

IST/Clearing Product: Installation Guide

Version 1.0

Revisions

|  |  |  |  |
| --- | --- | --- | --- |
| Release/Version/Date | Release Description | Sections Edited | Brief Revision Description |
| Release 1.0  Version 1.1  February 2014 |  |  | Initial Release of this Version. |

# Table of Contents

[Table of Contents 3](#_Toc379577616)

[Table of Figures 6](#_Toc379577617)

[Introduction 7](#_Toc379577618)

[Purpose 7](#_Toc379577619)

[Audience 7](#_Toc379577620)

[Prepare for Install 8](#_Toc379577621)

[Product Topology 9](#_Toc379577622)

[System Requirements 10](#_Toc379577623)

[Minimum Requirements 10](#_Toc379577624)

[Database System 10](#_Toc379577625)

[Web Server System 10](#_Toc379577626)

[Client PC Minimum Requirements: 10](#_Toc379577627)

[System Topology 11](#_Toc379577628)

[Clearing Installation and Runtime Environment 11](#_Toc379577629)

[Nodes 11](#_Toc379577630)

[Ports 12](#_Toc379577631)

[istnodeagt.cfg Ports 12](#_Toc379577632)

[File System 12](#_Toc379577633)

[Database Parameters 13](#_Toc379577634)

[Oracle Parameters 13](#_Toc379577635)

[DB2 Parameters 13](#_Toc379577636)

[Database Model 14](#_Toc379577637)

[Owner Service Accounts 15](#_Toc379577638)

[Database Roles 16](#_Toc379577639)

[Service Accounts and Role Assignment 17](#_Toc379577640)

[DB2 Users 18](#_Toc379577641)

[Assign Database Roles - Oracle 18](#_Toc379577642)

[Assign Database Roles – DB2 19](#_Toc379577643)

[Validate Release Files 20](#_Toc379577644)

[FIS Secure Code Delivery and Validation 21](#_Toc379577645)

[Installation and Runtime Directories, and Release Repository 22](#_Toc379577646)

[Administration, Release Repository and Runtime Directories 23](#_Toc379577647)

[Create Admin Accounts and the Application Runtime Directory 23](#_Toc379577648)

[Create GUI Application Administrator and GUI Deployment Directory 24](#_Toc379577649)

[IST System Installation Procedure 25](#_Toc379577650)

[Installing the IST/Clearing System 27](#_Toc379577651)

[Build a Node’s Runtime Environment 27](#_Toc379577652)

[Installing Multiple Times within a Day 32](#_Toc379577653)

[Service Packs, Release Candidates and Patches 32](#_Toc379577654)

[Configuring Nodes and Creating the Database Tables 34](#_Toc379577655)

[Configuring the Clearing Node and Creating the Database Tables 34](#_Toc379577656)

[Clearing node setup 35](#_Toc379577657)

[Enabling SSL for the IST Process 60](#_Toc379577658)

[Generate Node Certificates 60](#_Toc379577659)

[Import Certificates 65](#_Toc379577660)

[GUI Application Back-end SSL 65](#_Toc379577661)

[Setup the Runtime Environments 67](#_Toc379577662)

[Applying Upgrade Scripts 67](#_Toc379577663)

[Table Upgrade Scripts 67](#_Toc379577664)

[Database Record Scripts 68](#_Toc379577665)

[Back-out an Upgrade 69](#_Toc379577666)

[Install the GUI Application 71](#_Toc379577667)

[Extract the Contents of the Release File 71](#_Toc379577668)

[Build GUI Application Installation Environment 72](#_Toc379577669)

[GUI Application Database Tasks 76](#_Toc379577670)

[Installing the GUI Application 77](#_Toc379577671)

[IBM Websphere 7 77](#_Toc379577672)

[Refer to the IST GUI Application Installation: IBM Websphere guide for details 77](#_Toc379577673)

[.Oracle WebLogic 12c 77](#_Toc379577674)

[Tomcat 7 77](#_Toc379577675)

[Enabling SSL 78](#_Toc379577676)

[Java Application Server 79](#_Toc379577677)

[Initializing the System 81](#_Toc379577678)

[Start the Administration Processes 82](#_Toc379577679)

[Starting the Administrative Processes 82](#_Toc379577680)

[Stopping the Administrative Processes 82](#_Toc379577681)

[GUI Application First Time Login 82](#_Toc379577682)

[Add a clearing Type Node in IST Control 89](#_Toc379577683)

[Master Key Management 90](#_Toc379577684)

[Start Clearing 92](#_Toc379577685)

[Import XML Configuration Files 94](#_Toc379577686)

[Set Up The Configuration Service 95](#_Toc379577687)

[.profile" Entries 96](#_Toc379577688)

[Database Tables 98](#_Toc379577689)

[Assign Database Roles - Oracle 98](#_Toc379577690)

[Assign Database Roles – DB2 98](#_Toc379577691)

[Service Account Roles 101](#_Toc379577692)

[Glossary 102](#_Toc379577693)

[Initializing the System 103](#_Toc379577694)

[Start the Administration Processes 104](#_Toc379577695)

[Starting the Administrative Processes 104](#_Toc379577696)

[Stopping the Administrative Processes 104](#_Toc379577697)

[GUI Application First Time Login 104](#_Toc379577698)

[Add a clearing Type Node in IST Control 111](#_Toc379577699)

[Master Key Setup 112](#_Toc379577700)

[Start IST/Clearing 114](#_Toc379577701)

[Set Up The Configuration Service 117](#_Toc379577702)

[Clearing Application 118](#_Toc379577703)

[Statement of Confidentiality 119](#_Toc379577704)

# Table of Figures

[Figure 1: Installation Tasks 8](#_Toc379578293)

[Figure 2: Simple IST/Clearing System 9](#_Toc379578294)

[Figure 3: System Topology Sample Diagram 11](#_Toc379578295)

[Figure 4: Database Service Accounts (Schemas) 15](#_Toc379578296)

[Figure 5: Installation and Runtime Directories 22](#_Toc379578297)

[Figure 6: Install Nodes 27](#_Toc379578298)

[Figure 7 Build\_env = Files Selected for Installation 29](#_Toc379578299)

[Figure 8: Build\_env Installation In Progress 30](#_Toc379578300)

[Figure 9: Generate 61](#_Toc379578301)

[Figure 10: Organization Name 61](#_Toc379578302)

[Figure 11: File Suffix 62](#_Toc379578303)

[Figure 12: Keystore Password (a) 62](#_Toc379578304)

[Figure 13: Keystore Password Confirmation 63](#_Toc379578305)

[Figure 14: Keystore Password (b) 63](#_Toc379578306)

[Figure 15: Keystore Password (c) 64](#_Toc379578307)

[Figure 16: Import Certificate 66](#_Toc379578308)

[Figure 17: Install GUI Application 71](#_Toc379578309)

[Figure 18: Directory Structure for Staging GUI Releases 72](#_Toc379578310)

[Figure 19: IST-GUI Application Directory 73](#_Toc379578311)

[Figure 20: Files Selected for Installation 74](#_Toc379578312)

[Figure 21: Extracting Files to Directory 75](#_Toc379578313)

[Figure 22: Enabling SSL Option 78](#_Toc379578314)

[Figure 23: Enabling SSL 79](#_Toc379578315)

[Figure 24: IST Clearing SSL Enabled Process 80](#_Toc379578316)

[Figure 25: Initializing The System 81](#_Toc379578317)

[Figure 26: IST/Clearing Login 83](#_Toc379578318)

[Figure 27: Password Expired Page 84](#_Toc379578319)

[Figure 28: Password Change Successfully 85](#_Toc379578320)

[Figure 29: IST/Clearing Application Menu 86](#_Toc379578321)

[Figure 30: User Authentication Screen 87](#_Toc379578322)

[Figure 31: Generated Password Display 88](#_Toc379578323)

[Figure 32: User Group Screen 88](#_Toc379578324)

[Figure 33: IST Monitor 89](#_Toc379578325)

[Figure 34: IST Monitor- Add Node 90](#_Toc379578326)

[Figure 35: Configuration Service screen 95](#_Toc379578327)

[Figure 27: Initializing The System 103](#_Toc379578328)

[Figure 9: IST Application Login Page 105](#_Toc379578329)

[Figure 28: IST/MAS Login 105](#_Toc379578330)

[Figure 29: Password Expired Page 106](#_Toc379578331)

[Figure 30: Password Change Successfully 107](#_Toc379578332)

[Figure 31: IST/MAS Menu 108](#_Toc379578333)

[Figure 30: User Authentication Screen 109](#_Toc379578334)

[Figure 31: Generated Password Display 110](#_Toc379578335)

[Figure 32: User Group Screen 110](#_Toc379578336)

[Figure 33: IST Monitor 111](#_Toc379578337)

[Figure 34: IST Monitor- Add Node 112](#_Toc379578338)

[Figure 35: Configuration Service screen 117](#_Toc379578339)

# 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:

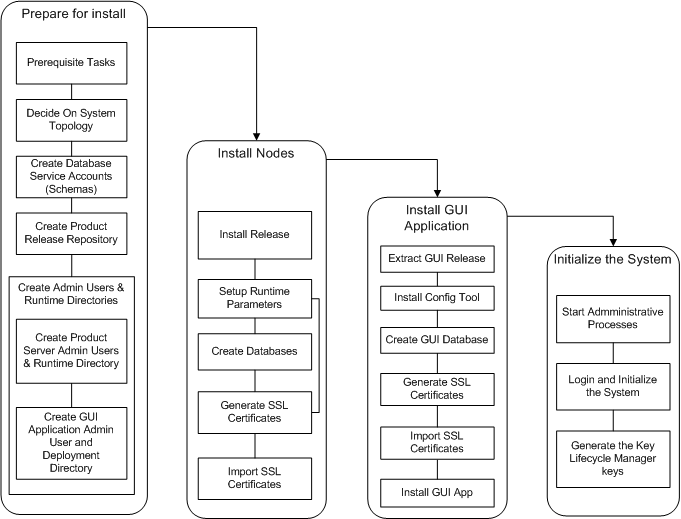


Figure 1: Installation Tasks

## 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 Sun® Solaris 2.10, Linux® LIN-2632-i686-64
* 10 GB of available hard-disk for installation.
* 200 GB for storage of sensitive files and logs.
* Perl Interpreter 5.6 or later.
* Java 7

### Database System

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

* Database (one of the following):
  + Oracle® 11.2
  + DB2 10.1
* 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 Server: IBM® WebSphere® 7, Apache® Tomcat® 7, Oracle® Weblogic 12c or 10.3.6.
* Java 6.
* 10 GB of available hard-disk.
* 10 GB Protected Directory. (For storage of sensitive files).

### Client PC Minimum Requirements:

Processor: Intel® i7 or equivalent;

* Microsoft® Windows® Windows 7®., Windows 8®.
* Web Browser with support for Adobe Flash Player 11 or later: Microsoft® Internet Explorer® 8
* 4GB of RAM.
* 500MB of available hard-disk space.
* Monitor - 1024x768 resolution or higher. A Widescreen is recommended for Monitoring and Control.

## 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](#_Database_Model) 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 each node in the system

|  |  |  |
| --- | --- | --- |
| 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 |
| Gui\_server\_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 |  | api.port |  |  |  |
| Tokenizer | tokenizer |  |  |  |  |

### 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 |

## File System

Files containing configuration and debug information are stored in a Protected Directory. Specify the absolute path to the directory to use to this information for each system in the list.

|  |  |  |
| --- | --- | --- |
| System | Description | Absolute Path |
| Clearing node | Used to store key and truststore files, configuration files containing passwords, debug files and data files. Specify for each node, |  |
| Web Application Server | Used to store key and truststore files, configuration data, protected class files and debug log files. |  |

## Database Parameters

### Oracle Parameters

For Oracle 11, 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" Entries 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](#_Database_Roles)”.
3. Assign roles as indicated in in [Role Assignments table](#_Service_Accounts_and) .



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.

clentown: 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.

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.

Application Service Accounts:

cl\_app: This service account will be used by the Clearing application to access the Clearing tables via a set of synonyms. Roles are assigned to provide select, insert, updated and delete privileges.

clentapp: This service account will be used by the authentication and entitlement processes to connect to the OAS and ENT tables via a set of synonyms. Roles are assigned to provide select, insert, updated and delete privileges.

cltokapp: This service account will be used by the tokenizer process to connect to the TOK tables via a set of synonyms. Roles are assigned to provide select, insert, updated and delete privileges.

clklcapp: This service account will be used by the key life cycle management processes to connect to the KLC tables via a set of synonyms. Roles are assigned to provide select, insert, updated and delete privileges

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.

APP and Individual services accounts must have privileges to create synonyms.

## 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 insert, update, delete on all Clearing tables in CLown.

clentapp\_role: Privileges to insert, update, delete on all authentication and entitlement tables in clentown.

cltokapp\_role: Privileges to insert, update, delete on all tokenizer tables in cltokown.

clklcapp\_role: Privileges to insert, update, delete on all key lifecycle tables in clklcown.

cl\_app\_read\_only\_role: Privileges to select the Clearing product tables created in CLown.

clentapp\_read\_only\_role: Privileges to select entitlement tables created in clentown.

cltokapp\_read\_only\_role: Privileges to select tokenizer tables created in cltokown.

clklcapp\_read\_only\_role: Privileges to select keylifecycle tables created in clklcown.

## 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, clapp\_read\_only\_role |  |
| Authentication and Entitlement | clentapp | clbasic\_role, clentapp\_role, clentapp\_read\_only\_role |  |
| Tokenizer | cltokapp | clbasic\_role, cltokapp\_role, cltokapp\_read\_only\_role |  |
| Key Lifecycle Management | clklcapp | clbasic\_role, clklcapp\_role, clklcapp\_read\_only\_role |  |
| Individual |  | clbasic\_role, cl\_app\_read\_only\_role, clentapp\_read\_only\_role |  |

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

### 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 |
| clentown | clearing |
| cltokown | clearing |
| clklcown | clearing |
| clt21own | clearing |
| cl\_app | clearing |
| clent\_app | clearing |
| cltok\_app | clearing |
| clklc\_app | clearing |
| clt21\_app | 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 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, clt21\_app\_read\_only\_role to <individual-user>;

alter user <individual-user> default role cl\_app\_read\_only\_role, clent\_app\_read\_only\_role, clt21\_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 clt21own;

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 clt21app\_role;

create role clt21app\_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.SQLC2J25 to role clbasic\_role;

grant EXECUTE on package NULLID.SQLC3J24 to role clbasic\_role;

grant EXECUTE on package NULLID.SQLC4J24 to role clbasic\_role;

grant EXECUTE on package NULLID.SQLC5J24 to role clbasic\_role;

grant EXECUTE on package NULLID.SQLC6J24 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, clt21own, cl\_own;

grant select on syscat.tables to cl\_own, clentown, clklcown, clt21own, cltokown;

grant select on syscat.indexes to cl\_own, clentown, clklcown, clt21own, cltokown;

grant select on syscat.schemata to cl\_own, clentown, clklcown, clt21own, cltokown;

grant select on syscat.columns to cl\_own, clentown, clklcown, clt21own, cltokown;

grant select on syscat.indexcoluse to cl\_own, clentown, clklcown, clt21own, cltokown;

grant select on syscat.tabconst to cl\_own, clentown, clklcown, clt21own, cltokown;

grant select on syscat.references to cl\_own, clentown, clklcown, clt21own, cltokown;

grant role clbasic\_role to cl\_own, clentown, clklcown, clt21own, 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 clt21app\_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 clt21app\_role, clt21app\_read\_only\_role to clt21app;

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:***

* CL\_2.4.0.00.04\_AIX-710\_201401120000001.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 Microsoft Windows or 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:
   1. On Windows
3. Open a cmd window and change directory to the location where the release is stored.
4. 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.

* 1. On UNIX
  2. 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\_2.4.0.00.04\_AIX-710\_201401120000001.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\_2.4.0.00.04\_AIX-710\_201401120000001.tar.gz.rcc

Decryption to CL\_2.4.0.00.04\_AIX-710\_201401120000001.tar.gz complete Validate processing completed successfully

1. 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\_7.7.0.00.04\_AIX-710\_BASE.tar.gz
* ./tgz/FO\_7.7.0.00.04\_AIX-710\_ORA-112.tar.gz
* ./tgz/CL\_2.4.0.00.04\_AIX-710\_BASE.tar.gz

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.



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)

1. 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

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

gzip -dc <decrypted\_file> | tar -xvf -

The release gzipped tar files and build\_env are extracted to $HOME/tgz.

## 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.

1. 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

1. Edit the user's ".profile" and add entries as described [in“.profile" Entries”](#_.profile"_Entries)
2. Login to the system and sudo to the generic guiadmin user.
3. Change directory to $HOME, "/apps/guiadmin/iststage" in the example.
4. Copy the decrypted file(s) obtained from the FISValidate procedure to the home directory, $HOME.
5. 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

Two tools are provided in the release: build\_env 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. For details on build\_env, refer to [“BUILD ENV”.](#_Build_a_Node’s)

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 admin 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 “Enabling SSL for the IST Process ” and the Setup GUI Application Back-end SSL in the respective IST GUI Application Installation Guide that describe the steps to generate the keystores and certificates required to enable SSL between the IST processes.
4. Follow the steps in “Initializing the System” 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:

* Creating tables and roles
* Creating Synonyms in each service account.

