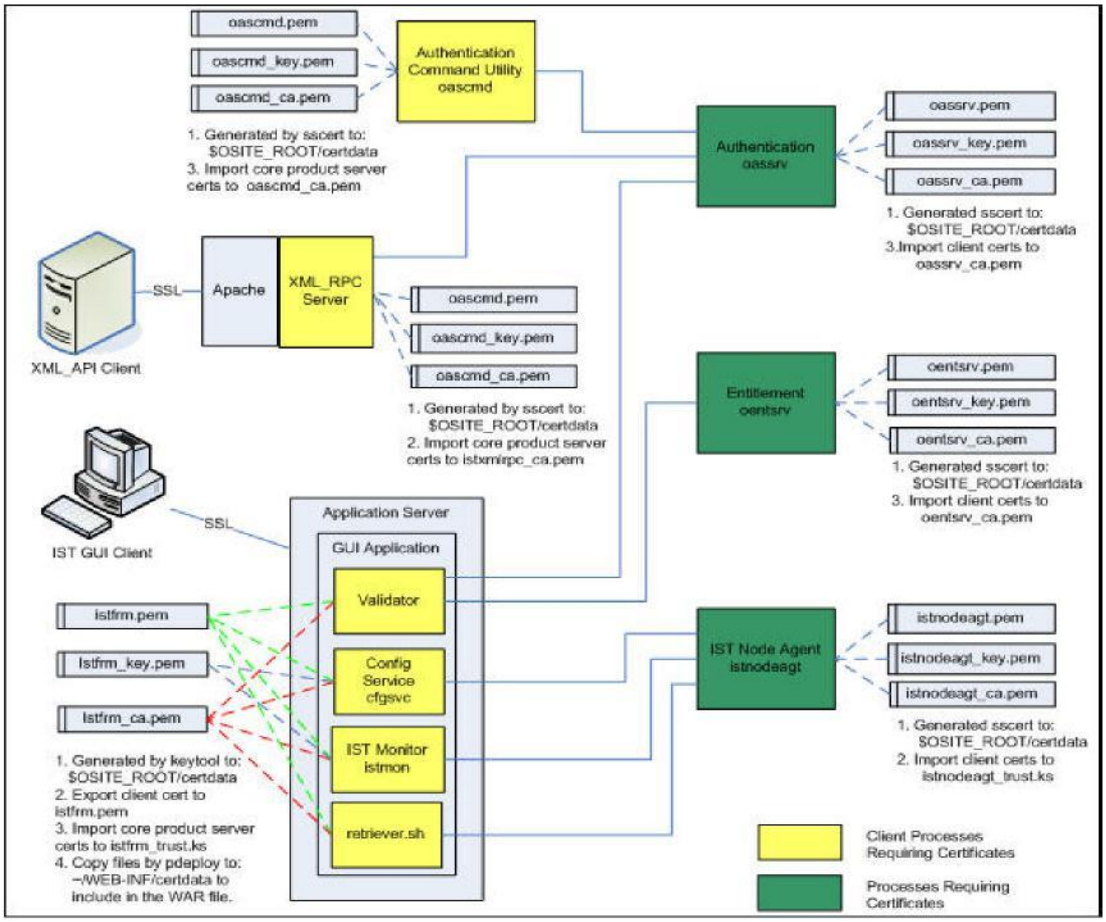

oascmd.pem
oascmd_key.pem
oascmd_ca.pem
Authentication Command Utility oascmd
1. Generated by sscert to: $OSITE_ROOT/certdata
3. Import core product server certs to oascmd_ca.pem
Authentication oassrv
oassrv.pem
oassrv_key.pem
oassrv_ca.pem
1. Generated sscert to: $OSITE_ROOT/certdata
3.Import client certs to oassrv_ca.pem
XML_API Client
SSL
Apache
XML_RPC Server
oascmd.pem
oascmd_key.pem
oascmd_ca.pem
1. Generated by sscert to: $OSITE_ROOT/certdata
2. Import core product server certs to istxmlrpc_ca.pem
Entitlement oentsrv
oentsrv.pem
oentsrv_key.pem
oentsrv_ca.pem
1. Generated sscert to: $OSITE_ROOT/certdata
3. Import client certs to oentsrv_ca.pem
IST GUI Client
SSL
Application Server
GUI Application
Validator
Config Service cfgsvc
IST Monitor istmon
retriever.sh
istfrm.pem
Istfrm_key.pem
Istfrm_ca.pem
1. Generated by keytool to: $OSITE_ROOT/certdata
2. Export client cert to istfrm.pem
3. Import core product server certs to istfrm_trust.ks
4. Copy files by pdeploy to: ~/WEB-INF/certdata to include in the WAR file.
IST Node Agent istnodeagt
istnodeagt.pem
istnodeagt_key.pem
istnodeagt_ca.pem
1. Generated sscert to: $OSITE_ROOT/certdata
2. Import client certs to istnodeagt_trust.ks
Client Processes Requiring Certificates
Processes Requiring Certificates

Figure 25: IST Clearing TLS Enabled Process

Initializing the System

The following describes the steps to initialize the system:

1. The system is installed and configured using pdeploy.
2. The administrative processes are started using an administrative account. The processes are: "istnodeagt", "oassrv" and "oentsrv".
3. The administrator logs into the GUI application, and is authenticated and entitled to use the Configuration Service and IST Control. The system will be initialized via the IST Control command window.
4. The administrator:
   a) Adds the node to be controlled in IST Control.
   b) Initializes the Key Life Cycle manager passphrase file.
   c) Generates the keys for the Key Life Cycle manager process.
   d) Initializes the system by starting the node. At this point the tokenization and the key management processes will be started.

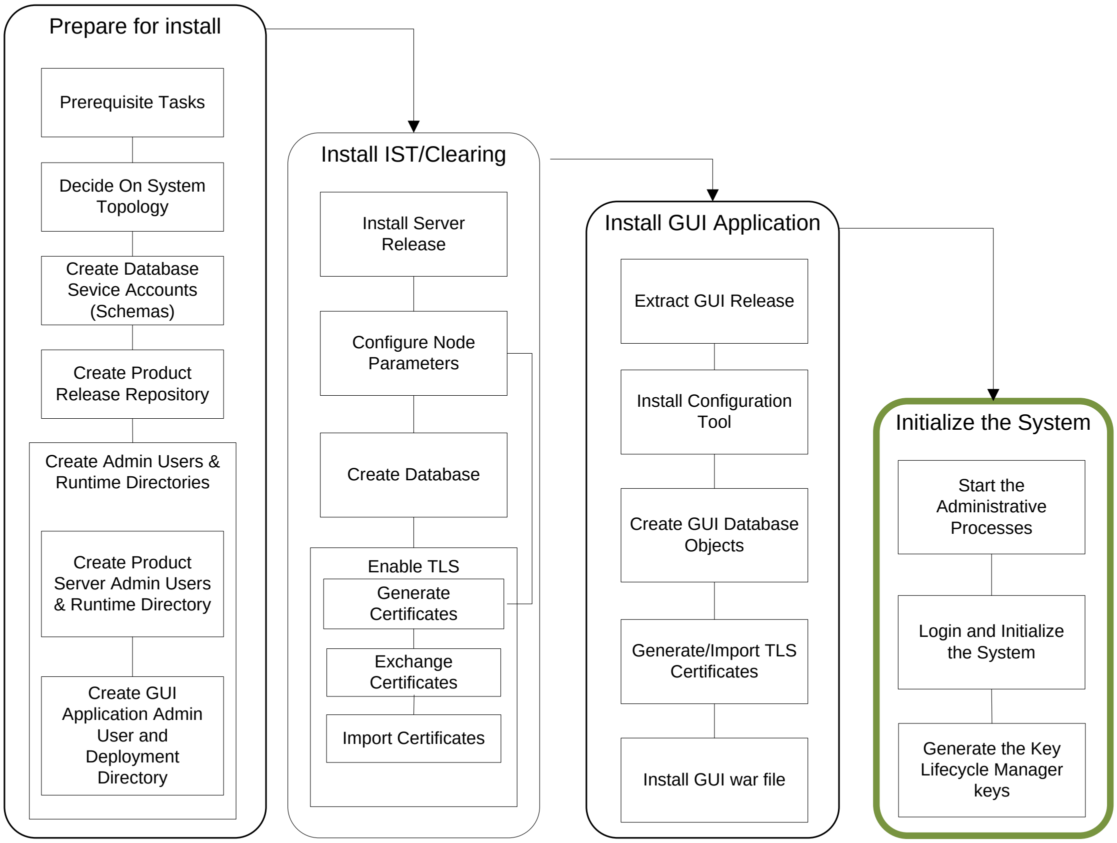

Prepare for install
Prerequisite Tasks
Decide On System Topology
Create Database Sevice Accounts (Schemas)
Create Product Release Repository
Create Admin Users & Runtime Directories
Create Product Server Admin Users & Runtime Directory
Create GUI Application Admin User and Deployment Directory
Install IST/Clearing
Install Server Release
Configure Node Parameters
Create Database
Enable TLS
Generate Certificates
Exchange Certificates
Import Certificates
Install GUI Application
Extract GUI Release
Install Configuration Tool
Create GUI Database Objects
Generate/Import TLS Certificates
Install GUI war file
Initialize the System
Start the Administrative Processes
Login and Initialize the System
Generate the Key Lifecycle Manager keys

Figure 26: Initializing The System

Start the Administration Processes

There are three administrative processes that must be started on each node. They are istnodeagt, oassrv and oentsrv.

Administrative processes are mutually exclusive processes. However, they must be started before access to the admin control interfaces, Configuration Service and IST Control is possible. These processes are started using an administrative account in each foundation region.