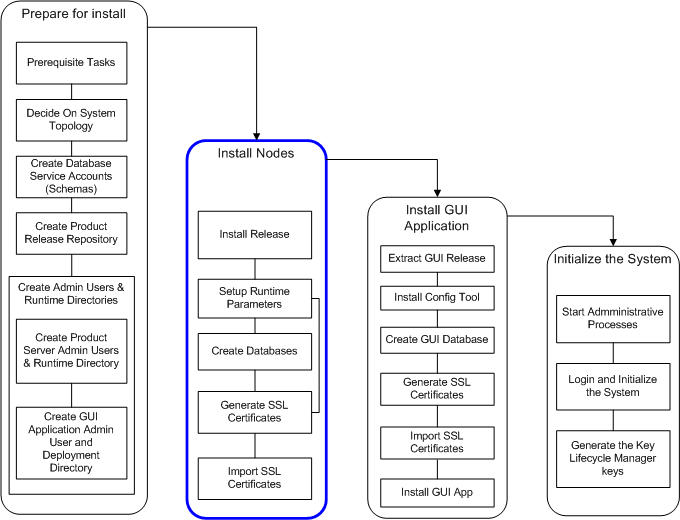


Figure 6: Install Nodes

## 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. 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 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.  In such cases contact support to clarify any doubts as to the com­patibility of the release. |
|  |  |

1. 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". |
|  |  |

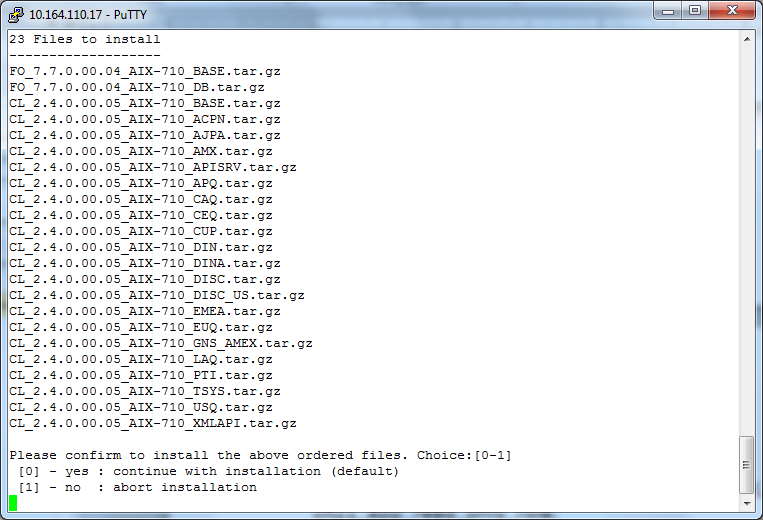


Figure 7 Build\_env = Files Selected for Installation

Build\_env displays a list of all selected packages selected for installation.

1. Select option 0 to continue installing or option 1 to abort the installation.

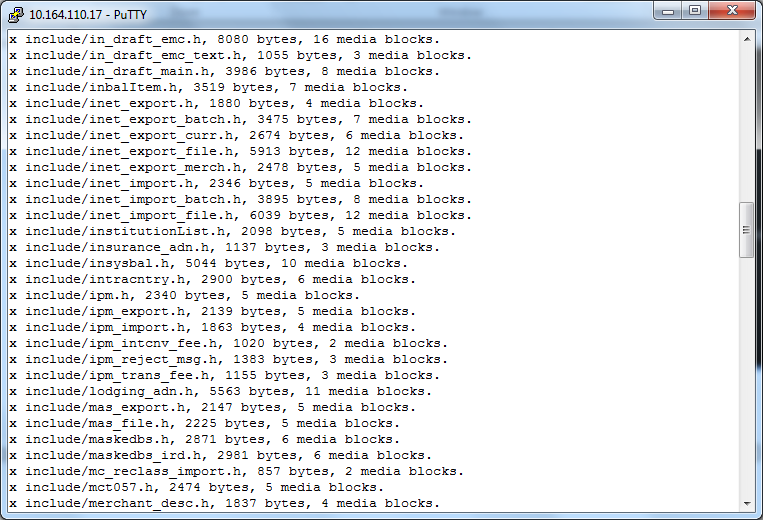


Figure 8: Build\_env Installation In Progress

1. 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.
2. Select Option 1

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

INFO: Skipped run test

INFO: Version 1.6

INFO: OsString=[AIX-710]

   = = = = = = = = = = = = = = = = = = = = = = = = = = = = =

   = = =                                               = = =

   = = =                 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-AIX-32.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-AIX-32.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 SHA1 (s1t-AIX-32.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-AIX-32.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

INFO: Installed 0 items(s)

Program Completed

For ecample 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:

1. 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: profile20140112

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.

1. 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:*** pdir20140112

This directory contains the installed product.

1. An installation log file, build\_env.log, is created and updated on subsequent installations.
2. Edit the admin user’s profile and change the pdir<date> to the newly ceated one above to ensure it is executed in next login.

## 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 pdir20140112 and you reinstall, pdir20140112 is renamed to pdir20140112\_1

The new installation will be created in pdir20140112.

|  |  |
| --- | --- |
| **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 profile<install\_date> in the user profile. |
|  |  |

## 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 can 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 5. Apply DB Tables Upgrade Script and/or Option 6. Apply DB Records Upgrade Script in each installation module. Alternatively a database administrator may apply the scripts.

The CL\_SUP 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 v1.154

Product Directory: /apps/clearing/pdir20140112 (240)

Install Server

+----------------------------------------+

| 0. Install Product |

| 1. Install Entitlement |

| 2. Install Tokenizer |

| 3. Install Key Life Cycle |

| 4. Enable SSL |

+----------------------------------------+

### Clearing node setup

In each of the options (0-3) steps 0, 1, 2, 3, and 7 are required to create the database tables for each of the four schemas to be created, and to configure the initial system parameters.

1. 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 v1.154

Product Directory: /apps/clearing/pdir20140112 (240)

Install Product

+----------------------------------------+

| 0. Setup System Parameters |

| 1. Apply System Parameters |

| 2. Prepare DB Scripts |

| 3. Create DB Tables |

| 4. Undo Create DB Tables |

| 5. Create DB Synonym |

| 6. Create DB Grant |

| 7. Insert DB System Records |

| 8. Insert DB Inst Base Records |

| 9. Insert DB Test Records |

|10. Apply DB Tables Upgrade Script |

|11. Apply DB Records Upgrade Script |

+----------------------------------------+

1. Select 0 Setup System Parameters

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

\_SYSTEM\_VARIABLES

Product Directory: /apps/clearing/pdir20140112 (240)

Product\_name [clearing ] Mb\_current\_node [clrnode ]

Database\_vendor [oracle ] Database\_name [padss ]

Database\_user [cl\_app ]

Database\_password [\*\*\*\*\* ]

Confirm\_db\_pwd [\*\*\*\*\* ]

Schema\_name [CL\_APP ]

Owner\_dbuser [clown ]

Owner\_dbpassword [\*\*\*\*\* ]

Owner\_dbpassword\_confirm [\*\*\*\*\* ]

Database\_tns\_name [PADSSHP ]

Tablespace [ ]

Index\_tablespace [ ]

Clob\_tablespace [ ]

Institution\_id [1 ]

Inst\_type [MAIN\_INST ]

Inst\_name [FIRST INSTITUTION ]

Inst\_curr\_code [840 ] System\_cntry\_code [840 ]

Protected\_directory [/apps/clearing/ENC

Export\_import\_pan\_in\_clear [y ]

Xml\_service\_host [10.164.110.17 ]

Xml\_service\_port [3300 ] Xml\_service\_ssl\_port [3301 ]

Xml\_enable\_auth [y ] Xml\_enable\_ent [y ]

Xml\_enable\_ssl [y ] Xml\_use\_ssl [y ]

Guiserver\_port [9991 ] Nodeagt\_msg\_port [9992 ]

Nodeagt\_ctrl\_port [9993 ] Nodeagt\_msg\_timeout [25000 ]

Nodeagt\_otracelevel [INFO ]

Nodeagt\_root\_trace\_level [WARNING ] Nodeagt\_use\_ssl [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 [n ]

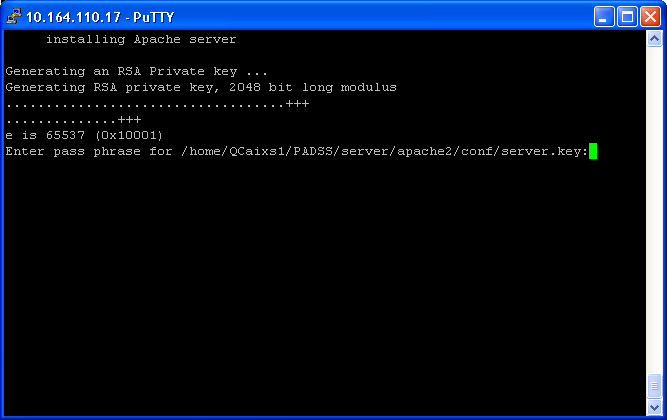
|  |  |
| --- | --- |
| Parameter | Description |
| Product\_name | The ID of the product that is to be configured. It is used to specify the server application to install. For a Clearing node set this to “clearing”. |
| Database\_vendor | The database vendor type:   * For Oracle enter: oracle * For 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.  Institution IDs 01 through 09 are reserved IDs and should not be used during deployment. |
| Inst\_type | The institution’s type:  MAIN\_INST — Main institution. There should only be one institution of this 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\_ssl\_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\_ssl\_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\_ssl | Indicates whether or not SSL 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 SSL certificate.  y = enable SSL.  n = disable SSL |
| Xml\_use\_ssl |  |
| Support\_unicode | An indicator specifying whether or not the unicode specific script is to be applied during installation.  y  n |
| Short\_db\_names | Whether or not shortnames should be used during database creation. |
| 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\_ssl | Indicates whether or not to enable SSL 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). |

1. Select 1. Apply System Parameters

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

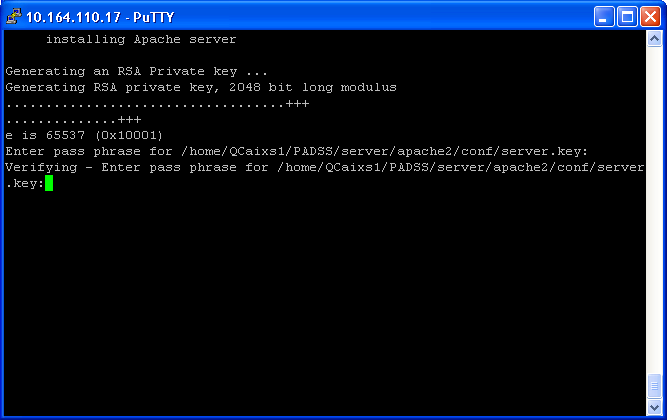
Istparam.cfg is created if one does not yet exist and the parameters dbm.dbuserid and dbm.dbpassword are updated with the database user and password respectively.

Apache2 installation should be done as below:



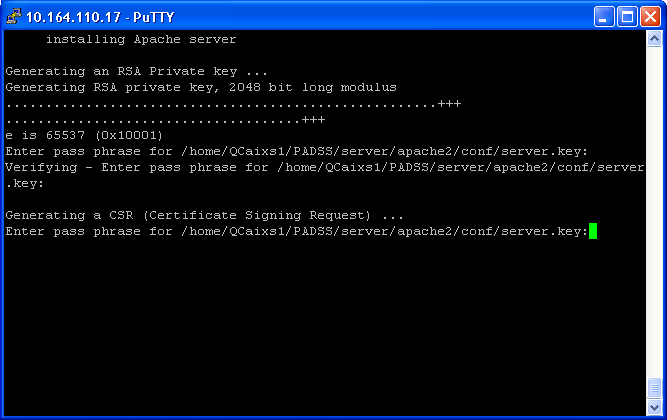
Enter pass phrase for /home/QCaixs1/PADSS/server/apache2/conf/server.key:

Give the passphrase key here and press enter.



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

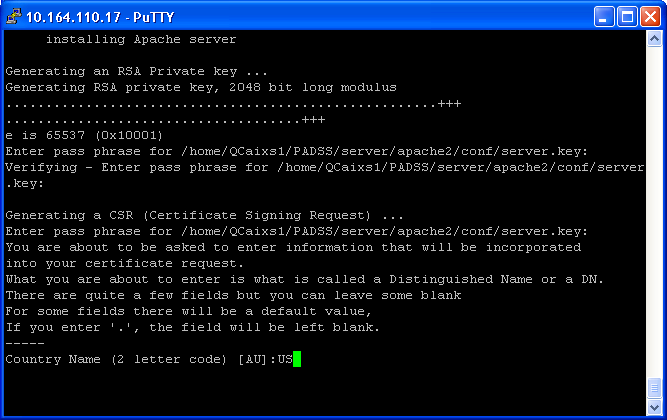
Confirm the Passphrase key which is entered in the previous screen. both should match.



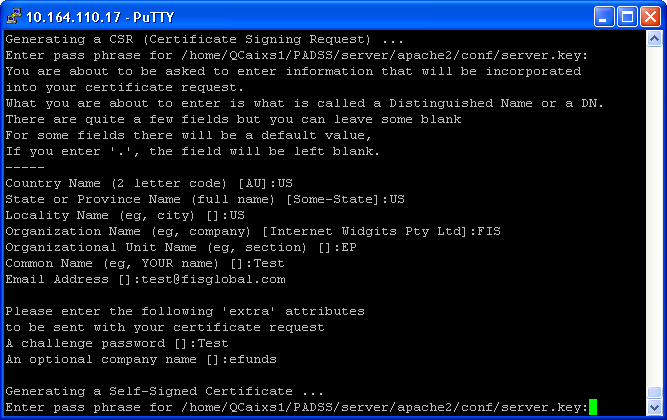
Generating a CSR (Certificate Signing Request) ...

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.



Country Name (2 letter code) [AU]:



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 4c through 4f. Otherwise go to step 4g.

1. 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

DONE creating additional configuration files

Scripts are generated for application to the CLown service account entered in Owner\_dbuser.

1. 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

Do you want to backup Product DB? (y/n) n

You are about to apply changes to the database.

Do you want to continue? (y/n) y

The table creation scripts are applied to the service account entered in Owner\_dbuser

1. Select 11. Create DB Synonym

This option is used to create synonyms in the CLapp account.

1. Select 10. 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

1. Select 7. 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

inserting initdata records

1. Select 8. 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

inserting instdata records

1. Press Esc twice to return to the Server Installation menu.
2. 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 v1.154

Product Directory: /apps/clearing/pdir20140112 (240)

Install Entitlement

+----------------------------------------+

| 0. Setup System Parameters |

| 1. Apply System Parameters |

| 2. Prepare DB Scripts |

| 3. Create DB Tables |

| 4. Undo Create DB Tables |

| 5. Create DB Synonym |

| 6. Create DB Grant |

| 7. Insert DB System Records |

| 8. Apply DB Tables Upgrade Script |

| 9. 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/Append DB Tables | Apply the table creation scripts prepared in option 3 |
| Undo Create/Append | Undo the changes applied in option 4. Applicable only if backup DB Tables was selected |
| Create DB Synonym | Creates synonyms in the APP service accounts when Method A is used for the DB standard. Otherwise not applicable. |
| Create DB Grant | Grants permission to roles in the CLown service account when Method A is used for the DB standard. Otherwise not applicable. |
| 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. |
| Insert DB System Records | Insert system records generated in option 3. For example the set of currency codes. |

1. 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: /apps/clearing/pdir20140112 (240)

Ent\_database\_vendor [oracle ]

Ent\_database\_name [padss ]

Ent\_database\_user [clent\_app ]

Ent\_database\_password [\*\*\*\*\* ]

Ent\_confirm\_db\_pwd [\*\*\*\*\* ]

Ent\_schema\_name [CLENTAPP ]

Entown\_dbuser [clentown ]

Entown\_dbpassword [\*\*\*\*\* ]

Entown\_dbpassword\_confirm [\*\*\*\*\* ]

Ent\_database\_tns\_name [PADSSHP ]

Ent\_port [8703 ] Ent\_use\_ssl [y ]

Ent\_authenticate\_peer [n ]

Security\_host [10.164.110.17 ]

Auth\_port [8701 ]

Auth\_control\_host [10.164.110.17 ]

Auth\_control\_port [8703 ] 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\_ssl [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. |
| Entown\_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. |
| Entown\_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 |
| Entown\_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\_ssl Specifies whether to not SSL is enabled for incoming | Specifies whether to not SSL is enabled for incoming requests. Set this to “y”. |
| Ent\_authenticate\_peer | Indicates whether or not to authenticate the SSL certificates for requests. Applicable only if SSL 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\_ssl | Specifies whether to not SSL is to be enabled on startup  for incoming requests. Set this to “y” |
| Auth\_authenticate\_peer | Indicates whether or not to authenticate the SSL certificates for requests. Applicable only if SSL is enabled.  y — authenticate peer.  Set this to “y” |

1. 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.

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

1. 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

DONE creating additional configuration files

Scripts are generated for application to the clentown service account entered Ent\_database\_user.

1. Select Create 3. Append 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

Do you want to backup Entitlement DB? (y/n) n

You are about to apply changes to the database.

Do you want to continue? (y/n) y

Scripts are applied to the clentown service account entered Ent\_database\_user.

1. Select 9. Create DB Synonym

This option is used to create synonyms in the clentapp account, the account used by the application to access the database..

1. Select 10. Create DB Grant

This option is used to grant privileges to the clentapp\_role and CL\_read\_only\_role.

1. Entitlement Option 7. 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

1. Press Esc twice to return to the Server Installation menu.
2. 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 v1.154

Product Directory: /apps/clearing/pdir20140112 (240)

Install Tokenizer

+----------------------------------------+

| 0. Setup System Parameters |

| 1. Apply System Parameters |

| 2. Prepare DB Scripts |

| 3. Create DB Tables |

| 4. Undo Create DB Tables |

| 5. Create DB Synonym |

| 6. Create DB Grant |

| 7. Insert DB System Records |

| 8. Apply DB Tables Upgrade Script |

| 9. 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/Append DB Tables | Apply the table creation scripts prepared in option 3 |
| Undo Create/Append | Undo the changes applied in option 4. Applicable only if backup DB Tables was selected |
| Create DB Synonym | Creates synonyms in the APP service accounts when Method A is used for the DB standard. Otherwise not applicable. |
| 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. |

\_TOK\_VARIABLES

Product Directory: /apps/clearing/pdir20140112 (240)

Start\_tokenizer [y ] Tok\_database\_vendor [oracle ]

Tok\_database\_name [padss ]

Tok\_database\_user [cltok\_app ]

Tok\_database\_password [\*\*\*\*\*\* ]

Tok\_confirm\_db\_pwd [\*\*\*\*\*\* ]

Tok\_schema\_name [CLTOKAPP ]

Tokown\_dbuser [cltokown ]

Tokown\_dbpassword [\*\*\*\*\*\* ]

Tokown\_dbpassword\_confirm [\*\*\*\*\*\* ]

Tok\_database\_tns\_name [PADSSHP ]

Tok\_idle\_timeout [120 ] Tok\_sess\_timeout [3600 ]

Tok\_timeout [0 ] Tok\_max\_client [100 ]

Tok\_standalone [n ] Tok\_use\_ssl [n ]

Tok\_server\_mbox [TOKEN ]

Tok\_host [10.164.110.17 ]

Tok\_port [3330 ]

Tok\_server\_cert\_file [ ]

Tok\_server\_key\_pwd\_file [ ]

Tok\_server\_key\_file [ ]

Tok\_ca\_cert\_file [ ]

Tok\_otracelevel [error ] Tok\_comm\_debug [0 ]

**Tokenization System Setup 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. |
| Tokown\_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. |
| Tokown\_dbpassword | The Database\_user’s password. The password is not displayed. |
| Tokown\_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 |  |
| Tok\_session\_timeout |  |
| Tok\_timeout | Number of seconds to wait for the tokenizer response |
| Tok\_maxlclient |  |
| Tok\_standalone |  |
| Tok\_use\_ssl |  |
| Tok\_server\_mbox | The tokenization server mailbox name.  default — TOKEN |
| Tok\_otracelevel\_tokenizer | The trace level to be set:   * FATAL * LOG * ERROR * WARNING * INFO * DUMP * DEBUG |
| 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 SSL is turned on, and only for the standalone tokenizer. |
| Tok\_server\_key\_pwd | This field is required are only used when SSL is turned on, and only for the standalone tokenizer. |
| Tok\_ca\_cert\_file | This field is required are only used when SSL is turned on, and only for the standalone tokenizer. |
| Tok\_otracelevel |  |
| Tok\_comm\_debug |  |
| Tok\_pan\_token\_mode | The mode to apply for tokenization requests:   * active — Apply tokenization algorithm * echo — Return the PAN without applying the tokenization algorithm. |

1. Select 1. Apply System Parameters

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

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

1. 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

DONE creating additional configuration files

Scripts are generated for application to the cltokown service account entered Tokown\_dbuser.

1. 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

Do you want to backup Tokenizer DB? (y/n) n

You are about to apply changes to the database.

Do you want to continue? (y/n) y

Scripts are applied to the cltokown service account entered in Tokown\_dbuser.

1. Select 8. Create DB Synonym

This option is used to create synonyms in the cltokapp account used by the application to connected to the database.

1. Select 9. Create DB Grant

This option is used to grant privileges to the cltokapp\_role and cltok\_read\_only\_role.

1. Tokenization Option 7. 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

1. Press Esc twice to return to the Server Installation menu.
2. 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:

Product Directory: /apps/clearing/pdir20140112 (240)

Install Key Life Cycle

+----------------------------------------+

| 0. Setup System Parameters |

| 1. Apply System Parameters |

| 2. Prepare DB Scripts |

| 3. Create DB Tables |

| 4. Undo Create DB Tables |

| 5. Create DB Synonym |

| 6. Create DB Grant |

| 7. Insert DB System Records |

| 8. Apply DB Tables Upgrade Script |

| 9. 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/Append DB Tables | Apply the table creation scripts prepared in option 3 |
| Undo Create/Append | Undo the changes applied in option 4. Applicable only if backup DB Tables was selected |
| Create DB Synonym | Creates synonyms in the APP service accounts when Method A is used for the DB standard. Otherwise not applicable. |
| 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. |

1. 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: /apps/clearing/pdir20140112 (240)

Klc\_database\_vendor [oracle ]

Klc\_database\_name [padss ]

Klc\_database\_user [clklc\_app ]

Klc\_database\_password [\*\*\*\*\* ]

Klc\_confirm\_db\_pwd [\*\*\*\*\* ]

Klc\_schema\_name [clklcapp ]

Klcown\_dbuser [clklcown ]

Klcown\_dbpassword [\*\*\*\*\* ]

Klcown\_dbpassword\_confirm [\*\*\*\*\* ]

Klc\_database\_tns\_name [PADSSHP ]

Klc\_otracelevel [error ]

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. |
| Klcown\_dbuser | The name of the database OWNER service account (e,g. clklcown) where the Clearing database objects reside. |
| Klcown\_dbpassword | The CLC owner’s password. |
| Klcown\_dbpassword \_confirm | The CLC 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\_tokenizer | The trace level to be set:   * FATAL * LOG * ERROR * WARNING * INFO * DUMP * DEBUG |
| Klc\_klcpf\_filename |  |

1. Select 1. Apply System Parameters

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

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

1. 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 DONE creating additional configuration files Replace

Scripts are generated for application to the clklcown service account entered in Klcown\_dbuser.

1. Select 3. Create DB Tables

This option is used to apply the database table creation scripts generated by option 3. 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

Do you want to backup Key Life Cycle DB? (y/n) n You are about to apply changes to the database.

Do you want to continue? (y/n) y

Scripts are applied to the clklcown service account entered in Klcown\_dbuser.

1. Select 9. Create DB Synonym

This option is used to create synonyms in the clklcapp account used by the application to access the Key Lifecycle database.

1. Select 10. Create DB Grant

This option is used to grant privileges to the clklcapp\_role and clklcapp\_read\_only\_role.

1. Press Esc twice to return to the Server Installation menu.
2. Select 7. Insert DB System Records

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

## Enabling SSL for the IST Process

The default installation enables SSL 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/pdir20140112 (240)

Enable SSL

+----------------------------------------+

| 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 SSL. Repeat this procedure for all nodes.

Refer to section Enabling SSL on page 73, for an overview of SSL within IST.

### Generate Node Certificates

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

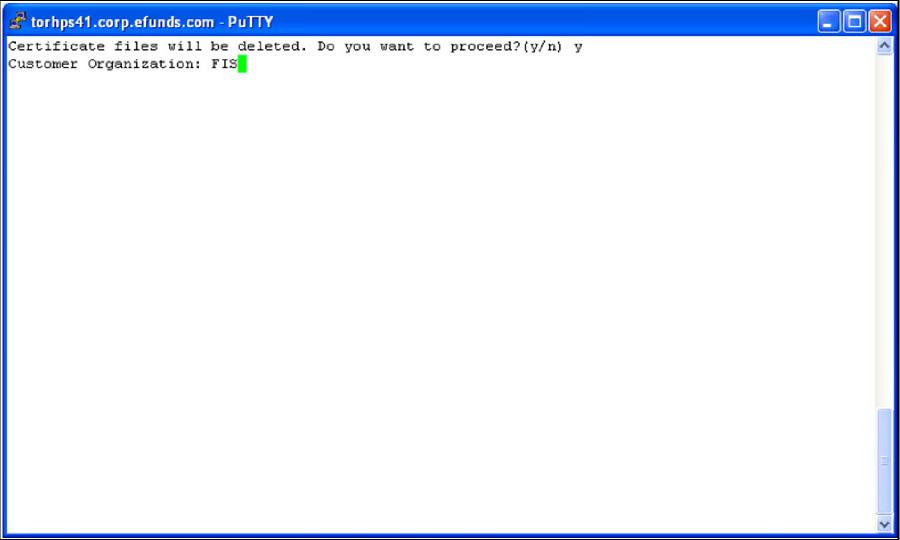


Figure 9: Generate

1. Enter the **organization name** (i.e your\_company\_name) to include in the certificates.

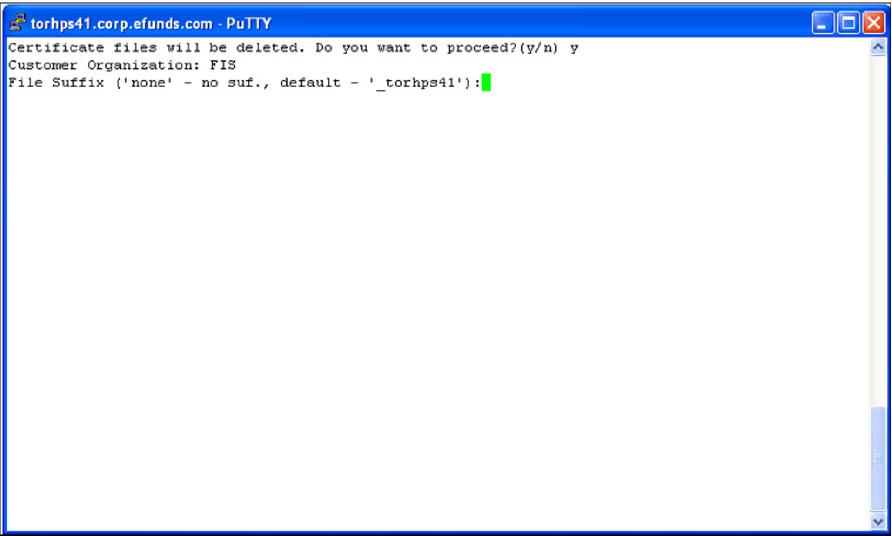


Figure 10: Organization Name

1. 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.

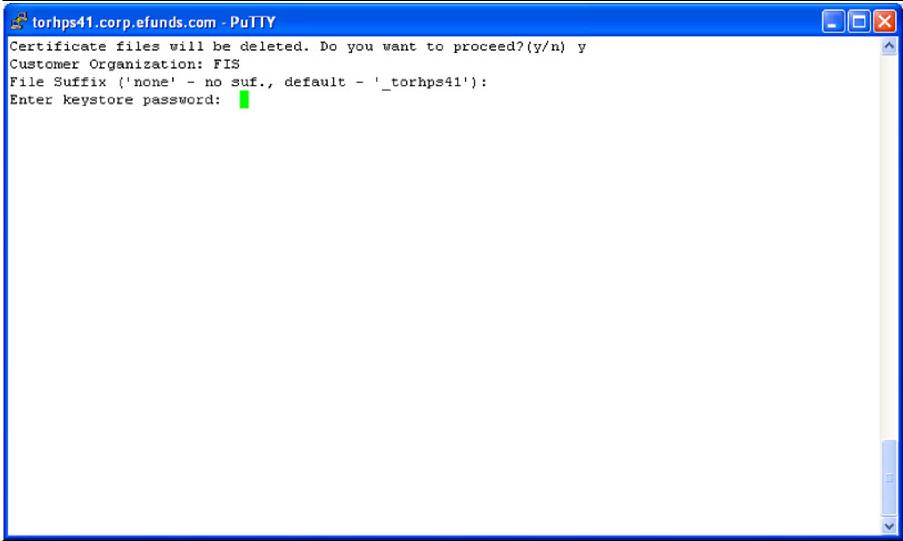


Figure 11: File Suffix

1. Enter the **keystore password**. This is the password you used for the Ssl\_key\_manager password.

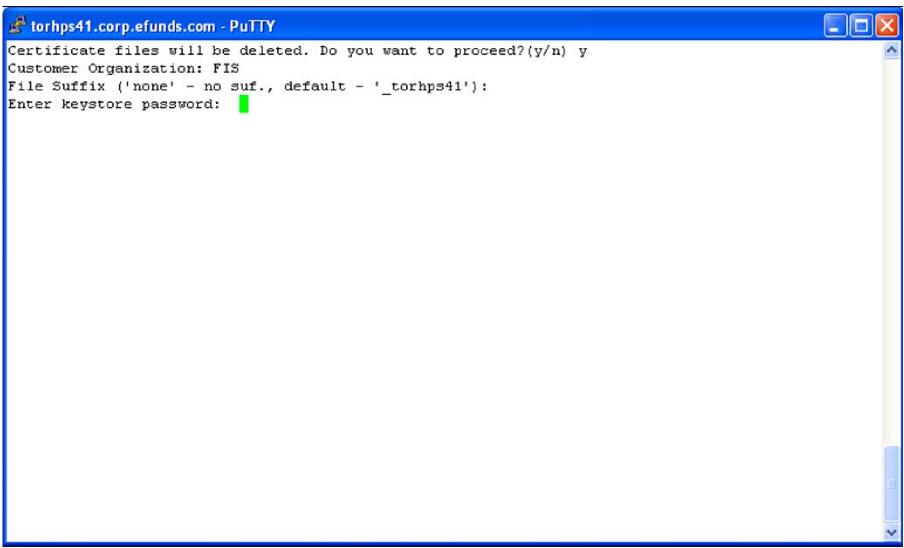


Figure 12: Keystore Password (a)

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



Figure 13: Keystore Password Confirmation

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

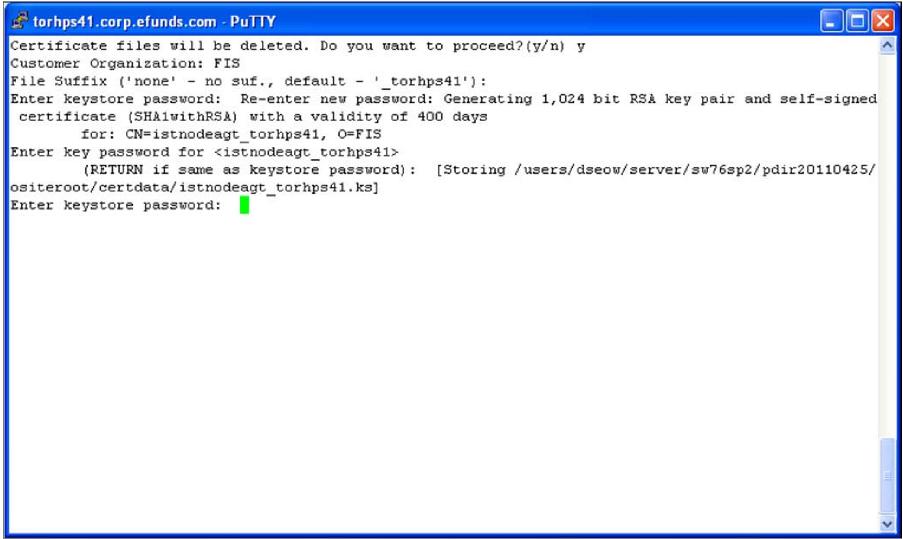


Figure 14: Keystore Password (b)

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



Figure 15: Keystore Password (c)

1. Assuming the suffix used in step file is “\_torhps41”, the following files are created for each of the administrative processes.

|  |  |
| --- | --- |
| File | Contents |
| ftpclient.pem | SSL certificate of the FTPS client |
| ftpclient\_ca.pem | FTPS client’s truststore |
| ftpclient\_key.pem | Private key corresponding to ftpclient.pem |
| ftpcmd.pem | SSL certificate of the FTPCMD |
| ftpcmd\_ca.pem | FTPCMD trustore. |
| ftpcmd\_key.pem | Private key corresponding to FTPCMD |
| ftpsrv.pem | SSL certificate of the file server |
| 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 | 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 . |
| Istnodeagt\_trust.ks |  |
| istxmlrpc.pem |  |
| istxmlrpc\_ca.pem |  |
| istxmlrpc\_key.pem |  |
| 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 | 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). |
| oentsrv\_ca.pem | The entitlement process’s trust-store |
| oentsrv\_key.pem | The entitlement process’s key-store. |
| oentsrv.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). |

1. 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 SSL

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:
3. Ensure the files above were transferred and copied to $OSITE\_ROOT/ certdata.
4. Run pdeploy and select Enable SSL.

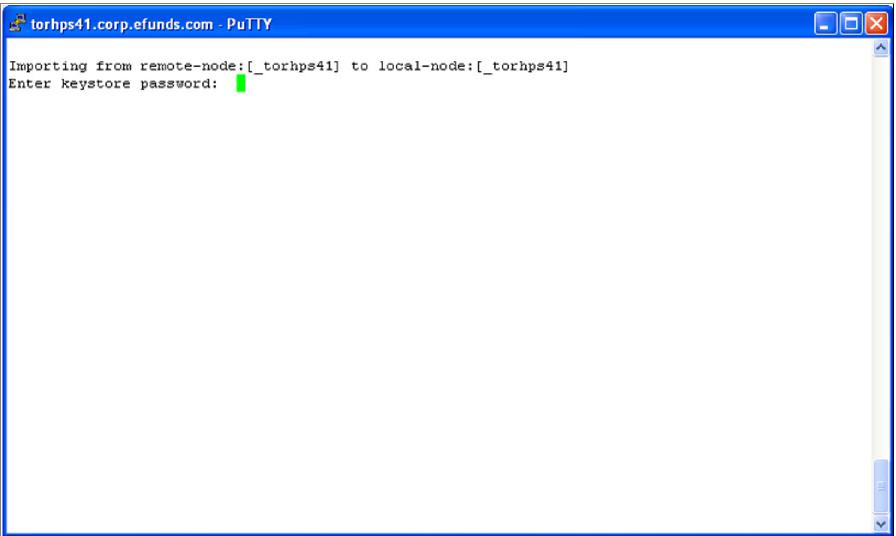
Select Import Certificates and enter “y” to proceed.