The admin control interfaces are used to configure, start, stop and manage the system.

Starting the Administrative Processes

On the Clearing node:

- Login as the admin user using an individual account.
- Type "istnodeagt" at the command line.
- Type "oassrv -b" at the command line. The prompt below is displayed:

  ```
  Enter PEM passphrase:
  ```

  Press Enter without entering a passphrase.
- Type "oentsrv -b" at the command line. The prompt below is displayed:

  ```
  Enter PEM passphrase:
  ```

  Press Enter without entering a passphrase.

Stopping the Administrative Processes

Login as the admin user using an individual account.To stop istnodeagt type "istnodeagtcmd stop" at the prompt.

- To stop oentsrv (entitlement):
  - type "ps -ef|grep oassrv" to get the process ID (pid).
  - type "kill <the_oassrv_pid>" to stop the entitlement process.
- To stop oassrv (authentication):
  - type "ps -ef|grep oentsrv" to get the process ID (pid).
  - enter "kill <the_oentsrv_pid>" to stop the authentication process.

GUI Application First Time Login

As part of the initial data loaded to the entitlement database, an admin user record is created. The admin has access to all applications and screens in the system. The username is "admin" and the initial password is "admin".

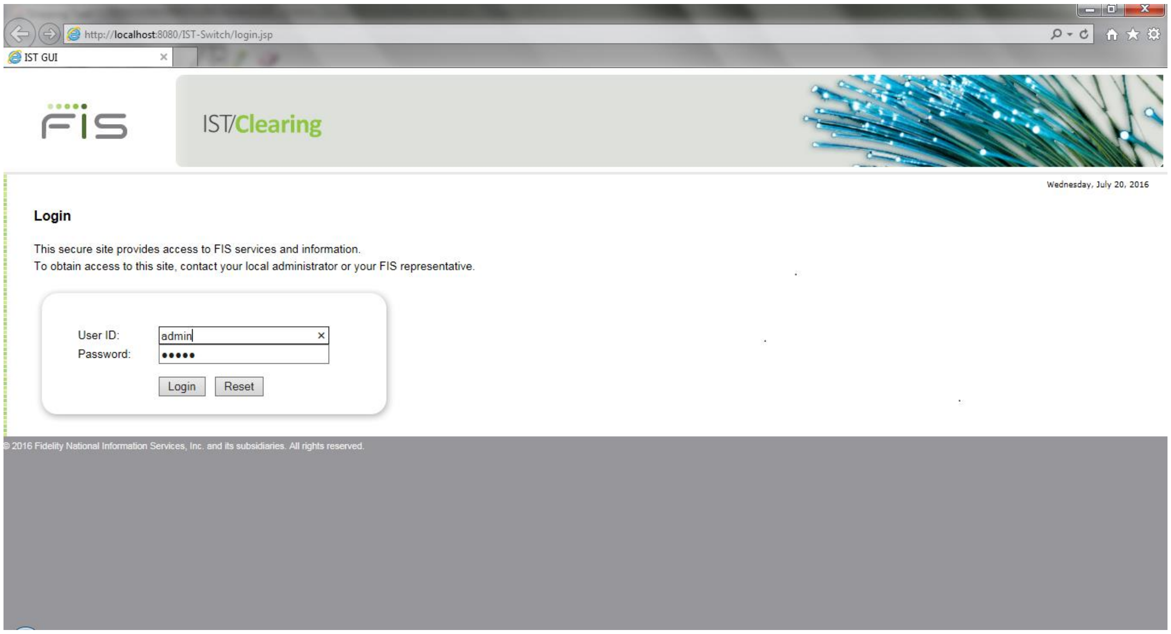
The admin user is forced to change the password the first time the account is used. The admin user must enter a password conforming to the security level setup during the installation.

To access the application enter the URL in a browser window, the welcome page is displayed followed by the login dialog.

The URL structure is as follows:

```
http://<web_server_host>:<port>/<context_root>/Main.html
```

Open a browser and enter the URL corresponding to the installed application. You will be redirected to a login page.



http://localhost:8080/IST-Switch/login.jsp

Wednesday, July 20, 2016

Login

This secure site provides access to FIS services and information.
To obtain access to this site, contact your local administrator or your FIS representative.

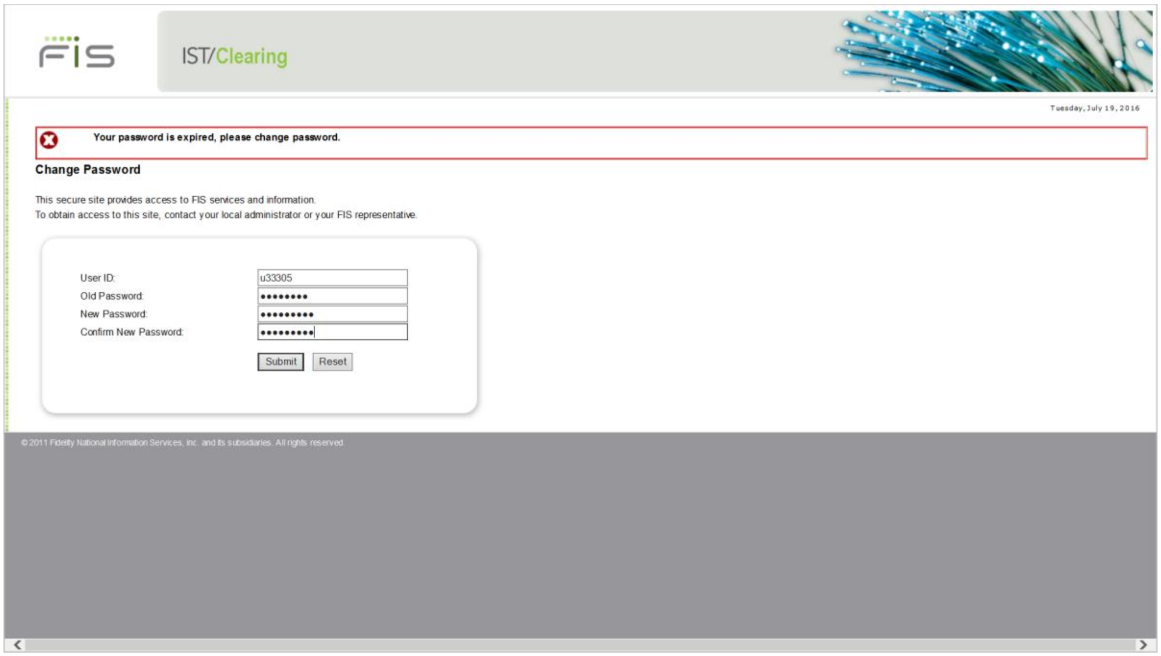
User ID: admin
Password: •••••

© 2016 Fidelity National Information Services, Inc. and its subsidiaries. All rights reserved.

Figure 27: IST Application Login Page

To login for the first time:

1. Enter the the initial user name create during Entitlement installation.
2. Enter initial user’s password.
3. Click **Login**.
4. The expired password page is displayed.



Tuesday, July 19, 2016

Your password is expired, please change password.

Change Password

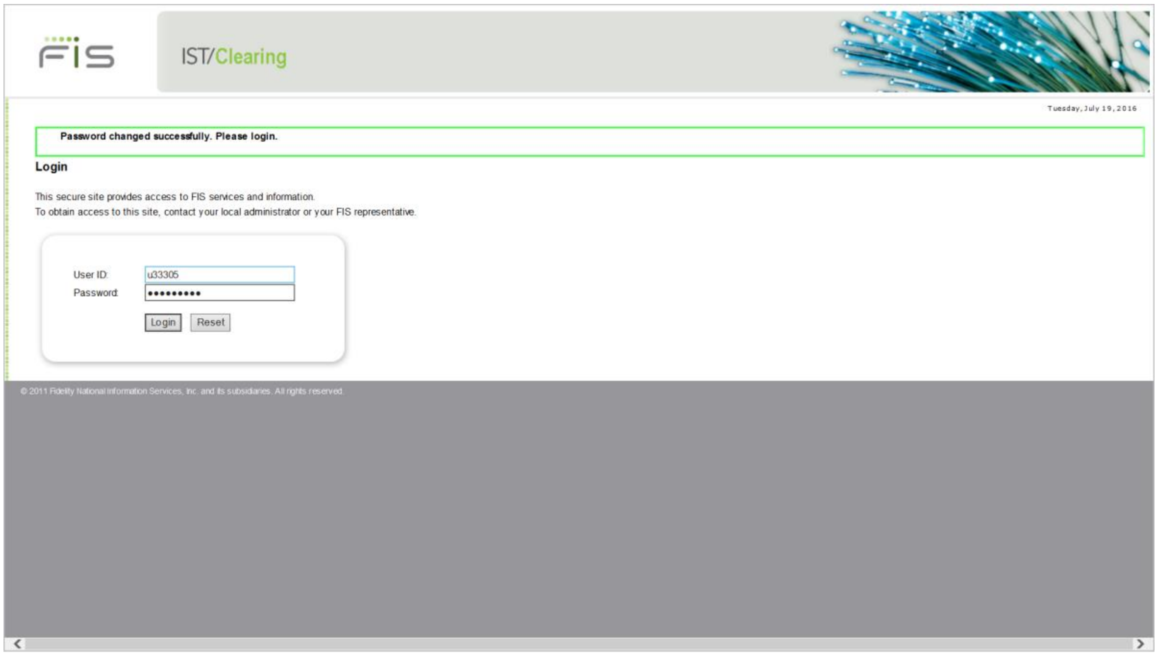
This secure site provides access to FIS services and information.
To obtain access to this site, contact your local administrator or your FIS representative.