Figure 16: 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 SSL. 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”](#_Starting_the_Administrative)

## 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 5 - Apply DB Tables Upgrade Script to apply scripts to upgrade the database tables.

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\_7610001\_00\_1.ora Ent upgrade script:- udm\_en\_7610001\_00\_1.ora

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

### Database Record Scripts

From the respective submenu select option 6 - 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**.

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\_kl\_7610001\_00\_1.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 | pdir20130809 | profile20130809 | First production |
| 2 | pdir20131129 | profile 20131129 | Service pack 2 |
| 3 | pdir20131129\_1 | profile 20131129\_1 | First install of 2 above. Can be discarded later. |
| 4 | pdir20131215 | profile 20131215 | Bad release, reverted to pdir20131215 until a subsequent patch |

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 pdir20130430 is the running environment and the previous version is pdir20130129,

to revert to the previous release:

1. Login as the admin user.
2. Remove the link to profile20130430:

rm profile

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

ln –s profile20130129 profile

1. Bring down the node.
2. Re-login to execute the updated profile to make "profile20130129" take effect.
3. 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.

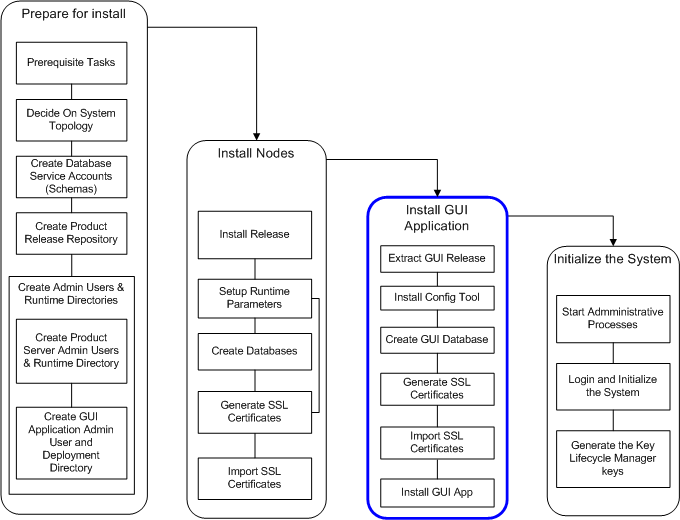


Figure 17: Install GUI Application

## 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.



Figure 18: 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:

1. 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” on page 202.

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

1. export HOME=/apps/guiapp
2. 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\_2.4.0.00.05\_AIX-612\_BASE\_SSO.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 -prod=CLC

The files are stored as illustrated in Figure 2.



Figure 19: 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 -prod=CLC

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

1. 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".

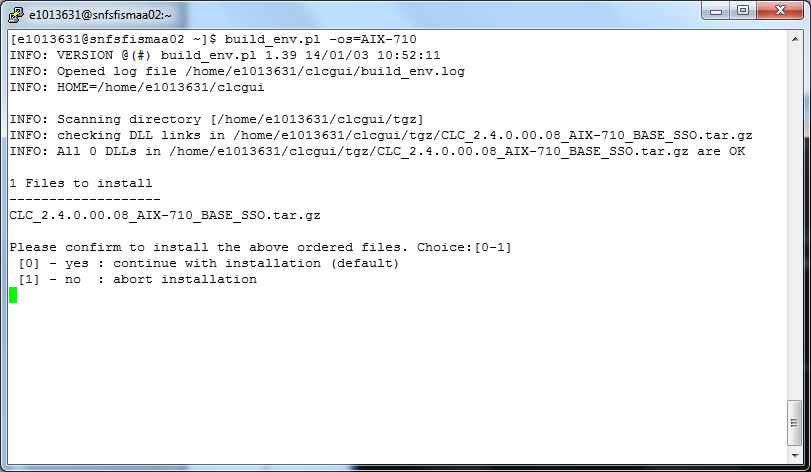


Figure 20: Files Selected for Installation

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.

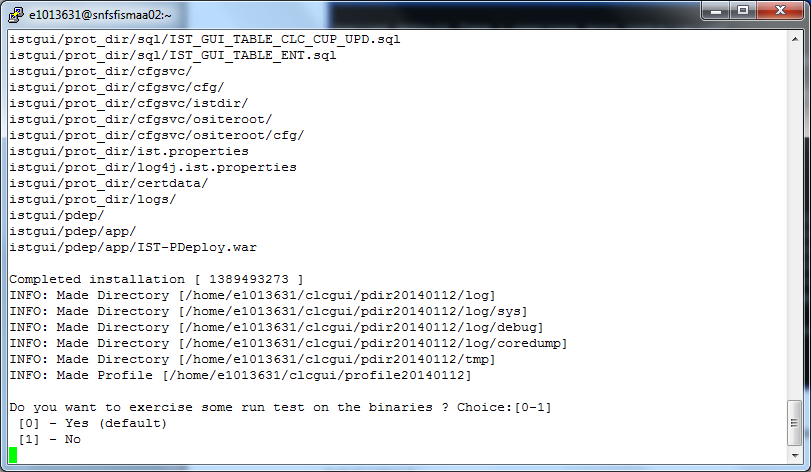


Figure 21: Extracting Files to Directory

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.

1. Select option 1.

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

INFO: Skipped run test

INFO: Version 1.6

INFO: OsString=[AIX-612]

INFO: bit reference binary /apps/istgui/pdir20140112/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 items(s)

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.** |
|  |  |

On completion the product directory and associated profile are created:

1. A file is created with name, profile<install\_date>.where,

profile is constant

install\_date is the date in the format yyyymmdd.

Example: profile20140112

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.

1. 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: pdir20140112

pdir20140112 current installed pdir<install \_date> on January 12, 2014.

pdir20140112\_1 previously installed pdir<install \_date> directory on January 12, 2014, moved to pdir<date>\_n.

The pdir<install\_date> directory contains the GUI files to be used in the deployment.

1. The file build\_env.log is updated with the installation information.
2. Edit the guiadmin's ".profile" and replace the ". ./profile<yyyymmdd> with the current profile<install\_date> filename created above. “.profile" Entries” for entries to include in the ".profile".

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

rm profile

ln –s profile<date> profile

1. Re-login to apply the changes above.

## GUI Application Database Tasks

You can choose to use the IST-PDeploy tool to perform the database tasks or have it done by a DBA.

# Installing the GUI Application

## IBM Websphere 7

## 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

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

# Enabling SSL

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

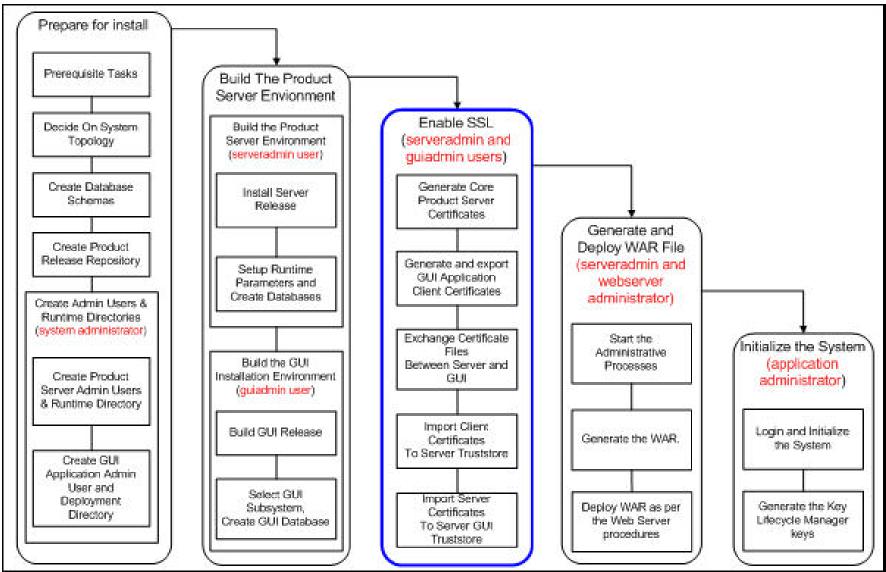


Figure 22: Enabling SSL Option

SSL is enabled at installation time using the options provided in the installation configuration tool, pdeploy. Enabling SSL 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



Figure 23: Enabling SSL

## Java Application Server

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

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

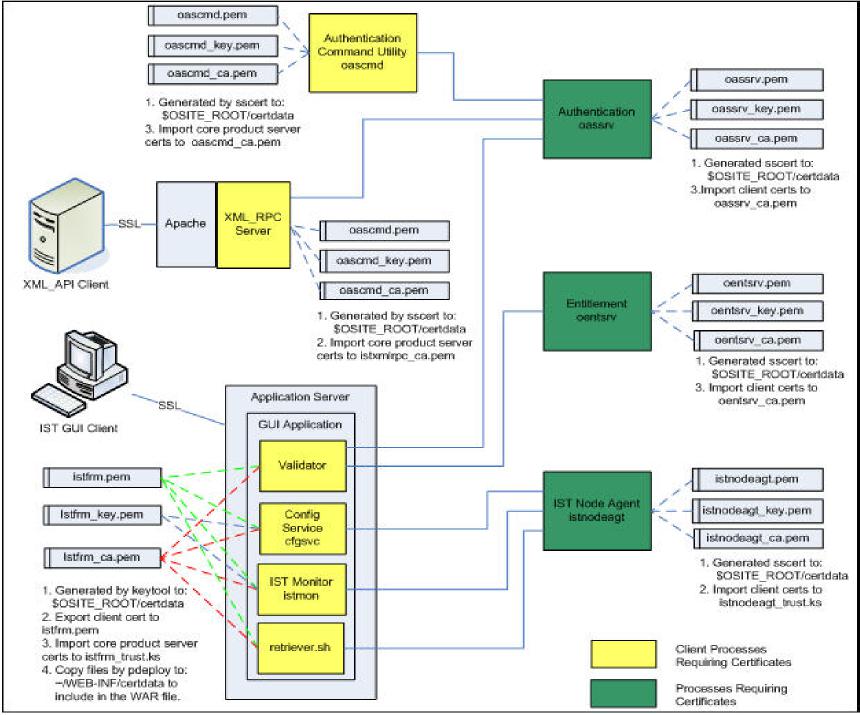


Figure 24: IST Clearing SSL Enabled Process

# 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:
5. Adds the node to be controlled in the IST Control.
6. Initializes the Key Life Cycle manager passphrase file.
7. Generates the keys for the Key Life Cycle manager process.
8. Initializes the system by starting each node. At this point the tokenization and the key management processes will be started.

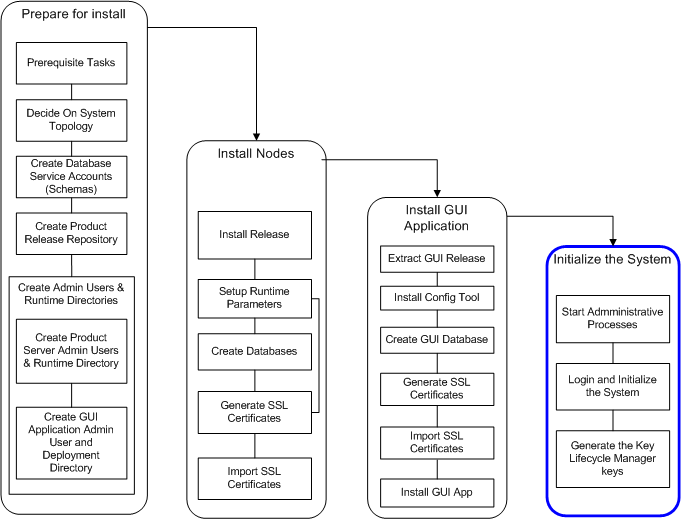


Figure 25: Initializing The System

## 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.

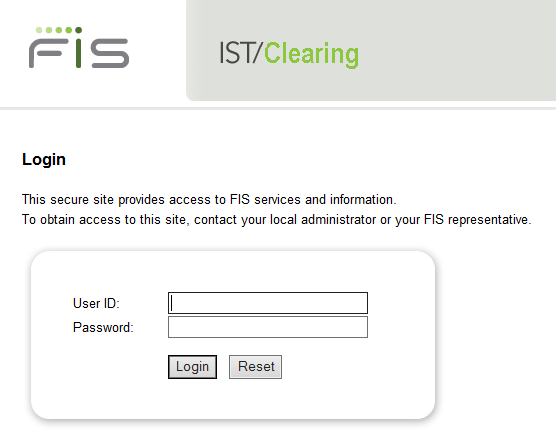


Figure 26: IST/Clearing Login

To login for the first time:

1. Enter the User ID of the admin user created during IST/Celaring installation ..
2. Enter the admin user’s password.
3. Click **Login**.
4. The expired password page is displayed.

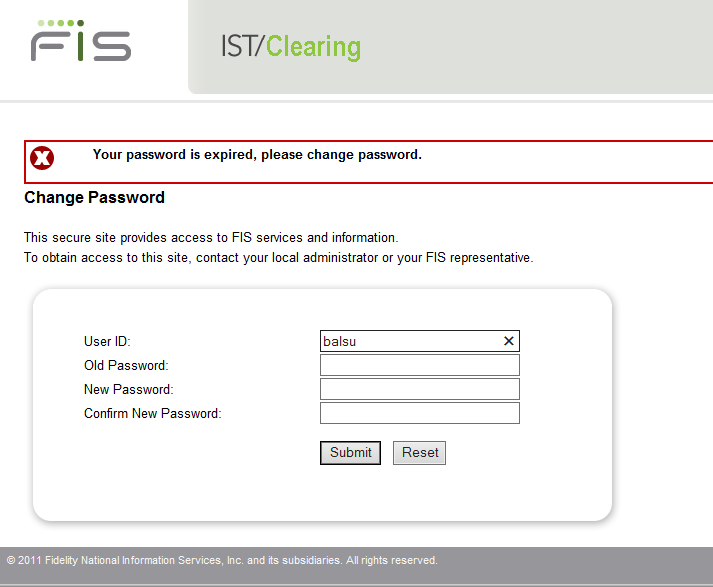


Figure 27: Password Expired Page

1. Enter the admin user’s password 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.

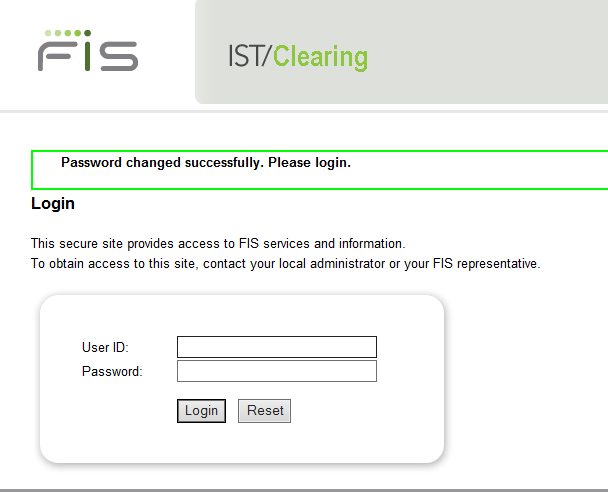


Figure 28: Password Change Successfully

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



Figure 29: IST/Clearing Application 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:

1. Select the ENT link to open the Authentication and Entitlement system .
2. Select User Authentication.

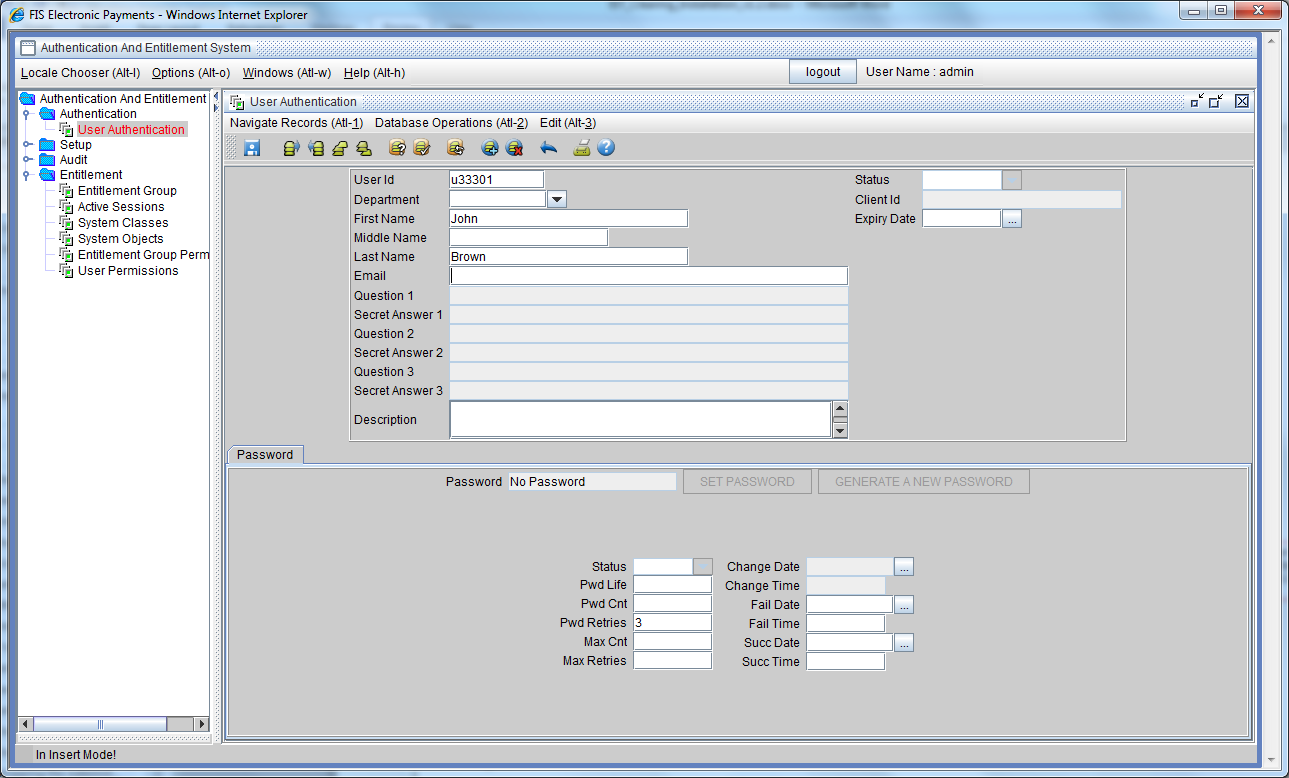


Figure 30: User Authentication Screen

1. Click Insert on the screen menu
2. Enter the **User ID**. This is the user's login name.
3. Enter the **user's first** and **last names**,
4. Enter **Email address**, and **Department** as necessray,
5. For active users leave the **Status** field empty.
6. 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.
7. 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.
8. 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 usre should be set to 3, and an administrator can be set up to 6.
9. 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.
10. 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.

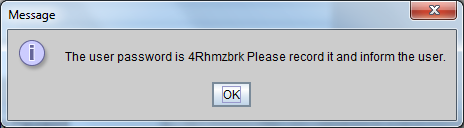


Figure 31: Generated Password Display

1. Copy the password so it can be sent to the user.
2. From the menu select open the Entitlement Group screen, Query the newly added user and display the detail record.
3. Click User Group.
4. Click the “Enter Query by Example” icon.
5. Click Execute Query.
6. Right Click on the Entitlement Object ID row and select Insert Record

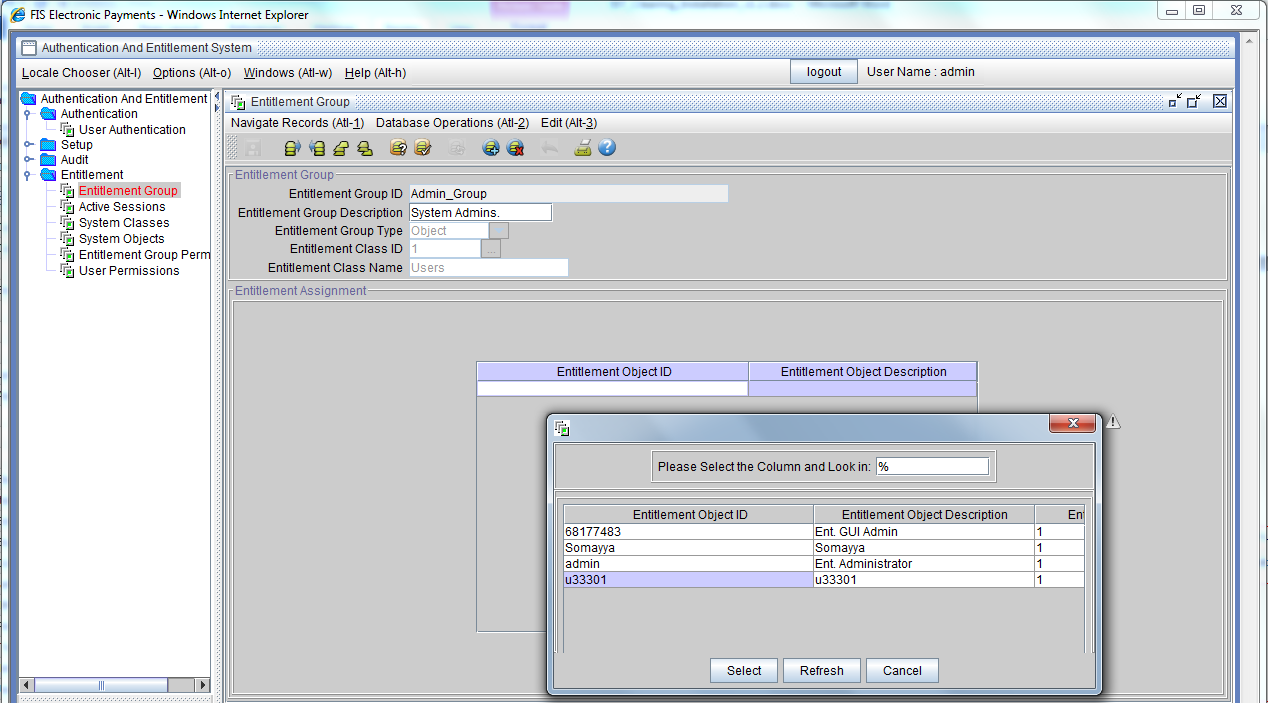


Figure 32: User Group Screen

1. Double click in the empty row to display the set of user records.
2. Select the user to assign to the group and click Select.
3. 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.

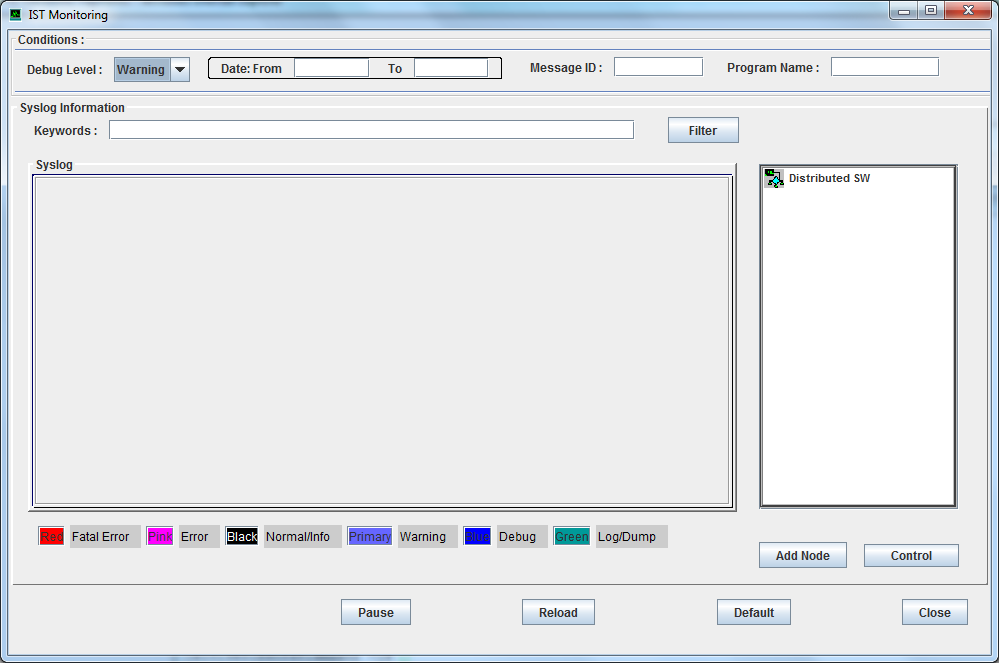


Figure 33: IST Monitor

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

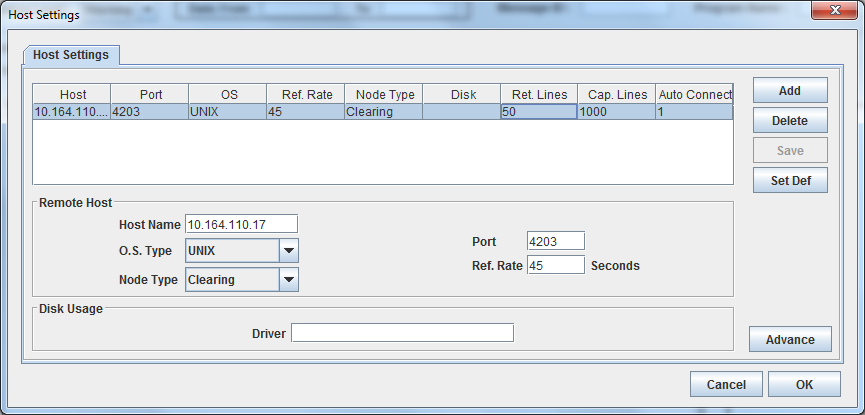
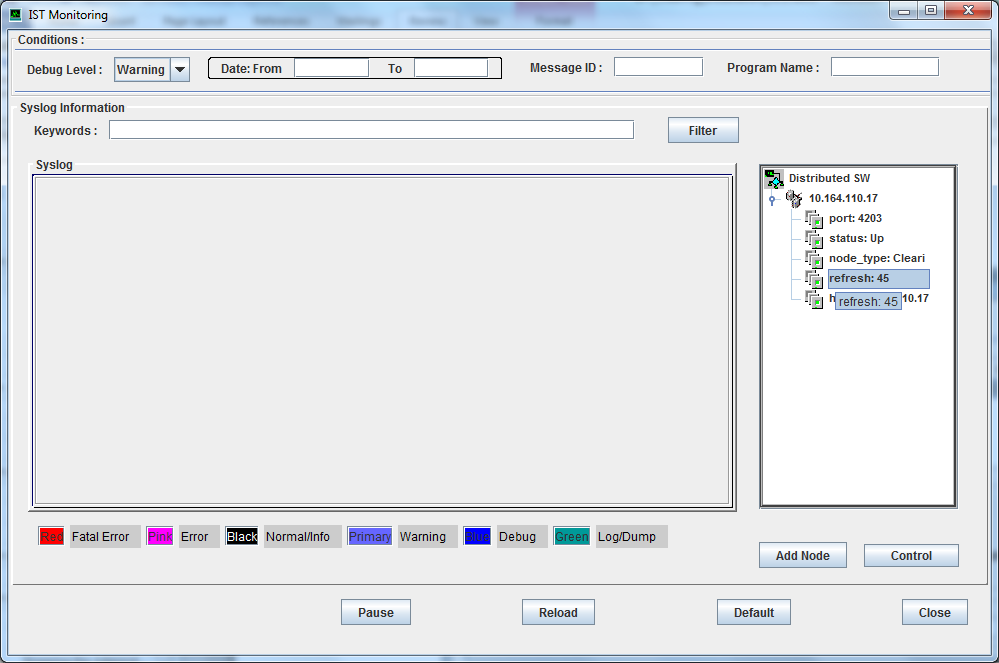


Figure 34: IST Monitor- Add Node

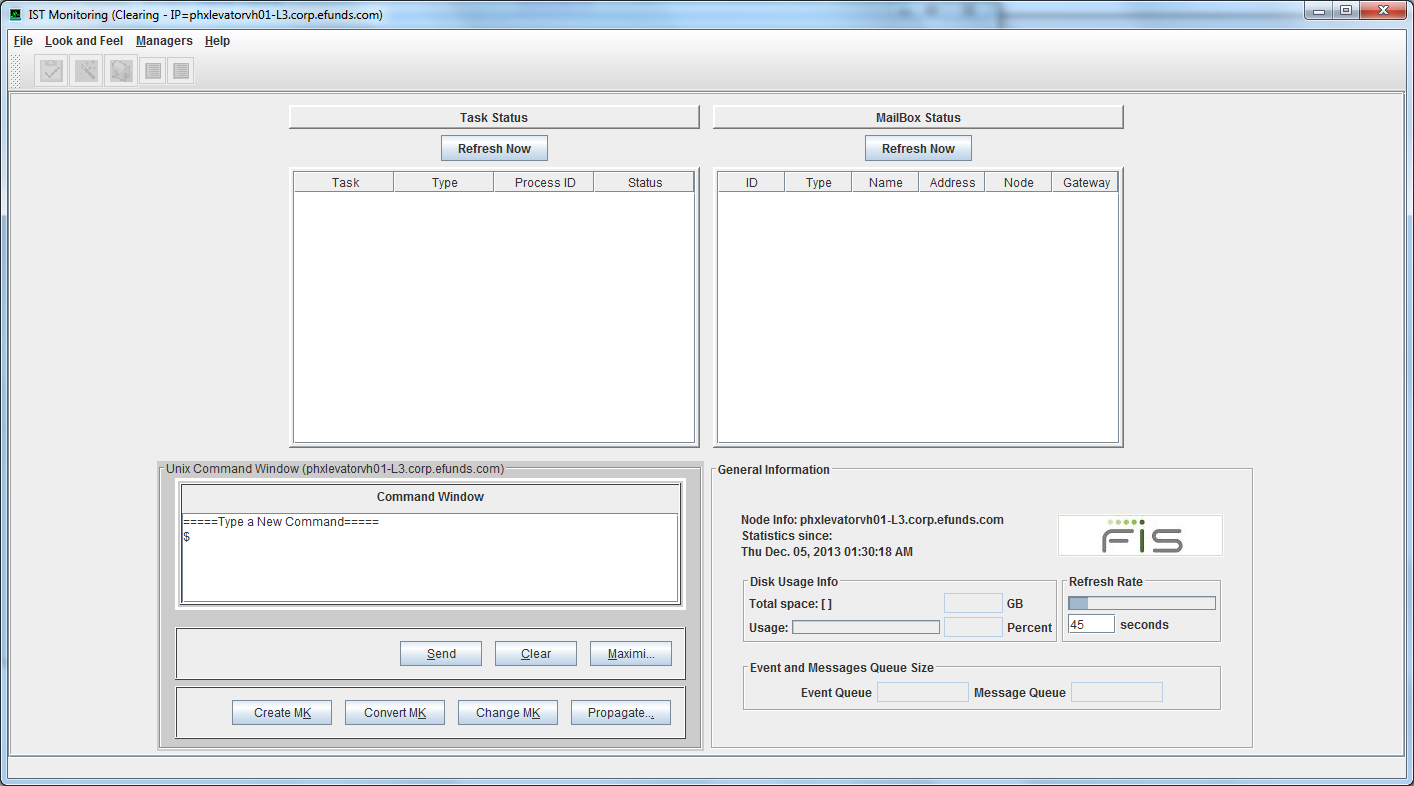
1. **Click Add**
2. Enter the IST/Clearing hostname or IP in the Host Name field.
3. Select Node Type “Clearing”
4. Enter the port istnodeagt port configured during the IST/Clearing installation.
5. Click **Save** button.
6. Click OK. The node appears in Nodes list.

## Master Key Management

In IST Monitor:



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

Four options are included to manage Tokenization master keys.  


Create MK:

invoke :  “tokenmas|run\_cmd|klc\_init\_master”.

Convert MK:

invoke :  “tokenmas|run\_cmd|km\_pass2tokmas”.

Change MK:

1. invoke :  “tokenmas|run\_cmd|klcutil –u”.
2. Invoke :  “tokenmas|run\_cmd|klcutil –t” on one node.
3. If success run  “mbrulecmd update token-keys” on all nodes.