User ID: u33305
Old Password: ••••••••
New Password: •••••••••
Confirm New Password: •••••••••

© 2011 Fidelity National Information Services, Inc. and its subsidiaries. All rights reserved.

Figure 28: Password Expired Page

1. Enter the default password "admin" in the **Old Password** field
2. Enter a new password in the **New Password** field. The password must conform to the complexity rules defined by the parameters that were setup during the "Install Entitlement" procedure.
3. Reenter the new password in the **Confirm New Password** field.
4. Click **Submit** button.
5. The change password success page is displayed.



Tuesday, July 19, 2016

Password changed successfully. Please login.

Login

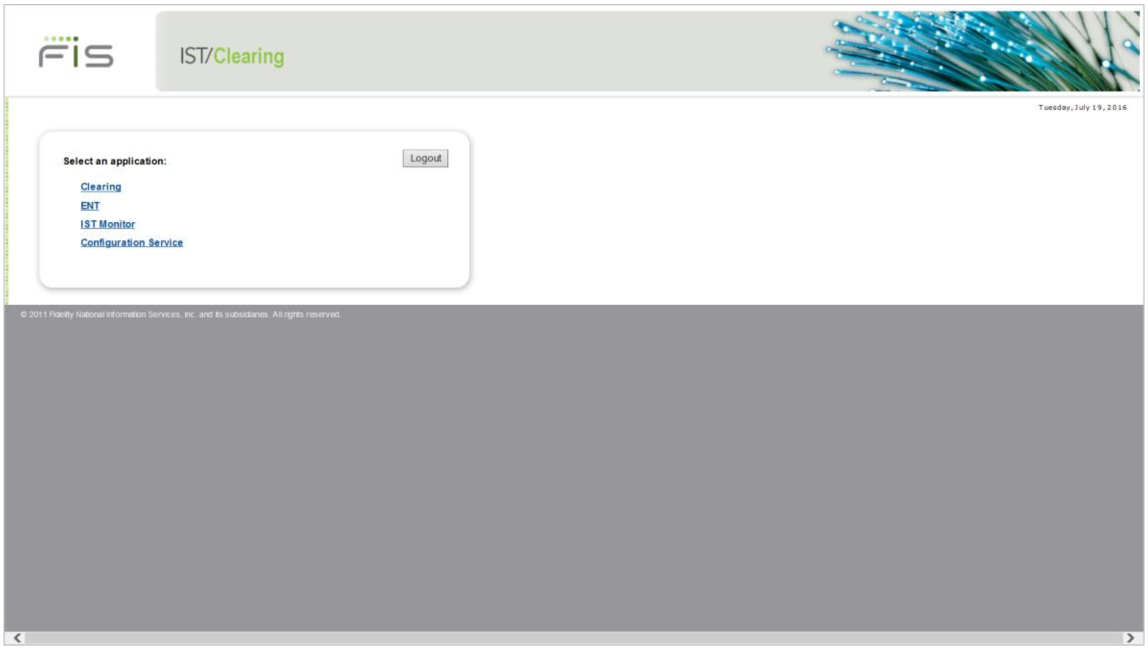
This secure site provides access to FIS services and information.
To obtain access to this site, contact your local administrator or your FIS representative.

User ID: u33305
Password: •••••••••

© 2011 Fidelity National Information Services, Inc. and its subsidiaries. All rights reserved.

Figure 29: Password Change Successfully

6. Enter "admin" as the User ID.
7. Enter the new password.
8. Click **Login**.
9. The Application select page is displayed.



© 2011 Fidelity National Information Services, Inc. and its subsidiaries. All rights reserved.

Figure 30: IST/Clearing Menu

At this point, other user accounts can be created and permissions assigned to access the system.

Accounts assigned to the Admin_Group have administrative privileges. To do this:

a) Select the ENT link to open the Authentication and Entitlement application.

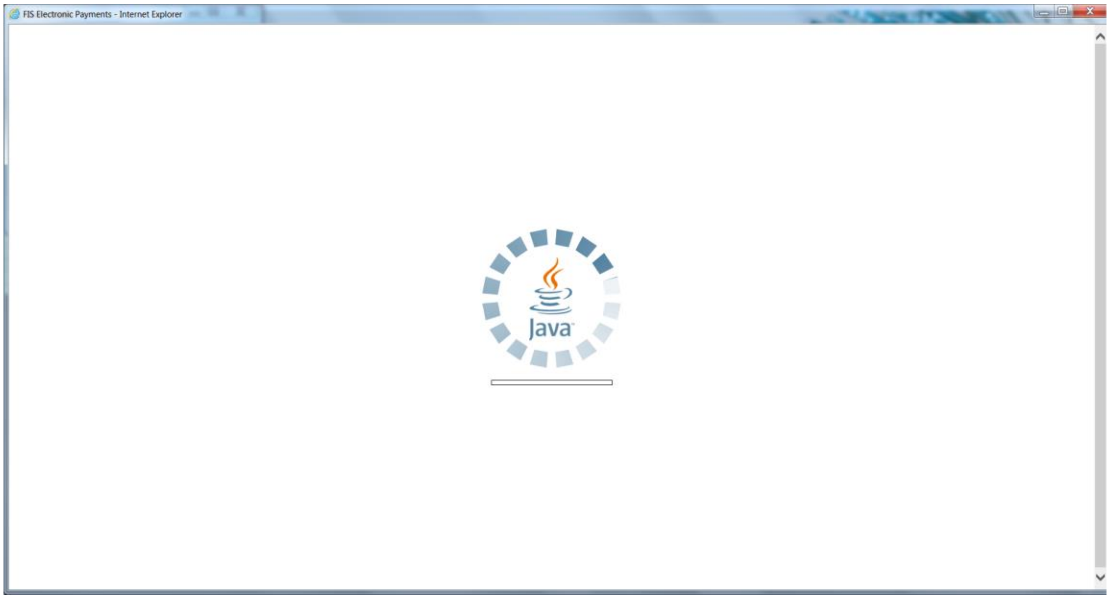
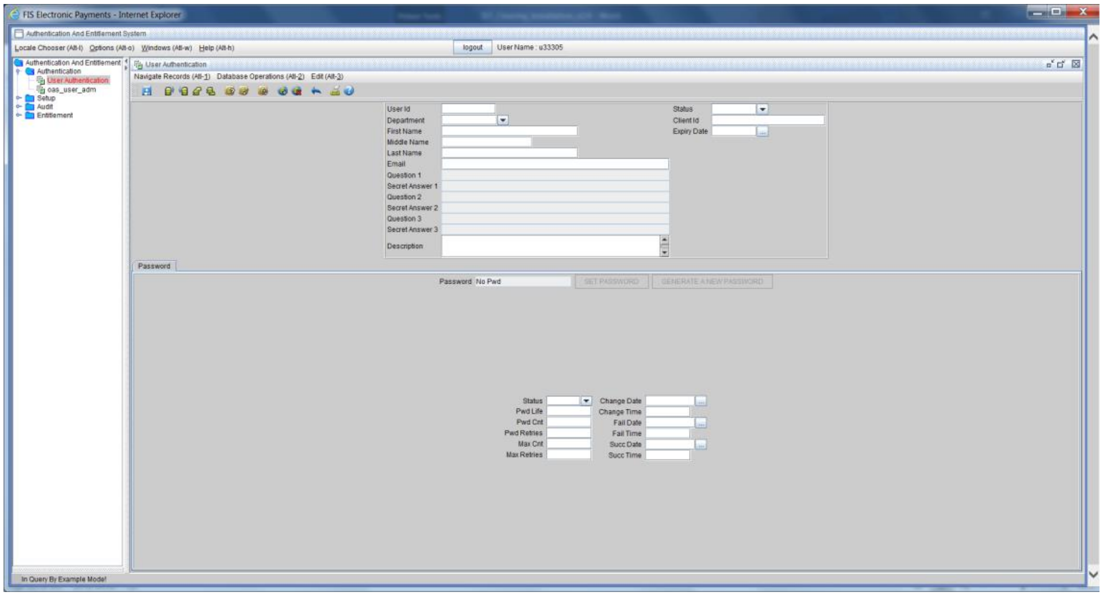


Figure 31: Select ENT



User Name : u33305

Password No Pwd

In Query By Example Mode!

Figure 32: User Authentication Screen

b) Click Insert on the screen menu

c) Enter the **User ID**. This is the user's login name.

d) Enter the **user's first** and **last names**,

e) Enter **Email address**, and **Department** as necessary,

f) For active users leave the **Status** field empty.

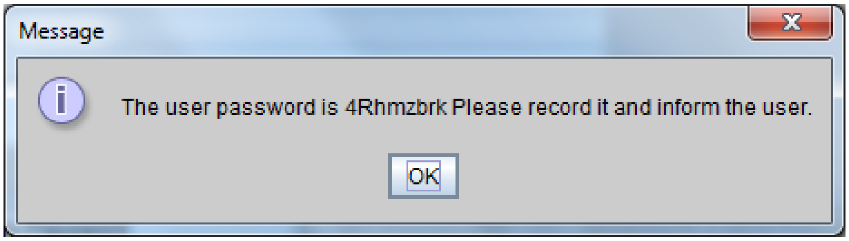
g) Leave **Password life** empty. This is the number of days after which a password change will be enforced. Leave it empty to default to the value configured in the Authentication server. The default is set to 30 when the authentication server is installed. The maximum value that can be entered is 45.

h) Set **Max password count**, if you want to force the user to change password after a number of successful logins. For example setting Max Cnt = 10 will force the user to change password after 10 successful logins.

i) Set **Max password retries** to the number of times the user is allowed to enter a wrong password before the account is locked out. This is set to 3. You can set a value between 1 and 6. Typically a regular user should be set to 3, and an administrator can be set up to 6.

j) Save the record by clicking the **Save** button. This will set the various dates in the tab, and create appropriate records in the entitlement tables.

k) On successful creation of the user account an initial password is generated. This password is to be given to the user in a secure manner. The user will be forced to change the password the first time it is used.