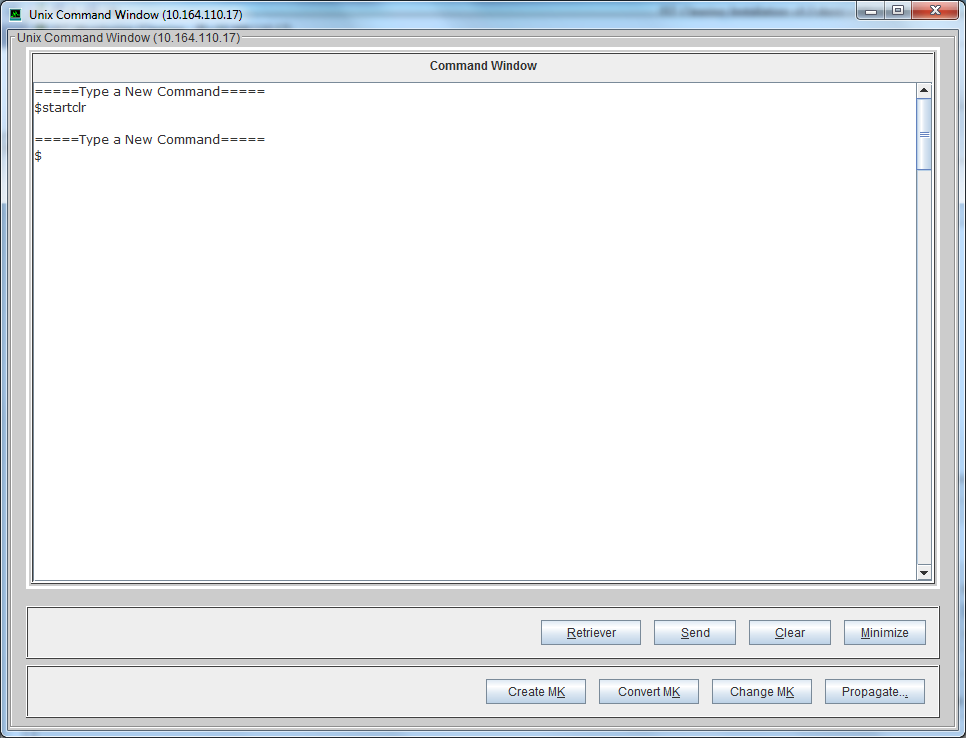
Propagate Master Key: (This is not applicable to clearing)

|  |  |
| --- | --- |
| **NOTE:** | A confirmation message will not be displayed on execution. |
|  |  |

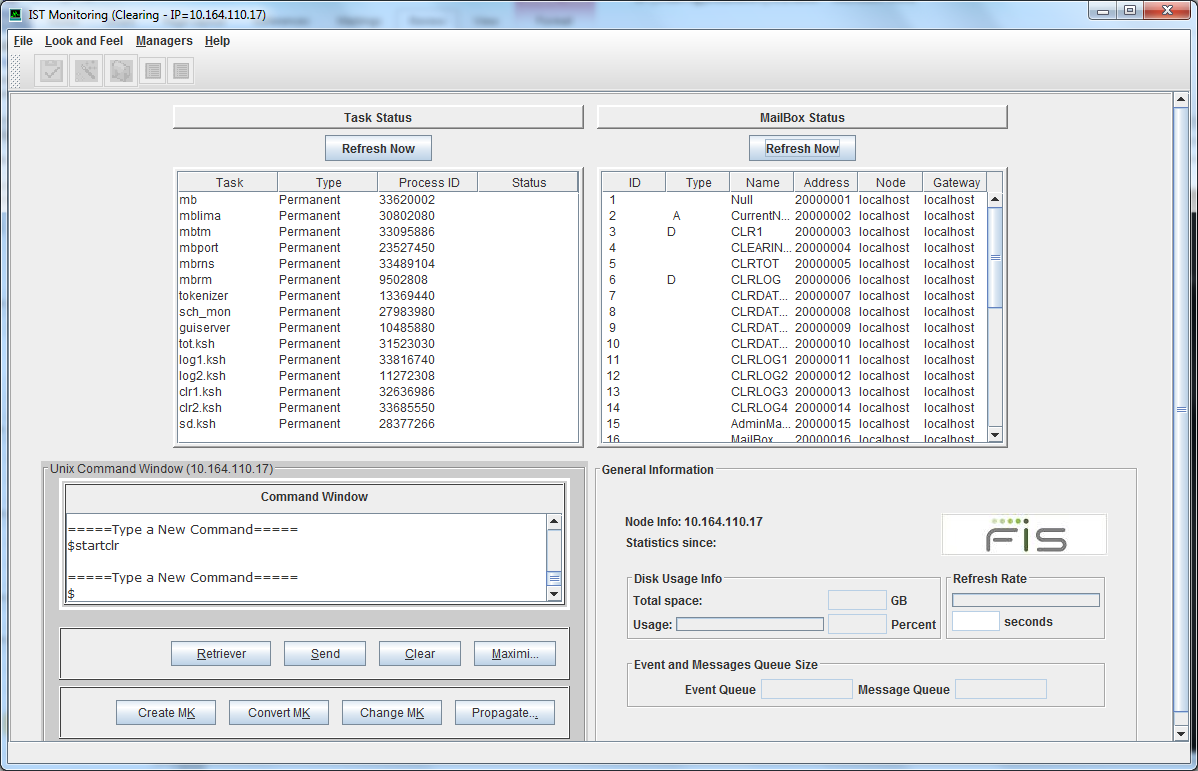
## Start Clearing

To start the IST/Clearing processes:

1. Click Maximize to mazimize the Command Window



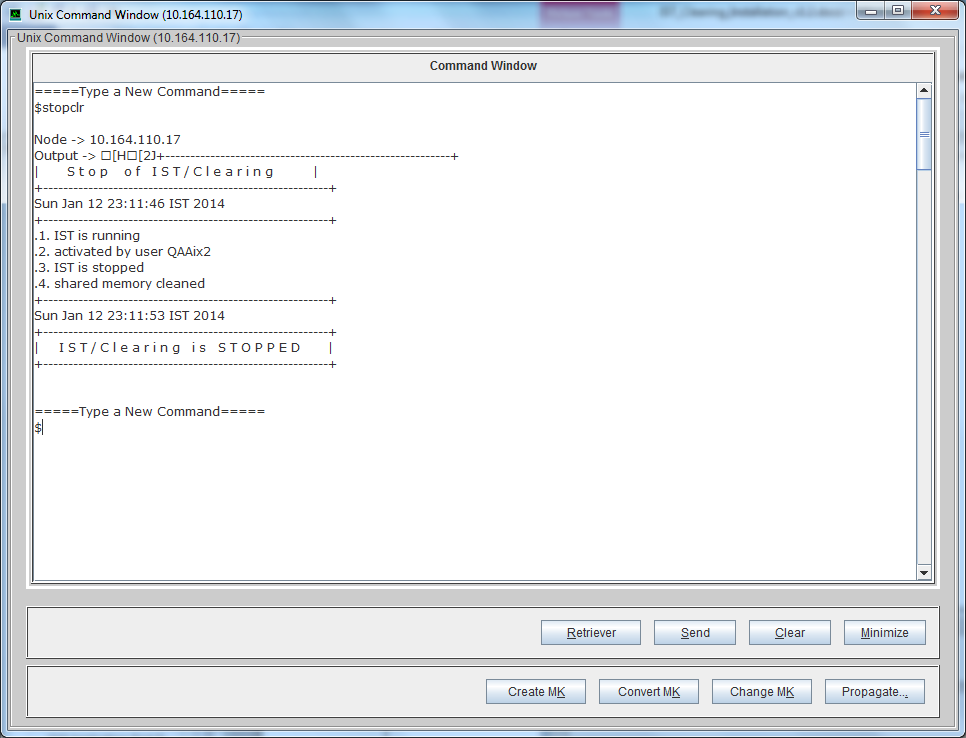
1. Enter startclr in the Command Window
2. Click Send
3. After te system starts Click Minimize on the Command Window



1. 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 mazimize the Command Window



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

## Import XML Configuration Files

In IST Monitor:

* + 1. Select the Clearing node
    2. Click Control
    3. Click the Retreiver button
    4. The XML files stored in $OPRODUCT\_ROOT/cfg on the IST/Clearing server will be imported for use in the GUI application.

This system is now ready for business level configuration using the Configuration Service.

# Set Up The Configuration Service

The Configuration Service screens are used to configure Clearing 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 Import XML Configuration Files section above.

To set up the configuration service:

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

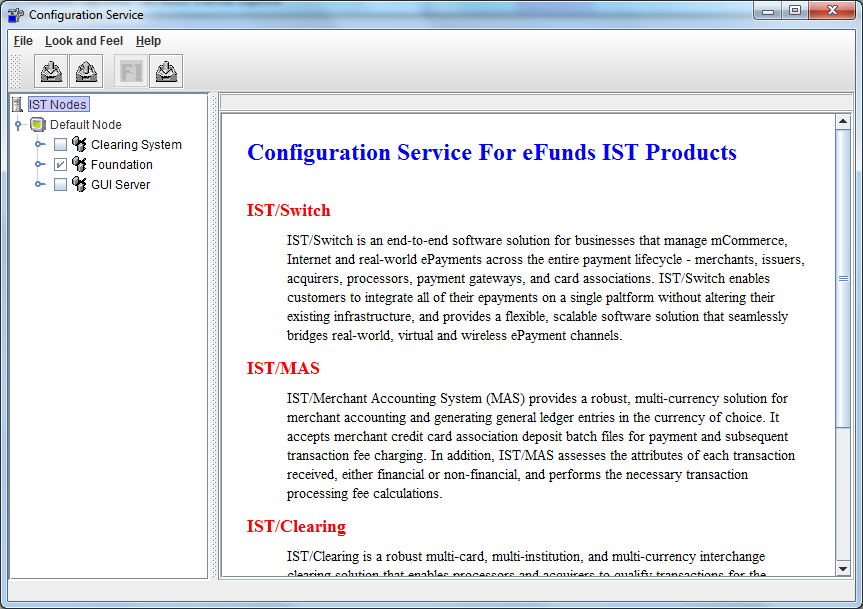


Figure 35: Configuration Service screen

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

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

# .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, clt21\_app\_read\_only\_role to <individual-user>;

alter user <individual-user> default role cl\_app\_read\_only\_role, clent\_app\_read\_only\_role, clt21\_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 clt21own;

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 clt21app\_role;

create role clt21app\_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.SQLC2J25 to role clbasic\_role;

grant EXECUTE on package NULLID.SQLC3J24 to role clbasic\_role;

grant EXECUTE on package NULLID.SQLC4J24 to role clbasic\_role;

grant EXECUTE on package NULLID.SQLC5J24 to role clbasic\_role;

grant EXECUTE on package NULLID.SQLC6J24 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, clt21own, cl\_own;

grant select on syscat.tables to cl\_own, clentown, clklcown, clt21own, cltokown;

grant select on syscat.indexes to cl\_own, clentown, clklcown, clt21own, cltokown;

grant select on syscat.schemata to cl\_own, clentown, clklcown, clt21own, cltokown;

grant select on syscat.columns to cl\_own, clentown, clklcown, clt21own, cltokown;

grant select on syscat.indexcoluse to cl\_own, clentown, clklcown, clt21own, cltokown;

grant select on syscat.tabconst to cl\_own, clentown, clklcown, clt21own, cltokown;

grant select on syscat.references to cl\_own, clentown, clklcown, clt21own, cltokown;

grant role clbasic\_role to cl\_own, clentown, clklcown, clt21own, 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 clt21app\_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 clt21app\_role, clt21app\_read\_only\_role to clt21app;

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:

1. of the server scripts generated by pdeploy and where to apply each.
2. 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. |

# 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:
5. Adds the node to be controlled in the IST Control.
6. Initializes the Key Life Cycle manager passphrase file.
7. Generates the keys for the Key Life Cycle manager process.
8. Initializes the system by starting each node. At this point the tokenization and the key management processes will be started.

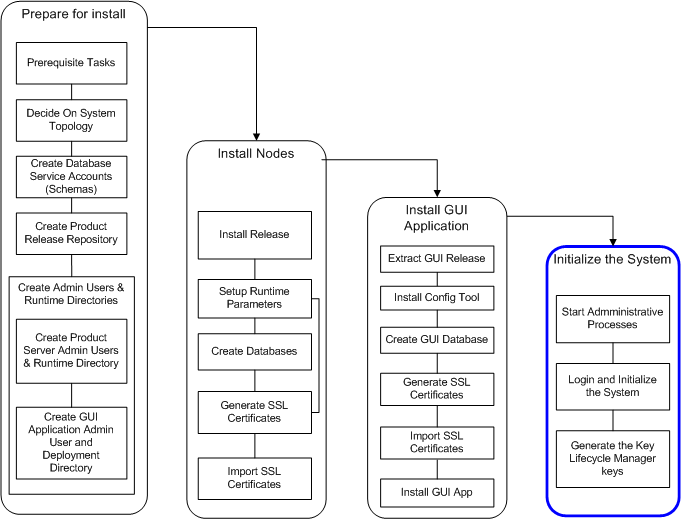


Figure 27: Initializing The System

## 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.

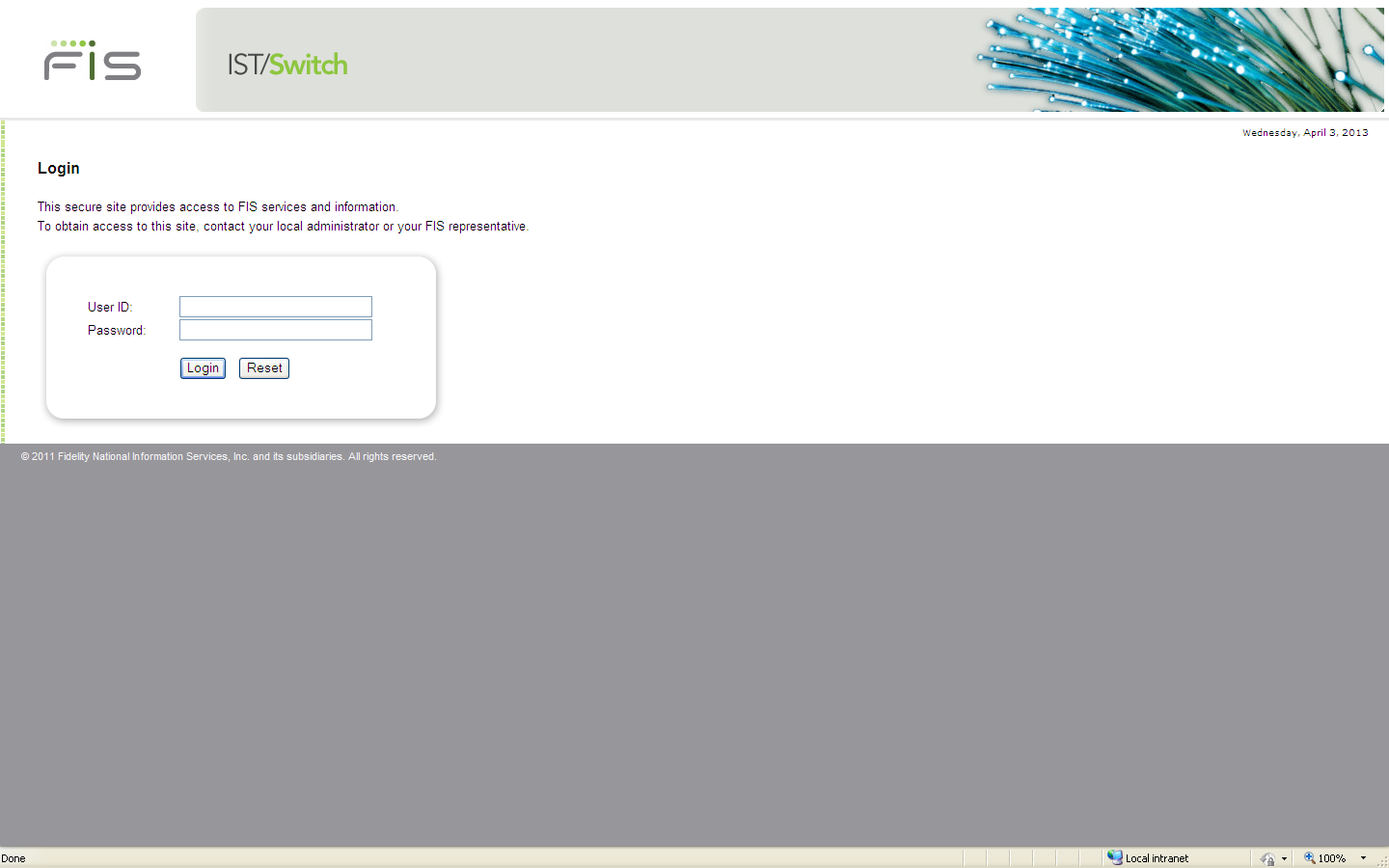


Figure 9: IST Application Login Page

Figure 28: IST/MAS Login

To login for the first time:

1. Enter the "admin" as the User ID.
2. Enter "admin" for the password.
3. Click **Login**.
4. The expired password page is displayed.

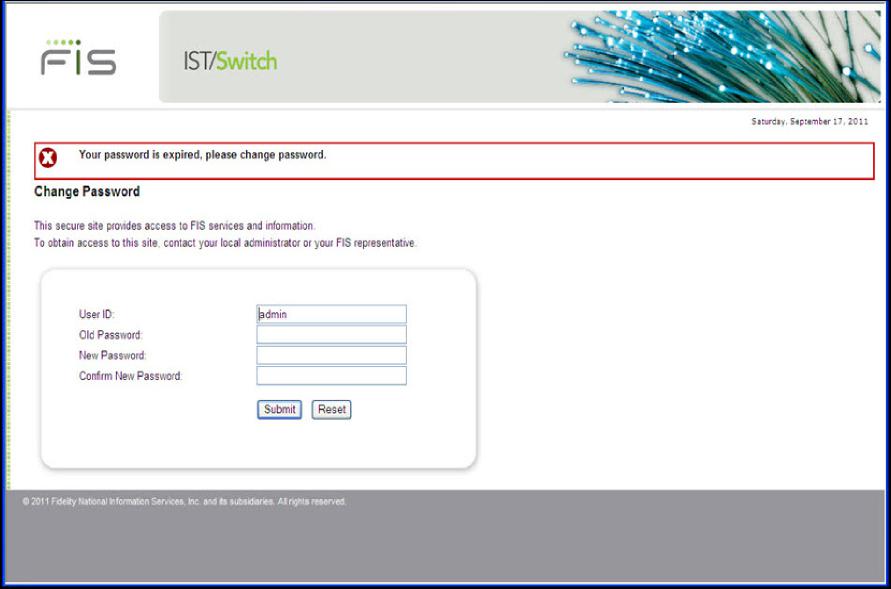


Figure 29: Password Expired Page

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.

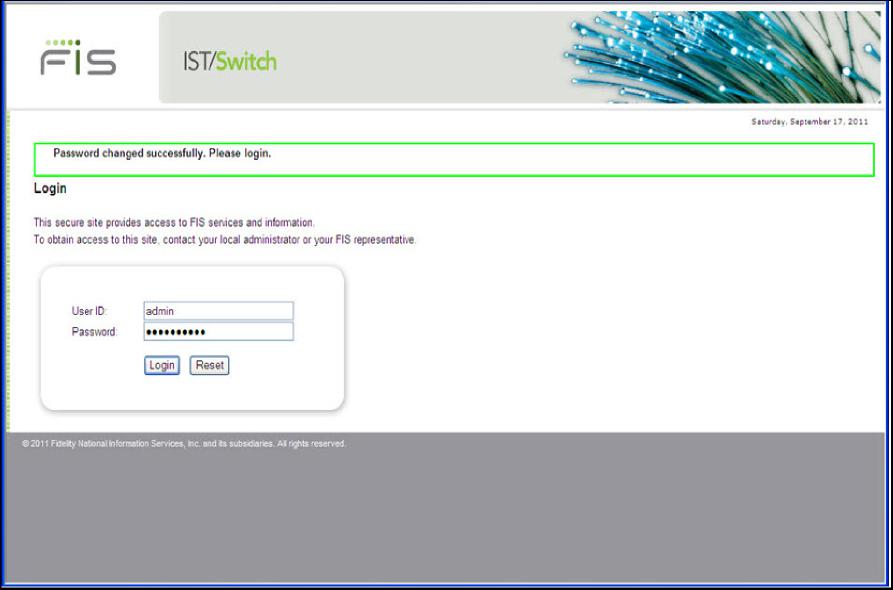


Figure 30: Password Change Successfully

1. Enter "admin" as the User ID.
2. Enter the new password.
3. Click **Login**.
4. The Application select page is displayed.

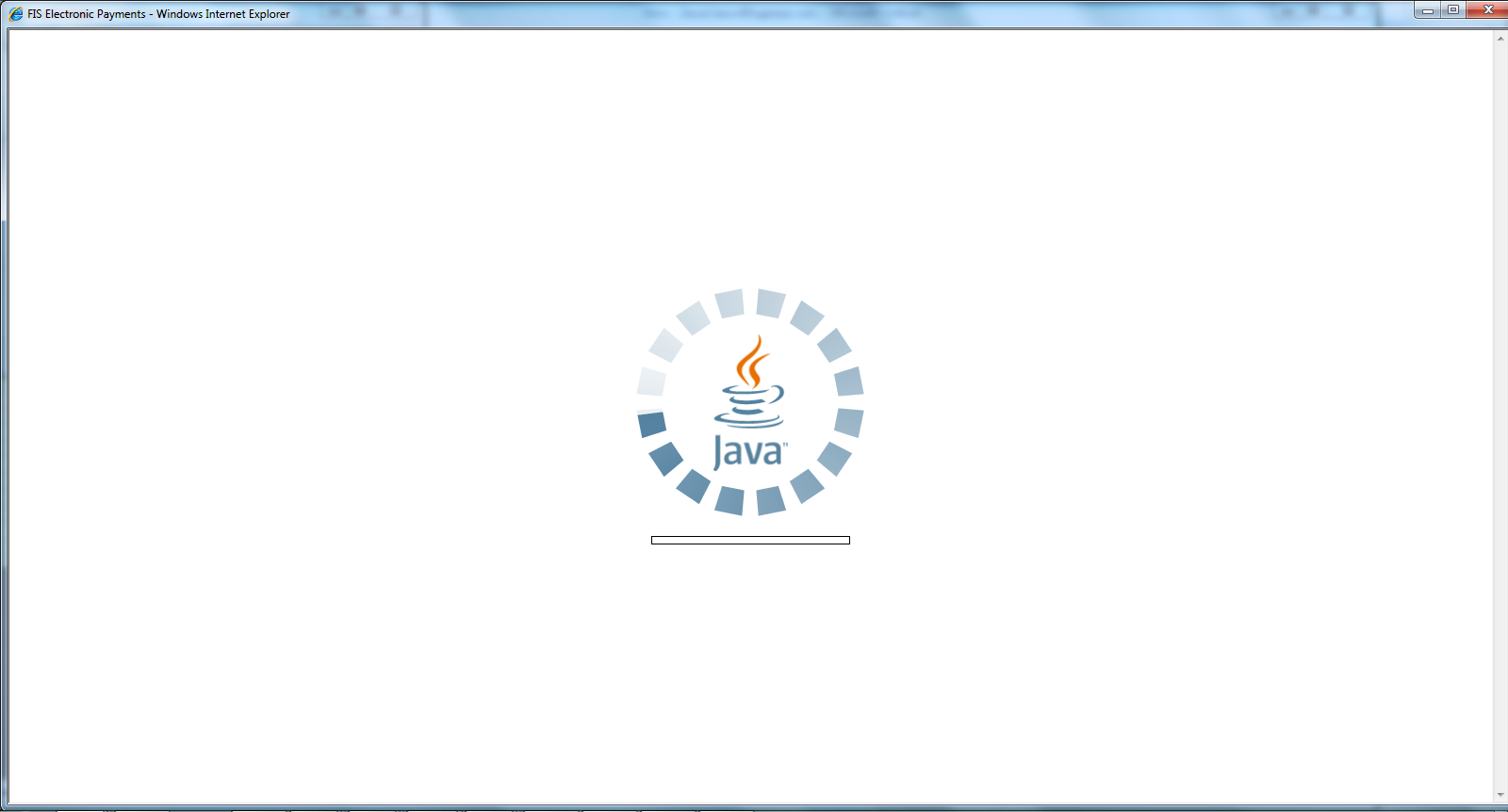


Figure 31: IST/MAS Menu

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:

1. Select the ENT link to open the Authentication and Entitlement application.



1. Select User Authentication.

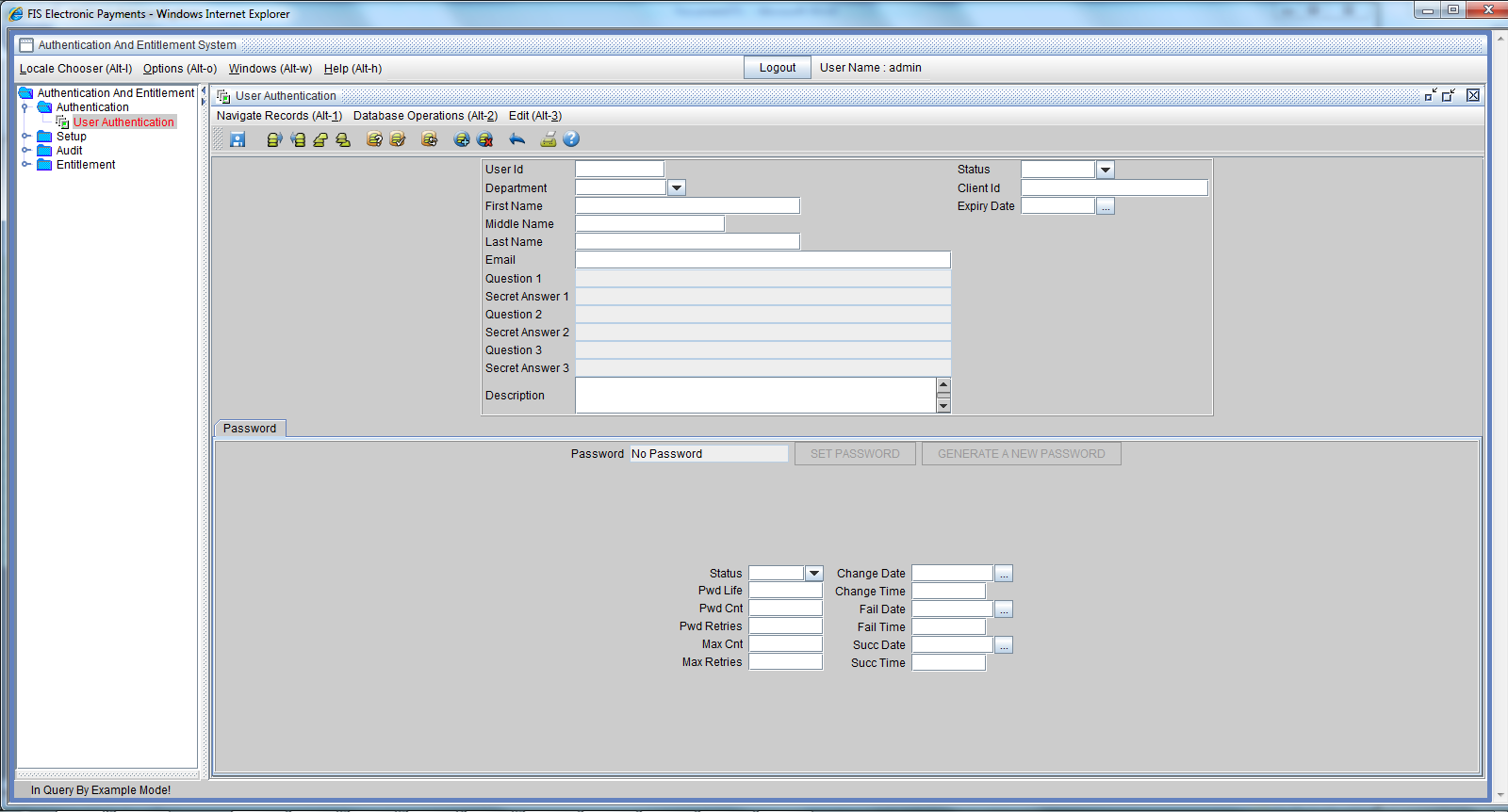


Figure 30: User Authentication Screen

1. Click Insert on the screen menu
2. Enter the **User ID**. This is the user's login name.
3. Enter the **user's first** and **last names**,
4. Enter **Email address**, and **Department** as necessary,
5. For active users leave the **Status** field empty.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.

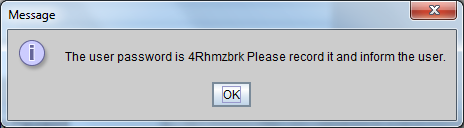


Figure 31: Generated Password Display

1. Copy the password so it can be sent to the user.
2. From the menu select open the Entitlement Group screen, Query the newly added user and display the detail record.
3. Click User Group.
4. Click the “Enter Query by Example” icon.
5. Click Execute Query.
6. Right Click on the Entitlement Object ID row and select Insert Record

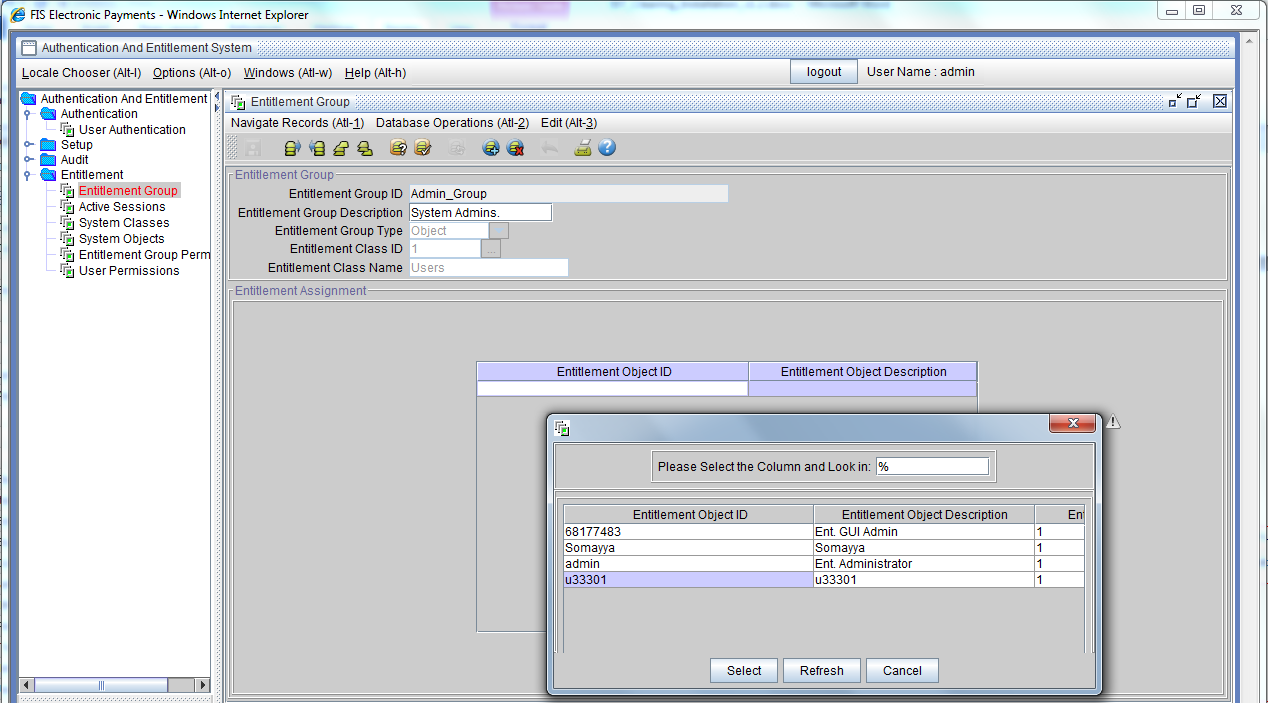


Figure 32: User Group Screen

1. Double click in the empty row to display the set of user records.
2. Select the user to assign to the group and click Select.
3. 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.

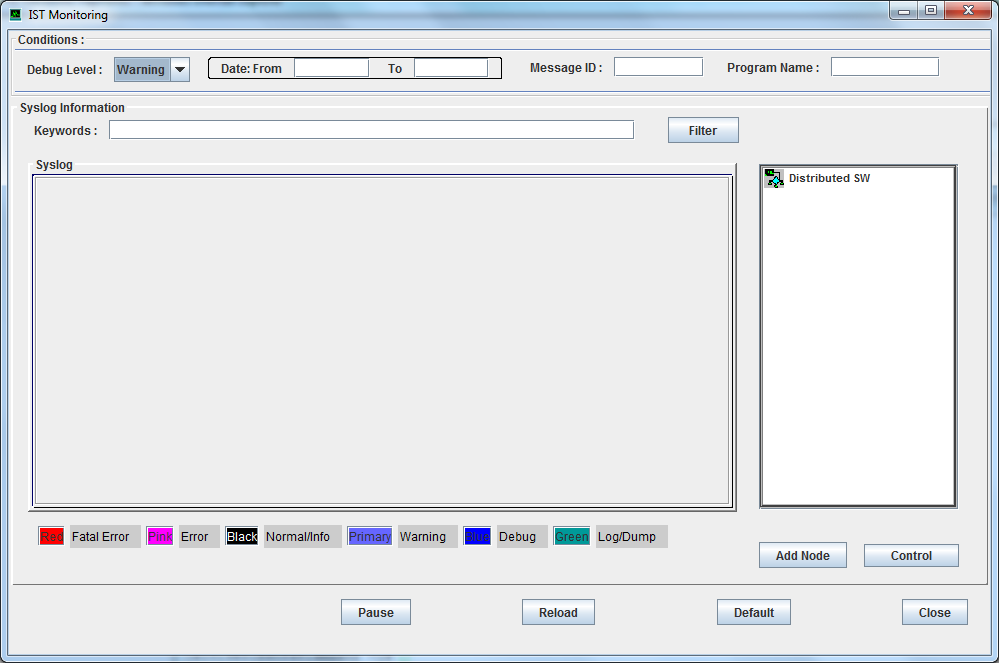


Figure 33: IST Monitor

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

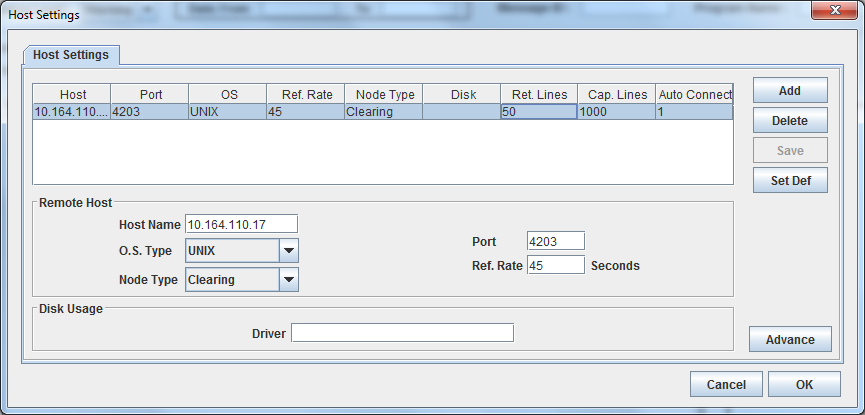


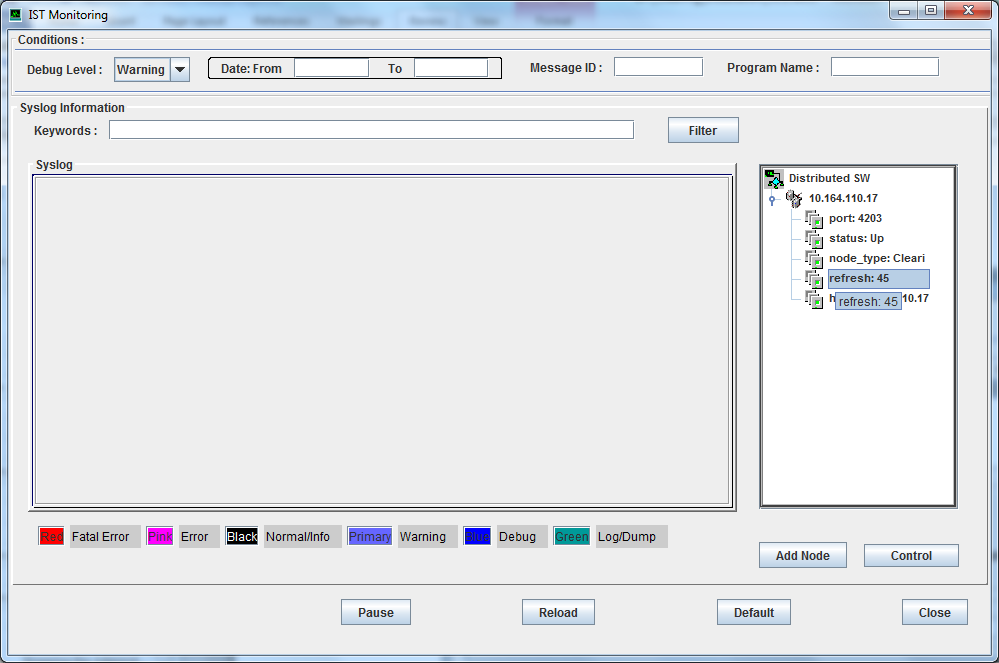
Figure 34: IST Monitor- Add Node

1. **Click Add**
2. Enter the IST/Clearing hostname or IP in the Host Name field.
3. Select Node Type “mas”
4. Enter the port istnodeagt port configured during the IST/Clearing installation.
5. Click **Save** button.
6. Click OK. The node appears in Nodes list.