Message

The user password is 4Rhmzbrk Please record it and inform the user.

Figure 33: Generated Password Display

l) Copy the password so it can be sent to the user.

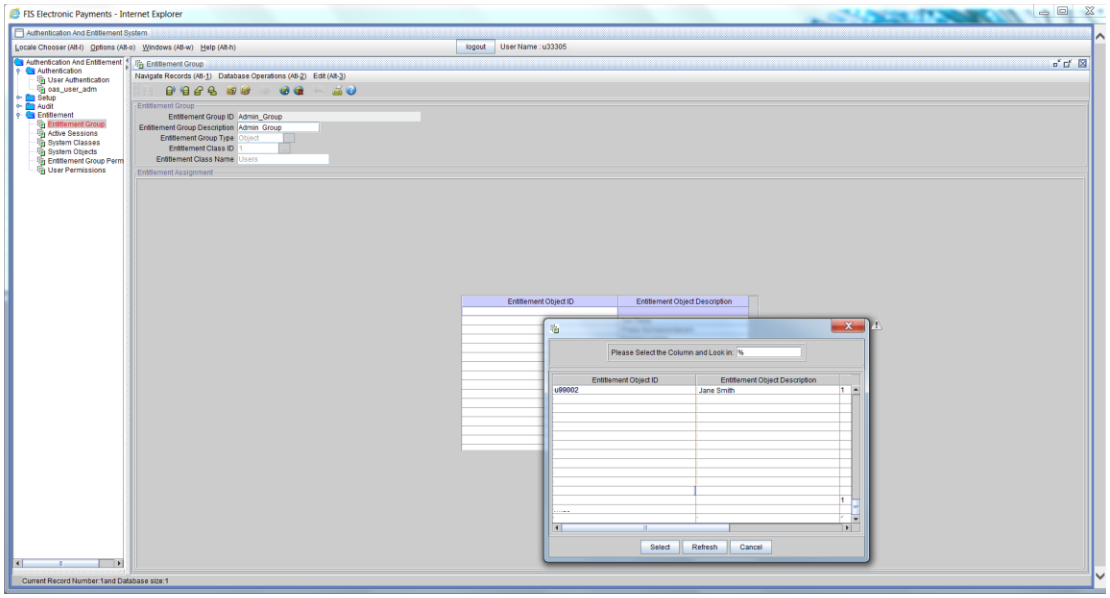
m) From the menu select open the Entitlement Group screen, Query the newly added user and display the detail record.

n) Click User Group.

o) Click the “Enter Query by Example” icon.

p) Click Execute Query.

q) Right Click on the Entitlement Object ID row and select Insert Record



User Name : u33305

Entitlement Group ID: Admin_Group
Entitlement Group Description: Admin Group
Entitlement Group Type: Object
Entitlement Class ID: 1
Entitlement Class Name: Users

Please Select the Column and Look in: %

Entitlement Object ID	Entitlement Object Description
u99002	Jane Smith

Current Record Number:1and Database size:1

Figure 34: User Group Screen

r) Double click in the empty row to display the set of user records.

s) Select the user to assign to the group and click Select.

t) Click **Save** button.

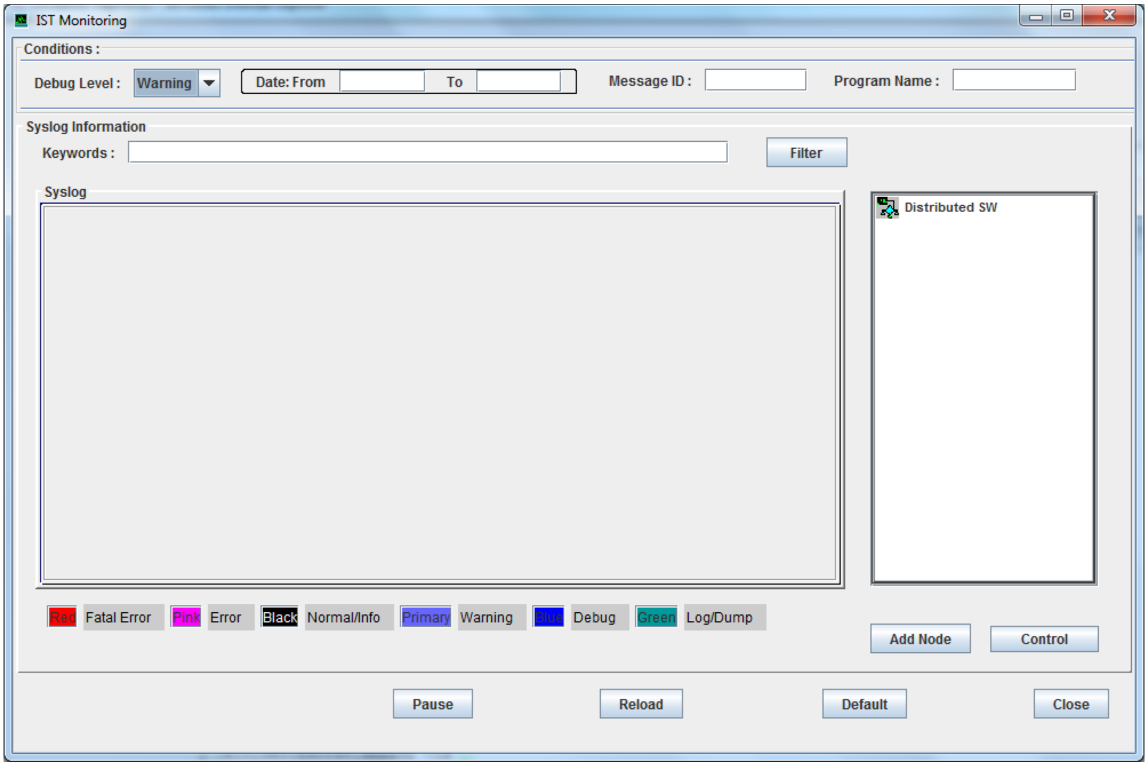
The new user account can now be used to administer the system.

For more information on user security, refer to the IST *User Authentication and Entitlement User Guide*

Add a clearing Type Node in IST Control

Before starting the system the Clearing node must be added in IST Control. Adding a node tells IST Control where to send requests for that node.

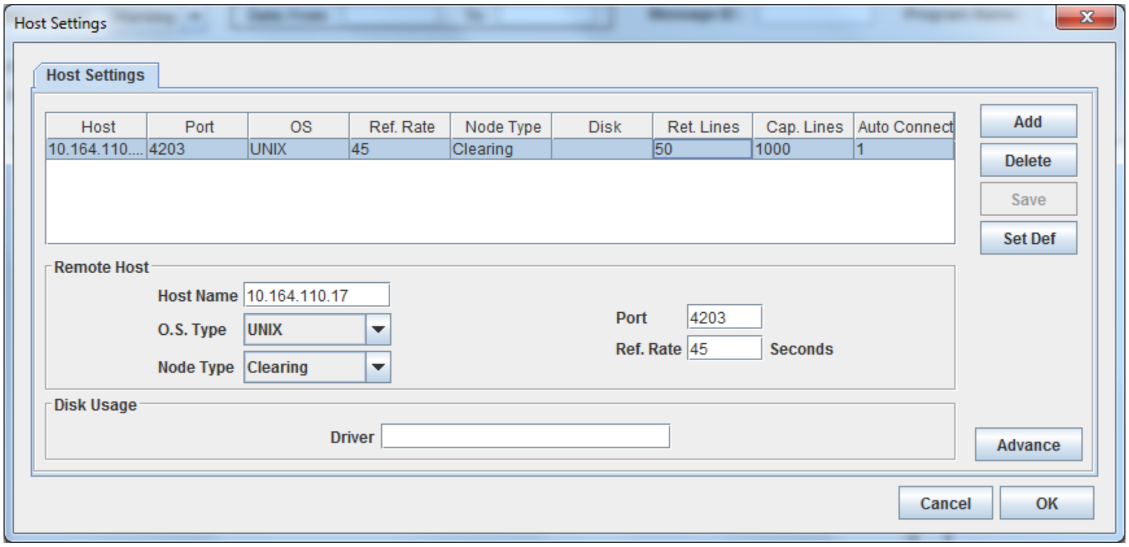
1. Login as the administrative user and open IST Control from the Monitor menu. And select IST Monitor on the Application Select page.