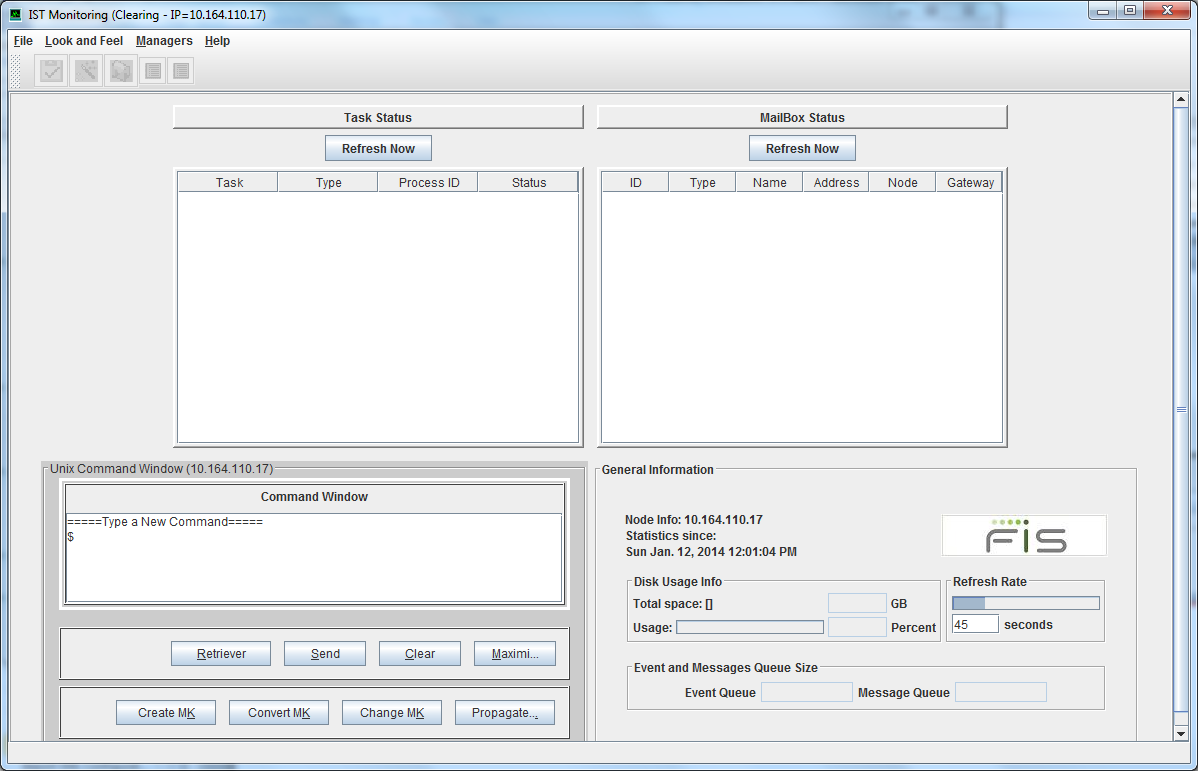
## Master Key Setup

Four options are included to manage Tokenization master keys.

In IST Monitor:



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



1. Click Create Master Key

Create MK:

invoke :  “tokenmas|run\_cmd|klc\_init\_master”.

Convert MK:

invoke :  “tokenmas|run\_cmd|km\_pass2tokmas”.

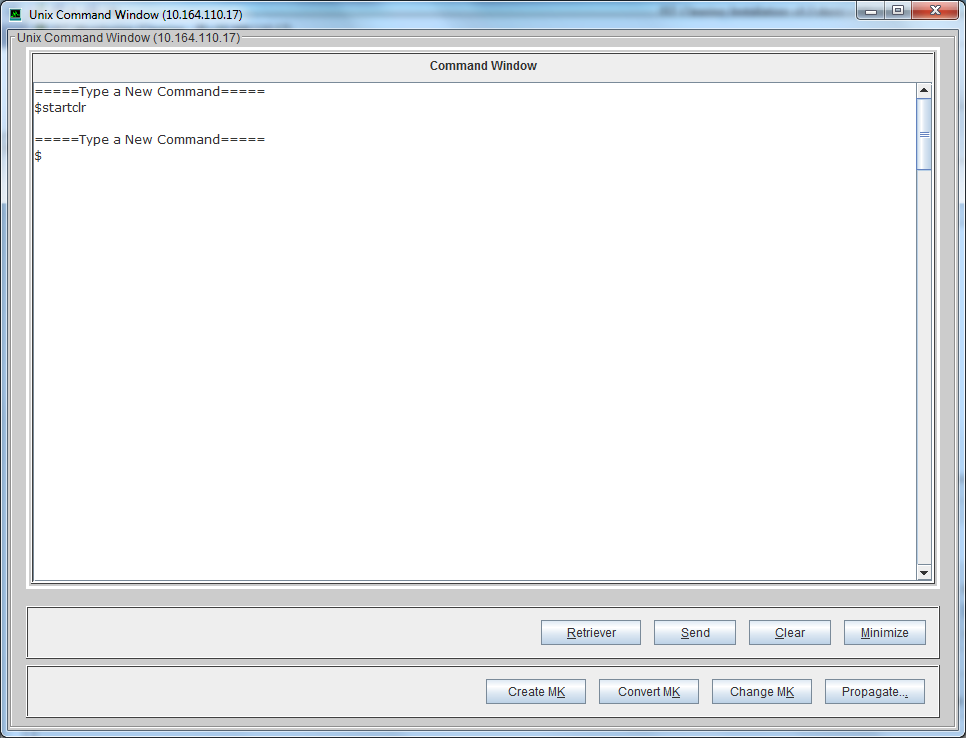
Change MK:

1. invoke :  “tokenmas|run\_cmd|klcutil –u”.
2. Invoke :  “tokenmas|run\_cmd|klcutil –t” on one node.
3. If success run  “mbrulecmd update token-keys” on all nodes.

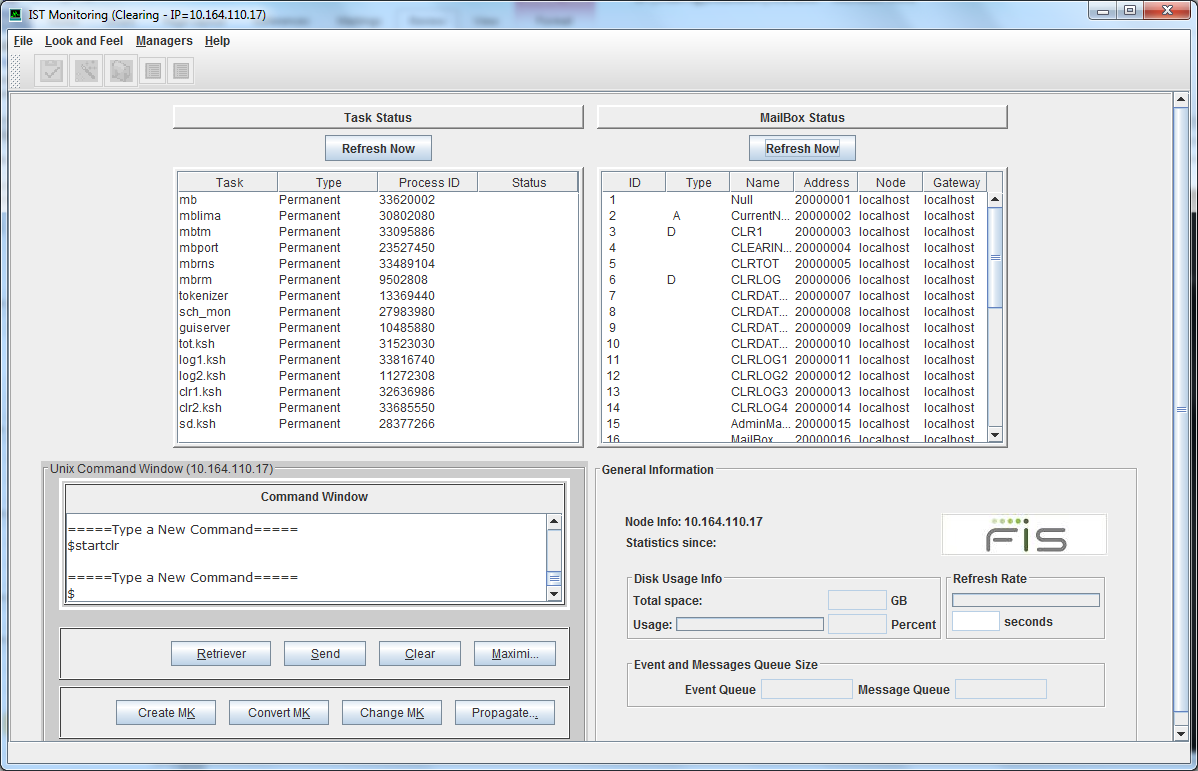
## Start IST/Clearing

To start the IST/Clearing processes:

1. Click Maximize to mazimize the Command Window



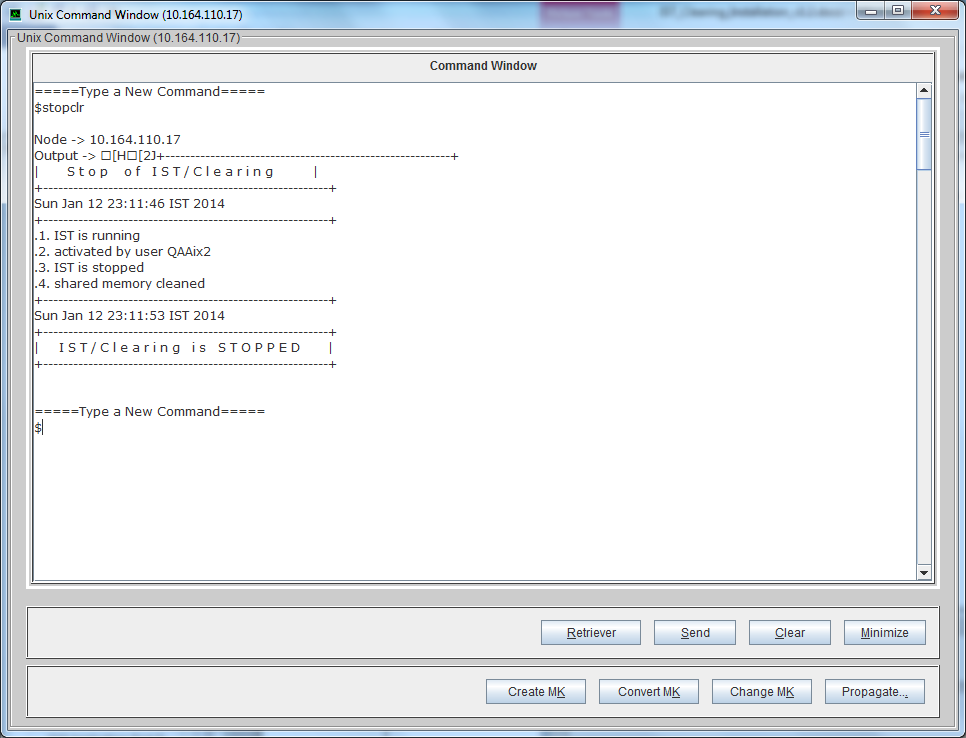
1. Enter startclr in the Command Window
2. Click Send
3. After the system starts Click Minimize on the Command Window



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

To stop the IST/MAS processes:

1. Click Maximize to maximize the Command Window



1. Enter stopclr in the Command Window
2. 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 Import XML Configuration Files section above.

To set up the configuration service:

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

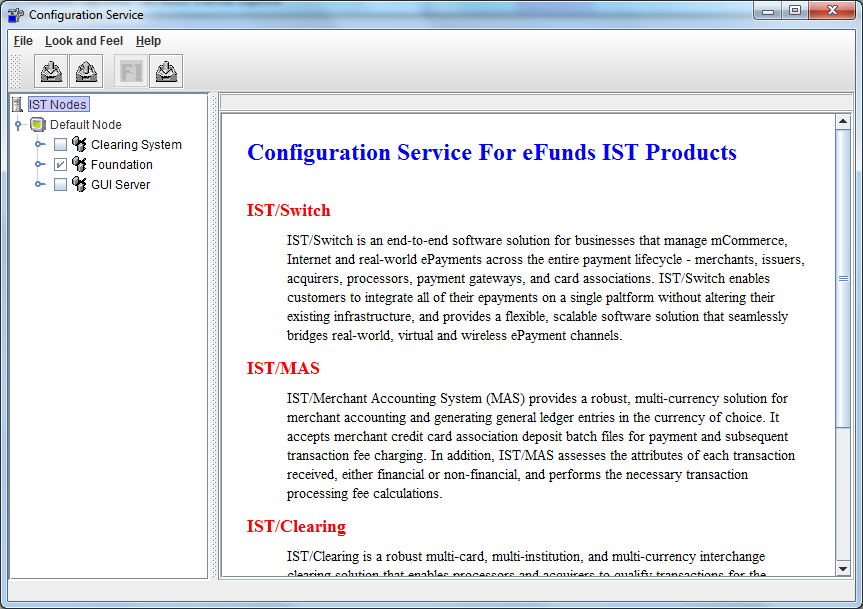
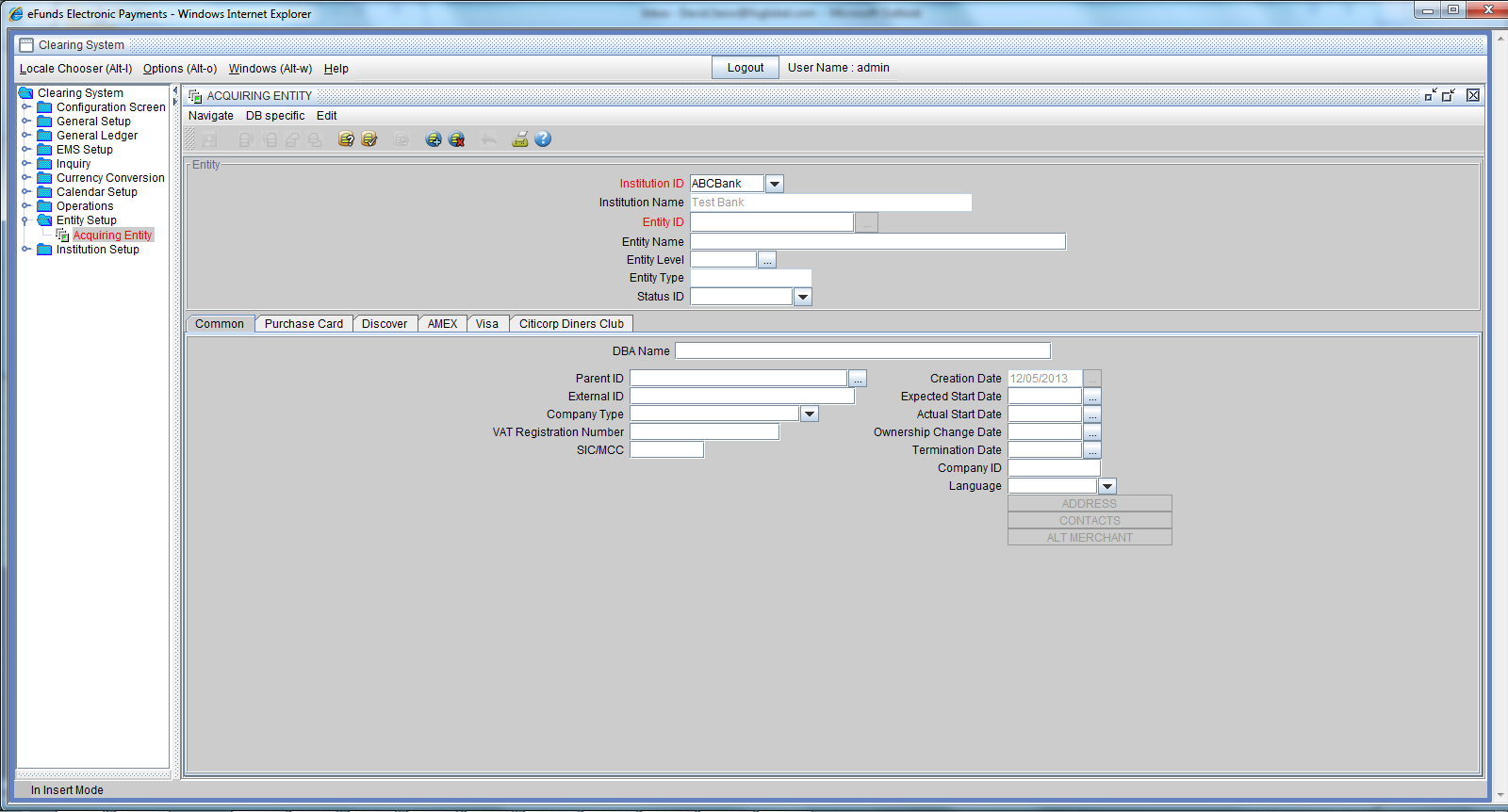


Figure 35: Configuration Service screen

1. Setup the parameters as required in the Default Node.
2. 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



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

# 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

Copyright© 2014 FIS.

All Rights Reserved.