Debug Level : Warning

Figure 35: IST Monitor

2. Click **Add Node** to display the window used to add nodes to control.



Host	Port	OS	Ref. Rate	Node Type	Disk	Ret. Lines	Cap. Lines	Auto Connect
10.164.110....	4203	UNIX	45	Clearing		50	1000	1

Host Name 10.164.110.17

O.S. Type UNIX

Node Type Clearing

Port 4203

Ref. Rate 45 Seconds

Figure 36: IST Monitor- Add Node

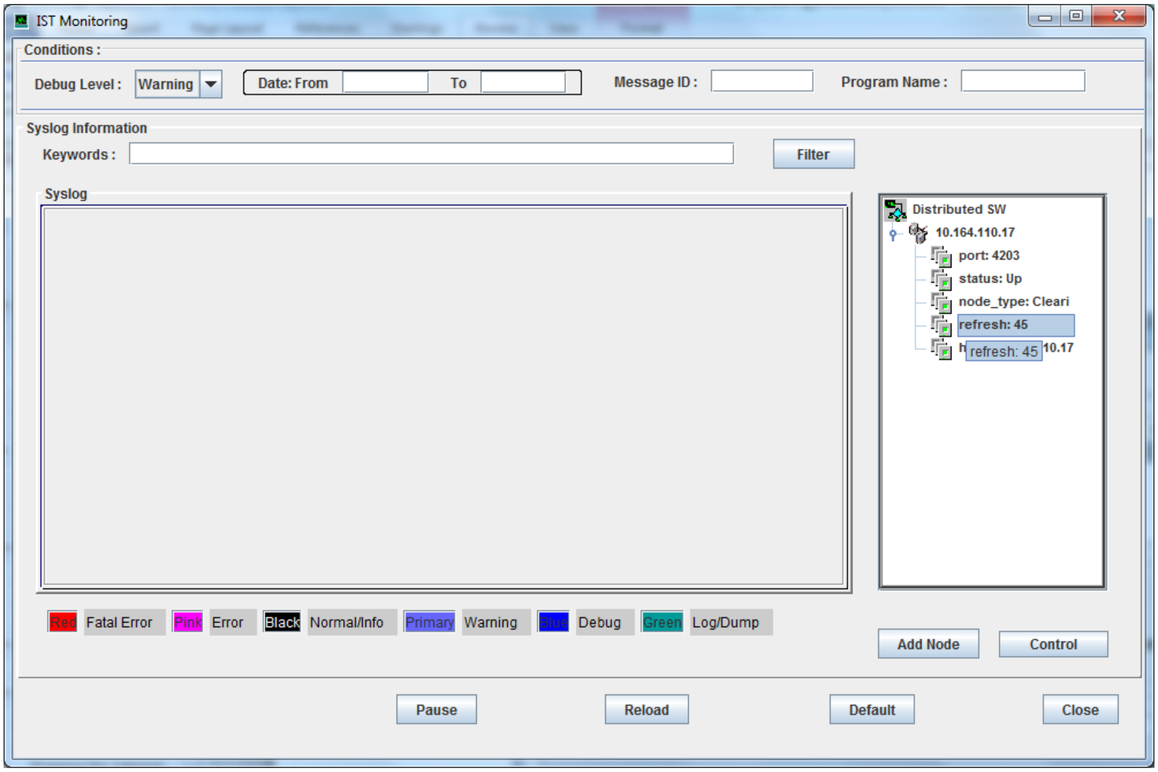
3. **Click Add**
4. Enter the IST/Clearing hostname or IP in the Host Name field.
5. Select Node Type “Clearing”

6. Enter the port istnodeagt port configured during the IST/Clearing installation.
7. Click **Save** button.
8. Click OK. The node appears in Nodes list.

Master Key Setup

Four options are included to manage Tokenization master keys.

In IST Monitor:

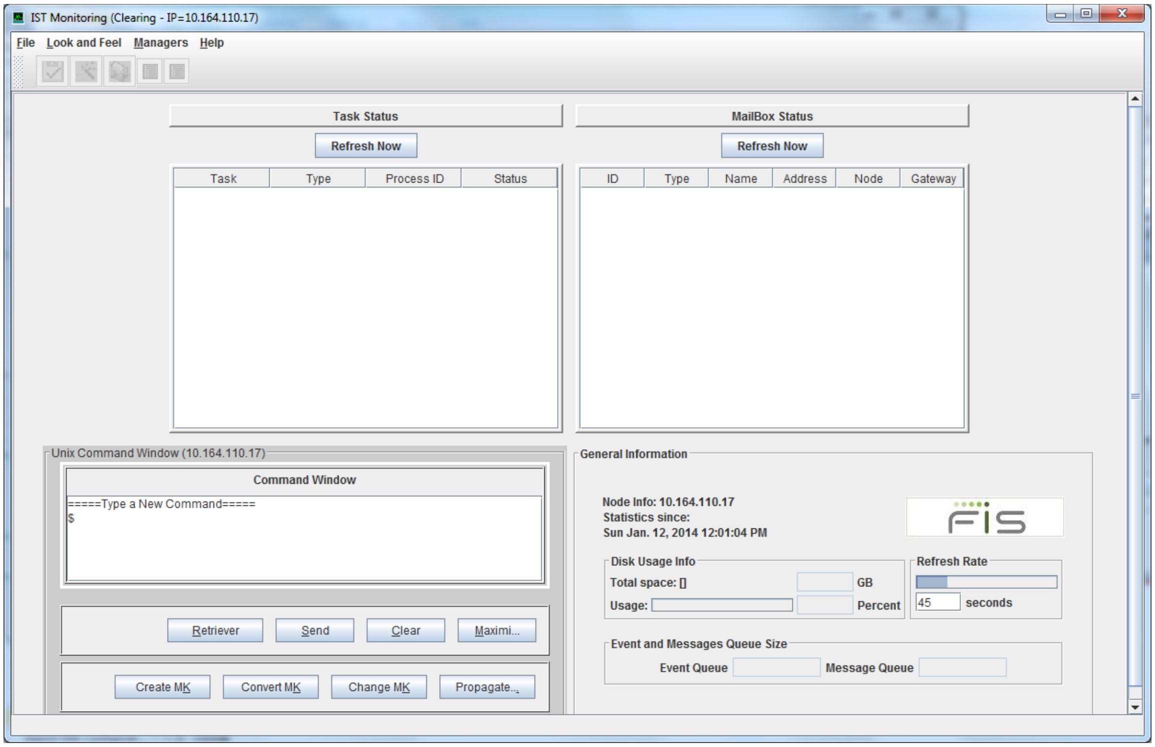


Debug Level : Warning

Distributed SW
- 10.164.110.17
  - port: 4203
  - status: Up
  - node_type: Cleari
  - refresh: 45
  - h refresh: 45 10.17

Figure 37: IST Monitor – Node

1. Select the Clearing node setup in the previous section.
2. Click Control



```
=====Type a New Command=====
$
```

Node Info: 10.164.110.17
Statistics since:
Sun Jan. 12, 2014 12:01:04 PM

Total space: [] GB

Usage: Percent

45 seconds

Figure 38: Create Master Key

3. Click Create Master Key

Create MK:

Invokes : “tokenmas|run_cmd|klc_init_master”.

Convert MK:

Invokes : “tokenmas|run_cmd|km_pass2tokmas”.

Change MK:

a) invokes : “tokenmas|run_cmd|klcutil –u”.

b) Invokes : “tokenmas|run_cmd|klcutil –t” on one node.

c) If successful run “mbrulecmd update token-keys” on all nodes.

Start IST/Clearing

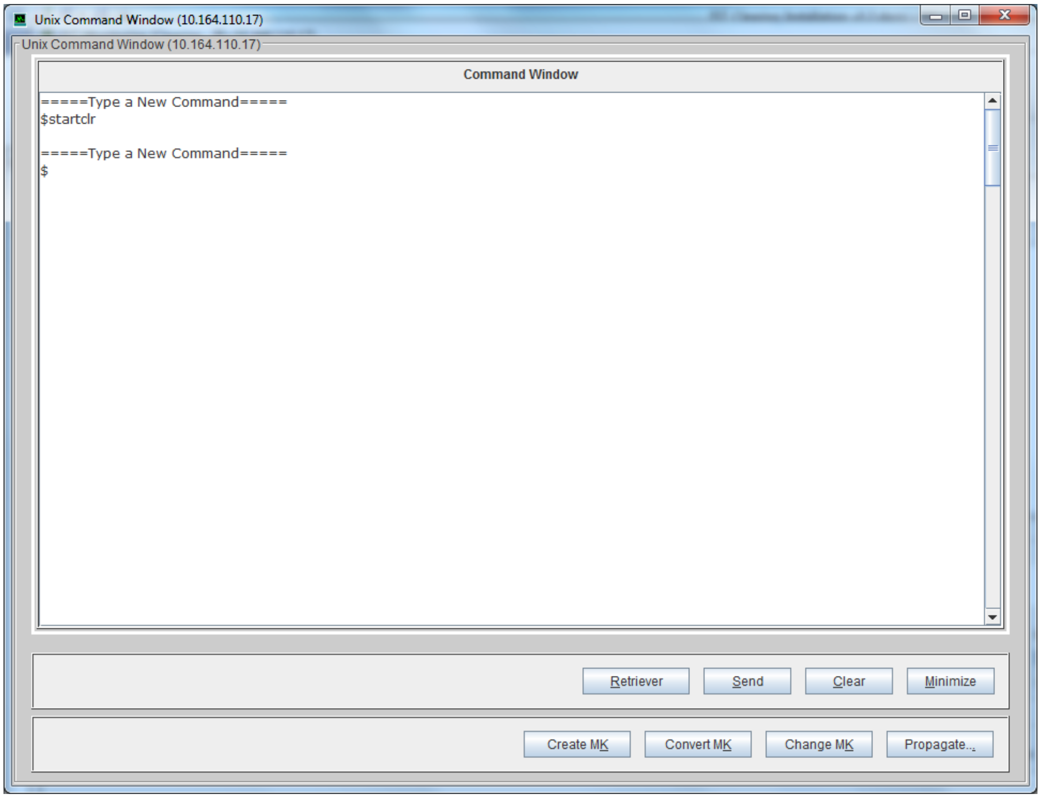
To start the IST/Clearing processes:

4. Before start of IST/Clearing, permissions need to be provided to the user who starts clearing.

   Refer to User_Access_Permission guide for further details:

   https://projectsites.fnfis.com/sites/EMEA/IFIDEV/157722/Reference%20Material%20PADSS%2021%20From%20Audit%20Site/INSTALLATION%20GUIDES/Clearing2.4/IST_Clearing_User_Access%20_Permission.docx

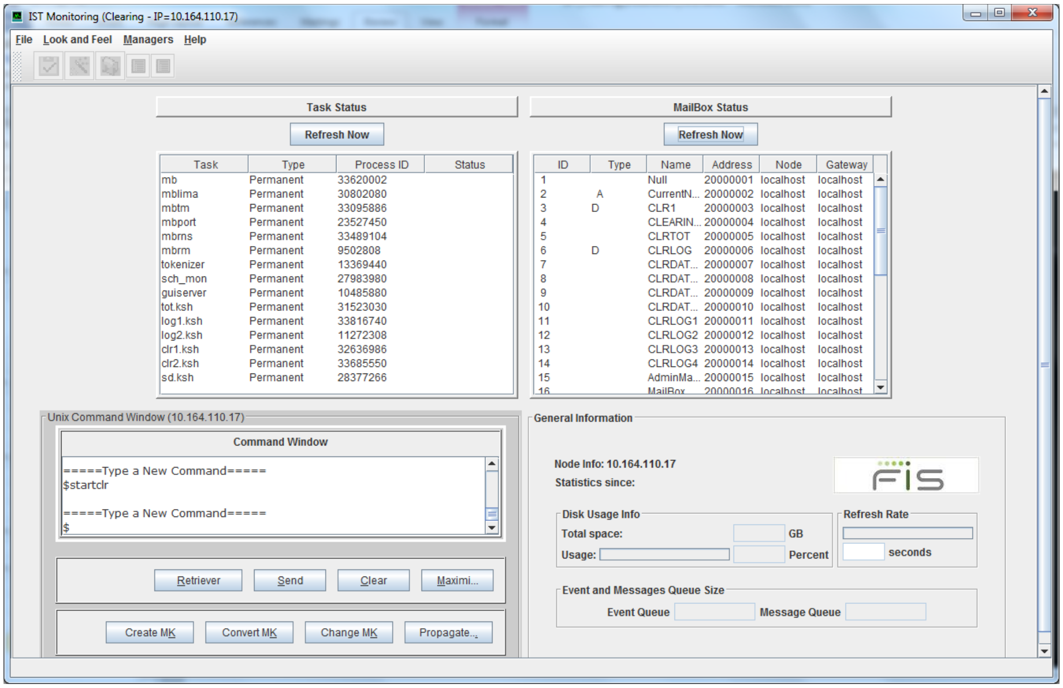
5. Click Maximize to mazimize the Command Window



```
=====Type a New Command=====
$startclr

=====Type a New Command=====
$
```

Figure 39: Unix Command Window

6. Enter startclr in the Command Window
7. Click Send
8. After the system starts Click Minimize on the Command Window



Task	Type	Process ID	Status
mb	Permanent	33620002	
mblima	Permanent	30802080	
mbtm	Permanent	33095886	
mbport	Permanent	23527450	
mbrns	Permanent	33489104	
mbrm	Permanent	9502808	
tokenizer	Permanent	13369440	
sch_mon	Permanent	27983980	
guiserver	Permanent	10485880	
tot.ksh	Permanent	31523030	
log1.ksh	Permanent	33816740	
log2.ksh	Permanent	11272308	
clr1.ksh	Permanent	32636986	
clr2.ksh	Permanent	33685550	
sd.ksh	Permanent	28377266	

ID	Type	Name	Address	Node	Gateway
1		Null	20000001	localhost	localhost
2	A	CurrentN...	20000002	localhost	localhost
3	D	CLR1	20000003	localhost	localhost
4		CLEARIN...	20000004	localhost	localhost
5		CLRTOT	20000005	localhost	localhost
6	D	CLRLOG	20000006	localhost	localhost
7		CLRDAT...	20000007	localhost	localhost
8		CLRDAT...	20000008	localhost	localhost
9		CLRDAT...	20000009	localhost	localhost
10		CLRDAT...	20000010	localhost	localhost
11		CLRLOG1	20000011	localhost	localhost
12		CLRLOG2	20000012	localhost	localhost
13		CLRLOG3	20000013	localhost	localhost
14		CLRLOG4	20000014	localhost	localhost
15		AdminMa...	20000015	localhost	localhost
16		MailBox	20000016	localhost	localhost

```
=====Type a New Command=====
$startclr

=====Type a New Command=====
$
```

Node Info: 10.164.110.17

Statistics since:

Total space: GB

Usage: Percent

seconds

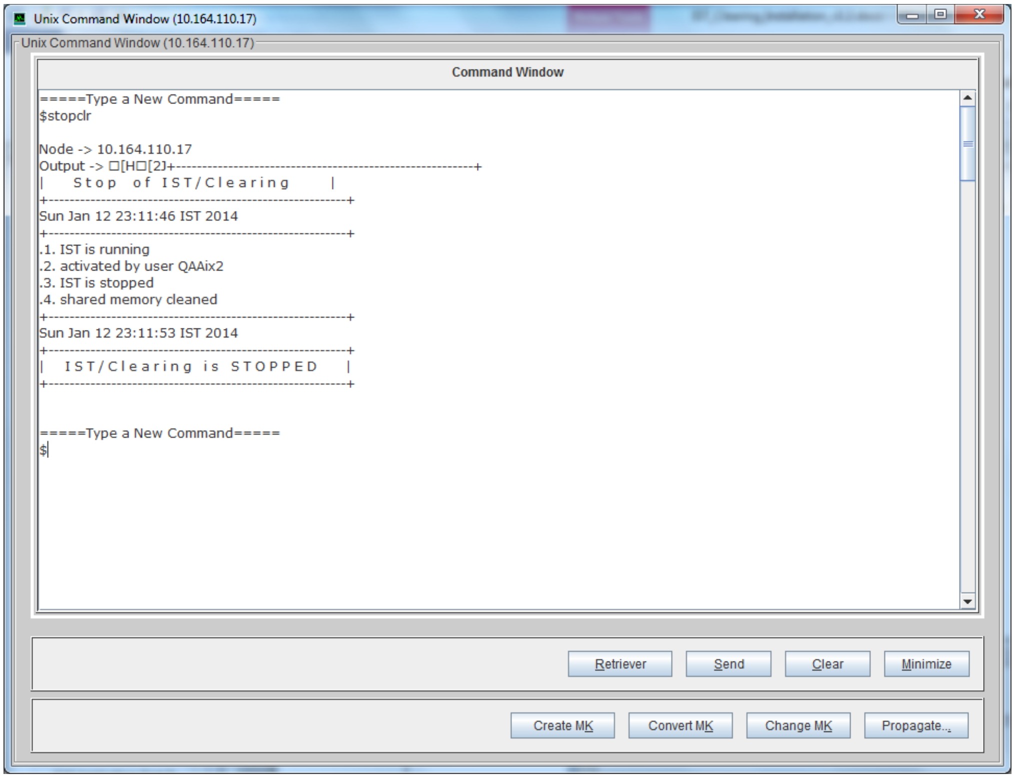
Event Queue Message Queue

Figure 40: IST Monitor – Task and Mailbox Display

9. Clicking the Refresh buttons will display the list of Tasks and Mailboxes once the system is running.

To stop the IST/Clearing processes:

1. Click Maximize to maximize the Command Window



```
=====Type a New Command=====
$stopclr

Node -> 10.164.110.17
Output -> □[H□[2J+--------------------------------------------------------+
|    Stop  of IST/Clearing     |
+--------------------------------------------------+
Sun Jan 12 23:11:46 IST 2014
+--------------------------------------------------+
.1. IST is running
.2. activated by user QAAix2
.3. IST is stopped
.4. shared memory cleaned
+--------------------------------------------------+
Sun Jan 12 23:11:53 IST 2014
+--------------------------------------------------+
|   IST/Clearing is STOPPED   |
+--------------------------------------------------+


=====Type a New Command=====
$
```

Figure 41: Stop Clearing

2. Enter stopclr in the Command Window
3. Click Send

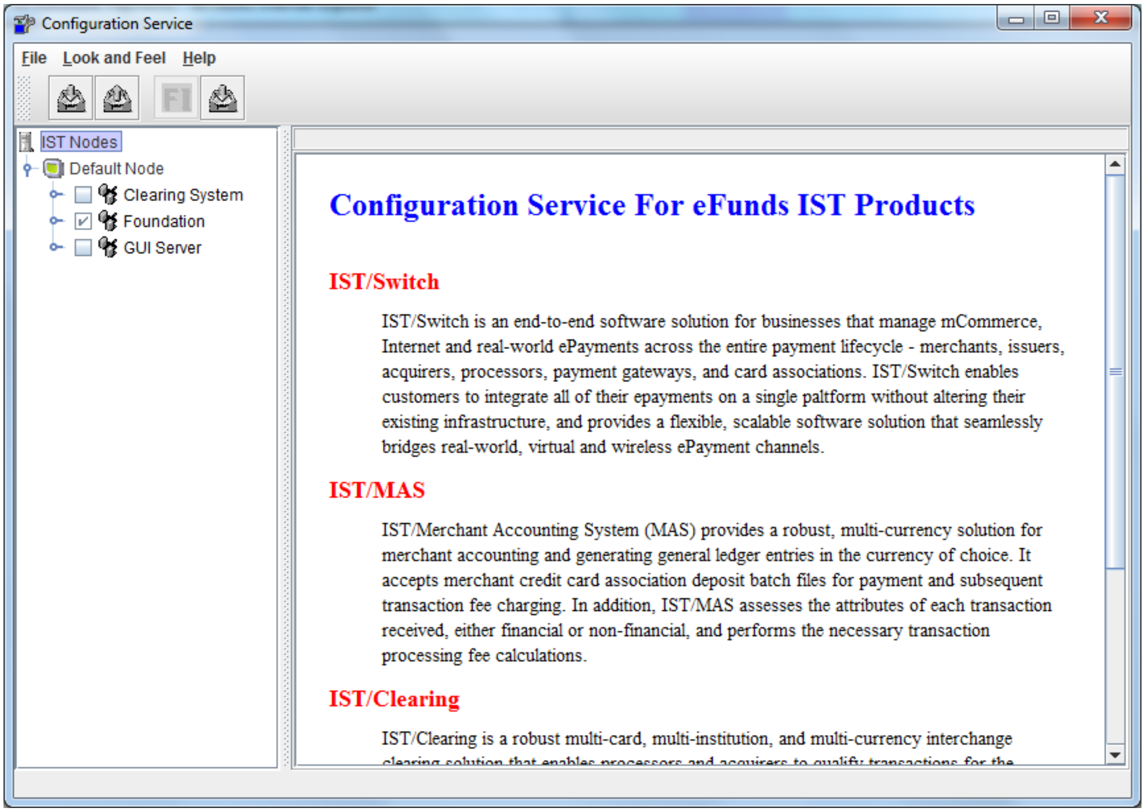
Set Up The Configuration Service

The Configuration Service screens are used to configure MAS parameters.

The configuration parameters that were setup during IST/Clearing installation will be reflected in the Configuration Service. The Configuration files used by Configuration Service are imported from the IST/Clearing node using the steps in the **Error! Reference source not found.** section above.

To set up the configuration service:

1. Select Configuration Service on the Application Select page to display the Configuration Service window.



Configuration Service For eFunds IST Products

IST/Switch

IST/Switch is an end-to-end software solution for businesses that manage mCommerce, Internet and real-world ePayments across the entire payment lifecycle - merchants, issuers, acquirers, processors, payment gateways, and card associations. IST/Switch enables customers to integrate all of their epayments on a single paltform without altering their existing infrastructure, and provides a flexible, scalable software solution that seamlessly bridges real-world, virtual and wireless ePayment channels.

IST/MAS

IST/Merchant Accounting System (MAS) provides a robust, multi-currency solution for merchant accounting and generating general ledger entries in the currency of choice. It accepts merchant credit card association deposit batch files for payment and subsequent transaction fee charging. In addition, IST/MAS assesses the attributes of each transaction received, either financial or non-financial, and performs the necessary transaction processing fee calculations.

IST/Clearing

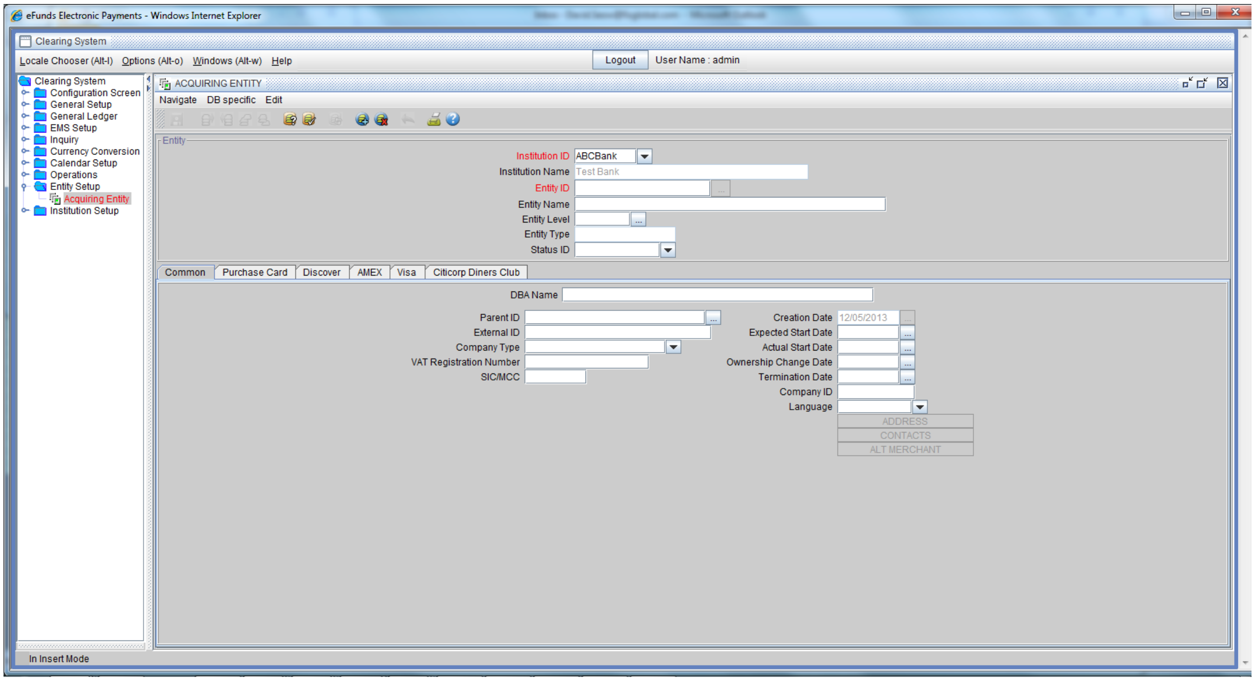
IST/Clearing is a robust multi-card, multi-institution, and multi-currency interchange clearing solution that enables processors and acquirers to qualify transactions for the

Figure 42: Configuration Service screen

2. Setup the parameters as required in the Default Node.
3. Click File Create New Node to create a mas node profile if required.

For details on setup and administration refer to the IST/Clearing Administration Guide.

Clearing Application



User Name : admin

Institution ID: ABCBank
Institution Name: Test Bank
Entity ID:
Entity Name:
Entity Level:
Entity Type:
Status ID:

DBA Name:

Parent ID:
External ID:
Company Type:
VAT Registration Number:
SIC/MCC:

Creation Date: 12/05/2013
Expected Start Date:
Actual Start Date:
Ownership Change Date:
Termination Date:
Company ID:
Language:

Figure 43: IST/Clearing - Sample Screen

For details about the screens refer the business and administration guides.

.profile" Entries

```
test -n "$TERM" || eval `tset -s -Q -m ':?vt220'`

# Set the location of the HOME directory e.g.
export HOME=/apps/clearing
ENV=$HOME/.kshrc; export ENV    # To set up korn shell (ksh)

# Add personal setup here.

# Set the Java path
export JAVA_HOME=/usr/java6

# For Oracle:
export ORACLE_HOME=/oracle/app/oracle/product/11.2.0/client_1
export TNS_ADMIN=$HOME/tns_admin


# ORACLE setup for language character set
# Add these entries only if a non-default character set is required.
# Change NLS_LANG as required

#If Database is UTF8
export NLS_LANG=AMERICAN_AMERICA.AL32UTF8

export NLS_NUMERIC_CHARACTERS=".,"


# For DB2:
# Execute the db2 profile. Change the path depending on your DB2 installation.
. /apps/db2/db2inst1/sqllib/db2profile

# Add entries to library paths as required.
# For Oracle add the path to the lib or lib32 for 11g or 10g # respectively.

# Solaris - Oracle 11g
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH: $ORACLE_HOME/lib: <library_path>

# Solaris - Oracle 10g
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH: $ORACLE_HOME/lib32: <library_path>

# HPUX - Oracle 11g
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib:<other_library_path>

# HPUX - Oracle 10g
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/ lib32:<other_library_path>

# AIX - Oracle 11g
export LIBPATH=$LIBPATH:$ORACLE_HOME/lib:<other_library_path>
```

```
# AIX - Oracle 10g
export LIBPATH=$LIBPATH:$ORACLE_HOME/lib32:<library_path>


#Set the PATH
export PATH=$HOME/tgz:$HOME/bin:$JAVA_HOME/bin:$ORACLE_HOME/bin:$PATH


export FCEDIT=vi
stty intr ^C kill ^U erase ^H echoe echok
umask 022
export CMMT_DUMP_MSG=1
export OBJECT_MODE=64
export TNS_ADMIN=$HOME/tns_admin

# Add the following for GUI environment
export JAVAGUI=$OPRODUCT_ROOT/javagui

# Set the OS environment variable required to set the syslog filename for
# IST Monitor
# For Solaris set <OS_IDENTIFIER> = SOLARIS
# For HP UX set <OS_IDENTIFIER> = HP_UX
# For AIX set <OS_IDENTIFIER> = AIX
export OS=<OS_IDENTIFIER>

# Set ISTMBREGION to a unique value for each product running in the same system.
# This is to override the default value of "1" set in profile<install_date>.
export ISTMBREGION=2

# If AIX include the EXTSHM environment variable to enable use of extended shared memory model.
export EXTSHM=MSEG

export UA_BASE=$OSITE_ROOT/cfg/ua
export TVSRepositoryName=$OPRODUCT_ROOT/cfg/TVSRepository

# Set the environment Variable for the Apache server used in the XML API module.
export WEBSERVER_HOME=/QAAix2/server/apache2
export PATH=$PATH:$WEBSERVER_HOME/bin

. $HOME/profile
cd $HOME

alias pdir='cd $OPRODUCT_ROOT'
alias debug='cd $OLOGDIR/debug'
alias site='cd $OSITE_ROOT'
alias cfg='cd $OSITE_ROOT/cfg'
alias jgui='cd $OPRODUCT_ROOT/javagui'
alias pd='cd $OSITE_ROOT/certdata/pdeploy'
alias cda='cd $OSITE_ROOT/certdata'

# For GUI
alias gp='cd $PRODUCT_ROOT/istgui/ist/app’
```

Database Tables

Assign Database Roles - Oracle

The database roles must be created before the IST tables. The following can be used to create roles and assigning grants to the service accounts:

```
create role cl_app_role;
create role cl_app_read_only_role;
create role clent_app_role;
create role clent_app_read_only_role;
create role cltok_app_role;
create role cltok_app_read_only_role;
create role clklc_app_role;
create role clklc_app_read_only_role;

grant cl_app_role, cl_app_read_only_role to cl_app;
alter user cl_app default role cl_app_role, cl_app_read_only_role;

grant clent_app_role, clent_app_read_only_role to clent_app;
alter user  clent_app default role clent_app_role, clent_app_read_only_role;

grant cltok_app_role, cltok_app_read_only_role to cltok_app;
alter user  cltok_app default role cltok_app_role, cltok_app_read_only_role;

grant clklc_app_role, clklc_app_read_only_role to clklc_app;
alter user clklc_app  default role clklc_app_role, clklc_app_read_only_role;

grant cl_app_read_only_role,  clent_app_read_only_role to <individual-user>;
alter user <individual-user> default role cl_app_read_only_role,  clent_app_read_only_role;
```

Assign Database Roles – DB2

In DB2 you must first create the roles before running the grants, otherwise the users will not get the correct privileges. The set of statements below is an sample set to setup a DB2 database for Clearing.

```
create database clearing on /istsw7/db2data dbpath on /u00/db2data/clearing restrictive;
connect to clearing;
create bufferpool bp32k size 100 automatic pagesize 32k;
create tablespace ts32k pagesize 32k bufferpool bp32k;
create schema authorization clentown;
create schema authorization cltokown;
create schema authorization clklcown;
create schema authorization cl_own;

create role cl_app_role;
create role cl_app_read_only_role;
create role clentapp_role;
create role clentapp_read_only_role;
create role cltokapp_role;
create role cltokapp_read_only_role;
create role clklcapp_role;
create role clklcapp_read_only_role;
create role clbasic_role;

grant connect on database to role clbasic_role;

grant usage on workload SYSDEFAULTUSERWORKLOAD to role clbasic_role;
grant use of tablespace userspace1 to role clbasic_role;
```

```
--
grant EXECUTE on package NULLID.SQLC2J23 to role clbasic_role;
grant EXECUTE on package NULLID.SQLC2J25 to role clbasic_role;
grant EXECUTE on package NULLID.SQLC3J22 to role clbasic_role;
grant EXECUTE on package NULLID.SQLC4J22 to role clbasic_role;
grant EXECUTE on package NULLID.SQLC5J22 to role clbasic_role;
grant EXECUTE on package NULLID.SQLC6J22 to role clbasic_role;
-- for CLI
grant EXECUTE on package NULLID.SYSSH100 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH101 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH102 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH200 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH201 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH202 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH300 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH301 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH302 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH400 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH401 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSH402 to role clbasic_role;
grant EXECUTE on package NULLID.SYSSN300 to role clbasic_role;

grant execute on package nullid.SYSSN100 to role clbasic_role;
grant execute on package nullid.SYSSN101 to role clbasic_role;
grant execute on package nullid.SYSSN102 to role clbasic_role;
grant execute on package nullid.SYSSN200 to role clbasic_role;
grant execute on package nullid.SYSSN201 to role clbasic_role;
grant execute on package nullid.SYSSN202 to role clbasic_role;
grant execute on package nullid.SYSSN300 to role clbasic_role;
grant execute on package nullid.SYSSN301 to role clbasic_role;
grant execute on package nullid.SYSSN302 to role clbasic_role;
grant execute on package nullid.SYSSN400 to role clbasic_role;
grant execute on package nullid.SYSSN401 to role clbasic_role;
grant execute on package nullid.SYSSN402 to role clbasic_role;

grant use of tablespace ts32k to role clbasic_role;

grant createtab on database to clentown, cltokown, clklcown,  cl_own;

grant select on syscat.tables to cl_own, clentown, clklcown,  cltokown;
grant select on syscat.indexes to cl_own, clentown, clklcown,  cltokown;
grant select on syscat.schemata to cl_own, clentown, clklcown,  cltokown;
grant select on syscat.columns to cl_own, clentown, clklcown,  cltokown;
grant select on syscat.indexcoluse to cl_own, clentown, clklcown,  cltokown;
grant select on syscat.tabconst to cl_own, clentown, clklcown,  cltokown;
grant select on syscat.references to cl_own, clentown, clklcown,  cltokown;

grant role clbasic_role to cl_own, clentown, clklcown,  cltokown;

grant role clbasic_role to role cl_app_read_only_role;
grant role clbasic_role to role clentapp_read_only_role;
grant role clbasic_role to role cltokapp_read_only_role;
grant role clbasic_role to role clklcapp_read_only_role;

grant cl_app_role, cl_app_read_only_role to cl_app;
grant clentapp_role, clentapp_read_only_role to clentapp;
grant cltokapp_role, cltokapp_read_only_role to cltokapp;
grant clklcapp_role, clklcapp_read_only_role to clklcapp;
```

Creating Database Tables.

Your DBA may choose to create the database tables manually instead of having them created through the pdeploy tool. The information in this section is used instead of the Create DB Tables option when the DBA chooses to create the database manually.

The scripts below are examples:

a) of the server scripts generated by pdeploy and where to apply each.

b) the set of GUI application scripts and where to apply each.

File	Method A
$OSITE_ROOT/dbutil/dba/ist	
1.1.create_tbls_CLapp_cl.ora	CLown
1.2.create_fkey_CLapp_cl.ora	CLown
1.3.initdata.ora	CLown
1.4.sysdata.ora	CLown
1.5.instdata.ora	CLown
1.6.testdata.ora	CLown
1.7.create_exec_CLapp_cl.ora	CLown; add privileges to CLapp_role
1.7.create_modi_CLapp_cl.ora	CLown; add privileges to CLapp_role
1.7.create_read_CLapp_cl.ora	CLown; add privileges to CLapp_read_only_role
1.7.create_syno_CLapp_cl.ora	CLapp
$OSITE_ROOT/dbutil/dba/ent	
2.1.create_tbls_clentapp_ent.ora	CLown
2.2.create_fkey_clentapp_ent.ora	CLown
2.3.entdata.ora	CLown
2.7.create_exec_clentapp_ent.ora	CLown; add privileges to clentapp_role
2.7.create_modi_clentapp_ent.ora	CLown; add privileges to clentapp_role
2.7.create_read_clentapp_ent.ora	CLown ; add privileges to clentapp_read_only_role
2.7.create_syno_clentapp_ent.ora	CLown

~/istgui/prot_dir/sql

Database Script	Create In
GUI_READ_MODI_ENT.sql	clentown
GUI_READ_MODI_IST.sql	CLown
GUI_SYNO_ENT.sql	clentapp
GUI_SYNO_IST.sql	CLapp
GUI_TABLES_ENT_DDL.db2	clentown
GUI_TABLES_ENT_DDL.ora	clentown
GUI_TABLES_IST_DDL.db2	CLown
GUI_TABLES_IST_DDL.ora	CLown
IST_GUI_TABLE_CLC.sql	CLown
IST_GUI_TABLE_ENT.sql	clentown
IST_ENT_O.sql	clentown
IST_ENT_SUBSYS_CFGSVC.sql	clentown
IST_ENT_SUBSYS_CLC_CUP_UPD.sql	clentown
IST_ENT_SUBSYS_CLC.sql	clentown
IST_ENT_SUBSYS_ENT.sql	clentown
IST_ENT_SUBSYS_ISTMON.sql	clentown

Service Account Roles

Module	Service Account	Role
Clearing	CLapp	CLapp_role, CLapp_read_only_role
Authentication and Entitlement	clentapp	clentapp_role, clentapp_read_only_role
Tokenizer	cltokapp	cltokapp_role, cltokapp_read_only_role
Key Lifecycle Management	clklcapp	clklcapp_role, clklcapp_read_only_role

Glossary

Keyword	Description
apm.src	Used to configure the list of processes managed by apm.
Authentication and Entitlement	Referred to as entitlement, this is the IST processes "oassrv" and "oentsrv" used to provide user security for the IST suite of products.
build_env	The installation tool used to create the product environment from a set of release files, supplied in “tar.gz” format.
Database	In IST terms this is the repository where the product tables are maintained.
GUI Application	The Graphical User Interface used with an IST product.
istparam.cfg	The configuration file used to specify server runtime parameters for an IST product.
Java Application Server	This is synonymous with the term web server.
Mailbox region	A region of memory where an instance of an IST/Foundation runs.
Node Agent	The term used to refer to the administrative process "istnodeagt". This process is required for configuration and monitoring for an IST product.
pdeploy	A configuration install tool used to perform initial server configuration setup and IST GUI application deployment after installation by build_env.
Product server	A set of processes used to run an IST product.
Release Repository	Directory where IST releases are stored. Typically separate directories are used to store server and GUI releases.
Schema	In IST terms this is synonymous with database and service account.
Clearing	The IST product that provides transaction clearing capability.
tgz	The name of the directory required by build_env and which is used as the store for IST product releases. This can be a logical directory on an accessible file system.

Statement of Confidentiality

This document is an unpublished work containing confidential and trade secret information of FIS and is protected by federal copyright law. It may not be copied or distributed in any form or medium, disclosed to third parties, or used in any manner not authorized in said license agreement except with prior authorization from FIS.

Trademarks

All other trademarks are the property of their owners.

Company, product and service names used by FIS within, or supplied with this document, may be trademarks or service marks of other persons or entities.

Copyright